Rigmor Söderberg

Från: [redacted] för FI FMA FPM <fi.fma.fpm@regeringskansliet.se>
Skickat: den 15 januari 2024 16:18
Till: bolagsverket@bolagsverket.se; registrator; customer.relations@euroclear.com; info@finansbolagen.se; webmaster@finansforbundet.se; finansinspektionen; info@fondbolagen.se; info@foretagarna.se; registrator; fra@fra.se; exp-hkv; forvaltningsrattenistockholm; ann.ekroth@getswish.se; imy; registrator; kammarrattenistockholm; registrator; lina.haglund@skfab.se; konkurrensverket; konsumentverket; kontakt; registrator; info; registrator; switchboardstockholm@nasdaqomx.com; contact@ngm.se; registrator; registrator kansli; pts; Regelrådet; ri; remisser@ri.se; justitieombudsmannen@jo.se; riksgalden; info@smaforetagarna.se; info@sparbankerna.se; info@juridicum.su.se; info@insurancesweden.se; info@svenskvardepappersmarknad.se; info@swedishbankers.se; info@sfm.se; kansliet@sjf.se; kansliet@kreditforeningen.se; mattias.grahn@saabgroup.com; loan@svenskaskeppshypotek.se; remisser@svensktnaringsliv.se; info@advokatsamfundet.se; info@sverigeskonsumenter.se; registratorn@riksbank.se; info@swefintech.se; info@houseoffinance.se; info@svca.se; sakerhetspolisen@sakerhetspolisen.se; info@techsverige.se; registrator; stab@tff.se; info@tu.se; vetenskapsradet@vr.se; vinnova
Kopia: Anna Stenberg; Alexander Dahlqvist; Sophie Avedal Edström; Anna Widenfalk; Jonas Sunding; FI Registrator; FI Redaktionen; Helene Ohlsson; Lotta Hardvik Cederstierna
Ämne: REMITTERING AV PROMEMORIA Digital operativ motståndskraft för finanssektorn
Bifogade filer: PM Digital operativ motståndskraft för finanssektorn TGA-WEBB.pdf; Remisslista_Digital operativ motståndskraft för finanssektorn.pdf

Uppföljningsflagga: Följ upp
Flagga: Har meddelandeflagga

Kategorier: Rigmor

Härmed remitteras **Promemorian Digital operativ motståndskraft för finanssektorn, Fi2024/00073**

Remissvaren ska ha kommit in till Finansdepartementet **senast den 15 april 2024.**

Svaren skickas per e-post till fi.remissvar@regeringskansliet.se och med kopia till anna.stenberg@regeringskansliet.se
Vänligen se även bifogat missiv för utförligare instruktion om hur svaren bör lämnas.

Observera att promemorian remitteras endast på detta sätt.

Kind regards/vänliga hälsningar

Q lpW J lfr
Kanslisekreterare
Finansdepartementet
Enheten för försäkring, pension – och myndighetsstyrning
SE-103 39 Stockholm Stockholm
Tel. +46 8 405 5330
nina.rico@regeringskansliet.se
www.government.se

Promemoria

Finansdepartementet
Finansmarknadsavdelningen

Digital operativ motståndskraft för finanssektorn

Fi2024/00073
Januari 2024

Innehållsförteckning

1 Promemorians huvudsakliga innehåll

Genom EU:s förordning om digital operativ motståndskraft för finanssektorn införs nya krav på företag inom den finansiella sektorn. Detta gäller bl.a. krav på företagens riskhantering när det gäller informations- och kommunikationsteknik, incidentrapportering, hantering av utlagd verksamhet och testning av digital operativ motståndskraft. Förordningen ska tillämpas från och med den 17 januari 2025. Samtidigt införs ändringar i flera EU-direktiv på finansmarknadsområdet.

EU-förordningen och direktivändringarna kräver vissa nationella lagstiftningsåtgärder. I denna promemoria föreslås därför en ny lag med kompletterande bestämmelser till EU-förordningen. Lagen innehåller bestämmelser om bl.a.

– ansvariga myndigheter för hotbildsstyrda penetrationstester,
– Finansinspektionens tillsynsbefogenheter,
– ingripanden och sanktioner vid överträdelser av EU-förordningen, och
– avgifter för att bekosta Finansinspektionens och Riksbankens verksamhet enligt EU-förordningen.

Därutöver föreslås ändringar i flera lagar på finansmarknadsområdet.

I promemorian lämnas också förslag till ändringar som rör överklaganden av Finansinspektionens beslut i vissa frågor som inte har samband med EU-förordningen.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 17 januari 2025.

2 Lagförslag

2.1 Förslag till lag med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

Lagens syfte

1 § Denna lag kompletterar 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, i denna lag kallad EU-förordningen.

Termer och uttryck i denna lag har samma betydelse som i EU-förordningen.

Behörig myndighet

2 § Av artikel 46 i EU-förordningen följer att Finansinspektionen är behörig myndighet enligt förordningen.

Avgifter till Finansinspektionen

3 § För att bekosta Finansinspektionens verksamhet enligt EU-förordningen och denna lag ska de finansiella entiteter som står under inspektionens tillsyn betala årliga avgifter.

Regeringen får meddela föreskrifter om avgifter enligt första stycket.

2 kap. Hotbildsstyrda penetrationstester

Finansinspektionen

1 § Finansinspektionen ska besluta om vilka finansiella entiteter som ska genomföra hotbildsstyrd penetrationstestning enligt artikel 26 i EU-förordningen. Finansinspektionen ska också besluta om hur ofta en finansiell entitet ska genomföra sådan testning.

Riksbanken

2 § Riksbanken ska övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt artikel 26 och 27 i EU-förordningen.

Riksbanken ska utfärda sådana intyg som avses i artikel 26.7 i EU-förordningen.

Samverkan

3 § Finansinspektionen ska ge Riksbanken tillfälle att yttra sig innan Finansinspektionen fattar beslut enligt 1 §.

Riksbanken ska ge Finansinspektionen tillfälle att yttra sig innan Riksbanken fattar beslut om hotbildsstyrd penetrationstestning som berör Finansinspektionens tillsynsverksamhet.

Finansinspektionen och Riksbanken ska lämna varandra de uppgifter som respektive myndighet behöver för samverkan.

Uppgiftsskyldighet

4 § På begäran av Riksbanken ska finansiella entiteter lämna de uppgifter som är nödvändiga för Riksbankens verksamhet enligt detta kapitel och artikel 26 och 27 i EU-förordningen.

Förelägganden

5 § Riksbanken får besluta om de förelägganden som behövs för att en finansiell entitet ska följa uppgiftsskyldigheten i 4 §.

Ett beslut om föreläggande får förenas med vite.

Avgifter till Riksbanken

6 § Riksbanken får ta ut avgifter från de finansiella entiteter som genomför hotbildsstyrd penetrationstestning.

Riksbanken får meddela föreskrifter om avgifter enligt första stycket.

3 kap. Tillsyn

Tillsynens omfattning

1 § Finansinspektionen har tillsyn över att finansiella entiteter följer bestämmelserna i EU-förordningen och denna lag.

Föreläggande om att lämna uppgifter

2 § För tillsynen enligt 1 § får Finansinspektionen förelägga

1. en fysisk eller juridisk person att tillhandahålla uppgifter, handlingar eller annat, och

2. den som förväntas kunna lämna upplysningar i saken att inställa sig till förhör på tid och plats som inspektionen bestämmer.

Första stycket gäller inte i den utsträckning uppgiftslämnandet skulle strida mot den i lag reglerade tystnadsplikten för advokater.

Platsundersökning

3 § Finansinspektionen får när det är nödvändigt för tillsynen enligt 1 § genomföra en undersökning i verksamhetslokalerna hos en finansiell entitet.

Verkställighet av beslut om viten

4 § Beslut om viten enligt EU-förordningen får verkställas enligt utsökningsbalken på samma sätt som en svensk dom som har fått laga kraft.

4 kap. Ingripanden

Ingripanden mot finansiella entiteter

1 § Finansinspektionen ska ingripa mot följande finansiella entiteter om de åsidosätter sina skyldigheter enligt EU-förordningen eller denna lag:

1. Svenska skeppshypotekskassan,
2. en leverantör av kryptotillgångstjänster,
3. en emittent av tillgångsanknutna token,
4. en pensionsstiftelse,
5. ett kreditvärderingsinstitut,
6. en administratör av kritiska referensvärden,
7. en leverantör av gräsrotsfinansieringstjänster,
8. ett värdepapperiseringsregister, och
9. ett transaktionsregister.

2 § Bestämmelser om ingripanden mot andra finansiella entiteter än de som anges i 1 § och som åsidosätter sina skyldigheter enligt EU-förordningen eller denna lag finns i de lagar som reglerar den berörda verksamheten.

3 § Ett ingripande mot Svenska skeppshypotekskassan ska ske genom ett beslut om föreläggande att inom en viss tid vidta en åtgärd eller upphöra med ett visst agerande.

4 § Ett ingripande mot en emittent av tillgångsanknutna token, en pensionsstiftelse, ett kreditvärderingsinstitut, ett värdepapperiseringsregister eller ett transaktionsregister ska ske genom ett beslut om

1. föreläggande att inom en viss tid vidta en viss åtgärd eller upphöra med ett visst agerande, eller
2. anmärkning.

5 § Ett ingripande mot en leverantör av kryptotillgångstjänster, en administratör av kritiska referensvärden eller en leverantör av gräsrotsfinansieringstjänster ska ske genom ett beslut om

1. föreläggande att inom en viss tid vidta en viss åtgärd eller upphöra med ett visst agerande, eller
2. anmärkning.

Om överträdelsen är allvarlig får den finansiella entitetens auktorisation återkallas eller, om det är tillräckligt, en varning meddelas.

6 § Ett ingripande enligt 3–5 §§ får inte ske om en överträdelse omfattas av ett föreläggande som har förenats med vite och en ansökan om utdömande av vitet har gjorts.

7 § Om ett beslut om anmärkning eller varning enligt 4 eller 5 § har meddelats, får Finansinspektionen besluta att den som har gjort sig skyldig till överträdelsen ska betala en sanktionsavgift.

8 § Om en auktorisation återkallas enligt 5 § får Finansinspektionen bestämma hur verksamheten ska avvecklas.

Ett beslut om återkallelse får förenas med förbud att fortsätta med hela eller delar av verksamheten.

Ingripanden mot vissa företrädare för finansiella entiteter

9 § Finansinspektionen ska ingripa mot någon som ingår i styrelsen för en finansiell entitet som anges i 1 § eller är dess verkställande direktör, eller ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i EU-förordningen.

Ett ingripande enligt första stycket får ske bara om den finansiella entitetens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande ska ske genom en eller båda av följande sanktioner:

1. beslut att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en sådan finansiell entitet, eller ersättare för någon av dem, eller
2. beslut om sanktionsavgift.

Sanktionsföreläggande

10 § Frågor om ingripande mot fysiska personer enligt 9 § tas upp av Finansinspektionen genom ett sanktionsföreläggande.

Ett sanktionsföreläggande innebär att den fysiska personen föreläggs att inom en viss tid godkänna en sanktion som är bestämd till tid eller belopp.

När ett sanktionsföreläggande har godkänts, gäller det som ett domstolsavgörande som fått laga kraft. Ett godkännande som görs efter den tid som angetts i föreläggandet är utan verkan.

11 § Ett sanktionsföreläggande ska innehålla uppgift om

1. den fysiska person som föreläggandet avser,
2. överträdelsen och de omständigheter som behövs för att kännetecknа den,
3. de bestämmelser som är tillämpliga på överträdelsen, och
4. den sanktion som föreläggs personen.

Sanktionsföreläggandet ska också innehålla en upplysning om att ansökan om sanktion kan komma att ges in till domstol, om sanktionsföreläggandet inte godkänns inom den tid som Finansinspektionen anger.

12 § Om ett sanktionsföreläggande inte har godkänts inom angiven tid, får Finansinspektionen ansöka hos domstol om att en sanktion ska beslutas. En sådan ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av Finansinspektionens beslut om ingripande mot den juridiska personen för samma överträdelse.

Prövningstillstånd krävs vid överklagande till kammarrätten.

13 § Ett sanktionsföreläggande enligt 10 § är utan verkan, om föreläggandet inte har delgetts den som det riktas mot inom två år från den tidpunkt då överträdelsen ägde rum. I ett sådant fall får inte heller någon sanktion enligt 12 § första stycket beslutas.

Sanktionsavgifter

14 § Sanktionsavgiften för en finansiell entitet som anges i 2 § och som är en juridisk person ska som högst fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade en miljon euro,
2. tio procent av den finansiella entitetens omsättning närmast föregående räkenskapsår eller, i förekommande fall, motsvarande omsättning på koncernnivå, eller
3. tre gånger den vinst som den finansiella entiteten har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

Sanktionsavgiften får inte bestämmas till ett lägre belopp än 5 000 kronor.

Om en överträdelse har skett under den juridiska personens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, får omsättningen uppskattas när den högsta sanktionsavgiften ska beräknas.

15 § Sanktionsavgiften för en leverantör av gräsrotsfinansieringstjänster får inte vara så stor att leverantören därefter inte uppfyller kraven enligt artikel 11 i Europaparlamentets och rådets förordning (EU) 2020/1503 av den 7 oktober 2020 om europeiska leverantörer av gräsrotsfinansieringstjänster för företag och om ändring av förordning (EU) 2017/1129 och direktiv (EU) 2019/1937 eller andra bestämmelser om soliditet och likviditet som gäller för leverantören.

16 § Sanktionsavgiften för en fysisk person ska som högst fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 500 000 euro, eller
2. tre gånger den vinst som den fysiska personen har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

17 § Sanktionsavgifter tillfaller staten.

Val av ingripande

18 § Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått samt graden av ansvar hos den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen.

19 § Utöver det som anges i 18 § ska det i försvårande riktning beaktas om den som har begått överträdelsen tidigare har begått en överträdelse. Vid denna bedömning ska särskild vikt fästas vid om överträdelserna är likartade och den tid som har gått mellan de olika överträdelserna.

I förmildrande riktning ska det beaktas om den som har begått överträdelsen

1. i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och
2. snabbt upphört med överträdelsen eller snabbt verkat för att överträdelsen ska upphöra, sedan den anmälts till eller påtalats av Finansinspektionen.

20 § När sanktionsavgiftens storlek ska fastställas ska särskild hänsyn tas till sådana omständigheter som anges i 18 och 19 §§ samt till den berörda fysiska eller juridiska personens finansiella ställning och, om det går att bestämma, den vinst som personen gjort till följd av överträdelsen.

21 § Finansinspektionen får avstå från ingripande, om

1. överträdelsen är ringa eller ursäktlig,
2. den fysiska eller juridiska personen i fråga gör rättelse,
3. den fysiska personen har verkat för att den juridiska personen gör rättelse, eller
4. någon annan myndighet eller något annat organ har vidtagit åtgärder mot den fysiska eller juridiska personen och dessa åtgärder bedöms tillräckliga.

Verkställighet av beslut om sanktionsavgift

22 § En sanktionsavgift ska betalas till Finansinspektionen inom 30 dagar efter det att ett beslut eller en dom om att ta ut avgiften har fått laga kraft eller ett sanktionsföreläggande har godkänts, eller efter den längre tid som anges i beslutet eller föreläggandet.

23 § Om sanktionsavgiften inte har betalats inom den tid som anges i 22 §, ska Finansinspektionen lämna avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

24 § En sanktionsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet eller domen om att ta ut avgiften fick laga kraft eller sanktionsföreläggandet godkändes.

Vite

25 § Ett beslut om föreläggande eller förbud får förenas med vite.

5 kap. Överklagande och beslut som ska gälla omedelbart

Överklagande av Finansinspektionens beslut

1 § Finansinspektionens beslut om sanktionsföreläggande enligt denna lag får inte överklagas.

Andra beslut som Finansinspektionen meddelar enligt denna lag och EU-förordningen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Överklagande av Riksbankens beslut

2 § Riksbankens beslut om föreläggande enligt 2 kap. 5 § och beslut om utfärdande av intyg enligt artikel 26.7 i EU-förordningen får överklagas till allmän förvaltningsdomstol.

Andra beslut som Riksbanken fattar enligt denna lag och EU-förordningen får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Beslut som kan gälla omedelbart

3 § Finansinspektionen får bestämma att ett beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart.

Denna lag träder i kraft den 17 januari 2025.

2.2 Förslag till lag om ändring i lagen (1967:531) om tryggande av pensionsutfästelse m.m.

Härigenom föreskrivs[1] att 16 g § lagen (1967:531) om tryggande av pensionsutfästelse m.m. ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
16 g §[2]	
En pensionsstiftelse som avses i 9 a § andra eller tredje stycket ska upprätta och följa riktlinjer för	
1. riskhantering,	
2. internrevision, och	
3. verksamhet som omfattas av uppdragsavtal.	
Pensionsstiftelsen ska upprätta och vid behov följa en beredskapsplan som säkerställer att verksamheten kan bedrivas kontinuerligt.	Pensionsstiftelsen ska upprätta och vid behov följa en beredskapsplan som säkerställer att verksamheten kan bedrivas kontinuerligt. *Stiftelsen ska ha sådana nätverks- och informationssystem som avses i 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.*
Pensionsstiftelsen ska upprätta och följa en sund ersättningspolicy för personer som leder eller övervakar verksamheten eller på annat sätt kan påverka riskerna i verksamheten. Stiftelsen ska regelbundet offentliggöra relevant information om ersättningspolicyn.	

Denna lag träder i kraft den 17 januari 2025.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse 2020:394.

2.3 Förslag till lag om ändring i trafikskadelagen (1975:1410)

Härigenom föreskrivs att 5 § trafikskadelagen (1975:1410)[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 §[2]

Trafikförsäkring får meddelas av

1. en försäkringsgivare som har fått tillstånd till det enligt 2 kap. 4 § försäkringsrörelselagen (2010:2043),
2. en försäkringsgivare som har fått tillstånd till det enligt 4 kap. 1 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, och
3. en EES-försäkringsgivare som är verksam i Sverige enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige.

En försäkringsgivare som får meddela trafikförsäkring är skyldig att på begäran meddela trafikförsäkring. I ett tillstånd enligt 2 kap. 4 § försäkringsrörelselagen eller 4 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige *kan* dock skyldigheten begränsas till att gälla försäkring åt personer som tillhör en viss yrkesgrupp eller intressegrupp eller som är bosatta inom ett visst område. Finansinspektionen *kan* efter ansökan besluta om motsvarande begränsning för försäkringsgivare som driver verksamhet här enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige. Finansinspektionens beslut får överklagas *hos regeringen*.	En försäkringsgivare som får meddela trafikförsäkring är skyldig att på begäran meddela trafikförsäkring. I ett tillstånd enligt 2 kap. 4 § försäkringsrörelselagen eller 4 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige *får* dock skyldigheten begränsas till att gälla försäkring åt personer som tillhör en viss yrkesgrupp eller intressegrupp eller som är bosatta inom ett visst område. Finansinspektionen *får* efter ansökan besluta om motsvarande begränsning för försäkringsgivare som driver verksamhet här enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige. Finansinspektionens beslut får överklagas *till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.*

En försäkringsgivare som avser att meddela trafikförsäkring genom gränsöverskridande verksamhet med stöd av 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige men som inte har fast driftställe i Sverige ska ha en representant här i landet.

[1] Lagen omtryckt 1994:43.
[2] Senaste lydelse 2023:666.

Representanten ska vara bosatt i Sverige eller vara en svensk juridisk person. Försäkringsgivaren ska utfärda en fullmakt för representanten att gentemot skadelidande företräda försäkringsgivaren och att själv eller genom någon annan tala och svara för denne angående försäkringsfall. Representanten ska även ha behörighet att företräda försäkringsgivaren vid kontroll av om det finns en giltig trafikförsäkring. Försäkringsgivaren ska informera försäkringstagarna om vem som är försäkringsgivarens representant och om dennes adress. Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om villkor för sådana representanter.

---

1. Denna lag träder i kraft den 17 januari 2025.
2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

2.4 Förslag till lag om ändring i lagen (1980:1097) om Svenska skeppshypotekskassan

Härigenom föreskrivs att 38 § lagen (1980:1097) om Svenska skeppshypotekskassan ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
38 §[1]	
Kassan står under tillsyn av Finansinspektionen.	
Vid meddelande av föreläggande eller förbud i samband med tillsynen *kan* Finansinspektionen förelägga vite.	Vid meddelande av föreläggande eller förbud i samband med tillsynen *får* Finansinspektionen förelägga vite.
Inspektionens beslut enligt denna lag får överklagas *hos regeringen*. Inspektionens beslut har omedelbar verkan, om inte annat beslutas.	Inspektionens beslut enligt denna lag får överklagas *till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten*. Inspektionens beslut har omedelbar verkan, om inte annat beslutas.
Regeringen meddelar ytterligare föreskrifter om tillsynsverksamheten.	

1. Denna lag träder i kraft den 17 januari 2025.
2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

[1] Senaste lydelse 1998:310.

2.5 Förslag till lag om ändring i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument

Härigenom föreskrivs att 9 kap. 12 § lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument[1] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
12 §[2]	
Finansinspektionen ska ingripa mot någon som ingår i en svensk värdepapperscentrals styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepapperscentralen	
1. tillhandahåller tjänster enligt avsnitten A, B och C i bilagan till förordningen om värdepapperscentraler, i den ursprungliga lydelsen, i strid med artiklarna 16, 25 eller 54 i förordningen,	
2. har fått auktorisationer som krävs enligt artikel 16 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen, genom osanna uppgifter eller andra olagliga metoder enligt artikel 20.1 b i förordningen,	
3. låtit bli att uppfylla kapitalkravet i strid med artikel 47.1 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,	
4. låtit bli att uppfylla de organisatoriska kraven i strid med artiklarna 26–30 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,	
5. låtit bli att följa uppföranderegelerna i strid med artiklarna 32–35 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,	
6. låtit bli att uppfylla kraven för värdepapperscentraltjänster i strid med artiklarna 37–41 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,	
7. låtit bli att uppfylla stabilitetskraven i strid med artiklarna 43–47 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,	
8. låtit bli att uppfylla kraven på länkar mellan värdepapperscentraler i strid med artikel 48 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen, *eller*	8. låtit bli att uppfylla kraven på länkar mellan värdepapperscentraler i strid med artikel 48 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
9. utan giltig grund vägrat att bevilja olika typer av tillträde i strid med artiklarna 49–53 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen.	9. utan giltig grund vägrat att bevilja olika typer av tillträde i strid med artiklarna 49–53 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen*, eller*
	10. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2,

[1] Senaste lydelse av lagens rubrik 2016:51.
[2] Senaste lydelse 2016:51.

	17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.
Ett ingripande enligt första stycket får ske endast om värdepapperscentralens överträdelse är allvarlig och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.	Ett ingripande enligt första stycket får ske endast om värdepapperscentralens överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, eller, för upprepade allvarliga överträdelser, permanent inte får vara styrelseledamot, verkställande direktör eller ersättare för någon av dem i värdepapperscentralen, eller
2. beslut om sanktionsavgift.

Denna lag träder i kraft den 17 januari 2025.

2.6 Förslag till lag om ändring i lagen (2004:46) om värdepappersfonder

Härigenom föreskrivs[1] att 2 kap. 17 § och 12 kap. 1 a § lagen (2004:46) om värdepappersfonder[2] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
17 §[3]	
Ett fondbolag ska ha sunda rutiner för 1. förvaltning av verksamheten och redovisning, 2. intern kontroll, och 3. drift och förvaltning av sina informationssystem.	
	Rutinerna enligt första stycket 3 ska uppfylla kraven i 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.
Fondbolaget ska särskilt – upprätta och tillämpa regler för styrelseledamöters och anställdas egna affärer med finansiella instrument,	*1.* upprätta och tillämpa regler för styrelseledamöters och anställdas egna affärer med finansiella instrument,
– dokumentera samtliga transaktioner som bolaget har genomfört för en värdepappersfonds räkning eller för ett sådant fondföretags räkning som avses i 12 § andra stycket eller 15 § andra stycket, och	*2.* dokumentera samtliga transaktioner som bolaget har genomfört för en värdepappersfonds räkning eller för ett sådant fondföretags räkning som avses i 12 § andra stycket eller 15 § andra stycket, och
– ha en organisation som minskar risken för intressekonflikter som kan påverka fondandelsägares eller andra kunders intressen negativt.	*3.* ha en organisation som minskar risken för intressekonflikter som kan påverka fondandelsägares eller andra kunders intressen negativt.

[1] Jfr Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag), i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.
[2] Senaste lydelse av lagens rubrik 2013:563.
[3] Senaste lydelse 2013:563.

12 kap.

1 a §[4]

Finansinspektionen ska ingripa mot någon som ingår i ett fondbolags styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om fondbolaget

1. har fått tillstånd att driva fondverksamhet genom att lämna falska uppgifter eller på annat otillbörligt sätt,

2. tillhandahåller diskretionär portföljförvaltning i strid med 1 kap. 4 §,

3. påbörjar marknadsföring av en av bolaget förvaltad värdepappersfond i ett annat land inom EES innan en underrättelse om detta gjorts hos Finansinspektionen i enlighet med 2 kap. 15 c §,

4. inte uppfyller grundläggande krav på organisation och drift av verksamheten enligt 2 kap. 17 eller 17 f § eller föreskrifter som har meddelats med stöd av 13 kap. 1 § 11 avseende dessa bestämmelser,

5. åsidosätter sina skyldigheter eller på annat sätt överträder det som anges om uppdragsavtal i någon av 4 kap. 4–6 §§ eller 7 § första stycket,

6. påbörjar förvaltning och marknadsföring av en värdepappersfond utan att fondbestämmelserna godkänts enligt 4 kap. 9 §,

7. vid upprepade tillfällen låter bli att upprätta eller tillhandahålla informationsbroschyr, faktablad, årsberättelse och halvårsberättelse i enlighet med 4 kap. 15–21 §§,

8. vid upprepade tillfällen placerar medel i en värdepappersfond i strid med det som anges i någon av 5 kap. 1, 3–22, 24 eller 25 §§ eller i föreskrifter som har meddelats med stöd av 13 kap. 1 § 21, 22, 24 och 25 avseende dessa bestämmelser,

9. inte uppfyller kraven på hantering av risker i 5 kap. 2 § första eller andra stycket eller i föreskrifter som har meddelats med stöd av 13 kap. 1 § 23 avseende dessa bestämmelser,

10. i strid med 11 kap. 5 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,

11. i strid med 11 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier i bolaget samt storleken på innehavet, *eller*

12. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen.

11. i strid med 11 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier i bolaget samt storleken på innehavet,

12. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen, *eller*

13. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–

[4] Senaste lydelse 2023:234.

25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Om en sådan person som anges i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 11 kap. 1 eller 4 § för förvärv eller avyttring av aktier i bolaget, ska första stycket 10 och 11 inte gälla för den personen i fråga om dessa aktier.

Ett ingripande enligt första stycket får ske endast om bolagets överträdelse är allvarlig och personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Ett ingripande enligt första stycket får ske endast om bolagets överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, eller, för upprepade allvarliga överträdelser, permanent inte får vara styrelseledamot eller verkställande direktör i ett fondbolag, eller ersättare för någon av dem, eller

2. beslut om sanktionsavgift.

Denna lag träder i kraft den 17 januari 2025.

2.7 Förslag till lag om ändring i lagen (2004:297) om bank- och finansieringsrörelse

Härigenom föreskrivs[1] att 6 kap. 2 §, 10 kap. 1 §, 15 kap. 1 a § och 17 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
2 §[2]	
Ett kreditinstitut ska identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med. Institutet ska se till att det har en tillfredsställande intern kontroll. Det ska också upprätta en återhämtningsplan eller koncernåterhämtningsplan enligt 6 a kap.	Ett kreditinstitut ska identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med. *Nätverks- och informationssystem ska uppfylla kraven i 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.* Institutet ska se till att det har en tillfredsställande intern kontroll. Det ska också upprätta en återhämtningsplan eller koncernåterhämtningsplan enligt 6 a kap.

Ett kreditinstitut ska särskilt se till att dess kreditrisker, marknadsrisker, operativa risker och andra risker sammantagna inte medför att institutets förmåga att fullgöra sina förpliktelser äventyras. För att uppfylla detta krav ska det åtminstone ha metoder som gör det möjligt att fortlöpande värdera och upprätthålla ett kapital som till belopp, slag och fördelning är tillräckligt för att täcka arten och nivån på de risker som det är eller kan komma att bli exponerat för. Institutet ska utvärdera dessa metoder för att säkerställa att de är heltäckande.

Ett kreditinstitut ska på grundval av de metoder som avses i andra stycket fastställa tillräckliga kapitalbasnivåer.

[1] Jfr Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse 2020:1209.

10 kap.

1 §[3]

För bankaktiebolag gäller föreskrifterna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller är särskilt föreskrivet. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag som gäller i stället för eller utöver bestämmelserna i aktiebolagslagen.

I fråga om bankaktiebolag ska det som anges om Bolagsverket i följande bestämmelser avse Finansinspektionen:

– 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,	*1.* 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,
–23 kap. 45 b § aktiebolagslagen,	*2.* 23 kap. 45 b § aktiebolagslagen,
– 24 kap. 47 § aktiebolagslagen, och	*3.* 24 kap. 47 § aktiebolagslagen, och
– 24 a kap. 24 § aktiebolagslagen.	*4.* 24 a kap. 24 § aktiebolagslagen.

15 kap.

1 a §[4]

Finansinspektionen ska ingripa mot någon som ingår i ett kreditinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om kreditinstitutet

1. har fått tillstånd att driva bank- eller finansieringsrörelse genom att lämna falska uppgifter eller på annat otillbörligt sätt,

2. i strid med 14 kap. 4 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,

3. i strid med 14 kap. 4 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier eller andelar i institutet samt storleken på innehaven,

4 inte uppfyller kraven i 6 kap. 1–3 c, 4, 4 a, 4 c eller 5 § eller i föreskrifter som har meddelats med stöd av 16 kap. 1 § 5,

5. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om efterlevnaden av skyldigheten att uppfylla kapitalbaskraven enligt artikel 92 i tillsynsförordningen, i strid med artikel 430.1 i den förordningen,

6. låter bli att rapportera eller lämnar ofullständig eller felaktig information till Finansinspektionen när det gäller data som avses i artikel 430a i tillsynsförordningen,

7. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om en stor exponering i strid med artikel 394.1 i tillsynsförordningen,

8. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om likviditet i strid med artikel 415.1 och 415.2 i tillsynsförordningen,

[3] Senaste lydelse 2022:1649.
[4] Senaste lydelse 2022:804.

9. låter bli att lämna uppgifter till Finansinspektionen eller lämnar ofullständig eller felaktig information om sin bruttosoliditet i strid med artikel 430.1 och 430.2 i tillsynsförordningen,

10. vid upprepade tillfällen eller systematiskt låter bli att hålla likvida tillgångar i strid med artikel 412 i tillsynsförordningen,

11. utsätter sig för en exponering som överskrider gränserna enligt artikel 395 i tillsynsförordningen,

12. är exponerat för kreditrisken i en värdepapperiseringsposition utan att uppfylla villkoren i artikel 405 i tillsynsförordningen,

13. låter bli att lämna information eller lämnar ofullständig eller felaktig information i strid med någon av artiklarna 431.1–431.3 och 451.1 i tillsynsförordningen,

14. gör betalningar till innehavare av instrument som ingår i institutets kapitalbas i strid med 8 kap. 3 och 4 §§ lagen (2014:966) om kapitalbuffertar eller artikel 28, 51 eller 63 i tillsynsförordningen, när dessa artiklar förbjuder sådana betalningar till innehavare av instrument som ingår i kapitalbasen,

15. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen,

16. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtfölja överföringar av medel och om upphävande av förordning (EG) nr 1781/2006,

17. har tillåtit en styrelseledamot, verkställande direktören eller ersättare för någon av dem att åta sig ett sådant uppdrag i institutet eller kvarstå i institutet trots att kraven i 3 kap. 2 § första stycket 4 eller 5, 10 kap. 8 a–8 c §§ eller 12 kap. 6 a–6 c §§ eller i föreskrifter som har meddelats med stöd av 16 kap. 1 § 3 inte är uppfyllda,

18. i strid med 6 a kap. 1 eller 2 § låter bli att upprätta eller lämna in en återhämtningsplan eller en koncernåterhämtningsplan,

19. i strid med 6 b kap. 11 § låter bli att anmäla att koncerninternt finansiellt stöd ska lämnas,

20. i strid med 13 kap. 4 a och 5 a §§ låter bli att underrätta Finansinspektionen om institutet fallerar eller sannolikt kommer att fallera,

21. inte uppfyller kravet på kapitalbas och kvalificerade skulder enligt 4 kap. lagen (2015:1016) om resolution eller i strid med 28 kap. 1 § samma lag låter bli att lämna begärda upplysningar till Riksgäldskontoret,

22. är ett moderföretag enligt artikel 4.1.15 i tillsynsförordningen och inte uppfyller kraven i del tre, fyra, sex eller sju i den förordningen eller 2 kap. 1 eller 2 § lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag på grupp- eller undergruppsnivå,

23. omfattas av tillståndsplikt enligt lagen (2003:1223) om utgivning av säkerställda obligationer och

a) har fått tillstånd att ge ut säkerställda obligationer genom att lämna falska uppgifter eller på något annat otillbörligt sätt,

b) driver verksamhet med säkerställda obligationer utan tillstånd,

c) ger ut säkerställda obligationer som inte uppfyller 3 kap. 1, 2, 3, 4, 5, 6, 7, 10, 11 eller 15 § eller 16 § andra stycket lagen om utgivning av säkerställda obligationer,

d) låter bli att lämna information eller lämnar ofullständig eller felaktig information i strid med 3 kap. 16 § första stycket lagen om utgivning av säkerställda obligationer, eller

e) vid upprepade tillfällen eller systematiskt låter bli att hålla likvida tillgångar i en sådan likviditetsbuffert som avses i 3 kap. 9 a § lagen om utgivning av säkerställda obligationer, *eller*

24. låter bli att lämna uppgifter om sin verksamhet med säkerställda obligationer till Finansinspektionen eller lämnar ofullständiga eller felaktiga uppgifter i strid med 13 kap. 3 §.

e) vid upprepade tillfällen eller systematiskt låter bli att hålla likvida tillgångar i en sådan likviditetsbuffert som avses i 3 kap. 9 a § lagen om utgivning av säkerställda obligationer,

24. låter bli att lämna uppgifter om sin verksamhet med säkerställda obligationer till Finansinspektionen eller lämnar ofullständiga eller felaktiga uppgifter i strid med 13 kap. 3 §, *eller*

25. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Om en sådan person som anges i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 14 kap. 1 eller 3 § för förvärv eller avyttring av aktier eller andelar i institutet, ska första stycket 2 och 3 inte gälla för den personen i fråga om dessa aktier eller andelar.

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett kreditinstitut, eller ersättare för någon av dem, eller

2. beslut om sanktionsavgift.

17 kap.

1 §[5]

Finansinspektionens beslut enligt 13 kap. 12 § och 15 kap. 9 a § och 18 § tredje stycket får inte överklagas.

Finansinspektionens beslut enligt 13 kap. 12 § och 15 kap. 9 a § och 18 § tredje stycket får inte överklagas. *Detsamma gäller för sådana beslut om förordnande av sakkunnig som avses i 10 kap. 1 § andra stycket 2–4.*

[5] Senaste lydelse 2018:817. Ändringen innebär bl.a. att andra stycket tas bort.

Finansinspektionens beslut som avses i 10 kap. 1 § andra stycket 1 får överklagas till regeringen.

Andra beslut av Finansinspektionen enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Inspektionen får bestämma att ett beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart.

---

1. Denna lag träder i kraft den 17 januari 2025.

2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

2.8 Förslag till lag om ändring i lagen (2007:528) om värdepappersmarknaden

Härigenom föreskrivs[1] i fråga om lagen (2007:528) om värdepappersmarknaden

dels att 8 kap. 10, 11 och 23 §§, 13 kap. 1, 1 a och 1 d §§ och 25 kap. 1 a, 1 e och 1 i §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 25 kap. 1 j och 1 k §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
10 §[2]	
Ett värdepappersinstitut ska ha tillräckliga system, resurser och rutiner för att institutet ska kunna tillhandahålla investeringstjänster och utföra investeringsverksamhet kontinuerligt och regelbundet.	Ett värdepappersinstitut ska ha tillräckliga system, resurser och rutiner för att institutet ska kunna tillhandahålla investeringstjänster och utföra investeringsverksamhet kontinuerligt och regelbundet. *Informations- och kommunikationstekniksystem ska uppfylla kraven i 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.*
Ett värdepappersinstitut ska ha sunda skyddsmekanismer för att säkerställa skyddet och autentiseringen vid informationsöverföring och för att minimera risken för dataförvanskning och obehörig åtkomst till informationen.	Ett värdepappersinstitut ska ha sunda skyddsmekanismer för att*, i enlighet med kraven i Europaparlamentets och rådets förordning (EU) 2022/2554,* säkerställa skyddet och autentiseringen vid informationsöverföring och för att minimera risken för dataförvanskning och obehörig åtkomst till informationen.

[1] Jfr Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse 2017:679.

11 §

Ett värdepappersinstitut *skall*	Ett värdepappersinstitut *ska*
1. tillämpa sunda rutiner för a) förvaltning av verksamheten, och b) redovisning,	
2. ha rutiner för intern kontroll,	2. ha rutiner för intern kontroll, *och*
3. ha effektiva metoder för riskbedömning*, och*	3. ha effektiva metoder för riskbedömning.
4. ha effektiv drift och förvaltning av sina informationssystem.	

23 §[3]

Ett värdepappersinstitut som bedriver algoritmisk handel ska ha effektiva system och riskkontroller som är anpassade för den verksamheten. Systemen och kontrollerna ska säkerställa att institutets handelssystem är motståndskraftiga och har tillräcklig kapacitet, att de omfattas av lämpliga handelströsklar och handelslimiter och att de förhindrar att felaktiga order skickas eller att systemet på annat sätt fungerar så att det kan skapa eller bidra till en oordnad marknad.	Ett värdepappersinstitut som bedriver algoritmisk handel ska ha effektiva system och riskkontroller som är anpassade för den verksamheten. Systemen och kontrollerna ska säkerställa att institutets handelssystem är motståndskraftiga och har tillräcklig kapacitet *i enlighet med kraven i kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554*, att de omfattas av lämpliga handelströsklar och handelslimiter och att de förhindrar att felaktiga order skickas eller att systemet på annat sätt fungerar så att det kan skapa eller bidra till en oordnad marknad.

Värdepappersinstitutet ska också ha effektiva system och åtgärder för riskkontroll för att säkerställa att handelssystemen inte kan användas för något ändamål som strider mot marknadsmissbruksförordningen eller mot reglerna på en handelsplats till vilken institutet är anslutet.

Värdepappersinstitutet ska ha inrättat effektiva arrangemang för kontinuerlig drift av verksamheten för att hantera driftavbrott i sina handelssystem *och ska se till att systemen är fullt testade och lämpligt övervakade för att säkerställa att de uppfyller kraven i första och andra styckena*.	Värdepappersinstitutet ska ha inrättat effektiva arrangemang för kontinuerlig drift av verksamheten för att hantera driftavbrott i sina handelssystem*, inbegripet en IKT-kontinuitetspolicy och IKT-kontinuitetsplaner samt IKT-relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik som inrättas i enlighet med artikel 11 i Europaparlamentets och rådets förordning (EU) 2022/2554. Institutet ska se till att systemen är fullt testade och*

[3] Senaste lydelse 2017:679.

	lämpligt övervakade för att säkerställa att de uppfyller kraven i första och andra styckena och kraven i kapitlen II och IV i Europaparlamentets och rådets förordning (EU) 2022/2554.

Värdepappersinstitutet ska dokumentera de åtgärder som det har vidtagit enligt första–tredje styckena så att Finansinspektionen har möjlighet att övervaka att institutet har följt denna lag.

13 kap.

1 §

En börs ska driva sin verksamhet hederligt, rättvist och professionellt och på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls.

När börsen driver en reglerad marknad, ska den tillämpa principerna om

1. fritt tillträde, som innebär att var och en som uppfyller de krav som ställs i denna lag och av börsen får delta i handeln,

2. neutralitet, som innebär att börsens regler för den reglerade marknaden tillämpas på ett likformigt sätt gentemot alla som deltar i handeln, och

3. god genomlysning, som innebär att deltagarna får en snabb, samtidig och korrekt information om handeln och att allmänheten får tillfälle att ta del av sådan information.

En börs ska också

1. identifiera och hantera de risker som kan uppstå i verksamheten,	1. identifiera och hantera de risker*, inbegripet IKT-risker i enlighet med kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554,* som kan uppstå i verksamheten, *och*
2. ha säkra tekniska system, samt	
3. identifiera och hantera de intressekonflikter som kan uppstå mellan börsens eller dess ägares intressen och intresset av att en reglerad marknad drivs i enlighet med första och andra styckena.	*2.* identifiera och hantera de intressekonflikter som kan uppstå mellan börsens eller dess ägares intressen och intresset av att en reglerad marknad drivs i enlighet med första och andra styckena.
En börs får inte i sitt regelverk ställa oskäliga krav på emittenter och deltagare vid en reglerad marknad. Vad som utgör ett oskäligt krav ska bedömas med hänsyn till dess ändamål, *EG-rätten* och övriga omständigheter.	En börs får inte i sitt regelverk ställa oskäliga krav på emittenter och deltagare vid en reglerad marknad. Vad som utgör ett oskäligt krav ska bedömas med hänsyn till dess ändamål, *EU-rätten* och övriga omständigheter.

1 a §[4]

En börs ska inrätta *effektiva system, förfaranden och arrangemang* för att säkerställa att handelssystemen	En börs ska inrätta *och upprätthålla en operativ motståndskraft i enlighet med kraven i kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554* för att säkerställa att handelssystemen
1. är motståndskraftiga,	
2. har tillräcklig kapacitet för att kunna hantera svåra påfrestningar på marknaden i fråga om order- och meddelandevolymer,	
3. kan upprätthålla ordnad handel vid förhållanden med påfrestningar på marknaden,	
4. är fullständigt testade, och	
5. garanterar kontinuitet i verksamheten vid eventuella driftavbrott i handelssystemet.	5. garanterar kontinuitet i verksamheten vid eventuella driftavbrott i handelssystemet*, inbegripet en IKT-kontinuitetspolicy och IKT-planer samt IKT-relaterade åtgärds- och återställningsplaner i enlighet med artikel 11 i Europaparlamentets och rådets förordning (EU) 2022/2554*.

1 d §[5]

En börs ska inrätta effektiva system, förfaranden och arrangemang för att säkerställa att deltagare som använder algoritmiska handelssystem på en reglerad marknad som börsen driver inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden och för att kunna hantera eventuella otillbörliga marknadsförhållanden som kan uppstå till följd av användningen av sådana algoritmiska handelssystem.

I de förfaranden som avses i första stycket ska det ingå

1. krav på deltagarna att utföra lämpliga tester av algoritmer och att tillhandahålla miljöer för att underlätta sådana tester,	1. krav på deltagarna att utföra lämpliga tester av algoritmer och att tillhandahålla miljöer för att underlätta sådana tester, *i enlighet med kraven i kapitlen II och IV i Europaparlamentets och rådets förordning (EU) 2022/2554,*
2. system för att begränsa andelen inte utförda order i förhållande till transaktionerna som kan läggas in i systemet av en deltagare,	
3. system för att det ska vara möjligt att bromsa orderflödet om det finns en risk för att taket för systemkapaciteten uppnås, och	
4. system för att begränsa och upprätthålla den minsta prisändring som får tillämpas på den reglerade marknaden.	

[4] Senaste lydelse 2017:679.
[5] Senaste lydelse 2017:679.

25 kap.

1 a §[6]

Finansinspektionen ska ingripa mot någon som ingår i ett svenskt värdepappersinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepappersinstitutet har åsidosatt sina skyldigheter enligt

1. 5 kap. 1, 3, 6 eller 7 §,
2. 6 kap. 1, 4 eller 6 §,
3. någon av 8 kap. 8 e eller 9–34 §§ eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 8 kap. 35 § 3–12,
4. någon av 9 kap. 1 §, 8 § tredje stycket, 9–12, 14–17 a, 19 a–41 eller 43 §§ eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 9 kap. 50 § 1, 3–9 eller 11,
5. någon av 11 kap. 1 §, 1 a § andra stycket, 1 b–4 a eller 12 §§ eller driver en tillväxtmarknad för små och medelstora företag trots att kraven i 13 § inte är uppfyllda,
6. någon av 13 kap. 1 a–1 j, 6 a eller 9 §§,
7. någon av 15 a kap. 7, 8 eller 10–14 §§,
8. 22 kap. 2 § andra stycket, 5 eller 6 § eller inte har följt ett beslut som meddelats av Finansinspektionen enligt 22 kap. 1 §, 2 § första stycket eller 3 §, *eller*
9. 23 kap. 2 § första stycket eller föreskrifter som meddelats med stöd av 23 kap. 15 § 1, eller inte har följt en begäran, ett föreläggande eller ett beslut som meddelats av Finansinspektionen enligt 23 kap. 2 § tredje stycket, 3 § första stycket, 3 a eller 3 b § eller har motsatt sig en undersökning enligt 23 kap. 4 §.

Föreslagen lydelse

8. 22 kap. 2 § andra stycket, 5 eller 6 § eller inte har följt ett beslut som meddelats av Finansinspektionen enligt 22 kap. 1 §, 2 § första stycket eller 3 §,
9. 23 kap. 2 § första stycket eller föreskrifter som meddelats med stöd av 23 kap. 15 § 1, eller inte har följt en begäran, ett föreläggande eller ett beslut som meddelats av Finansinspektionen enligt 23 kap. 2 § tredje stycket, 3 § första stycket, 3 a eller 3 b § eller har motsatt sig en undersökning enligt 23 kap. 4 §, *eller*
10. *någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.*

1 e §[7]

Finansinspektionen ska ingripa mot någon som ingår i en börs styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om börsen

1. har fått sitt tillstånd genom att lämna falska uppgifter eller på annat otillbörligt sätt,

[6] Senaste lydelse 2021:968.
[7] Senaste lydelse 2021:968.

2. har tillåtit en styrelseledamot, verkställande direktören eller ersättare för någon av dem att åta sig ett sådant uppdrag i företaget eller kvarstå i företaget trots att kraven i 12 kap. 2 § 4 eller 5 eller någon av 6 b–6 d §§ inte är uppfyllda,

3. har åsidosatt sina skyldigheter enligt

a) 8 kap. 21 § eller föreskrifter som meddelats med stöd av 8 kap. 35 § 12,

b) någon av 11 kap. 1 §, 1 a § andra stycket, 1 b–4 a eller 12 §§ eller driver en tillväxtmarknad för små och medelstora företag trots att kraven i 13 § inte är uppfyllda,

c) 12 kap. 6 e, 7 eller 10 § eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 12 kap. 11 § 2–4,

d) någon av 13 kap. 1–2, 6–7 a eller 9 §§ eller 12 § femte stycket eller föreskrifter som meddelats med stöd av 13 kap. 17 § 1,

e) 14 kap. 1, 2 eller 3 §,

f) 15 kap. 1, 2, 5, 9 eller 10 §,

g) någon av 15 a kap. 7, 8 eller 10–12 §§,

h) 22 kap. 2 § andra stycket, 5 eller 6 § eller inte har följt ett beslut som meddelats av Finansinspektionen enligt 22 kap. 1 eller 3 §, eller

i) 23 kap. 2 § första stycket eller föreskrifter som meddelats med stöd av 23 kap. 15 § 1, eller inte har följt en begäran, ett föreläggande eller ett beslut som meddelats av Finansinspektionen enligt 23 kap. 2 § andra stycket, 3 § första stycket eller 3 b § eller har motsatt sig en undersökning enligt 23 kap. 4 §,

4. i strid med 24 kap. 5 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där, *eller*

5. i strid med 24 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier eller andelar i företaget samt storleken på innehaven.

4. i strid med 24 kap. 5 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,

5. i strid med 24 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier eller andelar i företaget samt storleken på innehaven, *eller*

6. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Om en sådan person som avses i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 24 kap. 1 eller 4 § för förvärv eller avyttring av aktier eller andelar i företaget, ska första stycket 4 och 5 inte gälla för den personen i fråga om dessa aktier eller andelar.

1 i §[8]

Finansinspektionen ska ingripa mot någon som ingår i en central motparts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om den centrala motparten har åsidosatt sina skyldigheter enligt förordningen om återhämtning och resolution av centrala motparter genom att inte

1. utarbeta, upprätthålla och uppdatera en återhämtningsplan (artikel 9),

2. tillhandahålla nödvändiga uppgifter för att utarbeta resolutionsplan (artikel 13), eller

3. underrätta Finansinspektionen om att den centrala motparten fallerar eller sannolikt kommer att fallera (artikel 70.1).

Finansinspektionen ska även ingripa mot en sådan fysisk person som avses i första stycket om den centrala motparten har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en central motpart, eller ersättare för någon av dem, eller

2. sanktionsavgift.

Ett ingripande enligt första stycket får ske bara om den centrala motpartens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ett ingripande enligt första *eller andra* stycket får ske bara om den centrala motpartens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

1 j §

Finansinspektionen ska ingripa mot någon som ingår i en leverantör av datarapporteringstjänsters styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om leverantören har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

[8] Senaste lydelse 2022:743.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en leverantör av datarapporteringstjänster, eller ersättare för någon av dem, eller

2. sanktionsavgift.

Ett ingripande får ske bara om Finansinspektionen har tillsyn över leverantören av datarapporteringstjänster.

1 k §

Ett ingripande enligt 1 j § får ske bara om leverantören av datarapporteringstjänsters överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Denna lag träder i kraft den 17 januari 2025.

2.9 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 30 kap. 30 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 30 kap. 4 e §, och närmast före 30 kap. 4 e § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	30 kap.
	Verksamhet som rör digital operativ motståndskraft för finanssektorn
	4 e § *Sekretess gäller i en statlig myndighets verksamhet enligt 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* *1. för uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, om det kan antas att denne lider skada om uppgiften röjs, och* *2. för uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser.* *För uppgift i en allmän handling gäller sekretessen i högst tjugo år.*
30 §[1]	
Den tystnadsplikt som följer av 2 § första stycket första meningen, 4 § första stycket 2, 4 a § första stycket 2, 4 b § första stycket, 6 b § första stycket, 12 § första stycket	Den tystnadsplikt som följer av 2 § första stycket första meningen, 4 § första stycket 2, 4 a § första stycket 2, 4 b § första stycket, *4 e § första stycket 2,* 6 b § första

[1] Senaste lydelse 2022:744.

och andra stycket 2, 12 a § första stycket och andra stycket 2, 12 b § första stycket 2, 12 c § första stycket och andra stycket 2, 13 §, 15 § första stycket 2, 23 § första stycket 2, 23 a §, 23 b § och 27 § första stycket 2 och den tystnadsplikt som följer av ett förbehåll som gjorts med stöd av 9 § andra meningen, 14 § andra meningen, 26 § andra meningen eller 29 § andra meningen inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

stycket, 12 § första stycket och andra stycket 2, 12 a § första stycket och andra stycket 2, 12 b § första stycket 2, 12 c § första stycket och andra stycket 2, 13 §, 15 § första stycket 2, 23 § första stycket 2, 23 a §, 23 b § och 27 § första stycket 2 och den tystnadsplikt som följer av ett förbehåll som gjorts med stöd av 9 § andra meningen, 14 § andra meningen, 26 § andra meningen eller 29 § andra meningen inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 24 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om andra ekonomiska eller personliga förhållanden än affärs- och driftförhållanden för den som trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Den tystnadsplikt som följer av 18 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om en enskilds personliga förhållanden vars röjande kan vålla allvarligt men.

Denna lag träder i kraft den 17 januari 2025.

2.10 Förslag till lag om ändring i lagen (2010:751) om betaltjänster

Härigenom föreskrivs[1] i fråga om lagen (2010:751) om betaltjänster

dels att 5 b kap. 1 och 3 §§, 8 kap. 9, 16 a och 23 b §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 8 kap. 8 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

5 b kap.

1 §[2]

En betaltjänstleverantör ska ha ett system med lämpliga åtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker som är förknippade med de betaltjänster som den tillhandahåller. Inom ramen för detta system ska betaltjänstleverantören reglera hur incidenter ska hanteras.

För betaltjänstleverantörer som omfattas av 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 gäller även kapitel II i förordningen.

3 §[3]

En betaltjänstleverantör ska så snart det kan ske underrätta Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident som uppkommit i verksamheten. Finansinspektionen ska så snart det kan ske informera Riksbanken, andra berörda svenska myndigheter, Europeiska bankmyndigheten och Europeiska centralbanken.

Om incidenten påverkar eller kan påverka betaltjänstanvändarnas ekonomiska intressen, ska betaltjänstleverantören så snart det kan ske informera användarna om incidenten och om de åtgärder som kan vidtas för att begränsa risken för skada.

Första och andra styckena gäller inte för betaltjänstleverantörer som omfattas av bestämmelserna i

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse 2018:175.

[3] Senaste lydelse 2018:175.

Europaparlamentets och rådets förordning (EU) 2022/2554.

8 kap.

8 b §

Finansinspektionen ska ingripa mot någon som ingår i betalningsinstitutets styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om institutet har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett betalningsinstitut, eller ersättare för någon av dem, eller

2. sanktionsavgift.

9 §[4]

Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

Finansinspektionen får avstå från ingripande enligt 8 *och* 8 a §§ om

Finansinspektionen får avstå från ingripande enligt 8*,* 8 a *och 8 b* §§ om

1. en överträdelse är ringa eller ursäktlig,

2. betalningsinstitutet gör rättelse eller om den fysiska personen i betalningsinstitutets ledning verkat för att institutet gör rättelse, eller

3. någon annan myndighet har vidtagit åtgärder mot institutet eller den fysiska personen i betalningsinstitutets ledning som bedöms vara tillräckliga.

[4] Senaste lydelse 2017:652.

16 a§[5]

Frågor om ingripanden mot fysiska personer enligt 8 a *§* tas upp av Finansinspektionen genom sanktionsföreläggande.	Frågor om ingripanden mot fysiska personer enligt 8 a *och 8 b §§* tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

23 b §[6]

Finansinspektionen ska ingripa mot en person som ingår i en registrerad betaltjänstleverantörs styrelse eller är dess verkställande direktör eller på motsvarande sätt företräder betaltjänstleverantören, eller är ersättare för någon av dem, om den registrerade betaltjänstleverantören har befunnits ansvarig för en överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen eller en överträdelse av förordning (EU) 2015/847.

Ett ingripande enligt första stycket får ske endast om överträdelsen är allvarlig, upprepad eller systematisk och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Finansinspektionen ska även ingripa mot någon som ingår i en registrerad betaltjänstleverantörs styrelse eller är dess verkställande direktör eller på motsvarande sätt företräder betaltjänstleverantören, eller är ersättare för någon av dem, om den registrerade betaltjänstleverantören har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt tredje stycket får ske endast om den registrerade betaltjänstleverantörens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

[5] Senaste lydelse 2017:652.
[6] Senaste lydelse 2017:652.

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i första stycket hos en registrerad betaltjänstleverantör, eller

2. beslut om sanktionsavgift.

Denna lag träder i kraft den 17 januari 2025.

2.11 Förslag till lag om ändring i försäkringsrörelselagen (2010:2043)

Härigenom föreskrivs[1] i fråga om försäkringsrörelselagen (2010:2043)[2]

dels att 21 kap. 2 § ska upphöra att gälla,

dels att 10 kap. 3 §, 11 kap. 1 §, 18 kap. 2 a och 18 a §§ och 21 kap. 1 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 18 kap. 1 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
10 kap.	
3 §[3]	
Ett försäkringsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna bedrivas med kontinuitet och i enlighet med gällande regler.	Ett försäkringsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna bedrivas med kontinuitet och i enlighet med gällande regler. *Nätverks- och informationssystem ska uppfylla kraven i 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.*
	Ett försäkringsföretag ska ha en beredskapsplan.
11 kap.	
1 §[4]	
För försäkringsaktiebolag gäller föreskrifterna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller är särskilt föreskrivet. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag som gäller i stället för eller utöver bestämmelserna i aktiebolagslagen.	
I fråga om försäkringsaktiebolag ska det som anges om Bolagsverket i följande bestämmelser avse Finansinspektionen:	
– 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,	*1.* 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,
– 23 kap. 45 b § aktiebolagslagen,	*2.* 23 kap. 45 b § aktiebolagslagen,

[1] Jfr Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II), i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse av 21 kap. 2 § 2019:766.

[3] Senaste lydelse 2015:700.

[4] Senaste lydelse 2022:1650.

– 24 kap. 47 § aktiebolagslagen, och	*3.* 24 kap. 47 § aktiebolagslagen, och
– 24 a kap. 24 § aktiebolagslagen.	*4.* 24 a kap. 24 § aktiebolagslagen.

Bestämmelserna i 32 kap. aktiebolagslagen om aktiebolag med särskild vinstutdelningsbegränsning gäller inte för försäkringsaktiebolag.

18 kap.

1 b §

Finansinspektionen ska ingripa mot någon som ingår i försäkringsföretagets styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om företaget har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt första stycket får ske endast om företagets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

2 a §[5]

Ingripande enligt 1 a *§* sker genom	Ingripande enligt 1 a *och 1 b §§* sker genom
1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i 1 a § första stycket i ett försäkringsföretag, eller	1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i 1 a § första stycket *och 1 b § första stycket* i ett försäkringsföretag, eller
2. beslut om sanktionsavgift.	

18 a §[6]

Frågor om ingripanden mot fysiska personer för överträdelser enligt 1 a *§* tas upp av Finansinspektionen genom sanktionsföreläggande.	Frågor om ingripanden mot fysiska personer för överträdelser enligt 1 a *eller 1 b §* tas upp av Finansinspektionen genom sanktionsföreläggande.

[5] Senaste lydelse 2017:653.
[6] Senaste lydelse 2017:653.

Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

21 kap.

1 §[7]

Finansinspektionens beslut i ärenden enligt 17 kap. 13 § första stycket och 18 kap. 25 § andra stycket *samt beslut om sanktionsföreläggande* får inte överklagas.	Finansinspektionens beslut i ärenden enligt 17 kap. 13 § första stycket och 18 kap. 25 § andra stycket får inte överklagas. *Detsamma gäller för sådana beslut om förordnande av sakkunnig som avses i 11 kap. 1 § andra stycket 2–4 och för beslut om sanktionsföreläggande.*

Denna lag träder i kraft den 17 januari 2025.

[7] Senaste lydelse 2019:766.

2.12 Förslag till lag om ändring i lagen (2011:755) om elektroniska pengar

Härigenom föreskrivs i fråga om lagen (2011:755) om elektroniska pengar
dels att 5 kap. 9, 16 a och 23 b §§ ska ha följande lydelse,
dels att det ska införas en ny paragraf, 5 kap. 8 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	5 kap.
	8 b §
	Finansinspektionen ska ingripa mot någon som ingår i styrelsen för institutet för elektroniska pengar eller är dess verkställande direktör, eller ersättare för någon av dem, om institutet har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.
	Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.
	Ingripande får ske genom en eller båda av följande sanktioner:
	1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett institut för elektroniska pengar, eller ersättare för någon av dem, eller
	2. sanktionsavgift.

9 §[1]

Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

Finansinspektionen får avstå från ingripande enligt 8 *och* 8 a §§ om	Finansinspektionen får avstå från ingripande enligt 8*,* 8 a *och 8 b* §§ om

1. en överträdelse är ringa eller ursäktlig,
2. institutet för elektroniska pengar gör rättelse eller om den fysiska personen verkat för att institutet gör rättelse, eller
3. någon annan myndighet har vidtagit åtgärder mot institutet eller den fysiska personen som bedöms vara tillräckliga.

16 a§[2]

Frågor om ingripanden mot fysiska personer enligt 8 a *§* tas upp av Finansinspektionen genom sanktionsföreläggande.	Frågor om ingripanden mot fysiska personer enligt 8 a *eller 8 b §* tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

23 b §[3]

Finansinspektionen ska ingripa mot en person som ingår i den registrerade utgivarens styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om den registrerade utgivaren har befunnits ansvarig för överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen eller en överträdelse av förordning (EU) 2015/847.

Ett ingripande enligt första stycket får ske endast om överträdelsen är allvarlig, systematisk eller upprepad och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Finansinspektionen ska även ingripa mot någon som ingår i den registrerade utgivarens styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om den registrerade utgivaren, har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

[1] Senaste lydelse 2017:655.
[2] Senaste lydelse 2017:655.
[3] Senaste lydelse 2017:655.

Ett ingripande enligt tredje stycket får ske endast om den registrerade utgivarens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i första stycket hos en utgivare av elektroniska pengar, eller

2. beslut om sanktionsavgift.

Denna lag träder i kraft den 17 januari 2025.

2.13 Förslag till lag om ändring i lagen (2013:561) om förvaltare av alternativa investeringsfonder

Härigenom föreskrivs[1] i fråga om lagen (2013:561) om förvaltare av alternativa investeringsfonder

dels att 8 kap. 2 § och 14 kap. 13 a § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 14 kap. 1 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

8 kap.

2 §

En AIF-förvaltare ska ha sunda rutiner för

1. förvaltning av verksamheten och redovisning,
2. drift och förvaltning av sina informationssystem, och
3. intern kontroll.

Rutinerna enligt första stycket 2 ska uppfylla kraven i 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.

AIF-förvaltaren ska särskilt

1. upprätta och tillämpa regler för anställdas egna transaktioner,
2. upprätta och tillämpa regler för investeringar som görs för förvaltarens egen räkning,
3. ha rutiner för att kunna säkerställa att varje transaktion som genomförs för en alternativ investeringsfonds räkning är möjlig att rekonstruera i efterhand med avseende på dess ursprung, art, parter, tidpunkt och plats, samt
4. ha rutiner för att säkerställa att tillgångarna i de alternativa investeringsfonder som förvaltaren förvaltar investeras i enlighet med denna lag och andra författningar som reglerar verksamheten eller lagstiftningen i det land där fonden är etablerad samt fondbestämmelser, bolagsordning eller motsvarande regelverk.

[1] Jfr Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

14 kap.

1 b §

Finansinspektionen ska ingripa mot någon som ingår i en AIF-förvaltares ledning eller styrelse eller är förvaltarens verkställande direktör eller motsvarande, eller ersättare för någon av dem, om förvaltaren har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt första stycket får ske endast om AIF-förvaltarens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en AIF-förvaltare, eller ersättare för någon av dem, eller

2. sanktionsavgift.

13 a §[2]

Frågor om ingripanden mot fysiska personer enligt 1 a eller 9 a § tas upp av Finansinspektionen genom sanktionsföreläggande.

Frågor om ingripanden mot fysiska personer enligt 1 a, *1 b* eller 9 a § tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 12 kap. 9 a–9 d §§ lagen (2004:46) om värdepappersfonder.

Denna lag träder i kraft den 17 januari 2025.

[2] Senaste lydelse 2017:658.

2.14 Förslag till lag om ändring i lagen (2019:742) om tjänstepensionsföretag

Härigenom föreskrivs[1] i fråga om lagen (2019:742) om tjänstepensionsföretag

dels att 9 kap. 2 §, 10 kap. 1 §, 15 kap. 3, 4, 18, 20 och 23 §§ och 17 kap. 1 § ska ha följande lydelse,

dels att rubriken närmast efter rubriken till 15 kap. ska lyda ”Ingripande mot tjänstepensionsföretag och vissa fysiska personer”,

dels att det ska införas fyra nya paragrafer, 15 kap. 1 a §, 2 a §, 17 a § och 18 a §, av följande lydelse, och närmast före 15 kap. 18 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 kap.	
2 §	
Ett tjänstepensionsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna drivas med kontinuitet och i enlighet med gällande regler.	Ett tjänstepensionsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna drivas med kontinuitet och i enlighet med gällande regler. *Nätverks- och informationssystem ska uppfylla kraven i 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.*
	Ett tjänstepensionsföretag ska ha en beredskapsplan.
10 kap.	
1 §[2]	
För tjänstepensionsaktiebolag gäller bestämmelserna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller av sådana bestämmelser i försäkringsrörelselagen (2010:2043) som det hänvisas till i denna lag. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag eller i försäkringsrörelselagen som gäller i stället för eller utöver aktiebolagslagen.	
I fråga om tjänstepensionsaktiebolag ska det som sägs om Bolagsverket i följande bestämmelser avse Finansinspektionen:	

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut, i lydelsen enligt Europaparlamentets och rådets direktiv (EU) 2022/2556.

[2] Senaste lydelse 2022:1651.

– 8 kap. 9 och 30 §§ och 37 § andra stycket aktiebolagslagen,	*1.* 8 kap. 9 och 30 §§ och 37 § andra stycket aktiebolagslagen,
– 23 kap. 45 b § aktiebolagslagen,	*2.* 23 kap. 45 b § aktiebolagslagen,
– 24 kap. 47 § aktiebolagslagen, och	*3.* 24 kap. 47 § aktiebolagslagen, och
– 24 a kap. 24 § aktiebolagslagen.	*4.* 24 a kap. 24 § aktiebolagslagen.

Bestämmelserna i 32 kap. aktiebolagslagen om aktiebolag med särskild vinstutdelningsbegränsning gäller inte för tjänstepensionsaktiebolag.

15 kap.

1 a §

Finansinspektionen ska ingripa mot någon som ingår i tjänstepensionsföretagets styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om företaget har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt första stycket får ske endast om företagets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

2 a §

Ingripande enligt 1 a § sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i 1 a § första stycket i ett tjänstepensionsföretag, eller

2. beslut om sanktionsavgift.

3 §

Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

I försvårande riktning ska det beaktas om tjänstepensionsföretaget tidigare har begått en överträdelse.	I försvårande riktning ska det beaktas om tjänstepensionsföretaget tidigare har begått en överträdelse *eller om den fysiska*

	personen tidigare orsakat en sådan överträdelse.
I förmildrande riktning ska det beaktas om	
1. företaget i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och	1. företaget *eller den fysiska personen* i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och
2. företaget snabbt har upphört med överträdelsen sedan den anmälts till eller påtalats av Finansinspektionen.	2. företaget snabbt har upphört med överträdelsen*, eller den fysiska personen snabbt verkat för att överträdelsen ska upphöra,* sedan den anmälts till eller påtalats av Finansinspektionen.
4 §	
Finansinspektionen får avstå från ingripande om	
1. en överträdelse är ringa eller ursäktlig,	
2. tjänstepensionsföretaget gör rättelse, eller	2. tjänstepensionsföretaget gör rättelse *eller om den fysiska personen verkat för att företaget gör rättelse*, eller
3. någon annan myndighet har vidtagit åtgärder mot företaget och dessa åtgärder bedöms tillräckliga.	3. någon annan myndighet har vidtagit åtgärder mot företaget *eller den fysiska personen* och dessa åtgärder bedöms tillräckliga.
	17 a §
	En sanktionsavgift för en fysisk person ska som högst fastställas till det högsta av
	1. två gånger den vinst som den fysiska personen gjort till följd av regelöverträdelsen, om beloppet går att fastställa, eller
	2. ett belopp som per den 16 januari 2023 i kronor motsvarade fem miljoner euro.
	Avgiften tillfaller staten.
18 §	
När sanktionsavgiftens storlek fastställs, ska särskild hänsyn tas till sådana omständigheter som anges i 3 § samt till tjänstepensionsföretagets finansiella ställning och, om det går att fastställa, den vinst som gjorts till följd av regelöverträdelsen.	När sanktionsavgiftens storlek fastställs, ska särskild hänsyn tas till sådana omständigheter som anges i 3 § samt till tjänstepensionsföretagets *eller den fysiska personens* finansiella ställning och, om det går att fastställa, den vinst som gjorts till följd av regelöverträdelsen.

	Sanktionsföreläggande
	18 a § *Frågor om ingripanden mot fysiska personer för överträdelser enligt 1 a § tas upp av Finansinspektionen genom sanktionsföreläggande.* *Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.*
20 §	
En sanktionsavgift eller förseningsavgift ska betalas till Finansinspektionen inom 30 dagar efter det att beslutet om den har fått laga kraft eller inom den längre tid som anges i beslutet.	En sanktionsavgift eller förseningsavgift ska betalas till Finansinspektionen inom 30 dagar efter det att beslutet om den har fått laga kraft *eller sanktionsföreläggandet godkänts* eller inom den längre tid som anges i beslutet.
23 §	
En beslutad sanktionsavgift eller förseningsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft.	En beslutad sanktionsavgift eller förseningsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft *eller sanktionsföreläggandet godkändes*.
17 kap.	
1 §	
Finansinspektionens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.	Finansinspektionens beslut *om förordnande av sakkunnig som avses i 10 kap. 1 § andra stycket 2–4 och sanktionsföreläggande enligt 15 kap. 18 a § får inte överklagas. Andra beslut av Finansinspektionen* enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 17 januari 2025.

3 Ärendet

Europaparlamentet och rådet antog den 14 december 2022 förordningen (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, i det följande benämnd DORA-förordningen. Förordningen trädde i kraft den 16 januari 2023 och ska tillämpas från och med den 17 januari 2025. Förordningen finns i *bilaga 1*.

Genom förordningen införs nya krav på företag inom den finansiella sektorn. Detta gäller bl.a. krav på företagens riskhantering, incidentrapportering, företags hantering av utlagd verksamhet och testning av digital operativ motståndskraft hos företagen.

Tillsammans med DORA-förordningen har det gjorts ändringar i flera EU-direktiv på finansmarknadsområdet genom 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, i det följande benämnt ändringsdirektivet. Ändringarna ska tillämpas från och med den 17 januari 2025. Ändringsdirektivet finns i *bilaga 2*.

DORA-förordningen och ändringsdirektivet kräver vissa lagstiftningsåtgärder. I denna promemoria lämnas förslag om sådana åtgärder.

I promemorian lämnas också förslag till vissa ändringar som rör överklaganden av Finansinspektionens beslut i frågor som inte har samband med DORA-förordningen (se avsnitt 17).

4 EU:s förordning om digital operativ motståndskraft för finanssektorn

4.1 Bakgrund och förordningens syfte

DORA-förordningen syftar till att genom enhetliga krav i nätverks- och informationssystem uppnå en hög gemensam nivå av digital operativ motståndskraft i den finansiella sektorn (artikel 1.1). I kommissionens förslag till förordning samt i skälen till förordningen betonas de senaste årtiondenas snabba digitalisering (skäl 1) och hur användningen av informations- och kommunikationsteknologi (IKT) i dag är avgörande för driften av alla finansiella entiteters vanliga dagliga funktioner (skäl 2). Samtidigt påpekas att en ökad digitalisering innebär ökade sårbarheter (skäl 1) och att Europeiska systemrisknämnden i en rapport från 2020 bekräftar att den höga graden av sammanlänkning mellan finansiella entiteter, finansmarknader och finansmarknadsinfrastruktur kan utgöra en systemsårbarhet som kan få negativa konsekvenser för den finansiella stabiliteten i EU (skäl 3). Det enhetliga regelverk som nu styr unionens finansiella sektor och som reformerades efter finanskrisen 2008 syftar främst till att stärka den finansiella motståndskraften i finanssektorn

(skäl 5). Även om IKT-säkerhet och digital motståndskraft ingår i de operativa riskerna som omfattas av befintligt regelverk, uppmärksammas de inte i tillräckligt hög omfattning i unionslagstiftningen (skäl 5 och 8). Detta har lett till skillnader i lagstiftning och olika nationella regleringsoch tillsynsstrategier för IKT-risk, vilket riskerar att utgöra ett hinder för den inre marknadens funktion (skäl 9). Det har därför identifierats ett behov av att utveckla det gemensamma regelverket och tillsynssystemet för den finansiella sektorn så att det även omfattar harmoniserande bestämmelser kring digital operativ motståndskraft (skäl 8 och 11).

4.2 Andra EU-rättsakter om ökad motståndskraft

NIS2- och CER-direktiven

DORA-förordningen är en del av ett EU-rättsligt ramverk för en ökad motståndskraft inom EU. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i det följande benämnt NIS2-direktivet, ersätter det tidigare s.k. NIS-direktivet. NIS-direktivet var den första övergripande ramen för cybersäkerhet som antogs på unionsnivå. Syftet med NIS-direktivet var att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter. NIS-direktivet omfattar tre typer av finansiella entiteter, nämligen kreditinstitut, handelsplatser och centrala motparter. Direktivet har genomförts i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Tillämpningsområdet för NIS2-direktivet har utökats till att omfatta aktörer inom fler sektorer, men direktivet omfattar fortfarande samma typer av finansiella entiteter som det tidigare NIS-direktivet. NIS2-direktivet fastställer till skillnad från det tidigare direktivet enhetliga kriterier för att avgöra vilka entiteter som omfattas av dess tillämpningsområde utifrån en storleksbaserad regel. Ett större antal finansiella entiteter omfattas därför av NIS2-direktivet. I NIS2-direktivet skärps kraven på entiteterna genom minimikrav för åtgärder som ska tillämpas för att hantera risker kopplade till säkerheten i entiteters nätverks- och informationssystem. Direktivet innehåller även mer precisa rapporteringskrav. I likhet med vad som gäller enligt NIS-direktivet ska medlemsstaterna enligt NIS2-direktivet utse en eller flera behöriga myndigheter och en nationell gemensam kontaktpunkt. Liksom NIS-direktivet föreskriver även NIS2-direktivet att det ska finnas en eller flera enheter för hantering av it-säkerhetsincidenteter (s.k. CSIRT-enheter) som bl.a. ska ansvara för hanteringen av incidenter. I NIS2-direktivet åläggs dessa ytterligare uppgifter. NIS2-direktivet innehåller dessutom nya regler om ett ramverk för storskaliga cybersäkerhetsincidenter och cyberkriser. Varje medlemsstat ska enligt direktivet utse en eller flera behöriga myndigheter

som ansvarar för hanteringen av sådana incidenter och kriser (cyberkrishanteringsmyndighet). Vidare ställer NIS2-direkivet större krav på såväl strategisk som operativt samarbete mellan medlemsstaterna. I NIS2-direktivet regleras även nya former för samarbete mellan medlemsstaterna. Ett forum för samarbete är det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som ska verka stödjande vid samordning och hantering av storskaliga incidenter och cyberkriser.

Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i det följande benämnt CER-direktivet, innehåller bestämmelser som syftar till att förebygga, motstå och hantera störningar eller avbrott i samhällsviktig verksamhet, inbegripet kritisk infrastruktur. Direktivet inrättar en övergripande ram för att hantera kritiska entiteters motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller orsakade av människan, olyckshändelser eller avsiktligt framkallade faror (skäl 1–4). CER-direktivet ålägger de kritiska entiteterna skyldigheter att bl.a. vidta åtgärder för att stärka sin motståndskraft och att rapportera incidenter. Det innehåller också bestämmelser om tillsyn och sanktioner. Vidare fastställs i CER-direktivet en ram för samarbete mellan medlemsstaterna. CER-direktivet omfattar samma finansiella entiteter som NIS2-direktivet.

NIS2-direktivet och det kompletterande CER-direktivet ska vara genomförda i svensk rätt den 17 oktober 2024. Regeringen har gett en särskild utredare i uppdrag att föreslå de anpassningar av svensk rätt som är nödvändiga för att direktiven ska kunna genomföras (dir. 2023:30).

DORA-förordningen har företräde framför direktiven

Av NIS2- och CER-direktiven följer att berörda bestämmelser i direktiven inte ska vara tillämpliga om det i en sektorsspecifik EU-rättsakt ställs åtminstone likvärda krav som i direktiven på att entiteter ska vidta åtgärder för att stärka sin motståndskraft (artikel 4 i NIS2-direktivet och artikel 1.3 i CER-direktivet). DORA-förordningen är en sektorsspecifik EU-rättsakt i förhållande till NIS2- och CER-direktiven (artikel 1.2 i DORA-förordningen). I DORA-förordningen fastställs strängare krav på IKT-riskhantering och IKT-relaterad incidentrapportering än i NIS2-direktivet (jfr skäl 16 i DORA-förordningen). NIS2-direktivets bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet och om tillsyn och efterlevnadskontroll ska därför inte tillämpas på de finansiella entiteter som omfattas av direktivet (skäl 28 och artikel 4 i NIS2-direktivet). DORA-förordningens krav på IKT-riskhantering inbegriper även skydd av fysisk IKT-infrastruktur (jfr skäl 21 i CER-direktivet). De finansiella entiteterna ska därför även undantas från artikel 11 och kapitlen 3, 4 och 6 i CER-direktivet (artikel 8 i CER-direktivet). De finansiella entiteterna ska dock ingå i den förteckning som ska upprättas över entiteter som omfattas av direktiven (artikel 3.3 i NIS2 direktivet och artikel 6.3 i CER-direktivet).

Det har samtidigt ansetts viktigt att upprätthålla en stark koppling mellan finanssektorn och EU:s övergripande ram för cybersäkerhet för att säkerställa överensstämmelse med de strategier för cybersäkerhet som ska antas av medlemsstaterna och göra det möjligt för finansiella tillsynsmyndig-

heter att få kännedom om cyberincidenter som påverkar andra sektorer som omfattas av NIS2-direktivet (jfr skäl 16 i DORA-förordningen och skäl 28 i NIS2-direktivet). De europeiska tillsynsmyndigheterna och de behöriga myndigheterna enligt DORA-förordningen ska därför ha möjlighet att delta i samarbetsgruppens verksamhet och att utbyta information och samarbeta med de gemensamma kontaktpunkterna och med CSIRT-enheterna och de behöriga myndigheterna enligt NIS2-direktivet (artikel 47 i DORA-förordningen). De behöriga myndigheterna enligt DORA-förordningen ska även översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt NIS2-direktivet (artikel 19.6 c i DORA-förordningen). Medlemsstaterna kan även reglera att finansiella entiteter som frivilligt rapporterar betydande cyberhot till den behöriga myndigheten enligt DORA-förordningen även får vidarebefordra anmälan till en CSIRT-enhet (artikel 19.2) Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.

4.3 Tillämpningsområde

DORA-förordningen är tillämplig på de flesta fysiska och juridiska personer som är verksamma inom den finansiella sektorn förutom betalningssystemoperatörer och enheter som deltar i betalningshantering (artikel 2 och 58). I förordningen benämns dessa som finansiella entiteter (artikel 2.2). Förvaltare av alternativa investeringsfonder, försäkrings- och återförsäkringsföretag, tjänstepensionsinstitut och försäkrings- och återförsäkringsförmedlare som inte uppfyller vissa storlekskrav undantas från tillämpningsområdet. Från förordningens tillämpningsområde undantas även postgiroinstitut, försäkringsförmedlare som bedriver förmedling som sidoverksamhet och personer som omfattas av artikel 2 och 3 i Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU. Förordningen ger även möjlighet att undanta bl.a. Svenska skeppshypotekskassan från tillämpningsområdet.

Förordningen gäller för ett stort antal finansiella entiteter inom den finansiella sektorn där riskerna varierar utifrån den verksamhet som den enskilda entiteten får bedriva. Proportionalitetsprincipen är därmed central vid tillämpningen av förordningen (artikel 4 och skäl 21). Finansiella entiteter ska efterleva kraven i förordningen med beaktande av bland annat sin storlek och allmänna riskprofil samt karaktären på, omfattningen av och komplexiteten i sina tjänster. På samma sätt ska tillsynsmyndigheterna beakta de finansiella entiteternas tillämpning av proportionalitetsprincipen när de utövar sin tillsyn.

4.4 Centrala termer och uttryck i förordningen

4.4.1 Digital operativ motståndskraft

Digital operativ motståndskraft definieras i DORA-förordningen som en finansiell entitets förmåga att bygga upp, säkerställa och se över sin operativa integritet och tillförlitlighet genom att, direkt eller indirekt, med användning av tjänster från tredjepartsleverantörer av IKT-tjänster, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell entitet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet, inbegripet under avbrott (artikel 3.1). Begreppet syftar till att säkerställa både robusta IKT-system samt företagsledningar och organisationer som är rustade att stå emot och hantera alla möjliga former av IKT-relaterade incidenter.

4.4.2 IKT-tjänster

Med IKT-tjänster avses digitala tjänster och datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare. Detta omfattar maskinvara som tjänst och maskinvarutjänster som inbegriper tillhandahållande av teknisk support genom uppdateringar av programvara eller fast programvara från maskinvaruleverantören. Traditionella analoga telefontjänster omfattas däremot inte (artikel 3.21).

4.4.3 Finansiell entitet

Med finansiell entitet avses de aktörer på finansmarknaden, både juridiska och fysiska personer, som förordningen ska tillämpas på (artikel 2.1.a-t tillsammans med artikel 2.2). Tredjepartsleverantörer av IKT-tjänster, som också omfattas av förordningens tillämpningsområde, ingår däremot inte i begreppet ”finansiell entitet” (artikel 2.1 u jämförd med artikel 2.2).

4.4.4 Tredjepartsleverantör av IKT-tjänster

Tredjepartsleverantör av IKT-tjänster är ett företag som tillhandahåller IKT-tjänster (artikel 3.19).

4.4.5 Kritisk tredjepartsleverantör av IKT-tjänster

En tredjepartsleverantör av IKT-tjänster kan i vissa fall klassificeras som en kritisk tredjepartsleverantör av IKT-tjänster (artikel 3.23). Detta gäller bl.a. om det skulle ske en systempåverkan på stabiliteten, kontinuiteten eller kvaliteten på tillhandahållandet av finansiella tjänster om tredjepartsleverantören skulle drabbas av ett omfattande driftsavbrott (se artikel 31.2).

4.4.6 IKT-risk

IKT-risk är varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem som, om de inträffar, genom att orsaka negativa effekter i den digitala eller fysiska miljön kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är teknikberoende, funktioner och processer eller tillhandahållandet av tjänster (artikel 3.5).

4.4.7 IKT-tredjepartsrisk

Med IKT-tredjepartsrisk avses en IKT-risk som kan uppstå för en finansiell entitet i samband med dess användning av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster eller av underleverantörer till sådana leverantörer (artikel 3.18).

4.4.8 Hotbildsstyrd penetrationstestning

Hotbildsstyrd penetrationstestning avser en testram som efterliknar den taktik, teknik och de förfaranden som används av verkliga fientliga aktörer som uppfattas som ett genuint cyberhot. Testramen ska ge ett kontrollerat, skräddarsytt och underrättelsestyrt test (så kallat red team-test) av de kritiska produktionssystem som är i drift hos den finansiella entiteten (artikel 3.17).

4.5 IKT-riskhantering

DORA-förordningen redogör för vilka krav på IKT-riskhantering som ställs på de finansiella entiteterna. Finansiella entiteter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram som ska göra det möjligt för de finansiella entiteterna att säkerställa en hög nivå av digital operativ motståndskraft (artikel 6.1). IKT-riskhanteringsramen ska innehålla en strategi för digital operativ motståndskraft som inbegriper metoder för att hantera IKT-risker och genomförandet av tester av den digitala operativa motståndskraften (artikel 6.8). Metoder för att hantera IKT-risker avser bland annat regelbundna riskbedömningar (artikel 8), övervakning av IKT-systemens verksamhet (artikel 9), rutiner för säkerhetskopiering, återskapande och återställning (artikel 12) samt IKT-kontinuitetspolicys (artikel 11). Strategin ska uppdateras regelbundet (artikel 6).

En förenklad IKT-riskhanteringsram ska tillämpas för vissa finansiella entiteter (se artikel 16).

Finansiella entiteter ska registrera alla IKT-relaterade incidenter och betydande cyberhot och inrätta lämpliga förfaranden och processer för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av IKT-relaterade incidenter (artikel 17.1 och 17.2). Allvarliga IKT-relaterade incidenter ska rapporteras till den behöriga myndigheten (artikel 19). Finansiella entiteter får också på frivillig basis rapportera betydande cyberhot till den relevanta behöriga myndigheten.

Det finns också bestämmelser om klassificering av IKT-relaterade incidenter och cyberhot. Kommissionen har också möjlighet att komplettera förordningen med tekniska standarder inom detta område (artikel 18).

4.6 Testning av digital operativ motståndskraft

DORA-förordningen innehåller bestämmelser om testning av digital operativ motståndskraft. Enligt kapitlet ska varje finansiell entitet som en integrerad del av sin IKT-riskhanteringsram inrätta, upprätthålla och se över ett sunt och heltäckande program för testning (artikel 24.1). Testprogrammet ska innehålla bestämmelser om utförande av lämpliga tester såsom bl.a. sårbarhetsanalyser, nätverkssäkerhetsbedömningar, fysiska säkerhetsgranskningar och penetrationstester (artikel 25.1). Utifrån testresultatet ska den finansiella entiteten besluta en åtgärdsplan för att säkerställa att identifierade brister hanteras på ett tillfredsställande sätt (artikel 24.5).

Finansiella entiteter som är verksamma inom delsektorer för centrala finansiella tjänster och som har en central betydelse för systemet ska dessutom regelbundet genomföra avancerad testning baserad på hotbildsstyrd penetrationstestning (artikel 26.1 och 26.8 samt skäl 56). Sådana tester ska genomföras vart tredje år om inte ansvarig myndighet begär något annat.

4.7 Hantering av IKT-tredjepartsrisker

IKT-tredjepartsrisker ska hanteras som en integrerad del av IKT-riskhanteringsramen, vilken ska innehålla en strategi för IKT-tredjepartsrisk (artikel 28). Finansiella entiteter ska upprätthålla ett register med information om användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster och åtminstone årligen rapportera till den behöriga myndigheten om antalet nya arrangemang. Innan en finansiell entitet ingår ett kontraktsmässigt arrangemang om användning av IKT-tjänster ska den bland annat genomföra due diligence-granskning av potentiella tredjepartsleverantörer, identifiera och bedöma intressekonflikter som det kontraktsmässiga arrangemanget kan orsaka samt identifiera och bedöma alla relevanta risker i samband med det kontraktsmässiga arrangemanget, inbegripet möjligheten att sådana kontraktsmässiga arrangemang kan bidra till att förstärka IKT-koncentrationsrisken. Förordningen innehåller även krav på exitstrategier (artikel 28) och bestämmelser om innehållet i de kontraktsmässiga arrangemangen för användning av IKT-tjänster (artikel 30).

För kritiska tredjepartsleverantörer av IKT-tjänster inrättas ett särskilt tillsynsforum som en underkommitté till de europeiska tillsynsmyndigheterna (artikel 31–44).

4.8 Det fortsatta arbetet inom EU

4.8.1 Ytterligare bestämmelser

De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén, i vissa fall i samråd med antingen Europeiska unionens cybersäkerhetsbyrå (Enisa) eller med Europeiska centralbanken (ECB) eller med både Enisa och ECB, utarbeta förslag till tekniska standarder för tillsyn och genomförande på ett antal områden. Kommissionen har enligt förordningen befogenhet att anta sådana tekniska standarder (artiklarna 15, 16, 18, 20, 26, 28, 30 och 41).

Kommissionen ges enligt DORA-förordningen befogenhet att anta delegerade akter för att komplettera förordningens bestämmelser om vilka kriterier de europeiska tillsynsmyndigheterna ska tillämpa för att identifiera kritiska tredjepartsleverantörer av IKT-tjänster (artikel 31.6) och för att fastställa avgiftsbeloppen för tillsynen avseende kritiska tredjepartsleverantörer av IKT-tjänster (artikel 43.2).

4.8.2 Kommande utvärdering

Kommissionen ska senast den 17 januari 2028, efter samråd med de europeiska tillsynsmyndigheterna och ESRB, genomföra en översyn och överlämna en rapport för Europaparlamentet och rådet. Översynen ska bland annat omfatta vissa delar avseende tillämpningen av bestämmelserna om kritiska tredjepartsleverantörer av IKT-tjänster, den frivilliga karaktären avseende rapportering om betydande cyberhot samt lämpligheten i att utvidga förordningens tillämpningsområde till att omfatta försäkrings- och återförsäkringsförmedlare som använder automatiska försäljningssystem, men som på grund av sin storlek m.m. för närvarande exkluderas av förordningens tillämpningsområde (artikel 58.1). Kommissionen ska också senast den 17 januari 2026, efter samråd med de europeiska tillsynsmyndigheterna och kommittén för europeiska tillsynsorgan för revisorer, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet om behovet av att införa krav på digital operativ motståndskraft för lagstadgade revisorer (artikel 58.3).

Rapporterna får åtföljas av lagstiftningsförslag, om lämpligt.

Vidare ska kommissionen i samband med översynen av Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG, i det följande benämnt andra betaltjänstdirektivet, bedöma behovet av ökad cyberresiliens i betalningssystem och betalningshantering och lämpligheten i att utvidga DORA-förordningens tillämpningsområde till att även omfatta betalningssystemsoperatörer och enheter som deltar i betalningshantering (artikel 58.2 i DORA-förordningen).

5 Kompletterande bestämmelser i nationell rätt

5.1 En ny lag införs

Promemorians förslag: Det ska införas en ny lag med kompletterande bestämmelser till DORA-förordningen.

Bestämmelser om ingripande mot vissa företrädare för juridiska personer ska i första hand införas i befintlig lagstiftning.

Promemorians bedömning: Utgångspunkten bör vara att befintliga bestämmelser om ingripanden i respektive rörelselag ska tillämpas.

Skälen för promemorians förslag och bedömning: En EU-förordning är direkt tillämplig i varje medlemsstat. Till skillnad från ett EU-direktiv ska en EU-förordning inte, och får inte heller, genomföras i nationell rätt. Några särskilda åtgärder för att genomföra DORA-förordningen i svensk rätt ska därför inte vidtas. För att förordningen ska kunna tillämpas krävs likväl att medlemsstaterna inför vissa nationella bestämmelser. Det krävs bl.a. att medlemsstaterna inför administrativa åtgärder och avhjälpande åtgärder mot finansiella entiteter och personer som ingår i ledningen för dessa när den finansiella entiteten har gjort sig skyldig till en överträdelse av förordningen (artikel 50.4 och 50.5).

Genom DORA-förordningen införs harmoniserade regler om digital operativ motståndskraft och krav på hantering av IKT-risk för finanssektorn. Krav på hantering av IKT-risker har tidigare behandlats separat i olika EU-rättsakter, som en del av de operativa riskkraven. I Sverige finns det därför i dag inte någon lagstiftning som uttryckligen reglerar digital operativ motståndskraft och IKT-riskkrav (jfr avsnitt 4.1). DORA-förordningen har ett brett tillämpningsområde och ett stort antal företag på finansmarknadsområdet, s.k. finansiella entiteter, omfattas av kraven i förordningen. I avsnitt 5.3 föreslås att även Svenska skeppshypotekskassan ska omfattas.

För de flesta finansiella entiteter som omfattas av DORA-förordningen finns det i Sverige en särskild rörelsereglering, t.ex. lagen (2004:297) om bank- och finansieringsrörelse, med bestämmelser om bl.a. tillsynsbefogenheter och administrativa sanktioner vid överträdelser av respektive regelverk (se avsnitt 8.2.1). Tillsyns- och ingripandebestämmelserna i de olika rörelselagarna har samma uppbyggnad och överensstämmer i mångt och mycket med varandra. I huvudsak tillgodoser dessa bestämmelser kraven enligt DORA-förordningen. Vissa skillnader finns dock. Detta gäller t.ex. sanktionsavgifter där maximibeloppen skiljer sig åt liksom de ytterligare omständigheter som ska beaktas när avgiften bestäms. Utgångspunkten bör vara att befintliga bestämmelser i respektive rörelselag ska tillämpas. Det innebär att samma regler gäller för en finansiell entitet oavsett om verksamheten rör digital operativ motståndskraft eller verksamhet som den finansiella entiteten har tillstånd för. En sådan lagstiftningsmodell skapar även förutsättningar för att andra bestämmelser om t.ex. handräckning och beaktande av soliditets- och likviditetskrav vid fastställande av en sanktionsavgift (se t.ex. 25 kap. 9 § tredje stycket lagen [2007:528] om värdepappersmarknaden) blir tillämpliga vid ingripanden

enligt DORA-förordningen, vilket bedöms vara i enlighet med den reglering av behörig myndighets befogenheter som förordningen kräver (jfr artikel 46). Det behöver dock införas bestämmelser om ingripande mot personer som ingår i ledningen för en finansiell entitet (avsnitt 8.3). Även dessa bör införas i rörelselagarna för att åstadkomma en enhetlig reglering.

DORA-förordningen kräver även att behörig myndighet ska kunna ingripa med sanktioner och andra avhjälpande åtgärder mot vissa finansiella entiteter och personer i deras ledning som i dag saknar nationell rörelselagstiftning (avsnitt 8.2.2). Sådana kompletterande bestämmelser har i andra lagstiftningsärenden införts i en särskild lag med kompletterande bestämmelser (se t.ex. lagen [2013:287] med kompletterande bestämmelser till EU:s förordning om OTC-derivat, centrala motparter och transaktionsregister). Bestämmelser som är nödvändiga till följd av DORA-förordningen bör på motsvarande sätt tas in i en ny lag som kompletterar förordningen. Lagen bör benämnas lagen med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn, i det följande benämnd kompletteringslagen.

Kompletteringslagen bör utformas efter förebild av andra lagar som kompletterar EU-förordningar, se t.ex. lagen med kompletterande bestämmelser till EU:s förordning om OTC-derivat, centrala motparter och transaktionsregister.

Bestämmelserna i kompletteringslagen och ändringar i befintliga lagar bör utformas i linje med motsvarande bestämmelser på finansmarknadsområdet, förutsatt att detta är förenligt med DORA-förordningen. Inriktningen bör vidare vara att inte införa några bestämmelser som går utöver vad som krävs enligt förordningen.

5.2 Finansinspektionen är behörig myndighet

Promemorians förslag: En upplysningsbestämmelse ska införas i kompletteringslagen om att det följer av DORA-förordningen att Finansinspektionen är behörig myndighet enligt förordningen.

Skälen för promemorians förslag: Enligt DORA-förordningen ska tillsynen av de krav som ställs upp i förordningen säkerställas av de behöriga myndigheter som har utsetts i enlighet med vissa särskilt angivna EU-rättsakter (artikel 46). För svensk del är det Finansinspektionen som är behörig myndighet i samtliga fall. Det följer därför direkt av DORA-förordningen att Finansinspektionen är behörig myndighet enligt förordningen. En upplysningsbestämmelse om detta bör införas i kompletteringslagen.

5.3 Svenska skeppshypotekskassan

Promemorians förslag: Svenska skeppshypotekskassan ska inte undantas från tillämpningsområdet för DORA-förordningen.

Skälen för promemorians förslag: Medlemsstaterna får utesluta vissa enheter från tillämpningsområdet för DORA-förordningen. Svenska skeppshypotekskassan är en sådan enhet (artikel 2.4 i DORA-förordningen tillsammans med artikel 2.5.23 i Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG, i det följande benämnt kapitaltäckningsdirektivet.

Svenska skeppshypotekskassan behandlas som ett kreditinstitut vid tillämpning av EU:s regelverk om kapitaltäckning (1 kap. 2 § 7 lagen [2014:968] om särskild tillsyn över kreditinstitut och värdepappersbolag). Det innebär att de bestämmelser i Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 som gäller för kreditinstitut också gäller för Svenska skeppshypotekskassan, utom i fråga om bestämmelserna om stora exponeringar. I och med att DORA-förordningen ska gälla för kreditinstitut, bör förordningen också gälla för Svenska skeppshypotekskassan. Möjligheten enligt förordningen att undanta denna enhet bör därmed inte utnyttjas.

5.4 Hänvisningar till DORA-förordningen

Promemorians förslag: Hänvisningar till DORA-förordningen ska vara dynamiska, dvs. avse förordningen i den vid varje tidpunkt gällande lydelsen.

Skälen för promemorians förslag: Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. I några av de bestämmelser som nu föreslås krävs det en hänvisning till DORA-förordningen. För att eventuella ändringar i förordningen ska få omedelbart genomslag i den svenska lagstiftningen är det lämpligt att hänvisningarna till förordningen är dynamiska. När det gäller EU-förordningar är det också den hänvisningsteknik som har använts i senare lagstiftningsärenden (se t.ex. prop. 2016/17:22 s. 95–96, prop. 2020/21:66 s. 48–49, prop. 2020/21:206 s. 49 och prop. 2022/23:7 s. 89–90).

5.5 Förhållandet till nationella bestämmelser om säkerhet

Promemorians bedömning: DORA-förordningen föranleder inga ändringar i nationell lagstiftning inom områdena allmän säkerhet, försvar eller nationell säkerhet.

Skälen för promemorians bedömning: I DORA-förordningen anges att förordningen inte påverkar medlemsstaternas ansvar vad gäller väsentliga statliga funktioner inom områdena allmän säkerhet, försvar och nationell säkerhet i enlighet med unionsrätten, till exempel när det gäller tillhandahållande av information som står i strid med skyddet av den nationella säkerheten (se artikel 1.3 och skäl 17). I första hand berör detta säkerhetsskyddslagen (2018:585). Den lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (1 kap. 1 §). Den som till någon del bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd och dokumentera det i en säkerhetsskyddsanalys (2 kap. 1 §). Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter. Säkerhetsskyddsåtgärder kan avse informationssäkerhet, fysisk säkerhet och personalsäkerhet (2 kap. 2–4 §§). Finansinspektionen är tillsynsmyndighet för enskilda verksamhetsutövare inom området finansiella företag samt för motsvarande utländska företag som är etablerade i Sverige (8 kap. 1 § säkerhetsskyddsförordningen [2021:955]). Vissa företag som omfattas av DORA-förordningen omfattas alltså även av säkerhetsskyddslagens bestämmelser. Mot bakgrund av att DORA-förordningen inte ska påverka medlemsstaternas ansvar när det gäller bl.a. nationell säkerhet görs dock bedömningen att DORA-förordningen inte föranleder någon ändring i säkerhetsskyddslagen eller någon annan lagstiftning inom områdena allmän säkerhet, försvar och nationell säkerhet.

5.6 IKT-relaterade incidenter och cyberhot

Promemorians bedömning: Sverige bör inte utnyttja möjligheterna att bestämma att finansiella entiteter ska använda DORA-förordningens mallar när de överlämnar information om en IKT-relaterad incident till behörig myndighet eller CSIRT-enheter enligt NIS2-direktivet.

Möjligheten att bestämma att finansiella entiteter som frivilligt rapporterar om allvarliga cyberhot också får vidarebefordra en anmälan till den särskilt utsedda NIS2-myndigheten bör inte heller utnyttjas.

Skälen för promemorians bedömning

DORA-förordningen

I DORA-förordningen finns det flera bestämmelser om rapportering av allvarliga IKT-incidenter och betydande cyberhot. Allvarliga IKT-

relaterade incidenter ska rapporteras till den relevanta behöriga myndigheten (artikel 19.1). Rapporteringen inleds med en första anmälan. En anmälan följs upp av en delrapport

– så snart statusen för den ursprungliga incidenten har förändrats avsevärt eller hanteringen av den allvarliga IKT-relaterade incidenten har förändrats på grund av ny tillgänglig information,
– när så är lämpligt åtföljd av uppdaterade anmälningar varje gång en relevant statusuppdatering finns tillgänglig, samt
– på särskild begäran av den behöriga myndigheten.

Avslutningsvis görs en slutrapport när analysen av grundorsakerna har slutförts. Detta oavsett om begränsande åtgärder redan har vidtagits och när de faktiska påverkanssiffrorna finns tillgängliga för att ersätta uppskattningar (artikel 19.4).

Den första anmälan och rapporterna ska innehålla all information som är nödvändig för att den behöriga myndigheten ska kunna fastställa betydelsen av den allvarliga IKT-relaterade incidenten och även bedöma eventuella gränsöverskridande konsekvenser (artikel 19.1 femte stycket). Kommissionen har möjlighet att komplettera förordningen med tekniska standarder om själva rapporteringen (artikel 20).

Den behöriga myndigheten ska skyndsamt lämna närmare uppgifter om den allvarliga IKT-relaterade incidenten till flera andra myndigheter, t.ex. EBA (Europeiska bankmyndigheten), Esma (Europeiska värdepappers- och marknadsmyndigheten) eller Eiopa (Europeiska försäkrings- och tjänstepensionsmyndigheten) (artikel 19.6). EBA, Esma eller Eiopa och ECB (Europeiska centralbanken) ska därefter, i samråd med Enisa (Europeiska unionens cybersäkerhetsbyrå) och i samarbete med den relevanta behöriga myndigheten, bedöma huruvida den allvarliga IKT-relaterade incidenten är relevant för behöriga myndigheter i andra medlemsstater. Efter denna bedömning ska EBA, Esma eller Eiopa så snart som möjligt underrätta de relevanta behöriga myndigheterna i andra medlemsstater i ärendet. ECB ska underrätta medlemmarna i Europeiska centralbankssystemet om frågor som är relevanta för betalningssystemet. Baserat på denna underrättelse ska de behöriga myndigheterna vid behov vidta alla nödvändiga åtgärder för att skydda det finansiella systemets omedelbara stabilitet (artikel 19.7).

Den behöriga myndigheten ska bekräfta mottagandet av en första anmälan och av varje rapport. När så är möjligt, får myndigheten skyndsamt tillhandahålla relevant och proportionell återkoppling eller vägledning på hög nivå till den finansiella entiteten. Myndigheten får också diskutera åtgärder som tillämpas på finansiell entitetsnivå och sätt att minimera och mildra de negativa effekterna i den finansiella sektorn. Finansiella entiteter är dock fortsatt fullt ansvariga för hanteringen av och konsekvenserna av de IKT-relaterade incidenterna (artikel 22).

För cyberhot gäller att finansiella entiteter får rapportera betydande cyberhot till den relevanta behöriga myndigheten när de anser att hotet är relevant för det finansiella systemet, tjänsteanvändarna eller kunderna. Den relevanta behöriga myndigheten får i sin tur informera andra relevanta myndigheter (EBA, Esma, Eiopa m.fl.) om cyberhot som rapporteras till den. Medlemsstaterna får fastställa att de finansiella entiteter som rapporterar på frivillig grund också får vidarebefordra detta till de CSIRT-

enheter som utsetts eller inrättats i enlighet med NIS2-direktivet (artikel 19.2). Som för IKT-relaterade incidenter har kommissionen möjlighet att komplettera förordningen med tekniska standarder om själva rapporteringen av cyberhot (artikel 20).

I vissa fall ska en finansiell entitets kunder informeras. Så är fallet om en allvarlig IKT-relaterad incident inträffar och den påverkar kunders ekonomiska intressen. På motsvarande sätt gäller vid ett betydande cyberhot att den finansiella entiteten ska informera de kunder som kan påverkas av hotet (artikel 19.3).

Information till myndigheter och enheter enligt NIS2-direktivet

Som utvecklas i avsnitt 5.1 är DORA-förordningen direkt tillämplig och det behövs därmed inte några ytterligare bestämmelser för att finansiella entiteter ska vara skyldiga att rapportera om allvarliga IKT-relaterade incidenter på de sätt som anges i förordningen. På motsvarande sätt behövs det inte heller några bestämmelser för att Finansinspektionen ska kunna utföra de uppgifter som i förordningen anges för den behöriga myndigheten (se avsnitt 7.1).

Enligt DORA-förordningen ges medlemsstaterna ett visst handlingsutrymme för vad som ska gälla för rapportering av IKT-relaterade incidenter och frivillig anmälan av cyberhot. Medlemsstaterna får bestämma att vissa eller alla finansiella entiteter ska använda DORA-förordningens mallar för rapportering också när de överlämnar anmälan och rapporter till de behöriga myndigheterna eller de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS2-direktivet (artikel 19.1 sjätte stycket i DORA-förordningen, se även avsnitt 4.2). När det gäller frivillig rapportering av betydande cyberhot får medlemsstaterna fastställa att de finansiella entiteter som rapporterar på frivillig basis också får vidarebefordra en anmälan till de CSIRT-enheter som utsetts eller inrättats i enlighet med NIS2-direktivet (artikel 19.2 tredje stycket).

Det är av särskild vikt att relevanta myndigheter informeras om allvarliga IKT-relaterade incidenter och betydande cyberhot. Detta bör ske så snart det är möjligt. Det är angeläget att myndigheter får tillräcklig och korrekt information om vad som inträffat så att relevanta åtgärder kan vidtas. När det gäller finansiella entiteter torde det i första hand vara Finansinspektionen, som tillsynsmyndighet för dessa företag, som har nytta av information om en allvarlig IKT-relaterad incident. Detta blir också fallet då Finansinspektionen ska vara behörig myndighet enligt DORA-förordningen, se avsnitt 5.2, till vilken finansiella entiteter ska rapportera om en allvarlig IKT-relaterad incident (artikel 19.1 första stycket). Finansinspektionen ska sedan skyndsamt lämna över uppgifter till flera andra myndigheter, bl.a. den behöriga myndigheten, den gemensamma kontaktpunkten eller de CSIRTS-enheter som utsetts eller inrättats enligt NIS2-direktivet (artikel 19.6). Detta får anses tillräckligt för att relevanta myndigheter i ett tidigt skede får kännedom om en incident. Möjligheten enligt DORA-förordningen att bestämma om vilken information som en finansiell entitet ska lämna till myndigheter och enheter NIS2-direktivet (artikel 19.1 sjätte stycket) bör därför inte utnyttjas. Inte heller bör möjligheten att bestämma att en finansiell entitet som gör en frivillig

anmälan om ett allvarligt cyberhot också får vidarebefordra en anmälan till dessa myndigheter och enheter (artikel 19.2 tredje stycket) utnyttjas.

6 Hotbildsstyrda penetrationstester

6.1 Ansvariga myndigheter

Promemorians förslag: Finansinspektionen ska bestämma vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och hur ofta testerna ska ske.

Riksbanken ska övervaka och samordna hotbildsstyrda penetrationstester. Riksbanken ska även utfärda intyg om att testerna uppfyller kraven i DORA-förordningen.

Skälen för promemorians förslag

Krav på avancerade tester enligt DORA-förordningen

I DORA-förordningen finns det bestämmelser om testning av digital operativ motståndskraft (artikel 24–27). Vissa finansiella entiteter ska regelbundet genomföra avancerade tester med hjälp av hotbildsstyrd penetrationstestning. Syftet med testningen är att den finansiella entiteten ska kunna bedöma sin beredskap att hantera IKT-relaterade incidenter, identifiera svagheter, brister och luckor i den digitala operativa motståndskraften och snabbt genomföra korrigerande åtgärder. Det är särskilt finansiella entiteter som är verksamma inom delsektorer för centrala finansiella tjänster och som har en central betydelse för systemet som bör komma i fråga för hotbildsstyrda penetrationstester. Sådana tester ska genomföras vart tredje år om inte den behöriga myndigheten begär något annat (artikel 26.1 i DORA-förordningen).

De hotbildsstyrda penetrationstesterna ska utformas i enlighet med de av Europeiska centralbanken utvecklade testramverket TIBER-EU (TIBER= Threat Intelligence-Based Ethical Red teaming) och innehålla s.k. red-team-tester (artikel 26.11 se även skäl 56). Med red-team-tester menas att det anlitas en aktör som utger sig för att vara en antagonistisk part och som sedan har i uppdrag att försöka göra ett intrång mot en organisation. Uppdraget utförs på beställning av organisationen i fråga och aktören ska efter avslutat uppdrag rapportera tillbaka till uppdragsgivaren. Avsikten med hela övningen är att identifiera sårbarheten i syfte att organisationen kan stärka sitt försvar.

När testet har avslutats och efter det att rapporter och åtgärdsplaner har godkänts ska den finansiella entiteten förses med ett intyg som bekräftar att testet genomförts i enlighet med kraven i DORA-förordningen. Syftet med intyget är att möjliggöra ömsesidigt erkännande av hotbildsstyrda penetrationstester mellan behöriga myndigheter i olika medlemsstater (artikel 26.7). Intyget bör användas enbart för ömsesidigt erkännande och bör inte utesluta några uppföljningsåtgärder som krävs för att hantera den IKT-risk som den finansiella entiteten är utsatt för. Avsikten med intyget

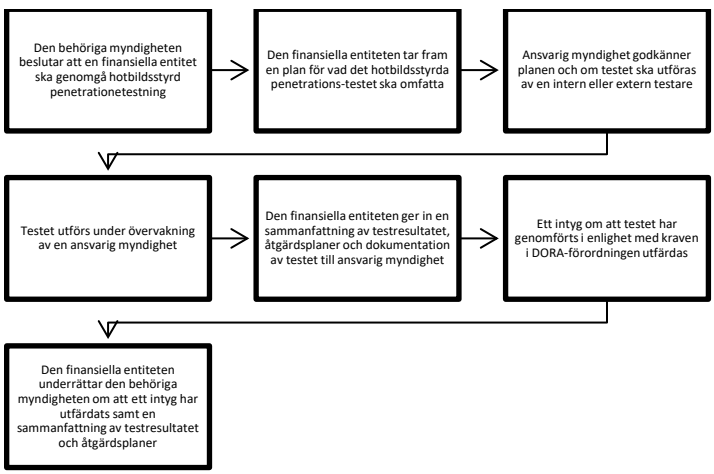
är inte att det ska innebära tillsynsmyndighetens godkännande av den finansiella entitetens kapacitet att hantera och begränsa IKT-risk (skäl 61).

De finansiella entiteterna är enligt förordningen skyldiga att genomföra hotbildsstyrda penetrationstester (artikel 26.1). De behöriga myndigheterna har enligt förordningen vissa uppgifter kopplade till testningen. I ett första steg ska myndigheterna identifiera vilka finansiella entiteter som ska testas (artikel 26.8 tredje stycket). Myndigheterna ska också godkänna en finansiell entitets bedömning av vad som ska testas, dvs. om ett test ska omfatta flera eller alla av en finansiell entitets kritiska eller viktiga funktioner och ska utföras på produktionssystem i drift som stöder sådana funktioner (artikel 26.2). Själva testerna ska för de allra flesta finansiella entiteter utföras av en oberoende part (artikel 24.4). Detta hindrar inte att en finansiell entitet använder en intern testare, men det ställer särskilda krav på bl.a. avsatta resurser och hanteringen av intressekonflikter (artikel 26.8 och 27). Användande av en intern testare kräver även ett särskilt godkännande av den ansvariga myndigheten (artikel 27.2 a). Vart tredje test ska dock utföras av en extern testare (artikel 26.8 första stycket).

För att dra nytta av den expertis som redan i vissa fall förvärvats med avseende på genomförandet av TIBER-EU, finns möjligheten för medlemsstaterna att utse en enda offentlig myndighet inom finanssektorn för alla frågor som rör hotbildsstyrd penetrationstestning och ge myndigheten alla befogenheter och uppgifter i detta syfte (artikel 26.9). Om ingen sådan myndighet utses får en behörig myndighet delegera uppgifter som rör sådan testning till en annan nationell myndighet inom den finansiella sektorn (artikel 26.10).

Genomförandet av den hotbildsstyrda penetrationstestningen i enlighet med det som anges ovan kan även beskrivas enligt det förfarandet som anges i figur 7.1.

Figur 7.1 Hotbilsstyrd penetrationstestning



Bör en eller flera myndigheter ansvara för testningen?

Som anges ovan har medlemsstaterna enligt förordningen möjlighet att utse en enda offentlig myndighet för alla frågor som rör hotbildsstyrd penetrationstestning och ge myndigheten alla befogenheter och uppgifter i detta syfte (artikel 26.9). Det måste dock vara en myndighet inom den finansiella sektorn. Frågan är om denna möjlighet bör utnyttjas eller om flera myndigheter bör ansvara för dessa frågor.

I Sverige finns det tre myndigheter i den finansiella sektorn som kan vara aktuella. Dessa är Finansinspektionen, Sveriges riksbank (Riksbanken) och Riksgäldskontoret.

Finansinspektionen är som behörig myndighet enligt DORA-förordningen den myndighet som utövar tillsyn över de finansiella entiteter som kan komma att omfattas att krav på hotbildsstyrda penetrationstester. Som tillsynsmyndighet på finansmarknadsområdet är Finansinspektionen den myndighet som kan antas ha mest regelbunden och upparbetad kontakt med samtliga finansiella entiteter som kommer att kunna omfattas av krav på tester. Inspektionen är också den myndighet som i dag har bäst kännedom om de finansiella entiteternas riskprofiler och entiteternas betydelse för den finansiella stabiliteten. Det kan samtidigt ifrågasättas om den myndighet som utövar tillsyn också ska ha aktiv del i den typ av testverksamhet som ska utföras enligt DORA-förordningen. Finansinspektionen har i dag inte någon verksamhet som rör hotbildsstyrda penetrationstester. Om Finansinspektionen ska utföra all testverksamhet skulle det innebära ett utvidgat uppdrag, bortom det nuvarande kärnuppdraget om tillsyn, regelgivning och tillståndsprövning som rör finansiella marknader och finansiella företag.

Riksbanken utövar inte tillsyn över enskilda företag och har en, i förhållande till Finansinspektionen, begränsad kontakt med företag som är verksamma inom den finansiella sektorn. Riksbanken samordnar och övervakar dock redan hotbildsstyrda penetrationstester. Systemviktiga finansiella företag har möjlighet att hos Riksbanken genomföra frivilliga tester som regleras i TIBER-EU. Riksbanken har, som centralbank, en samordnande roll och är även kontaktpunkt i förhållande till andra länders TIBER-program. Ett uppdrag att även ansvara för testverksamhet enligt DORA-förordningen innebär dock att Riksbanken kan komma att behöva utvidga denna verksamhet. Det beror på att fler finansiella företag kommer att behöva genomgå tester enligt förordningen än vad som hittills erbjudits inom ramen för TIBER-EU. Riksbanken saknar å andra sidan den ingående kunskap om de enskilda finansiella entiteterna och deras riskprofiler som en tillsynsmyndighet besitter. Inte heller innebär myndighetens nuvarande verksamhet sådan myndighetsutövning mot enskild som den hotbildsstyrda penetrationstestningen enligt DORA-förordningen kommer att medföra.

Även Riksgäldskontoret verkar inom den finansiella sektorn och skulle därmed kunna komma i fråga för uppgifter enligt DORA-förordningen. Riksgäldskontoret har i och för sig vissa uppgifter som rör finansiella entiteter då myndigheten bl.a. är resolutionsmyndighet. I förhållande till Finansinspektionen är dessa uppgifter mer begränsade och omfattar bara vissa företag inom det finansiella området. Inte heller bedriver Riksgäldskontoret i dag någon form av testning av digital operativ motstånds-

kraft som påminner om den testning som ska utföras enligt förordningen, t.ex. TIBER-EU.

Sammantaget framstår det som mindre ändamålsenligt att ge någon av Finansinspektionen, Riksbanken eller Riksgäldskontoret ansvaret för alla frågor som rör hotbildsstyrd penetrationstestning i Sverige. I stället bör Finansinspektionen och Riksbanken dela på ansvaret.

Finansinspektionen – Riksbanken

Som utgångspunkt bör de kompetenser som Finansinspektionen och Riksbanken redan besitter tas tillvara vid fördelningen av ansvaret för olika delar av den hotbildsstyrda penetrationstestningen.

Finansinspektionen bör därför ansvara för uppgifter som ligger inom ramen för eller har nära anknytning till myndighetens nuvarande uppdrag, i första hand tillsynsverksamheten. Inspektionen bör i och med det vara den myndighet som enligt DORA-förordningen ska besluta vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och med vilken frekvens, dvs. hur ofta.

Som lyfts ovan finns det uppgifter inom den hotbildsstyrda penetrationstestningen som det är mindre lämpligt att en tillsynsmyndighet utför. I första hand gäller det uppgifter som innebär att samordna och övervaka hotbildsstyrda penetrationstester. Detta omfattar att initiera en ny testomgång med en finansiell entitet, att validera vilka kritiska eller viktiga funktioner som ska omfattas av testningen (artikel 26.2 tredje stycket) och säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i förordningen (artikel 27). Med att övervaka och samordna avses även att säkerställa att den finansiella entiteten tillämpar den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen. Riksbankens kompetens och erfarenhet av att genomföra hotbildsstyrda penetrationstester inom ramverket för TIBER-EU bör tas tillvara. Riksbanken bör därmed övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt DORA-förordningen. Riksbanken bör också ges i uppgift att utfärda ett sådant intyg som avses i artikel 26.7 i DORA-förordningen.

Bestämmelser om denna ansvarsfördelning, i enlighet med artikel 26.9 och 26.10 i DORA-förordningen, bör tas in i kompletteringslagen.

6.2 Samverkan mellan Finansinspektionen och Riksbanken

Promemorians förslag: Finansinspektionen ska ge Riksbanken tillfälle att yttra sig innan inspektionen fattar beslut om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och om hur ofta den finansiella entiteten ska genomföra sådana tester.

Riksbanken ska ge Finansinspektionen möjlighet att yttra sig innan Riksbanken fattar beslut rörande testningen som berör Finansinspektionens tillsynsverksamhet.

Finansinspektionen och Riksbanken ska lämna varandra de uppgifter som respektive myndighet behöver för samverkan.

Skälen för promemorians förslag

Möjlighet att yttra sig

I avsnitt 6.1 föreslås att både Finansinspektionen och Riksbanken ska utföra uppgifter avseende de hotbildsstyrda penetrationstester som ska genomföras enligt DORA-förordningen. När ansvaret på detta sätt delas mellan två myndigheter är det viktigt med samarbete dem emellan. Detta är inte nödvändigt för alla delar av verksamheten, men fyller en viktig funktion i situationer där ett beslut som fattas av den ena myndigheten påverkar den andra myndighetens verksamhet. Det är inte alla åtgärder som vidtas i arbetet med hotbildsstyrda penetrationstester som påverkar den andra myndighetens verksamhet. Det finns därför inte skäl att kräva en generell samverkan mellan myndigheterna. Både Finansinspektionens och Riksbankens uppgifter kan dock väntas innefatta moment som påverkar den andra myndighetens verksamhet. I dessa delar bör det införas bestämmelser som reglerar hur Riksbanken och Finansinspektionen ska samverka med varandra.

Finansinspektionens beslut om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och hur ofta dessa tester ska utföras kommer att påverka Riksbankens verksamhet. Finansinspektionen bör därför ge Riksbanken möjlighet att yttra sig innan inspektionen fattar beslut i dessa frågor.

Riksbankens verksamhet med att övervaka och samordna genomförandet av de hotbildsstyrda penetrationstesterna involverar till stor del inte Finansinspektionen och dess tillsynsverksamhet då testerna ska vara skilda från tillsynen över de enskilda finansiella entiteterna. Vissa beslut och ställningstaganden kräver dock enligt DORA-förordningen den behöriga myndighetens, dvs. tillsynsmyndighetens, medverkan. Så är t.ex. fallet när det gäller validering av vilka delar av den finansiella entitetens verksamhet som ska omfattas av testningen (artikel 26.2) och ett godkännande att använda interna testare (artikel 27.2). Det kan även uppstå andra situationer som direkt berör Finansinspektionens tillsynsverksamhet. Riksbanken bör därför ge Finansinspektionen möjlighet att yttra sig innan Riksbanken fattar beslut som påverkar Finansinspektionens tillsynsverksamhet.

Utbyte av känsliga uppgifter

Sekretess föreslås gälla för vissa uppgifter i en statlig myndighets verksamhet enligt DORA-förordningen (se förslagen i avsnitt 9). Det är möjligt att Finansinspektionen och Riksbanken, inom ramen för den samverkan som föreslås ovan, kan behöva utbyta uppgifter som omfattas av sekretess.

Sekretess hindrar i och för sig inte att en uppgift lämnas till en annan myndighet om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet (10 kap. 2 § offentlighets- och sekretesslagen [2009:400]). En sekretessbelagd uppgift kan också lämnas till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda (10 kap. 27 § offentlighets- och sekretesslagen).

Det är tveksamt om dessa bestämmelser i offentlighets- och sekretesslagen är tillräckliga för att Finansinspektionen och Riksbanken ska kunna samverka och lämna uppgifter till varandra på det sätt som krävs för att de

ska kunna fullgöra sina uppgifter enligt DORA-förordningen och kompletteringslagen. I första hand är det den mottagande myndigheten som behöver information för att kunna fullgöra sina uppgifter. Riksbanken behöver uppgifter från Finansinspektionen för att kunna fatta beslut om testningen. På motsvarande sätt kan Finansinspektionen behöva uppgifter från Riksbanken för att fatta ett beslut vilka finansiella entiteter som ska genomgå testningen. Denna typ av informationsutbyte kan inte ske med stöd av bestämmelsen om nödvändigt utlämnande (10 kap. 2 §) då ett sådant utlämnande bara är möjligt för att den utlämnande myndigheten ska kunna fullgöra sitt uppdrag. Ett utlämnande bör i och för sig kunna ske med stöd av generalklausulen (10 kap. 27 §) under förutsättning att det står klart att intresset av ett utlämnande har företräde framför det intresse som sekretessen ska skydda. Ett mer rutinmässigt utlämnande bör dock bara i undantagsfall kunna ske med stöd den bestämmelsen (se prop. 1979/80:2 Del A s. 327).

För att Finansinspektionen och Riksbanken ska kunna utföra sina uppgifter enligt DORA-förordningen och kompletteringslagen bör det krävas ett nära samarbete, med ett omfattande och kontinuerligt informationsutbyte. Det bör lämpligen införas en bestämmelse om att myndigheterna ska lämna vissa uppgifter till varandra. På så sätt tydliggörs skyldigheterna för myndigheterna. En sådan bestämmelse medför också att sekretess inte hindrar att en uppgift lämnas (10 kap. 28 §) och ett utlämnande blir därmed inte beroende av att bestämmelsen om nödvändigt utlämnande (10 kap. 2 §) eller generalklausulen (10 kap. 27 §) är tillämplig. Det bör därför införas en särskild uppgiftsskyldighet mellan Finansinspektionen och Riksbanken som möjliggör ett utbyte av uppgifter utan hinder av sekretess. Uppgiftsskyldigheten bör begränsas till de områden som myndigheterna ska samverka med varandra om.

6.3 Uppgiftsskyldighet

Promemorians förslag: På begäran av Riksbanken ska finansiella entiteter lämna de uppgifter som är nödvändiga för Riksbankens verksamhet som rör hotbildsstyrda penetrationstester.

Riksbanken ska få besluta om de förelägganden som behövs för att en finansiell entitet ska följa sin uppgiftsskyldighet i förhållande till Riksbanken.

Ett beslut om föreläggande ska kunna förenas med vite.

Skälen för promemorians förslag: Som utvecklas i avsnitt 7.1 är Finansinspektionen behörig myndighet enligt DORA-förordningen. Detta innebär också att Riksbanken saknar de befogenheter som en behörig myndighet ska ha enligt förordningen (se artikel 46 och 50).

Genomförandet av den hotbildsstyrda penetrationstestningen bör i huvudsak ske genom frivillig dialog och samarbete mellan de finansiella entiteter som utför testerna och Riksbanken. Samtidigt rör det sig om krav enligt såväl DORA-förordningen som kompletteringslagen. Riksbanken har inte någon generell befogenhet att säkerställa att de finansiella entiteterna följer myndighetens anvisningar.

För att Riksbanken ska kunna övervaka och samordna testerna (se avsnitt 6.1) bör myndigheten ges möjlighet att begära in uppgifter av den finansiella entiteten. Detta bör bara gälla de uppgifter som är nödvändiga för Riksbankens verksamhet som rör de hotbildsstyrda penetrationstesterna. Om den finansiella entiteten inte följer Riksbankens begäran bör Riksbanken kunna förelägga den finansiella entiteten att lämna den efterfrågade informationen. Ett föreläggande om att lämna uppgifter bör kunna förenas med vite.

Det är tillåtet att finansiella entiteter anlitar underleverantörer eller s.k. tredjepartsleverantörer av IKT-tjänster. I de fall där ett hotbildsstyrt penetrationstest även ska omfatta den verksamhet som bedrivs av en tredjepartsleverantör av IKT-tjänster kommer även dessa leverantörer att omfattas av testet. Enligt DORA-förordningen är det ändå den finansiella entiteten som har fullt ansvar för att säkerställa att förordningen efterlevs och ska vidta nödvändiga åtgärder och skyddsåtgärder för att säkerställa att berörda tredjepartsleverantörer av IKT-tjänster deltar i den hotbildsstyrda penetrationstestningen (artikel 26.3). Det får anses vara tillräckligt att skyldigheten att lämna uppgifter gäller för den finansiella entiteten även i dessa situationer.

En bestämmelse om uppgiftsskyldighet bör tas in i kompletteringslagen. Bestämmelsen bör utformas efter förebild av motsvarande bestämmelse om uppgiftsskyldighet i lagen (2022:1568) om Sveriges riksbank (12 kap. 1 §).

7 Tillsyn

7.1 Tillsynens omfattning

Promemorians förslag: Finansinspektionen ska ha tillsyn över att finansiella entiteter följer DORA-förordningen och kompletteringslagen.

Skälen för promemorians förslag: Enligt DORA-förordningen ska de behöriga myndigheterna säkerställa efterlevnaden av förordningen i enlighet med de befogenheter som myndigheten tilldelats i de EU-rättsakter som anger behörig myndighet för de finansiella entiteterna (artikel 46). I svensk rätt regleras Finansinspektionens tillsyns- och utredningsbefogenheter i finansiella entiteters rörelselagstiftning och lagar som kompletterar olika EU-förordningar på finansmarknadsområdet.

Enligt DORA-förordningen ska de behöriga myndigheterna även ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt förordningen. I förordningen anges uttryckligen de utredningsbefogenheter som den behöriga myndigheten som minst ska ha (artikel 50.2). I förordningen anges också att utövandet av befogenheterna kan ske direkt, i samarbete med eller genom delegering till andra myndigheter eller genom ansökan till de behöriga rättsliga myndigheterna (artikel 51.1).

Bestämmelserna i DORA-förordningen om de behöriga myndigheternas tillsyn riktar sig till myndigheterna och är direkt tillämpliga. När lagen med kompletterande bestämmelser till EU:s förordning om en paneuropeisk privat pensionsprodukt (PEPP-produkt) infördes gjordes dock bedömningen att det för tydlighets skull bör framgå av kompletteringslagen att Finansinspektionen, som behörig myndighet, har tillsyn över EU-förordningen och kompletteringslagen (se prop. 2022/23:7 s. 145). Detta bör gälla också i detta lagstiftningsärende. Det bör därför framgå av kompletteringslagen att Finansinspektionen har tillsyn över att finansiella entiteter följer DORA-förordningen och kompletteringslagen.

De utredningsbefogenheter som i dag finns på finansmarknadsområdet innefattar i huvudsak de befogenheter som anges i DORA-förordningen. För flertalet av de finansiella entiteter som omfattas av rörelselagstiftning på finansmarknadsområdet har Finansinspektionen redan vissa tillsyns- och utredningsbefogenheter som är tillämpliga även när det gäller tillsynen av att entiteten följer kraven i DORA-förordningen (se t.ex. 23 kap. 1 § lagen om värdepappersmarknaden, 13 kap. 2 § lagen [2004:297] om bank- och finansieringsrörelse och 17 kap. 2 § försäkringsrörelselagen [2010:2043]).

En konsekvens av att det i kompletteringslagen införs bestämmelser om Finansinspektionens utredningsbefogenheter är att det därigenom uppstår viss dubbelreglering. Det handlar framför allt om möjligheterna att inhämta uppgifter, hålla förhör och genomföra platsundersökningar. Motsvarande överlappning förekommer dock redan på finansmarknadsområdet (se 18 kap. 1 § försäkringsrörelselagen och 8 kap. 3 § lagen [2018:1219] om försäkringsdistribution, se även prop. 2017/18:216 s. 90–91). Finansinspektionen har i en sådan situation möjlighet att välja vilken bestämmelse som den ska lägga till grund för sin åtgärd.

7.2 Rätt att få tillgång till dokument och information

Promemorians förslag: För tillsynen över att bestämmelserna i DORA-förordningen följs ska Finansinspektionen få förelägga en fysisk eller juridisk person att tillhandahålla uppgifter, handlingar eller annat.

Finansinspektionen ska även få förelägga den som förväntas kunna lämna upplysningar i saken att inställa sig till förhör.

Ett föreläggande om upplysningar eller om inställelse till förhör ska få förenas med vite.

Ett föreläggande om upplysningar eller om inställelse till förhör ska dock inte få strida mot den i lag reglerade tystnadsplikten för advokater.

Skälen för promemorians förslag: Enligt DORA-förordningen ska den behöriga myndigheten få tillgång till alla dokument eller uppgifter i vilken form som helst som enligt den behöriga myndigheten är relevanta för fullgörandet av dess uppgifter och få eller ta en kopia av dem (artikel 50.2 a). Den behöriga myndigheten ska även kunna kalla till sig företrädare för finansiella entiteter och be dem om muntliga eller skriftliga för-

klaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren samt höra vilken annan fysisk eller juridisk person som helst som går med på att höras i syfte att samla in information om föremålet för utredningen (artikel 50.2 b). Befogenheterna i DORA-förordningen är en minimireglering som tillåter medlemsstaterna att föreskriva att dess behöriga myndigheter ska ha ytterligare befogenheter.

För tillsynen över att DORA-förordningen, kompletteringslagen och föreskrifter som meddelats med stöd av den lagen följs, bör Finansinspektionen ha möjlighet att begära in uppgifter och handlingar eller annat. I likhet med det som gäller enligt andra lagar på finansmarknadsområdet bör inspektionen även få kalla den som kan förväntas kunna lämna upplysningar i saken till förhör (se t.ex. 23 kap. 3 § lagen om värdepappersmarknaden). Bestämmelserna i den nya kompletteringslagen bör utformas på samma sätt som i de lagarna.

Finansinspektionen har enligt andra lagar på finansmarknadsområdet även möjlighet att besluta om vite (se t.ex. 25 kap. 29 § lagen om värdepappersmarknaden). Det saknas skäl att behandla den nu aktuella situationen på något annat sätt. Finansinspektionen bör därför få motsvarande möjlighet att besluta om vite när den fattar tillsynsbeslut enligt den nya kompletteringslagen.

I likhet med andra lagar på finansmarknadsområdet bör det i den nya kompletteringslagen tas in en uttrycklig bestämmelse om att en begäran om upplysningar eller ett beslut om inställelse till förhör inte får strida mot den i lag reglerade tystnadsplikten för advokater (se t.ex. 23 kap. 3 § lagen om värdepappersmarknaden).

Det är endast när det gäller advokater som det är befogat att Finansinspektionen har en skyldighet att i samband med föreläggandet beakta tystnadsplikten. Detta eftersom det bör kunna antas att Finansinspektionen känner till att den person som ska föreläggas är advokat eller annan som kan omfattas av den lagreglerade tystnadsplikten för advokater. Något motsvarande antagande kan emellertid inte göras beträffande andra personer som omfattas av en lagstadgad tystnadsplikt (se prop. 2018/19:38 s. 33). Frågan om den person som omfattas av en sådan tystnadsplikt har en skyldighet att lämna uppgifter till Finansinspektionen får avgöras i det enskilda fallet och beror på vilken tystnadsplikt det är fråga om (jfr Kammarrätten i Stockholms dom den 28 september 2006 i mål nr 4514–06).

7.3 Rätt att utföra platsundersökningar

Promemorians förslag: Om det är nödvändigt för tillsynen, ska Finansinspektionen få genomföra en undersökning i verksamhetslokalerna hos en finansiell entitet.

Skälen för promemorians förslag: Enligt DORA-förordningen ska den behöriga myndigheten kunna utföra kontroller eller inspektioner på plats (artikel 50.2 b). För att Finansinspektionen ska ha de befogenheter som krävs enligt förordningen bör inspektionen få rätt att genomföra platsundersökningar.

Finansinspektionen har befogenhet att genomföra platsundersökningar enligt flera lagar på finansmarknadsområdet (se t.ex. 23 kap. 4 § lagen om värdepappersmarknaden). I de lagarna gäller i huvudsak att en platsundersökning endast kan avse den person som står under tillsyn och endast göras i en sådan persons verksamhetslokaler (se prop. 2006/07:115 s. 493, prop. 2018/19:4 s. 53, prop. 2018/19:83 s. 85 och prop. 2019/20:37 s. 37). Utifrån vad som hittills framkommit bör detta vara tillräckligt också för den nu aktuella tillsynen. Det innebär att Finansinspektionen, om det är nödvändigt för tillsynen över att en finansiell entitet följer bestämmelserna i DORA-förordningen och kompletteringslagen, bör få genomföra en undersökning i dennes verksamhetslokaler.

I likhet med det som gäller enligt andra lagar på finansmarknadsområdet saknas anledning att ge Finansinspektionen rätt att använda tvångsmedel för att genomföra platsundersökningar (jfr prop. 2022/23:7 s. 148).

Liksom när det gäller andra åtgärder krävs att en platsundersökning aldrig får vara mer långtgående än vad som behövs och att det avsedda resultatet av en sådan undersökning står i rimligt förhållande till de olägenheter som kan antas uppstå för den som undersökningen riktas mot (se 5 § förvaltningslagen [2017:900]).

7.4 Finansinspektionens uppföljning av den ledande tillsynsmyndighetens rekommendationer

Promemorians bedömning: Det behövs inte några ytterligare bestämmelser för att Finansinspektionen ska kunna förbjuda användningen eller införandet av en tjänst som tillhandahålls av en kritisk tredjepartsleverantör.

Skälen för promemorians bedömning: Enligt DORA-förordningen ska tillsynen av kritiska tredjepartsleverantörer av IKT-tjänster utföras på unionsnivå av den ledande tillsynsmyndigheten (artikel 31). En av de tre europeiska tillsynsmyndigheterna EBA, Esma eller Eiopa ska utses till ledande tillsynsmyndighet för var och en av de kritiska tredjepartsleverantörerna. För att utföra sina uppgifter enligt DORA-förordningen får den ledande tillsynsmyndigheten bl.a. genomföra allmänna utredningar och inspektioner (artikel 38 och 39). Inom tre månader efter slutförandet av en utredning eller en inspektion, ska den ledande tillsynsmyndigheten anta rekommendationer som riktar sig till den kritiska tredjepartsleverantören (artikel 40.3).

Den ledande tillsynsmyndigheten ska bistås av en gemensam undersökningsgrupp, som ska bestå av personal från de europeiska tillsynsmyndigheterna, relevanta behöriga myndigheter och, på frivillig basis, personal från nationell behörig myndighet enligt NIS2-direktivet och nationell behörig myndighet från den medlemsstat där den kritiska tredjepartsleverantören är etablerad (artikel 40). Den ledande tillsynsmyndigheten kan även delegera befogenheter till tjänstemän och andra personer (se artiklarna 37–39 i DORA-förordningen). Befogenheterna för

den ledande tillsynsmyndigheten att bedriva tillsyn och ingripa mot kritiska tredjepartsleverantörer regleras direkt i DORA-förordningen.

Efterlevnaden av rekommendationerna till kritiska tredjepartsleverantörer ska ingå i de behöriga myndigheternas tillsyn av de finansiella entiteterna (artikel 42). Om Finansinspektionen bedömer att en finansiell entitet i sin hantering av IKT-tredjepartsrisker inte tar hänsyn till eller i tillräcklig utsträckning hanterar de specifika risker som identifieras i rekommendationen får inspektionen underrätta den finansiella entiteten om att inspektionen kan komma att vidta åtgärder i avsaknad av lämpliga kontraktsmässiga arrangemang för hantering av sådana risker (artikel 42.4). Som en sista utväg får Finansinspektionen fatta beslut om att finansiella entiteter tillfälligt, helt eller delvis, ska avbryta användningen eller införandet av en tjänst som tillhandahålls av den kritiska tredjepartsleverantören till dess att riskerna har åtgärdats. Vid behov får Finansinspektionen även kräva att finansiella entiteter helt eller delvis ska avsluta relevanta kontraktsmässiga arrangemang som har ingåtts med de kritiska tredjepartsleverantörerna (artikel 42.6). Sådana beslut ska fattas i enlighet med artikel 50 om administrativa sanktioner och avhjälpande åtgärder i förordningen. I avsnitt 8.2 föreslås Finansinspektionen kunna ingripa, med stöd av kompletteringslagen eller med befintliga bestämmelser i rörelselagarna, mot finansiella entiteter genom beslut om föreläggande att inom viss tid vidta en viss åtgärd eller upphöra med ett visst agerande. Med stöd av detta har inspektionen möjlighet att fatta de beslut som krävs enligt artikel 40.6.

7.5 Verkställighet av den ledande tillsynsmyndighetens beslut om viten

Promemorians förslag: Beslut om viten enligt DORA-förordningen ska få verkställas enligt utsökningsbalkens bestämmelser på samma sätt som en svensk dom som har fått laga kraft.

Skälen för promemorians förslag: Enligt DORA-förordningen ska den ledande tillsynsmyndighetens beslut om viten vara verkställbara (artikel 35.9). Verkställigheten ska följa de civilprocessrättsliga regler som gäller i den medlemsstat inom vars territorium inspektionerna och åtkomsten ska genomföras. Beslut om viten enligt DORA-förordningen, som fattas av den ledande tillsynsmyndigheten, bör därför få verkställas enligt utsökningsbalken på samma sätt som en svensk dom som har fått laga kraft. En bestämmelse om detta bör utformas efter förebild av det som gäller enligt motsvarande bestämmelser för verkställighet av Esmas beslut om viten enligt förordningen om marknader för finansiella instrument (se 23 kap. 4 b § lagen om värdepappersmarknaden och prop. 2020/21:24 s. 47).

Enligt DORA-förordningen ska domstolarna i den berörda medlemsstaten vara behöriga att pröva klagomål som rör oegentligheter i verkställigheten (artikel 35.9). Kronofogdemyndigheten är den myndighet som kommer att ansvara för den praktiska verkställigheten (1 kap. 3 § utsökningsbalken) och myndighetens beslut kan överklagas till allmän domstol

(18 kap. samma balk). Eftersom det är den ledande tillsynsmyndigheten som har rätt att besluta om sådana viten kommer verkställigheten av EU-myndighetens beslut att hanteras som enskilda mål, om det inte föreskrivs att sådana fordringar ska hanteras som allmänt mål (1 kap. 6 § andra stycket samma balk). På liknande sätt som i tidigare lagstiftningsärenden bedöms det inte finnas skäl att föreskriva om detta (se t.ex. prop. 2020/21:24 s. 47). De nu aktuella besluten bör alltså hanteras som enskilda mål.

8 Ingripanden

8.1 Överträdelser bör inte kriminaliseras

Promemorians bedömning: Det bör inte införas några bestämmelser om straffansvar för överträdelser av DORA-förordningen.

Skälen för promemorians bedömning: Enligt DORA-förordningen får medlemsstaterna besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt (artikel 52.1). Detta innebär att medlemsstaterna har ett handlingsutrymme att, i stället för att införa administrativa sanktioner och andra avhjälpande åtgärder, kriminalisera överträdelser.

Svensk rätt innehåller inte någon straffrättslig reglering som tar sikte på de överträdelser som anges i DORA-förordningen. Frågor om sanktioner på finansmarknadsområdet har varit föremål för överväganden vid genomförandet av eller anpassningen av svensk rätt till en rad EU-rättsakter (se t.ex. prop. 2022/23:7 s. 150). Regeringen har därvid bedömt att det inte är aktuellt att använda straffrättsliga sanktioner i stället för administrativa sanktioner. Inte heller när det gäller överträdelser av DORA-förordningen finns det skäl att införa straffrättsliga sanktioner. Sanktioner vid överträdelser av den förordningen bör därför vara av administrativt slag.

8.2 Ingripanden mot finansiella entiteter

8.2.1 Ingripanden med stöd av befintliga bestämmelser i rörelselagar på finansmarknadsområdet

Promemorians förslag: I kompletteringslagen ska det införas en upplysningsbestämmelse om att bestämmelser om ingripanden mot finansiella entiteter som åsidosätter sina skyldigheter enligt DORA-förordningen eller kompletteringslagen finns i de lagar som reglerar den berörda entitetens verksamhet.

Promemorians bedömning: Finansinspektionens ingripandebefogenheter är tillräckliga för att uppfylla förordningens krav.

Skälen för promemorians förslag och bedömning

Ingripandemöjligheter enligt andra lagar

Enligt DORA-förordningen ska medlemsstaterna fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av förordningen och säkerställa att de genomförs effektivt. Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande (artikel 50.3). Förordningen innehåller inte någon uppräkning av vilka överträdelser av de materiella bestämmelserna som ska kunna leda till ingripanden. Det är en skillnad jämfört med flera andra EU-rättsakter på finansmarknadsområdet. Det finns därför inte skäl att ange vilka överträdelser av DORA-förordningen som ska kunna medföra ingripande i en s.k. överträdelsekatalog.

Som framgår av avsnitt 4.3 är DORA-förordningen tillämplig på nästan alla finansiella entiteter som verkar på finansmarknadsområdet. Bestämmelser om ingripanden mot dessa finns i regel i rörelselagarna för olika finansiella entiteter. För kreditinstitut finns en bestämmelse i lagen om bank- och finansieringsrörelse enligt vilken Finansinspektionen ska ingripa om ett kreditinstitut har åsidosatt sina skyldigheter enligt den lagen eller andra författningar som reglerar institutets verksamhet (15 kap. 1 §). Motsvarande bestämmelser finns för betalningsinstitut och leverantörer av kontoinformationstjänster i lagen (2010:751) om betaltjänster (8 kap. 8 §), där betalningsinstitut är en juridisk person som har tillstånd att tillhandahålla betaltjänster. Betaltjänstleverantörer som beviljats undantag från tillståndsplikt och leverantörer av kontoinformationstjänster är i Sverige registrerade betaltjänstleverantörer (se prop. 2017/18:77 s. 217 och 8 kap. 23 § lagen om betaltjänster). Vidare finns det för institut för elektroniska pengar och registrerade utgivare (institut för elektroniska pengar som är undantagna från tillståndsplikt) bestämmelser i lagen (2011:755) om elektroniska pengar (1 kap. 2 § 7 och 11, 5 kap. 8 och 23 §§), för värdepappersföretag, som när det rör sig om svenska företag benämns värdepappersbolag, i lagen om värdepappersmarknaden (25 kap. 1 §), för värdepapperscentraler i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument (9 kap. 11 §), för centrala motparter i lagen om värdepappersmarknaden (1 kap. 1 a § första stycket och 25 kap. 1 §), för handelsplatser och leverantörer av datarapporteringstjänster i lagen om värdepappersmarknaden (25 kap. 1 §), för förvaltare av alternativa investeringsfonder i lagen (2013:561) om förvaltare av alternativa investeringsfonder (14 kap. 1 §), för förvaltningsbolag, som i lagen (2004:46) om värdepappersfonder benämns fondbolag (10 kap 1 §), för försäkringsföretag (inklusive återförsäkringsbolag) i försäkringsrörelselagen (18 kap. 1 §) och för tjänstepensionsföretag i dess egenskap av tjänstepensionsinstitut i lagen (2019:742) om tjänstepensionsföretag (15 kap. 1 §).

Med författningar enligt de ovan angivna rörelselagarna avses även EU-förordningar (se bl.a. prop. 2021/22:169 s. 59 och prop. 2006/07:115 s. 635–636. Bestämmelserna om ingripanden i rörelselagarna omfattar därmed även finansiella entiteters skyldigheter enligt DORA-förordningen. För ovan uppräknade finansiella entiteter har Finansinspektionen således redan befogenhet enligt svensk rätt att ingripa vid överträdelser av bestämmelserna i DORA-förordningen. Som framgår av avsnitt 5.1 saknas det skäl att därutöver införa bestämmelser i kompletteringslagen om

ingripanden mot dessa finansiella entiteter vid överträdelser av DORA-förordningen. DORA-förordningen kräver därför, i denna del, inte någon lagstiftningsåtgärd. Frågor om ingripanden mot finansiella entiteter som inte omfattas av en svensk rörelselag behandlas i avsnitt 8.2.2.

DORA-förordningens krav på införande av ingripandebefogenheter tillgodoses av gällande rätt

De behöriga myndigheterna ska enligt artikel 50.4 i DORA-förordningen kunna vidta vissa angivna administrativa sanktioner och andra avhjälpande åtgärder vid överträdelser av förordningen. De åtgärder det åtminstone ska bli fråga om är föreläggande om att upphöra med sitt agerande (punkt a), kräva att varje praxis eller beteende som strider mot förordningen tillfälligt eller permanent upphör och förhindra en upprepning av dessa (punkt b), vidta vilken typ av åtgärd som helst, även av ekonomisk art, för att säkerställa att finansiella entiteter fortsätter att uppfylla rättsliga krav (punkt c), kräva tillgång till befintliga uppgifter om datatrafik som innehas av en teleoperatör, i den mån det är tillåtet i nationell rätt (punkt d) och utfärda offentliga meddelanden, inbegripet offentliga uttalanden, med uppgift om identitet och överträdelsens art (punkt e).

De olika rörelselagarna på finansmarknadsområdet innehåller bestämmelser om hur Finansinspektionen kan ingripa (dvs. besluta om sanktioner och andra åtgärder) mot olika finansiella entiteter. Finansinspektionen har enligt dessa lagar möjlighet att ingripa genom föreläggande att vidta rättelse inom viss tid, genom förbud att verkställa beslut eller genom anmärkning. Om en överträdelse är allvarlig, ska den finansiella entitetens tillstånd återkallas, eller om det är tillräckligt varning meddelas. Förelägganden och förbud kan förenas med vite. Vid anmärkning och varning kan sanktionsavgifter påföras.

Det finns sedan många år en strävan efter enhetliga ingripandemöjligheter på finansmarknadsområdet. Utgångspunkten har varit lagstiftningsmodellen på bankområdet. Motsvarande modell har sedan införts i de andra rörelselagarna på finansmarknadsområdet (se t.ex. 25 kap. 1 § lagen om värdepappersmarknaden och 18 kap. 2 § försäkringsrörelselagen).

Enligt gällande rätt har således Finansinspektionen möjlighet att förelägga en finansiell entitet att upphöra med ett agerande. Vidare gäller att om en finansiell entitets tillstånd återkallas, kan Finansinspektionen förena beslutet om återkallelse med ett förbud om att fortsätta rörelsen (se t.ex. 25 kap. 6 § andra stycket lagen om värdepappersmarknaden). Motsvarande bestämmelser finns i EU-rättsakter på finansmarknadsområdet (se t.ex. artikel 42.2 första stycket a i Europaparlamentets och rådets förordning (EU) 2016/1011 av den 8 juni 2016 om index som används som referensvärden för finansiella instrument och finansiella avtal eller för att mäta investeringsfonders resultat, och om ändring av direktiven 2008/48/EG och 2014/17/EU och förordning (EU) nr 596/2014 och artiklarna 69.2 första stycket k och 70.6 b i Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU, i det följande benämnt MiFID II).

Bestämmelserna i ovan nämnda lagar om att Finansinspektionen kan kräva att ett visst agerande upphör och inte upprepas har i en rad tidigare lagstiftningsärenden bedömts uppfylla motsvarande krav i andra EU-rättsakter (se t.ex. prop. 2013/14:228 s. 234 och prop. 2016/17:162 s. 488–490 och 528–529). Det finns inte anledning att göra en annan bedömning i detta lagstiftningsärende i förhållande till kraven i artikel 50.4 a och b i DORA-förordningen. Dessa ingripandeåtgärder, tillsammans med andra åtgärder i form av anmärkning, varning och återkallelse av tillstånd, får också anses uppfylla kraven i förordningen om att den behöriga myndigheten ska kunna vidta vilken typ av åtgärd som helst, även av ekonomisk art, för att säkerställa att finansiella entiteter fortsätter att uppfylla rättsliga krav (artikel 50.4 c).

Vidare ska den behöriga myndigheten, i den mån det är tillåtet enligt nationell rätt, kunna få ut befintliga uppgifter över datatrafik som innehas av en teleoperatör, om det finns rimliga misstankar om överträdelser och om sådana uppgifter kan vara av betydelse för att undersöka överträdelser av reglerna i DORA-förordningen (artikel 50.4 d). I tidigare lagstiftningsärenden har det gjorts bedömningen att Finansinspektionen inte bör ges rätt att begära ut uppgifter om datatrafik från teleoperatör (se prop. 2015/16:170 s. 68–69 och prop. 2016/17:22 s. 161–165). De principer och krav för utlämnande av uppgifter över datatrafik som innehas av en teleoperatör som normalt tillämpas i Sverige bör tillämpas även i detta fall. För uppgifter över datatrafik som innehas av en teleoperatör har i svensk rätt avvägningen mellan den enskildes integritetsskydd och möjligheterna att kunna utreda brott lett till att det krävs brott av en viss svårighetsgrad för att brottsbekämpande myndigheter ska få tillgång till uppgifterna. Finansinspektionens utredningar på det område som omfattas av DORA-förordningen rör inte brott eller företeelser som tidigare varit kriminaliserade. Finansinspektionens bör därför inte heller ges en sådan rätt när det gäller DORA-förordningen.

Den behöriga myndigheten ska enligt DORA-förordningen även kunna besluta om ett offentligt meddelande med uppgift om den fysiska eller juridiska personens identitet och överträdelsens art (artikel 50.4 e). En befogenhet att utfärda offentliga meddelanden ska inbegripa offentliga uttalanden. En möjlighet för Finansinspektionen att meddela ett beslut om anmärkning bör, i enlighet med bedömningar i tidigare lagstiftningsärenden, uppfylla dessa krav i förordningen (se prop. 2019/20:37 s. 52 och prop. 2022/23:7 s. 156).

Sammantaget har Finansinspektionen därför, genom gällande bestämmelser i svensk rätt, i huvudsak de befogenheter att ingripa mot finansiella entiteter som krävs enligt i förordningen. Det bör dock, för tydlighets skull, i kompletteringslagen tas in en upplysningsbestämmelse om att bestämmelser om ingripanden mot finansiella entiteter som åsidosätter sina skyldigheter enligt DORA-förordningen eller kompletteringslagen finns i de lagar som reglerar deras verksamhet. Ingripanden mot personer som ingår i ledningen för finansiella entiteter behandlas i avsnitt 8.3.

8.2.2 Ingripanden med stöd av kompletteringslagen

Promemorians förslag: I kompletteringslagen ska det införas bestämmelser om ingripanden vid överträdelser av DORA-förordningen och kompletteringslagen mot vissa finansiella entiteter.

Finansinspektionen ska få ingripa mot
– Svenska skeppshypotekskassan,
– en emittent av tillgångsanknutna token,
– en pensionsstiftelse,
– ett kreditvärderingsinstitut,
– ett värdepapperiseringsregister, eller
– ett transaktionsregister

om de åsidosätter sina skyldigheter enligt DORA-förordningen eller kompletteringslagen. Ett ingripande mot Svenska skeppshypotekskassan ska få ske genom ett beslut om föreläggande att inom viss tid vidta en särskild åtgärd eller upphöra med ett visst agerande. Ett ingripande mot de övriga uppräknade finansiella entiteterna ska få ske genom ett beslut om föreläggande att inom viss tid vidta en särskild åtgärd eller upphöra med ett visst agerande eller anmärkning.

Finansinspektionen ska vidare få ingripa mot
– en leverantör av kryptotillgångstjänster,
– en administratör av kritiska referensvärden, eller
– en leverantör av gräsrotsfinansieringstjänster

om de åsidosätter sina skyldigheter enligt DORA-förordningen eller kompletteringslagen. Ett ingripande ska få ske genom ett beslut om föreläggande att inom viss tid vidta en särskild åtgärd eller upphöra med ett agerande eller anmärkning. Vid allvarliga överträdelser ska även ett ingripande få ske genom beslut om återkallelse av auktorisation eller, om det är tillräckligt, varning.

Ett ingripande får inte ske om överträdelsen omfattas av ett föreläggande som har förenats med vite och en ansökan om vitet har gjorts.

Om ett beslut om anmärkning eller varning har meddelats, får Finansinspektionen besluta att den som har gjort sig skyldig till överträdelsen ska betala en sanktionsavgift.

Om auktorisationen återkallas ska Finansinspektionen få besluta om hur verksamheten ska avvecklas. Ett beslut om återkallelse ska få förenas med ett förbud att fortsätta rörelsen. Ett sådant beslut ska få förenas med vite.

Skälen för promemorians förslag

Bestämmelser i kompletteringslagen

DORA-förordningen omfattar även vissa finansiella entiteter som saknar en svensk rörelselag. Det gäller leverantörer av kryptotillgångstjänster, emittenter av tillgångsanknutna token, kreditvärderingsinstitut, administratörer av kritiska referensvärden, leverantörer av gräsrotsfinansieringstjänster, värdepapperiseringsregister och transaktionsregister. Dessa regleras i stället genom direkt tillämpliga EU-förordningar som kompletteras av vissa nationella svenska bestämmelser i en kompletteringslag (se t.ex. lagen [2021:899] med kompletterande bestämmelser till EU:s förord-

ning om gräsrotsfinansiering och lagen [2018:2024] med kompletterande bestämmelser till EU:s förordning om referensvärden). Möjligheten för Finansinspektionen att ingripa mot dessa finansiella entiteter är begränsade till överträdelser av respektive EU-förordning. Detta avviker från de finansiella entiteter som behandlas i avsnitt 8.2.1, t.ex. kreditinstitut, som omfattas av en svensk rörelselag där det finns en generell bestämmelse som ger Finansinspektionen möjlighet att ingripa om entiteten har åsidosatt en bestämmelse som gäller för dess verksamhet (se t.ex. 15 kap. 1 § lagen om bank- och finansieringsrörelse). För finansiella entiteter som inte omfattas av en rörelselag saknas därmed enligt gällande bestämmelser möjlighet för Finansinspektionen att ingripa om en sådan finansiell entitet gör sig skyldig till en överträdelse av DORA-förordningen. För att uppfylla kraven enligt förordningen behöver det således införas en sådan möjlighet för Finansinspektionen. Bestämmelser om detta bör tas in i kompletteringslagen (se avsnitt 8.2.2).

I Sverige finns det två typer av tjänstepensionsinstitut; tjänstepensionsföretag och pensionsstiftelser. Tjänstepensionsföretag behandlas ovan i avsnitt 8.2.1. Pensionsstiftelser omfattas i och för sig av en svensk rörelselag, lagen (1967:531) om tryggande av pensionsutfästelse m.m. Den lagen skiljer sig dock från de andra rörelselagarna på finansmarknadsområdet och Finansinspektionen har, i förhållande till de andra lagarna, begränsade möjligheter att ingripa mot en pensionsstiftelse. Finansinspektionens tillsyn och möjligheter att ingripa är kopplade till de krav som följer av Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut, i det följande benämnt andra tjänstepensionsdirektivet, och en stiftelses förvaltning (se 35 § lagen om tryggande av pensionsutfästelse m.m. jämförd med t.ex. 18 kap. 1 § försäkringsrörelselagen). För att uppfylla kraven enligt DORA-förordningen krävs att det införs bestämmelser om ingripanden mot en pensionsstiftelse. Sådana bestämmelser bör lämpligen tas in i kompletteringslagen.

När det gäller leverantörer av kryptotillgångstjänster och emittenter av tillgångsanknutna token så har nationella bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937 ännu inte införts. Finansinspektionen bör likväl kunna ingripa mot leverantörer av kryptotillstångstjänster och emittenter av tillgångsanknutna token om denne åsidosätter sina skyldigheter enligt DORA-förordningen med stöd av kompletteringslagen. I likhet med vad som föreslås för andra finansiella entiteter som saknar rörelselag, bör sådana bestämmelser tas in i kompletteringslagen.

Ingripandebefogenheterna bör som utgångspunkt vara desamma i kompletteringslagen som i de olika rörelselagarna.

Föreläggande att upphöra med en överträdelse och att inte upprepa den

Inom finansmarknadsområdet gäller vanligtvis att Finansinspektionen kan ingripa genom föreläggande att vidta rättelse vid överträdelser (se t.ex. 3 kap. 1 § första stycket 1 lagen [2019:1215] med kompletterande bestämmelser till EU:s förordning om värdepapperisering). Finansinspektionen

bör ges denna möjlighet till ingripanden även enligt den nya kompletteringslagen. Ett föreläggande bör kunna riktas både mot juridiska och fysiska personer (jfr prop. 2020/21:206 s. 76 och prop. 2018/19:4 s. 68).

Eftersom en överträdelse även kan bestå i underlåtenhet att uppfylla vissa krav, bör Finansinspektionen också kunna förelägga den finansiella entiteten att vidta en positiv åtgärd för att uppfylla kraven i DORA-förordningen. I likhet med det som gäller enligt annan lagstiftning på finansmarknadsområdet, bör Finansinspektionen också ha möjlighet att förelägga den som har överträtt DORA-förordningen att inom viss tid vidta en åtgärd för att komma till rätta med situationen eller att upphöra med ett agerande (jfr t.ex. 3 § första stycket 2 lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering).

I likhet med det som gäller enligt andra lagar på finansmarknadsområdet bör ett föreläggande enligt kompletteringslagen få förenas med vite (jfr t.ex. 4 kap. 3 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering).

Återkallelse av auktorisation, varning och anmärkning

Som anges i avsnitt 8.2.1 ska bestämmelserna om ingripanden i rörelselagstiftningen på finansmarknadsområdet tillämpas vid de finansiella entiteternas överträdelser av DORA-förordningen. Vid allvarliga överträdelser av förordningen kan Finansinspektionen därför återkalla tillståndet för en finansiell entitet eller besluta om en varning (se t.ex. 15 kap. 1 § tredje stycket lagen om bank- och finansieringsrörelse).

Leverantörer av kryptotillgångstjänster, administratörer av kritiska referensvärden och leverantörer av gräsrotsfinansieringstjänster har krav på auktorisation av en behörig myndighet, dvs särskilt tillstånd, för att få bedriva verksamhet och i och med det vara en finansiell entitet. Om en sådan finansiell entitet inte följer bestämmelserna i de EU-förordningar som reglerar deras verksamhet får den behöriga myndigheten återkalla auktorisationen (se t.ex. 3 kap. 2 § 3 lagen [2021:899] med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering).

Vid allvarliga överträdelser av DORA-förordningen bör Finansinspektionen även med stöd av kompletteringslagen kunna återkalla auktorisationen för dessa finansiella entiteter eller, om det är tillräckligt, besluta om en varning. En återkallelse av auktorisation är den allvarligaste formen av ingripande. Eftersom ett sådant ingripande får stora konsekvenser såväl för den finansiella entiteten, som dess kunder bör det inte ske utan starka skäl. Varning bör därför, i enlighet med vad som gäller enligt andra lagar på finansmarkansområdet, vara ett alternativ till återkallelse som Finansinspektionen får tillgripa när förutsättningarna för återkallelse i och för sig föreligger, men en varning i det enskilda fallet framstår som en tillräcklig åtgärd (se t.ex. 3 kap. 2 § 3 lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering).

I de olika rörelselagarna finns det också en möjlighet att ingripa genom beslut om anmärkning när det är fråga om överträdelser som inte är så allvarliga att det finns förutsättningar att återkalla tillståndet eller besluta om varning (se t.ex. 18 kap. 2 § första stycket försäkringsrörelselagen, se även prop. 2006/07:115 s. 499). Finansinspektionen bör även vid över-

trädelse av DORA-förordningen ha möjlighet att besluta om anmärkning enligt kompletteringslagen.

Liksom det som gäller enligt andra lagar på finansmarknadsområdet bör sanktionerna anmärkning och varning kunna förenas med sanktionsavgifter (se t.ex. 3 kap. 3 § lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering). Sanktionsavgiftens storlek behandlas i avsnitt 8.4.

Ett ingripande genom ett föreläggande att vidta rättelse och ett beslut om anmärkning bör inte komma i fråga för samma överträdelse. Ingripande genom föreläggande kan endast användas när det krävs för att få den finansiella entiteten i fråga att vidta åtgärder för att rätta till något. En anmärkning bör användas när det inte finns något att åtgärda men överträdelsen likväl bör medföra en sanktion (jfr prop. 2002/03:139 s. 548 och prop. 2022/23:7 s. 156).

Vid återkallelse av auktorisation gäller enligt flera rörelselagar på finansmarknadsområdet att Finansinspektionen har möjlighet att bestämma hur avvecklingen av rörelsen ska ske (se t.ex. 15 kap. 4 § lagen om bank- och finansieringsrörelse). Genom dessa bestämmelser får Finansinspektionen möjlighet att i sitt beslut om återkallelse ge anvisningar om hur rörelsen ska avvecklas. Därigenom ges utrymme att ta hänsyn till individuella förhållanden hos den verksamhet som beslutet avser (se prop. 1990/91:142 s. 175, prop.1991/92:113 s. 208 och prop. 2006/07:115 s. 639). En motsvarande bestämmelse bör införas i kompletteringslagen eftersom det är av vikt att även sådana finansiella entiteteter, vars auktorisation kan återkallas med stöd av kompletteringslagen, avvecklas på ett ordnat sätt. I likhet med det som gäller i ovan nämnda rörelselagar bör ett beslut om återkallelse av auktorisation få förenas med förbud att fortsätta verksamheten och ett sådant förbud förenas med vite.

Överträdelsen omfattas av ett föreläggande som förenats med vite

Som konstaterats i flera lagstiftningsärenden får termen straff i den mening som avses i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) även anses omfatta t.ex. vite (artikel 4 i sjunde tilläggsprotokollet till Europakonventionen, se prop. 2022/23:7 s. 153 och prop. 2020/21:206 s. 75). Om ett vite har dömts ut bör det inte vara möjligt att besluta om en sanktion för samma sak. I avsnitt 7.2 föreslås att Finansinspektionen ska få utfärda förelägganden om att tillhandahålla uppgifter eller inställa sig till förhör. Ovan föreslås att ett förbud att fortsätta verksamheten efter tillståndet återkallats och i avsnitt 8.3 föreslås ett förbud att vara styrelseledamot eller verkställande direktör eller ersättare för någon av dem ska få förenas med vite. Om ett föreläggande förenas med vite och det inte följs, bör Finansinspektionen välja mellan att ansöka om utdömande av vitet eller att ingripa mot överträdelsen (jfr prop. 2016/17:22 s. 228). Det bör därför tas in en bestämmelse i kompletteringslagen om att ingripande inte får ske om överträdelsen omfattas av ett föreläggande som har förenats med vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Ingripanden mot Svenska skeppshypotekskassan

I avsnitt 5.3 föreslås Svenska skeppshypotekskassan omfattas av DORA-förordningen. I kompletteringslagen bör det därför införas en möjlighet för Finansinspektionen att ingripa mot Svenska skeppshypotekskassan om kassan åsidosätter sina skyldigheter enligt förordningen eller kompletteringslagen.

Finansinspektionen bör kunna ingripa genom att rikta ett föreläggande mot Svenska skeppshypotekskassan att inom viss tid vita en åtgärd eller upphöra med ett visst agerande. Det motsvarar nuvarande ingripandebefogenheter på finansmarknadsområdet mot kassan (se 8 kap. 1 § lagen om särskild tillsyn över kreditinstitut och värdepappersbolag). En sådan bestämmelse bör därför införas i den nya kompletteringslagen.

8.3 Ingripanden mot vissa företrädare för finansiella entiteter

Promemorians förslag: Finansinspektionen ska få ingripa mot någon som ingår i styrelsen för en finansiell entitet eller är dess verkställande direktör, eller ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter enligt DORA-förordningen.

Ett ingripande ska få ske bara om den finansiella entitetetens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande ska få ske genom en eller båda av följande administrativa sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en sådan finansiell entitet, eller ersättare för någon av dem, eller
2. sanktionsavgift.

Ett beslut om förbud mot att vara styrelseledamot eller verkställande direktör, eller ersättare för någon av dem, ska få förenas med vite.

Frågor om ingripanden mot fysiska personer ska tas upp av Finansinspektionen genom ett sanktionsföreläggande. Ett godkänt sanktionsföreläggande gäller som ett domstolsavgörande som har fått laga kraft.

Det ska införas en bestämmelse om vilka uppgifter ett sanktionsföreläggande ska innehålla.

Om ett sanktionsföreläggande inte har godkänts inom angiven tid ska Finansinspektionen få ansöka hos domstol om att en sanktion ska beslutas. En sådan ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av Finansinspektionens beslut om ingripande mot den finansiella entiteten. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Ett sanktionsföreläggande ska vara utan verkan om föreläggandet inte har delgetts den som det riktas mot inom viss tid, oavsett om det gäller handläggningen vid Finansinspektionen eller i domstol.

Skälen för promemorians förslag

Bestämmelser behöver införas i rörelselagarna och i kompletteringslagen

Enligt DORA-förordningen ska medlemsstaterna ge den behöriga myndigheten befogenhet att, vid en juridisk persons överträdelse, tillämpa administrativa sanktioner och avhjälpande åtgärder på medlemmar i ledningsorganet och på andra personer som enligt nationell rätt är ansvariga för överträdelsen (artikel 50.5).

I rörelselagarna på finansmarknadsområdet finns det bestämmelser om ingripanden mot fysiska personer som ingår i ledningen för en finansiell entitet. Finansinspektionens möjligheter att ingripa är i dessa fall begränsade till överträdelser i rörelselagarna eller till överträdelser av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (t.ex. 15 kap. 1 a § lagen om bank- och finansieringsrörelse och 18 kap. 1 a § försäkringsrörelselagen). I gällande svensk rätt finns det således inte någon möjlighet att ingripa mot fysiska personer som ingår i ledningen för en finansiell entitet när den juridiska personen har åsidosatt sina skyldigheter enligt DORA-förordningen. Det bör därför införas bestämmelser om detta. För att skapa en enhetlig reglering, bör bestämmelserna i första hand införas i de rörelselagar som redan har tillämpliga bestämmelser om ingripanden, t.ex. lagen om bank- och finansieringsrörelse (se avsnitt 8.2.1). Bestämmelser om ingripanden mot personer i ledningen för finansiella entiteter som inte omfattas av en rörelselag bör införas i kompletteringslagen, t.ex. leverantörer av gräsrotsfinansieringstjänster (se avsnitt 8.2.2).

En uppräkning av de överträdelser som kan föranleda ingripande

När motsvarande regler om ingripande infördes mot fysiska personer för ett företags överträdelser lyfte regeringen fram att det med hänsyn till bl.a. rättssäkerhet och förutsebarhet för den enskilde finns skäl att uttryckligen i lag ange de överträdelser som kan föranleda sanktion, inte minst eftersom bestämmelserna kan anses ha straffrättslig karaktär (se prop. 2016/17:162 s. 536–537 och de hänvisningar som görs där). Dessa argument gäller fortfarande. De överträdelser av en finansiell entitet som kan föranleda en sanktion mot en ansvarig fysisk person bör därför anges uttryckligen i bestämmelserna i rörelselagarna och i kompletteringslagen.

Kretsen av personer som ska omfattas av bestämmelser om ingripande

Kretsen fysiska personer som ska kunna bli föremål för en sanktion eller en åtgärd anges i DORA-förordningen på ett i allt väsentligt samma sätt som i motsvarande bestämmelser i andra EU-rättsakter på finansmarknadsområdet (artikel 50.5 i DORA-förordningen jämförd med t.ex. kapitaltäckningsdirektivet. Bestämmelserna i det direktivet har genomförts i svensk rätt genom bestämmelser i lagen om bank- och finansieringsrörelse (15 kap. 1 a §) och lagen om värdepappersmarknaden (25 kap. 1 a § första stycket). När kapitaltäckningsdirektivet genomfördes ansågs att den personkrets som kan träffas av administrativa sanktioner och åtgärder bör utgöras av styrelsen, den verkställande direktören och ersättare för dessa (prop. 2014/15:57 s. 39–40). Samma bedömning

gjordes vid genomförandet av MiFID II i fråga om ingripanden mot personer i ledningsorgan för värdepappersinstitut och börser (prop. 2016/17:162 s. 537–538). Det finns inte skäl att göra någon annan bedömning när det gäller kretsen av fysiska personer som Finansinspektionen bör kunna ingripa mot vid en juridisk persons överträdelse av DORA-förordningen. Ingripanden bör därför kunna ske mot den som ingår i styrelsen för en finansiell entitet eller är dess verkställande direktör, eller ersättare för någon av dem.

Förutsättningarna för ingripande bör vara desamma som i annan lagstiftning på finansmarknadsområdet

Förutsättningarna för ett ingripande mot ledamöter i den juridiska personenens styrelse, dess verkställande direktör eller ersättare för dessa bör vara desamma som i annan lagstiftning på finansmarknadsområdet (se t.ex. 15 kap. 1 a § lagen om bank- och finansieringsrörelse). Finansinspektionen bör därför få ingripa mot personer som ingår i ledningsorganet för en finansiell entitet genom förbud att utöva ledningsuppdrag eller genom sanktionsavgift. Dessa två sanktioner bör också kunna kombineras. Därutöver bör det krävas att överträdelsen är allvarlig och att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen, eftersom sanktionerna endast ska kunna komma i fråga i särskilt allvarliga fall och de har straffrättslig karaktär (se prop. 2016/17:162 s. 539–542 och de hänvisningar som görs där). Samma hänsyn gör sig gällande vid utformningen av de bestämmelser som föreslås i rörelselagarna och i den nya kompletteringslagen. Befogenheterna att tillämpa administrativa sanktioner och avhjälpande åtgärder mot fysiska personer som ingår i ledningsorganet för en finansiell entitet ska ges med förbehåll för villkor som föreskrivs i nationell rätt (artikel 50.5). DORA-förordningen hindrar därför inte att ett sådant ingripande villkoras på det sättet.

I annan lagstiftning på finansmarknadsområdet gäller i allmänhet att ett förbud mot att utöva ledningsfunktioner ska gälla för viss tid, lägst tre år och högst tio år (se t.ex. 15 kap. 1 a § tredje stycket i lagen om bank- och finansieringsrörelse). Detsamma bör gälla även för den möjlighet att besluta om förbud att utöva ledningsfunktioner som nu föreslås. Ett sådant förbud bör få förenas med vite. Bestämmelser om detta bör tas in i den nya kompletteringslagen, vilket överensstämmer med det som kommer att gälla enligt de olika rörelselagarna.

Ingripande bör ske genom ett sanktionsföreläggande

Ingripande mot fysiska personer som ingår i ledningsorganet för en finansiell entitet bör, i likhet med det som gäller enligt andra lagar på finansmarknadsområdet, ske genom ett sanktionsföreläggande (se t.ex. 25 kap. 10 a § lagen om värdepappersmarknaden, se även prop. 2016/17:162 s. 536 och de hänvisningar som görs där). Ett sanktionsföreläggande innebär att den fysiska personen föreläggs att inom en viss tid godkänna ett ingripande som är bestämt till tid eller belopp. När ett sanktionsföreläggande har godkänts gäller det som ett domstolsavgörande som har fått laga kraft. Det innebär bl.a. att föreläggandet kan verkställas enligt utsökningsbalken om avgiften inte betalas (jfr prop. 2014/15:57 s. 61). Ett

godkännande som görs efter den tid som anges i föreläggandet är utan verkan.

Ett sanktionsföreläggande bör, i likhet med det som gäller enligt andra lagar på finansmarknadsområdet, innehålla vissa uppgifter (se t.ex. 25 kap. 10 b § lagen om värdepappersmarknaden). I kompletteringslagen och de aktuella rörelselagar som saknar bestämmelser om förelägganden bör det därför anges att ett sanktionsföreläggande ska innehålla en uppgift om den fysiska person som föreläggandet avser, en uppgift om överträdelsen och de omständigheter som behövs för att kännetecknа den, uppgift de bestämmelser som är tillämpliga på överträdelsen, och om den sanktion som föreläggs personen. Föreläggandet bör också innehålla en upplysning om att en ansökan om sanktion kan komma att ges in till domstol, om föreläggandet inte godkänns inom den tid som Finansinspektionen anger.

Beträffande processen för ingripande om ett sanktionsföreläggande inte godkänns, görs samma bedömning som i tidigare lagstiftningsärenden om sanktioner mot fysiska personer som ingår i en juridisk persons ledningsorgan (se prop. 2014/15:57 s. 61–62.).

Finansinspektionen bör alltså ha möjlighet att ansöka hos domstol om att en sanktion ska beslutas enligt de lagarna. En sådan ansökan bör göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av Finansinspektionens beslut om ingripande mot den juridiska personen för samma överträdelse. Prövningstillstånd bör krävas vid överklagande till kammarrätten. Vidare bör ett sanktionsföreläggande mot en fysisk person vara utan verkan om föreläggandet inte har delgetts personen inom två år från den tidpunkt då överträdelsen ägde rum. I ett sådant fall bör inte heller domstol få besluta om en sanktion.

Bestämmelserna om sanktionsföreläggande i kompletteringslagen och berörda rörelselagar bör utformas efter förebild av motsvarande bestämmelser i andra lagar på finansmarknadsområdet (se t.ex. 25 kap. 10 c och 10 d §§ lagen om värdepappersmarknaden).

8.4 Beräkning av sanktionsavgift

Promemorians förslag: En sanktionsavgift för en leverantör av kryptotillgångstjänster, en emittent av tillgångsanknutna token, en pensionsstiftelse, ett kreditvärderingsinstitut, en administratör av kritiska referensvärden, en leverantör av gräsrotsfinansieringstjänster, ett värdepapperiseringsregister och ett transaktionsregister som är en juridisk person ska högst kunna fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade en miljon euro,
2. tio procent av den finansiella entitetens omsättning närmast föregående räkenskapsår eller, i förekommande fall, motsvarande omsättning på koncernnivå, eller
3. tre gånger den vinst den finansiella entiteten har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

Sanktionsavgiften ska inte få bestämmas till ett lägre belopp än 5 000 kronor.

Sanktionsavgiften för en leverantör av gräsrotsfinansieringstjänster ska inte få vara så stor att leverantören därefter inte uppfyller de krav om soliditet och likviditet som gäller för leverantören.

Om överträdelsen har skett under den juridiska personens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, ska omsättningen få uppskattas när den högsta sanktionsavgiften ska beräknas.

Sanktionsavgiften för en fysisk person ska som högst kunna fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 500 000 euro, eller

2. tre gånger den vinst som den fysiska personen har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

Sanktionsavgifterna ska tillfalla staten.

Promemorians bedömning: Tillämpliga bestämmelser i rörelselagarna om beräkning av sanktionsavgift är tillräckliga för att uppfylla DORA-förordningens krav.

Skälen för promemorians förslag och bedömning

Beräkningsgrunder

DORA-förordningen innehåller inte några bestämmelser om storleken på sanktionsavgifter. Det är en skillnad jämfört med flera andra EU-rättsakter på finansmarknadsområdet, som innehåller detaljerade bestämmelser om beräkningsgrunder för sanktionsavgifter. Dessa har genomförts i rörelselagstiftning och lagar som kompletterar olika EU-rättsakter på finansmarknadsområdet (se t.ex. 25 kap. 9 och 9 a §§ lagen om värdepappersmarknaden och 3 kap. 12 och 13 §§ lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering).

De sanktionsavgifter som får tas ut vid överträdelser av de olika EU-rättsakterna ska i de flesta fall kunna tillämpas på ett antal olika överträdelser, på fysiska personer och företag av olika storlek och med olika ekonomiska resurser och i samtliga medlemsstater. Maximibeloppen i de olika fallen är således bestämda för att vara tillräckligt avskräckande och för att kunna uppväga eventuella vinster som en person har gjort genom att överträda EU-rättsakterna.

För juridiska personer finns i de flesta fall tre alternativa beräkningsmetoder för avgifterna:

1. sanktionsavgiften ska kunna uppgå till det högsta av ett bestämt belopp i euro eller, i medlemsstater vars valuta inte är euro, motsvarande värde i nationell valuta vid ett bestämt datum,

2. en viss procentsats av den juridiska personens totala årsomsättning, eller i förekommande fall motsvarande omsättning på koncernivå, eller

3. ett visst antal gånger beloppet för den vinst som erhållits genom överträdelsen, om den kan fastställas.

Den lägsta sanktionsavgift som får tas ut är 5 000 kr. För fysiska personer används beräkningsmetoderna ett och tre.

I flera lagar på finansmarknadsområdet finns det bestämmelser som förhindrar att en sanktionsavgift bestäms till ett så stort belopp att företaget därefter inte uppfyller de krav på soliditet och likviditet som gäller enligt

rörelseregleringen (se t.ex. 15 kap. 8 § tredje stycket lagen om bank- och finansieringsrörelse, 25 kap. 9 § tredje stycket lagen om värdepappersmarknaden, 18 kap. 17 § tredje stycket försäkringsrörelselagen). Avsikten är att förhindra att uttaget av avgiften leder till att tillståndet att bedriva verksamheten måste återkallas (se prop. 2006/07:115 s. 640–641).

Befintliga bestämmelser i rörelselagarna om sanktionsavgifter ska tillämpas

Ovan förslås att Finansinspektionen ska kunna ingripa mot finansiella entiteter med stöd av bestämmelserna i rörelselagarna på finansmarknadsområdet (avsnitt 8.2.1). Det föreslås även att det ska införas bestämmelser i rörelselagarna om att Finansinspektionen ska kunna ingripa mot fysiska personer som ingår i ledningsorganet för dessa finansiella entiteter när den juridiska personen har åsidosatt sina skyldigheter enligt vissa bestämmelser i DORA-förordningen (avsnitt 8.3). Detta innebär att bestämmelserna om sanktionsavgifter i rörelselagarna blir tillämpliga vid sådana överträdelser.

Bestämmelser om sanktionsavgifter i kompletteringslagen

Det behöver införas bestämmelser i kompletteringslagen om beräkning av sanktionsavgifter för de överträdelser av DORA-förordningen som en leverantör av kryptotillstångstjänster, en emittent av tillgångsanknutna token, en pensionsstiftelse, ett kreditvärderingsinstitut, en administratör av kritiska referensvärden, en leverantör av gräsrotsfinansieringstjänster, ett värdepapperiseringsregister och ett transaktionsregister gör sig skyldiga till.

I flera lagar med kompletterande bestämmelser till de EU-förordningar som reglerar dessa finansiella entiteter finns det bestämmelser med motsvarande beräkningsgrunder som i andra lagar på finansmarknadsområdet (se t.ex. 4 kap. 6 § lagen med kompletterande bestämmelser till EU:s förordning om referensvärden). Bestämmelser om sanktionsavgifter för juridiska och fysiska personer i den nya kompletteringslagen till DORA-förordningen bör utformas på samma sätt.

På samma sätt som i andra lagar på finansmarknadsområdet bör det belopp som en sanktionsavgift ska kunna uppgå till anges med ett belopp i svenska kronor som per datumet för ikraftträdande av EU-rättsakten motsvarar ett visst belopp i euro (se t.ex. 25 kap. 9 § första punkten lagen om värdepappermarkaden). Sanktionsavgiften för juridiska personer bör kunna uppgå till högst en miljon euro och för fysiska personer till 500 000 euro. När EU-rättsakter genomförs i svensk rätt har det i ett flertal fall hänvisats till den valutakurs som motsvarar den s.k. fixingkurs, i äldre lagstiftningsärenden benämnd mittkurs, som dagligen fastställs av Nasdaq Stockholm AB (se t.ex. prop. 2020/21:206 s. 85–86) och publiceras på Riksbankens webbplats. Det är lämpligt att tillämpa denna fixingkurs för omräkning av sanktionsavgiften även i detta fall. Enligt fixingkursen den 16 januari 2023, det datum då DORA-förordningen trädde i kraft, motsvarade i 1 euro 11,2691 svenska kronor. Eftersom beloppet för sanktionsavgiften knyts till eurons kurs ett visst datum kommer omräkningen mellan euro och svenska kronor inte att förändras.

Den sanktionsavgift som Finansinspektionen får ta ut av en juridisk person enligt den nya kompletteringslagen bör, som gäller enligt andra lagar på finansmarknadsområdet, inte få bestämmas till ett lägre belopp än 5 000 kronor (se t.ex. 15 kap. 8 § lagen om bank- och finansieringsrörelse och 25 kap. 9 § lagen om värdepappersmarknaden).

När en finansiell entitet ingår i en koncern ska omsättningen som regel beräknas utifrån koncernredovisningen. I andra lagar på finansmarknadsområdet anges att omsättningen i förekommande fall ska bestämmas utifrån ”motsvarande omsättning på koncernnivå” (se t.ex. 25 kap. 9 § andra punkten lagen om värdepappersmarknaden). Avsikten är att omsättning från verksamhet i koncernen som redovisas utifrån samma redovisningsregler ska ligga till grund för beräkningen av den högsta sanktionsavgiften (se prop. 2016/17:162 s. 600–602). Detta bör även gälla enligt den nya kompletteringslagen.

I flera lagar på finansmarknadsområdet finns det bestämmelser som tar sikte på en situation där en överträdelse av en juridisk person har ägt rum under företagets första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga (se t.ex. 25 kap. 9 § andra stycket lagen om värdepappersmarknaden). I sådana fall får det göras en uppskattning av omsättningen. Det är endast i de fall det, av de skäl som anges i bestämmelserna, inte går att beräkna avgiftens storlek som en uppskattad omsättning får läggas till grund för sanktionsavgiftens storlek. En motsvarande bestämmelse bör införas i den nya kompletteringslagen.

I 3 kap. 10 § lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering föreskrivs att sanktionsavgiften inte får vara så stor att leverantörens skyldigheter enligt andra bestämmelser om soliditet och likviditet äventyras (se prop. 2020/21:206 s. 85). En motsvarande bestämmelse bör införas i den nya kompletteringslagen.

8.5 Omständigheter som ska vara styrande vid ett beslut om ingripande

Promemorians förslag: Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått samt graden av ansvar för den som har begått överträdelsen.

Finansinspektionen ska i försvårande riktning beakta om den fysiska eller juridiska personen tidigare har begått en överträdelse. Vid denna bedömning ska särskild vikt fästas vid om överträdelserna är likartade och den tid som har gått mellan de olika överträdelserna.

I förmildrande riktning ska det beaktas om den som har begått överträdelsen i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och snabbt upphört med överträdelsen eller snabbt verkat för att överträdelsen ska upphöra, sedan den anmälts till eller påtalats av Finansinspektionen.

De omständigheter som ska vara styrande vid valet av ingripande ska beaktas även vid bestämmande av sanktionsavgiftens storlek. Utöver

detta ska särskild hänsyn tas till den juridiska eller fysiska personens finansiella ställning och den vinst som gjorts till följd av överträdelsen, om vinsten går att bestämma.

Finansinspektionen ska få avstå från ett ingripande om överträdelsen är ringa eller ursäktlig, den fysiska eller juridiska personen i fråga gör en rättelse, den fysiska personen har verkat för att den juridiska personen gör en rättelse, någon annan myndighet eller något annat organ har vidtagit åtgärder mot den fysiska eller juridiska personen och dessa åtgärder bedöms som tillräckliga.

Promemorians bedömning: Tillämpliga bestämmelser i rörelselagarna om omständigheter som ska beaktas vid val av sanktion är tillräckliga för att uppfylla DORA-förordningens krav.

Skälen för promemorians förslag och bedömning

Tillämpliga bestämmelser i rörelselagarna

Enligt DORA-förordningen ska de behöriga myndigheterna ta hänsyn till alla relevanta omständigheter när de fastställer typ och nivå på administrativa sanktioner eller avhjälpande åtgärder (artikel 51.2).

I förordningen anges särskilt att den behöriga myndigheten ska ta hänsyn till om överträdelsen är avsiktlig eller om den beror på försummelse. Vidare finns följande, icke uttömmande, uppräkning av omständigheter som ska beaktas (artikel 51.2 a–g).

a) Överträdelsens väsentlighet, svårighetsgrad och varaktighet.

b) Graden av ansvar hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen.

c) Den finansiella styrkan hos den fysiska eller juridiska personen som har gjort sig skyldig till överträdelsen.

d) Omfattningen av de vinster som erhållits eller av förluster som undvikits av den fysiska eller juridiska personen som gjort sig skyldig till överträdelsen, i de mån de kan bestämmas.

e) Förluster för tredje parter orsakade av överträdelsen, i den mån de kan fastställas.

f) Viljan hos den ansvariga fysiska eller juridiska personen att samarbete med den behöriga myndigheten, utan att det påverkar behovet av att säkerställa återföring av den vinst som den fysiska eller juridiska personen gjort eller de förluster som denne undvikit.

g) Tidigare överträdelser av den fysiska eller juridiska personens som har gjort sig skyldig till överträdelsen.

Liknande regler finns i flera EU-rättsakter på finansmarknadsområdet (se t.ex. artikel 72.2 i MiFID II). Bestämmelserna i de rättsakterna har införts i svensk rätt i rörelselagarna och i kompletterande lagar på finansmarknadsområdet (se t.ex. 25 kap. 2 § första stycket och 2 a § i lagen om värdepappersmarknaden och 3 kap. 13–16 §§ i lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering. I dessa lagar anges således vilka omständigheter som ska beaktas vid valet mellan olika situationer. Dessa bestämmelser torde uppfylla kraven i DORA-förordningen.

Bestämmelser i kompletteringslagen

Bestämmelsen i DORA-förordningen är, i likhet med motsvarande bestämmelse i Europaparlamentets och rådets förordning (EU) 2017/1129 av den 14 juni 2017 om prospekt som ska offentliggöras när värdepapper erbjuds till allmänheten eller tas upp till handel på en reglerad marknad, och om upphävande av direktiv 2003/71/EG, i det följande benämnt EU:s prospektförordning (artikel 39), utformad så att den är riktad till den behöriga myndigheten. Det skulle därför kunna förstås som att den är direkt tillämplig. Vid införandet av lagen med kompletterande bestämmelser till EU:s prospektförordning gjordes dock bedömningen att det, för att främja förutsägbarheten och enhetligheten i tillämpningen av bestämmelserna, är en rimlig utgångspunkt att de omständigheter som anges i den förordningen om val av sanktioner anges även i lag (prop. 2018/19:83 s. 102–104). Samma bedömning gjordes vid införandet av lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering och lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering (se prop. 2019/20:37 s. 63 och 2020/21:206 s. 88).

Det finns inte skäl att nu göra någon annan bedömning. De omständigheter som anges i DORA-förordningen bör därför anges även i den nya kompletteringslagen. För att inte begränsa utrymmet för egna bedömningar och möjligheter att ta hänsyn till särskilda omständigheter i det enskilda fallet bör dock lagtexten utgöra en exemplifierande, dvs inte en uttömmande, uppräkning av omständigheter som ska beaktas vid val av sanktion. Det går inte att reglera vilken relativ vikt som ska tillmätas olika omständigheter eller hur de ska vägas i det enskilda fallet. Detta är i stället något som ankommer på tillämpande myndighet eller domstol (se även prop. 2013/14:228 s. 237–239).

Den modell som har valts i tidigare lagstiftningsärenden utgår från att det bör stå klart vad som ska vara utgångspunkten vid val av ingripande. Därutöver bör det anges vilka omständigheter som i vart fall bör tillåtas att inverka på beslutet om vilken form av ingripande som slutligen ska väljas. De omständigheter som räknas upp i DORA-förordningen kan därmed delas in i sådana som är hänförliga till själva överträdelsen, och sådana som är att hänföra till den finansiella situationen hos den som begått den aktuella överträdelsen respektive sådana omständigheter som inträffat före eller efter överträdelsen och som är relevanta att beakta.

Med omständigheter som är hänförliga till själva överträdelsen bör avses objektiva faktorer som överträdelsens konkreta och potentiella effekter på det finansiella systemet, överträdelsens allvar och varaktighet och om det finns tredje parter som har orsakats förlust av överträdelsen. Det senare bör, liksom vid tidigare införanden av liknande bestämmelser i EU-rättsakter på finansmarknadsområdet, motsvaras av uttrycket ”skador som uppstått” (se prop. 2015/16:26 s. 104–106). Vid bedömningen av själva överträdelsen bör hänsyn även tas till sådant som i DORA-förordningen uttrycks som ”graden av ansvar” (artikel 51.2 b). Med detta avses i huvudsak att någon kan vara mer eller mindre ansvarig för en överträdelse och ha en omfattande eller mer begränsad kännedom om de omständigheter som utgör överträdelsen. Detta innefattar även om överträdelsen är uppsåtlig eller om den har begåtts av oaktsamhet. Om nämnda faktorer bildar utgångspunkt för valet av ingripande kan därefter det slutliga utfallet

påverkas av faktorer som inte är att hänföra till själva överträdelsen. Till sådana omständigheter bör hänföras omfattningen av erhållna fördelar till följd av överträdelsen, tidigare överträdelser och agerandet hos den som begått överträdelsen efter det att överträdelsen har avslöjats.

Omständigheter som bör beaktas särskilt vid fastställande av sanktionsavgiftens storlek

När Finansinspektionen ingriper genom beslut om sanktionsavgift enligt den nya kompletteringslagen bör inspektionen, vid fastställande av storleken på sanktionsavgiften, ta hänsyn till samtliga relevanta omständigheter. Detta inbegriper sådana omständigheter som ska beaktas vid valet av ingripande. I fråga om sanktionsavgiftens storlek är det därutöver särskilt relevant att beakta den aktuella personens finansiella ställning och storleken på den vinst som personen gjort till följd av överträdelsen. Ovan föreslås att de omständigheter som enligt DORA-förordningen särskilt ska beaktas vid fastställande av val av ingripande ska anges i kompletteringslagen. För att främja förutsägbarheten och enhetligheten bör även de omständigheter som ska beaktas särskilt vid fastställandet av sanktionsavgiftens storlek anges i lagen.

I DORA-förordningen anges att den finansiella styrkan hos den fysiska eller juridiska personen ska beaktas (artikel 51.2 c). I andra lagstiftningsärenden på finansmarknadsområdet har den finansiella ställningen bestämts utifrån den juridiska personens totala omsättning eller den ansvariga fysiska personens årsinkomst. Även andra ekonomiska förhållanden, såsom underhållsskyldighet i fråga om fysisk person och förmögenhetsförhållanden, bör dock kunna beaktas (se prop. 2020/21:206 s. 90).

I DORA-förordningen anges att omfattningen av de vinster som erhållits eller förluster som undvikits av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen ska beaktas (artikel 51.2 d). I likhet med de bedömningar som gjorts i tidigare lagstiftningsärenden av motsvarande bestämmelser i andra EU-rättsakter, bör i bestämmelsen i den nya kompletteringslagen enbart vinst anges (se t.ex. prop. 2016/17:162 s. 602–603). Den vinst som gjorts avser ett nettobelopp och omfattar de intäkter som erhållits och de förluster som undvikits, dvs. den fördel som faktiskt erhållits (jfr samma prop. s. 603).

Finansinspektionen ska kunna avstå från ett ingripande

För att de administrativa sanktionerna ska vara proportionerliga bör Finansinspektionen, liksom enligt andra lagar på finansmarknadsområdet, kunna avstå från ett ingripande i vissa situationer (se t.ex. 25 kap. 2 § andra stycket lagen om värdepappersmarknaden).

I huvudsak bör Finansinspektionen kunna avstå från ett ingripande i samma situationer som enligt andra lagar på finansmarknadsområdet (jfr samma som ovan). Finansinspektionen bör således kunna avstå från ett ingripande om överträdelsen är ringa eller ursäktlig, den juridiska eller fysiska personen i fråga gör rättelse eller den fysiska personen har verkat för att den juridiska personen gör rättelse. Inspektionen bör också kunna avstå från ett ingripande om någon annan myndighet eller något annat organ har vidtagit åtgärder mot den juridiska eller fysiska personen och dessa åtgärder bedöms tillräckliga. Detta täcker ett stort antal situationer,

t.ex. en risk för dubbelprövning (jfr 5 kap. 17 § 3 lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning och prop. 2016/17:22 s. 392). Till skillnad från t.ex. lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning torde det inte bli aktuellt med ingripanden mot mycket unga och omyndiga personer (se samma prop. s. 227 och 392). Det är därmed svårt att se några ytterligare fall då Finansinspektionen bör kunna avstå från ett ingripande. I den nya kompletteringslagen bör det därmed inte införas någon generell möjlighet för Finansinspektionen att avstå från ingripande om det finns andra särskilda skäl.

8.6 Betalning, preskription och verkställighet

Promemorians förslag: En sanktionsavgift som tas ut med stöd av kompletteringslagen ska betalas inom 30 dagar efter det att ett beslut om att ta ut avgiften har fått laga kraft eller sanktionsföreläggandet godkänts eller den längre tid som anges i beslutet eller föreläggandet. Om sanktionsavgiften inte betalas inom denna tid, ska Finansinspektionen lämna den obetalda avgiften för indrivning.

Sanktionsavgift som beslutats ska falla bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet eller domen fick laga kraft eller sanktionsföreläggandet godkändes.

Skälen för promemorians förslag: I DORA-förordningen finns det inte några regler om betalning av sanktionsavgifter, preskription och verkställighet. Medlemsstaterna har således möjlighet att själva avgöra vad som ska gälla i sådana frågor. Bestämmelserna om betalning, preskription och verkställighet i kompletteringslagen bör utformas efter förebild av motsvarande bestämmelser i andra lagar på finansmarknadsområdet (se t.ex. 25 kap. 25–28 §§ lagen om värdepappersmarknaden). Enligt dessa bestämmelser ska en avgift betalas till Finansinspektionen inom 30 dagar efter det att ett beslut om avgiften har fått laga kraft eller den längre tid som anges i beslutet. Samma ordning bör gälla för sanktionsavgifter som beslutas med anledning av överträdelser av DORA-förordningen.

Vidare gäller enligt samma bestämmelser att ett beslut av Finansinspektionen om en sanktionsavgift får verkställas enligt utsökningsbalken. Om avgiften inte betalas i rätt tid, ska Finansinspektionen lämna den obetalda avgiften för indrivning. Samma ordning bör gälla för sanktionsavgifter som beslutas med anledning av överträdelser av DORA-förordningen.

Finansinspektionens beslut om sanktionsavgift ska kunna överklagas (se avsnitt 15.1). Beslutet är därmed ett sådant beslut som enligt 3 kap. 1 § första stycket 6 a och 20 § första stycket utsökningsbalken får verkställas som en exekutionstitel när beslutet har fått laga kraft (se prop. 2021/22:206). Det behövs därför ingen särskild föreskrift om att beslutet får verkställas enligt utsökningsbalken. Även ett godkänt sanktionsföreläggande kan verkställas (se avsnitt 8.3).

När det gäller frågan om preskription anges i flera lagar på finansmarknadsområdet att en sanktionsavgift som beslutats faller bort i den utsträckning verkställighet inte har skett inom fem år (se t.ex. 5 kap. 25 § lagen med kompletterande bestämmelser till EU:s marknadsmissbruks-

förordning). Samma preskriptionstid bör gälla för sanktionsavgifter som beslutas med anledning av överträdelser av DORA-förordningen. Med verkställighet avses faktiska verkställighetsåtgärder. Preskriptionen är absolut. Det betyder att fullgörande inte kan krävas efter det att fem år har gått sedan beslutet fått laga kraft, även om verkställighet har skett under femårsperioden avseende en del av sanktionsavgiften. Det som preskriberas är den del av avgiften som ännu inte har drivits in (se prop. 2016/17:22 s. 255–257).

9 Sekretess

Promemorians förslag: Sekretess ska gälla i en statlig myndighets verksamhet enligt DORA-förordningen för

1. uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, om det kan antas att denne lider skada om uppgiften röjs, och
2. uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser.

För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Tystnadsplikten för uppgifter som förekommer i statlig myndighets verksamhet enligt DORA-förordningen ska ges företräde framför meddelarfriheten när det gäller uppgifter om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser.

Skälen för promemorians förslag

DORA-förordningen

I DORA-förordningen anges att all konfidentiell information som är föremål för mottagande, utbyte eller förmedling enligt förordningen ska omfattas av särskilda villkor för tystnadsplikt (artikel 55.1). Med detta avses att tystnadsplikt ska tillämpas för alla personer som arbetar eller har arbetat för de behöriga myndigheterna enligt förordningen, eller för en myndighet eller ett marknadsföretag eller en fysisk eller juridisk person som dessa behöriga myndigheter har delegerat sina befogenheter till, inbegripet revisorer och experter som arbetar på den behöriga myndighetens uppdrag (artikel 55.2). Information som omfattas av tystnadsplikt, inbegripet informationsutbyte mellan behöriga myndigheter enligt förordningen och behöriga myndigheter som har utsetts eller inrättats i enlighet med NIS2-direktivet, får inte lämnas ut till någon annan person eller myndighet utom när detta föreskrivs i unionsrätt eller nationell rätt (artikel 55.3). All information som utbyts mellan de behöriga myndigheterna enligt DORA-förordningen och som avser affärs- eller driftsförhållanden och andra ekonomiska eller personliga förhållanden ska anses vara konfidentiell och omfattas av tystnadsplikt, utom när den behöriga myndigheten vid den tidpunkt då informationen lämnas anger att informationen får

lämnas ut eller om det är nödvändigt att lämna ut informationen i samband med rättsliga förfaranden (artikel 55.4).

Offentlighets- och sekretesslagen

Bestämmelser om tystnadsplikt i det allmännas verksamhet finns i offentlighets- och sekretesslagen. Sekretess gäller enligt den lagen för vissa uppgifter i en statlig myndighets verksamhet som består i tillståndsgivning eller tillsyn med avseende på bank- och kreditväsendet, värdepappersmarknaden eller försäkringsväsendet (30 kap. 4 §). Det som skyddas av sekretess är bl.a. uppgifter om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, om det kan antas att denne lider skada om uppgiften röjs. Sekretess gäller också för uppgifter om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser. För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Bestämmelsen i offentlighets- och sekretesslagen (30 kap. 4 §) bör uppfylla DORA-förordningens krav på vad som ska skyddas, dvs. information som utbyts mellan de behöriga myndigheterna enligt förordningen och som avser affärs- eller driftsförhållanden och andra ekonomiska eller personliga förhållanden. Sekretessen är dock begränsad till uppgifter som förekommer vid tillståndsgivning eller tillsyn med avseende på bank- och kreditväsendet, värdepappersmarknaden eller försäkringsväsendet. Även om ordet tillsyn inte ska ges en alltför snäv tolkning (se prop. 1979/80:2 Del A s. 233), bör det inte omfatta all verksamhet som svenska myndigheter ska bedriva med stöd av DORA-förordningen och den lag som föreslås. Verksamhet som rör incidentrapportering och testning (se artikel 19 och 26 i förordningen och avsnitt 5.6 och 6) är skilda från tillsyn och bör i och med det inte omfattas av bestämmelsen. Inte heller omfattar bestämmelsen all verksamhet som bedrivs av finansiella entiteter. Så är t.ex. fallet för pensionsstiftelser som inte bedriver verksamhet som är hänförlig till något av bank- och kreditväsendet, värdepappersmarknaden eller försäkringsväsendet (30 kap. 4 § jämförd med 4 b § offentlighets- och sekretesslagen).

Sekretess gäller även för uppgifter som en myndighet får från ett utländskt organ på grund av en bindande EU-rättsakt, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Motsvarande sekretess gäller för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt (15 kap. 1 a § offentlighets- och sekretesslagen). Denna sekretess bör omfatta det samarbete som enligt DORA-förordningen ska ske mellan Finansinspektionen och Riksbanken och de europeiska tillsynsmyndigheterna EBA, Esma och Eiopa (se avsnitt 11). Denna sekretess är dock begränsad till uppgifter som kommer till svenska myndigheter från utländska organ eller uppgifter som svenska myndigheter inhämtar för att lämna vidare till utländska organ. Inte heller denna bestämmelse bör fullt ut omfatta den verksamhet som de svenska myndigheterna, Finansinspektionen och Riksbanken, ska bedriva enligt DORA-förordningen. De svenska myndigheterna kommer att behöva inhämta och hantera en stor mängd uppgifter i andra syften än att

lämna vidare uppgifterna till utländska organ, t.ex. inom tillsyns- och testverksamheten som i första hand kommer ske utan inblandning av de europeiska tillsynsmyndigheterna.

En ny bestämmelse om sekretess – föremål och räckvidd

För att fullt ut uppfylla kraven i DORA-förordningen (artikel 55.4) bör det införas en särskild bestämmelse om sekretess.

Frågan om sekretess ska gälla eller inte och sekretessens räckvidd och styrka är alltid en avvägning mellan olika intressen och lagstiftning bör inte införas som onödigt avlägsnar sig från den grundlagsfästa offentlighetsprincipen. Som en genomgående princip i svensk rätt gäller därför att sekretess bör gälla endast i den omfattning som är nödvändigt för att skydda det intresse som ligger till grund för bestämmelsen.

De uppgifter som behöver skyddas av sekretess enligt DORA-förordningen bör i huvudsak vara samma uppgifter som förekommer vid tillståndsgivning och tillsyn på finansmarknadsområdet och då skyddas av 30 kap. 4 § offentlighets- och sekretesslagen. Det bör därmed i båda fallen röra sig om uppgifter dels om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, dels om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser. I båda fallen rör det sig om känsliga uppgifter som om de sprids kan leda till allvarlig skada för både företagen och det finansiella systemet. Uppgifter som rör verksamhet enligt DORA-förordningen är dessutom av särskilt känslig karaktär då de specifikt rör företagets digitala motståndskraft och i och med det förmågan att upprätthålla driften av verksamheten och utan avbrott tillhandahålla finansiella tjänster. Ett företag bör som utgångspunkt lida skada av att denna typ av uppgifter lämnas ut. Sekretess bör därför gälla för uppgifter som förekommer i en statlig myndighets verksamhet enligt DORA-förordningen. Om sekretessen gäller för statlig myndighets verksamhet kommer den att gälla oavsett om uppgiften förekommer vid verksamhet hos Finansinspektionen eller hos Riksbanken som båda ges uppgifter enligt DORA-förordningen (se avsnitt 6 och 7). Genom att sekretess bara bör gälla verksamhet enligt förordningen blir sekretessen inte mer omfattande än vad som krävs enligt förordningen.

Sekretessens styrka

Utformningen av en sekretessbestämmelse ska vara ett resultat av en avvägning mellan insyns- och sekretessintressena (jfr prop. 1979/80:2 Del A s. 75–76). Rätten att ta del av allmänna handlingar är en medborgerlig rättighet som utgör en viktig del av vårt demokratiska statsskick. Syftet med denna rätt är, som det kommer till uttryck i 2 kap. 1 § tryckfrihetsförordningen, att främja ett fritt meningsutbyte och en allsidig upplysning. Genom tillgången till allmänna handlingar underlättas en fri åsiktsbildning, en fri och på fakta grundad debatt i skilda samhällsfrågor liksom den medborgerliga kontrollen av den offentliga maktutövningen.

För det allmänna förtroendet för myndigheterna är det viktigt att information som rör hur myndigheterna agerar för att säkerställa att de finansiella entiteterna uppfyller kraven enligt DORA-förordningen, och i och med det utan avbrott kan erbjuda konsumenter säkra finansiella

tjänster, kan offentliggöras i så stor utsträckning som möjligt. Ett bristande förtroende kan både medföra svårigheter som annars inte skulle ha uppstått och försvåra myndigheternas arbete. Mot detta ska emellertid ställas de potentiella konsekvenser som kan komma av ett offentliggörande av känsliga uppgifter för ett företag.

Som anges ovan bör det vara samma känsliga uppgifter som förekommer vid en myndighets verksamhet enligt DORA-förordningen som vid en myndighets tillstånds- och tillsynsverksamhet. Behovet av skydd bör vara detsamma oavsett i vilken verksamhet som uppgifterna förekommer. En bestämmelse om sekretess för verksamhet enligt DORA-förordningen bör därför utformas efter förebild av den sekretess som gäller vid tillsyn och tillstånd på finansmarknadsområdet (30 kap. 4 § offentlighets- och sekretesslagen). Detta underlättar hanteringen då sekretessen så långt möjligt blir densamma oavsett om en uppgift förekommer i myndighetens tillstånds- och tillsynsverksamhet eller i verksamhet som följer av DORA-förordningen.

Enligt bestämmelsen om sekretess för tillstånd och tillsyn (30 kap. 4 § offentlighets- och sekretesslagen) gäller sekretess dels för uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, dels för uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser. Sekretessen enligt den nya bestämmelsen för verksamhet enligt DORA-förordningen bör ges denna omfattning.

Vid tillstånds- och tillsynsverksamhet gäller ett rakt skaderekvisit för uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, dvs. en presumtion för offentlighet om uppgiften förekommer i sådan verksamhet (30 kap. 4 § första stycket 1 offentlighets- och sekretesslagen). I enlighet med vad som ovan anförts bör detta också gälla enligt den nya bestämmelsen.

När det gäller tredjemansuppgifter, dvs uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser, är det svårt att få en överblick över vilka uppgifter som är känsliga och vilka som inte är det. Vanligtvis är tredjemannen en enskild som står i affärsförbindelse med ett företag som omfattas av DORA-förordningen utan att själv omfattas av förordningen och dess krav. Tredjemannens verksamhet bör som huvudregel vara specialiserad och i första hand riktad mot företag. Det rör sig således, till skillnad mot den som myndighetens verksamhet avser, inte om en verksamhet där konsumenter erbjuds finansiella tjänster. Intresset för allmänheten att ta del av denna typ av uppgifter bör vara mer begränsat. I dessa fall finns det därför skäl för ett starkare skydd. Liksom gäller för tredjemansuppgifter i tillstånds- och tillsynsverksamhet (30 kap. 4 § första stycket 2 offentlighets- och sekretesslagen), bör det enligt den nya bestämmelsen inte finnas något skaderekvisit för sådana uppgifter, dvs. en absolut sekretess.

Sekretesstid

För uppgift i en allmän handling gäller sekretessen vid tillstånds- och tillsynsverksamhet på finansmarknadsområdet i högst tjugo år (30 kap. 4 §

andra stycket offentlighets- och sekretesslagen). Detta bör också gälla enligt den sekretess som nu föreslås.

Utlämnande utan hinder av sekretess

Oavsett den sekretess som nu föreslås bör ett utlämnande kunna ske i vissa fall. Detta gäller för att Finansinspektionen och Riksbanken ska kunna fullgöra uppgifter enligt DORA-förordningen eller kompletteringslagen. I avsnitt 6.2 föreslås en särskild bestämmelse om uppgiftsskyldighet mellan Finansinspektionen och Riksbanken som ger myndigheterna möjlighet att lämna ut uppgifter till varandra. Uppgiftsskyldigheten medför att sekretessen bryts med stöd av bestämmelsen i 10 kap. 28 § första stycket offentlighets- och sekretesslagen. När det gäller svenska myndigheters samarbete med utländska myndigheter kan uppgifter lämnas ut med stöd av 8 kap. 3 § offentlighets- och sekretesslagen (se avsnitt 11). I vissa fall bör ett utlämnande kunna ske som ett nödvändigt utlämnande (10 kap. 2 § offentlighets- och sekretesslagen) eller med stöd av generalklausulen (10 kap. 27 § offentlighets- och sekretesslagen) Det har hittills inte förekommit att det krävs ytterligare sekretessbrytande bestämmelser för Finansinspektionens och Riksbankens verksamhet enligt DORA-förordningen och kompletteringslagen.

Rätten att meddela och offentliggöra uppgifter

I enlighet med vad som gäller för tillstånds- och tillsynsverksamhet på finansmarknadsområdet (30 kap. 30 § första stycket offentlighets- och sekretesslagen) bör den tystnadsplikt som följer av den nya bestämmelsen inte inskränka rätten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter när det gäller uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser.

När det gäller tredjemansuppgifter föreslås ovan en absolut sekretess enligt den nya bestämmelsen. Detta starkare skydd bör av samma skäl som anförs för sekretessen gälla även i fråga om tystnadsplikt. Därmed bör, som gäller för motsvarande uppgifter enligt 30 kap 4 § offentlighets- och sekretesslagen, den tystnadsplikt som följer av den nya bestämmelsen inskränka rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

10 Offentliggöranden av beslut

Promemorians bedömning: Kraven i DORA-förordningen om att den behöriga myndigheten ska offentliggöra beslut om administrativa sanktioner kräver inte någon lagstiftningsåtgärd.

Skälen för promemorians bedömning: I DORA-förordningen finns det särskilda bestämmelser om offentliggörande av beslut. De behöriga myndigheterna ska offentliggöra alla beslut om att ålägga en administrativ

sanktion som inte kan överklagas efter det att sanktionens adressat har underrättats om beslutet. Detta ska ske utan dröjsmål och på myndighetens officiella webbplats (artikel 54.1). Ett offentliggörande ska innehålla information om överträdelsens typ och art, de ansvariga personernas identitet och ålagda sanktioner (artikel 54.2). I vissa fall kan den behöriga myndigheten skjuta upp offentliggörandet, under en period offentliggöra ett anonymiserat beslut eller helt avstå från ett offentliggörande. Så är t.ex. fallet om myndigheten anser att ett offentliggörande av de juridiska personernas identitet eller av de fysiska personernas identitet och personuppgifter är oproportionellt, kan hota stabiliteten på de finansiella marknaderna, kan äventyra en pågående brottsutredning eller kan vålla den berörda personen oproportionell skada (artikel 54.3). I DORA-förordningen finns också bestämmelser om hur den behöriga myndigheten ska agera om ett beslut om administrativ sanktion överklagas (artikel 54.5) och att offentliggörandet bara ska ske så länge det är nödvändigt och inte längre än fem år (artikel 54.6).

Det som anges i DORA-förordningen om offentliggörande av beslut är formulerat som en skyldighet för de behöriga myndigheterna och får därmed anses vara direkt tillämpligt för dem. Det är därför inte nödvändigt att vidta några lagstiftningsåtgärder för att det som anges i förordningen ska gälla för Finansinspektionen (den svenska behöriga myndigheten, se avsnitt 5.1).

En fråga som uppkommer är emellertid om ett sådant offentliggörande som beskrivs i förordningen är förenligt med bestämmelserna om sekretess i offentlighets- och sekretesslagen. I avsnitt 9 föreslås en ny bestämmelse om sekretess i en statlig myndighets verksamhet enligt DORA-förordningen. Denna sekretess bör gälla för de beslut som Finansinspektionen enligt förordningen ska offentliggöra (se artikel 54 i förordningen). Sekretess gäller därmed för uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, dvs. en finansiell entitet, om det kan antas att denne lider skada om uppgiften röjs. Presumtionen är att Finansinspektionen får offentliggöra uppgifter om åtgärder eller sanktioner men att sekretess råder om det kan antas att den berörde lider skada om uppgiften röjs.

DORA-förordningen förutsätter ett offentliggörande av beslut om att påföra en administrativ sanktion, men tillåter samtidigt att besluten offentliggörs anonymiserat (artikel 54.3 b). Det finns också en möjlighet att i vissa fall inte alls offentliggöra beslutet (artikel 54.3 c) eller skjuta upp offentliggörandet (artikel 54.3 a). Motsvarande bestämmelser om offentliggöranden finns bl.a. i kapitaltäckningsdirektivet och Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012. I lagstiftningsärenden med anledning av de bestämmelserna gjordes bedömningen att den sekretess som föreskrivs i offentlighets- och sekretesslagen inte utgör hinder för att offentliggöra beslut (se prop. 2013/14:228 s. 233–234. och prop. 2015/16:10 s. 244–245). Det finns inte anledning att göra någon annan bedömning när det gäller förhållandet mellan den sekretess som nu föreslås (avsnitt 9) och bestämmelserna om offentliggörande i DORA-förordningen.

Eftersom kravet på offentliggörande av beslut också gäller beslut som rör fysiska personer uppkommer även frågan om gällande regelverk för hantering av personuppgifter hindrar att kraven i DORA-förordningen uppfylls. I DORA-förordningen anges att personuppgifterna ska behandlas i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), i det följande benämnt EU:s dataskyddsförordning, eller Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG beroende på vilken förordning som är tillämplig (artikel 56 första stycket). Möjligheten att offentliggöra ett beslut i anonymiserad form (artikel 54.3 b) innebär i sig ett skydd för personuppgifter. Som ansetts i tidigare lagstiftningsärende (prop. 2020/21:206 s. 92), bör gällande regelverk för hantering av personuppgifter inte innebära något hinder för kraven på offentliggörande av beslut enligt DORA-förordningen.

11 Samarbete mellan myndigheter

Promemorians bedömning: Det informationsutbyte som enligt DORA-förordningen ska ske mellan myndigheter kan komma till stånd inom ramen för gällande svensk rätt.

Skälen för promemorians bedömning: I DORA-förordningen finns det flera bestämmelser om samarbete både mellan behöriga myndigheter och mellan behöriga myndigheter och europeiska myndigheter och andra organ. Till exempel ska de behöriga myndigheterna och den ledande tillsynsmyndigheten (någon av EBA, Esma eller Eiopa) ömsesidigt utbyta all relevant information om kritiska tredjepartsleverantörer av IKT-tjänster som är nödvändig för att de ska kunna utföra sina respektive uppgifter enligt förordningen (artikel 48.2 i DORA-förordningen). De europeiska tillsynsmyndigheterna EBA, Esma och Eiopa får, i samarbete med bl.a. behöriga myndigheter, inrätta mekanismer för att möjliggöra utbyte av effektiv praxis mellan olika finansiella sektorer för att öka situationsmedvetenheten och identifiera gemensamma sårbarheter och risker på it-området (artikel 49.1 första stycket). Vidare ska de behöriga myndigheterna, de europeiska tillsynsmyndigheterna och ECB nära samordna sin tillsyn för att identifiera och åtgärda överträdelser av förordningen, utarbeta och främja bästa praxis, underlätta samarbete, främja en konsekvent tolkning och tillhandahålla bedömningar över jurisdiktionsgränserna om det uppstår meningsskiljaktigheter (artikel 49.2).

Frågor om samarbete mellan olika myndigheter på finansmarknadsområdet, såväl nationella som europeiska, har berörts i flera lagstiftningsärenden. I propositionen Kompletterande bestämmelser till EU:s förord-

ning om faktablad för Priip-produkter (prop. 2016/17:78 s. 49) anfördes i huvudsak följande. Beträffande Finansinspektionens möjlighet att lämna ut uppgifter till utländska myndigheter kan det inledningsvis konstateras att det kan komma att handla om uppgifter som omfattas av sekretess (t.ex. 30 kap. 4 eller 6 § offentlighets- och sekretesslagen). En svensk myndighets möjlighet att lämna ut sekretessbelagda uppgifter till en utländsk myndighet regleras i 8 kap. 3 § offentlighets- och sekretesslagen. Uppgift som är sekretessbelagd enligt offentlighets- och sekretesslagen får inte lämnas ut till utländsk myndighet eller mellanfolklig organisation i andra fall än då utlämnandet sker i enlighet med föreskrift i lag eller förordning eller då uppgiften i motsvarande fall skulle få lämnas ut till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller mellanfolkliga organisationen. En bestämmelse i en EU-förordning är att jämställa med en bestämmelse i svensk lag eller förordning (jfr prop. 1998/99:18 s. 41 och prop. 1999/2000:126 s. 160 och 283).

Bestämmelserna i DORA-förordningen om informationsutbyte mellan myndigheter ger därmed, som konstaterats i flera tidigare lagstiftningsärenden för motsvarande bestämmelser, Finansinspektionen goda möjligheter att lämna ut handlingar och uppgifter till andra behöriga myndigheter och de europeiska tillsynsmyndigheterna (se prop. 2011/12:40 s. 20, prop. 2011/12:175 s. 31 och prop. 2012/13:72 s. 34). Det informationsutbyte mellan myndigheter som ska äga rum enligt DORA-förordningen kan därmed komma till stånd inom ramen för gällande svensk rätt.

För samarbetet mellan Finansinspektionen och Riksbanken, se avsnitt 6.2.

12 Informationsutbyte mellan finansiella entiteter

Promemorians bedömning: Kraven i DORA-förordningen om att finansiella entiteter ska få utbyta information med varandra kräver inte någon lagstiftningsåtgärd.

Skälen för promemorians bedömning: I DORA-förordningen finns bestämmelser om informationsutbyte mellan finansiella entiteter (artikel 45). Finansiella entiteter får utbyta information och underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, i den mån sådant utbyte av information och underrättelser

a) syftar till att förbättra finansiella entiteters digitala operativa motståndskraft, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra cyberhotens spridningsförmåga, varvid försvarsförmåga, metoder för att upptäcka hot, begränsningsstrategier eller åtgärds- och återställningsfaser stöds,

b) äger rum inom betrodda grupper av finansiella entiteter,

c) genomförs genom arrangemang för informationsutbyte som skyddar den potentiellt känsliga karaktären hos den information som utbyts och som styrs av uppföranderegler med full respekt för affärshemligheter, skydd av personuppgifter i enlighet med EU:s dataskyddsförordning och riktlinjer för konkurrenspolitiken.

I DORA-förordningen anges också att arrangemang för informationsutbyte ska innehålla fastställda villkor för deltagande och, när så är lämpligt, närmare uppgifter om offentliga myndigheters deltagande och på vilket sätt dessa kan knytas till arrangemangen för informationsutbyte, om deltagandet av tredjepartsleverantörer av IKT-tjänster och om operativa delar, inbegripet användningen av särskilda it-plattformar (artikel 45.2). Finansiella entiteter ska underrätta de behöriga myndigheterna om sitt deltagande i arrangemang för informationsutbyte, när deras medlemskap har godkänts eller, i tillämpliga fall, när medlemskapet upphör. Detta så snart det har skett (artikel 45.3).

Vidare framförs i skälen till förordningen (skäl 32) att IKT-risker blir alltmer komplexa och sofistikerade och därmed kommer effektiva åtgärder för att upptäcka och förebygga en IKT-risk att i hög grad vara beroende av ett regelbundet utbyte mellan finansiella entiteter av underrättelser om hot och sårbarhet. Informationsutbyte bidrar till att skapa ökad medvetenhet om cyberhot. Tveksamheter om vilken typ av information som kan delas med andra marknadsaktörer, eller med myndigheter som inte är tillsynsmyndigheter leder till att användbar information inte lämnas ut. Finansiella entiteter bör därför uppmuntras att sinsemellan utbyta information och underrättelser om cyberhot, och kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt bedöma, övervaka, försvara och reagera på cyberhot genom att delta i arrangemang för informationsutbyte. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av mekanismer för frivilligt informationsutbyte som, när de genomförs i betrodda miljöer, skulle hjälpa finanssektorn att förebygga och kollektivt reagera på cyberhot genom att snabbt begränsa spridningen av IKT-risk och hindra potentiella spridningseffekter genom de finansiella kanalerna.

Bestämmelserna i DORA-förordningen är, som utvecklas i avsnitt 5, direkt tillämpliga och ger i och med det finansiella entiteter möjlighet att dela information på det sätt som anges i förordningen även utan svenska lagstiftningsåtgärder. Information får dock inte delas på ett sätt som strider mot bestämmelser som begränsar möjligheterna att dela information, t.ex. bestämmelser om tystnadsplikt, personuppgiftsskydd eller konkurrens.

13 Hantering av personuppgifter

Promemorians bedömning: EU:s dataskyddsförordning, lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning utgör en tillräcklig reglering för den personuppgiftsbehandling som kommer att ske med anledning av DORA-förordningen och kompletteringslagen. Det behöver således inte införas någon ytterligare reglering om denna behandling.

Skälen för promemorians bedömning: I DORA-förordningen anges att de europeiska tillsynsmyndigheterna och de behöriga myndigheterna endast får behandla personuppgifter om det är nödvändigt för att de ska kunna fullgöra sina respektive skyldigheter och uppgifter enligt förordningen, särskilt när det gäller utredning, inspektion, begäran om information, kommunikation, offentliggörande, utvärdering, verifiering, bedömning och utarbetande av tillsynsplaner (artikel 56.1). Personuppgifterna ska då behandlas i enlighet med EU:s dataskyddsförordning eller förordning (EU) 2018/1725, beroende på vilken som är tillämplig. Utom där annat föreskrivs i andra sektorsspecifika rättsakter, ska de personuppgifter som hanteras lagras till dess att de tillämpliga tillsynsuppgifterna fullgjorts och under alla omständigheter i högst 15 år, utom i fall av pågående domstolsförfaranden som kräver ytterligare lagring av sådana uppgifter (artikel 56.2).

EU:s dataskyddsförordning utgör den generella regleringen för personuppgiftsbehandling inom EU. Förordningen kompletteras i Sverige av bl.a. lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Personuppgifter kommer att behandlas till följd av DORA-förordningen och kompletteringslagen, dvs den lag med kompletterande bestämmelser till DORA-förordningen som nu föreslås (se avsnitt 5.1). Detta gäller såväl hos enskilda (t.ex. finansiella entiteter och tredjepartsleverantörer av IKT-tjänster), som hos myndigheter, i första hand Finansinspektionen och Riksbanken.

För att få behandla personuppgifter krävs att det finns en rättslig grund för behandlingen (artikel 6.1 i EU:s dataskyddsförordning).

Finansiella entiteter och tredjepartsleverantörer av IKT-tjänster kan behöva behandla olika personuppgifter. I första hand rör det sig om namn och kontaktuppgifter för ledningspersoner för sådana aktörer. Det bör också kunna röra sig om motsvarande uppgifter till tredje part, t.ex. en uppdragstagare. När det gäller den behandling av personuppgifter som kan komma att ske hos finansiella entiteter och tredjepartsleverantörer av IKT-tjänster kommer behandlingen antingen att vara nödvändig för att de ska fullgöra en rättslig förpliktelse enligt DORA-förordningen eller kompletteringslagen (artikel 6.1 c i EU:s dataskyddsförordning) eller ske för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås till följd av den verksamhet som bedrivs (artikel 6.1 b i EU:s dataskyddsförordning). Den rättsliga grunden är, såvitt gäller att fullgöra en rättslig

förpliktelse, fastställd i DORA-förordningen och kompletteringslagen (jfr artikel 6.3 i EU:s dataskyddsförordning).

Finansinspektionen kan bl.a. behöva behandla personuppgifter som är nödvändiga för tillsynen över att förordningen följs, t.ex. namn och kontaktuppgifter till ledningspersoner hos finansiella entiteter och tredjepartsleverantörer av IKT-tjänster. Liknande personuppgifter bör även kunna förekomma i handlingar som inspektionen får del av inom ramen för sin tillsyn (se avsnitt 7.2 och 7.3). Inspektionen kan också komma att behandla personuppgifter inom ramen för samarbetet mellan olika myndigheter, t.ex. någon av de europeiska tillsynsmyndigheterna EBA, Esma och Eiopa (se avsnitt 11). Frågan om offentliggörande av personuppgifter i samband med Finansinspektionens beslut om administrativa sanktioner och åtgärder behandlas i avsnitt 10. När det gäller Finansinspektionens behandling av personuppgifter är den behandlingen nödvändig för att myndigheten ska kunna utföra sina uppgifter enligt DORA-förordningen och kompletteringslagen. Den rättsliga grunden för personuppgiftsbehandlingen är således att den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (artikel 6.1 e i EU:s dataskyddsförordning). Den rättsliga grunden är fastställd i DORA-förordningen och kompletteringslagen (jfr artikel 6.3 i EU:s dataskyddsförordning). Finansinspektionens ansvar för att utöva tillsyn och samarbeta med andra tillsynsmyndigheter, både nationella och europeiska, kan också ses som en rättslig förpliktelse (se artikel 6.1 c i EU:s dataskyddsförordning). Samma gäller för den testning som Riksbanken ska ansvara för enligt DORA-förordningen och kompletteringslagen (se avsnitt 6.1). Också i dessa fall är rättsliga grunden är fastställd i DORA-förordningen och kompletteringslagen (jfr artikel 6.3 i EU:s dataskyddsförordning).

Som nämns ovan kommer personuppgiftsbehandlingen med anledning av DORA-förordningen och kompletteringslagen i huvudsak att bestå av namn och kontaktuppgifter till ledningspersoner hos finansiella entiteter och tredjepartsleverantörer av IKT-tjänster eller uppdragstagare till sådana aktörer. Det bör inte bli aktuellt för vare sig enskilda eller myndigheter att behandla sådana särskilda kategorier av personuppgifter som avses i EU:s dataskyddsförordning (jfr artikel 9 i den förordningen). Risken för intrång i den personliga integriteten får därmed anses begränsad. Det eventuella integritetsintrång som behandlingen av personuppgifter innebär får anses stå i proportion till de behov som motiverar behandlingen. Sammanfattningsvis görs bedömningen att den personuppgiftsbehandling som förslagen ger upphov till är förenlig med EU:s dataskyddsförordning. Befintlig reglering på personuppgiftsområdet utgör tillräcklig reglering för den personuppgiftsbehandling som kommer med anledning av DORA-förordningen och kompletteringslagen.

14 Avgifter

14.1 Finansinspektionens verksamhet

Promemorians förslag: Finansiella entiteter som står under Finansinspektionens tillsyn ska med årliga avgifter bekosta inspektionens verksamhet enligt DORA-förordningen och kompletteringslagen.

Regeringen ska få meddela föreskrifter om avgifter.

Skälen för promemorians förslag: Finansinspektionen kommer att få ytterligare arbetsuppgifter i och med DORA-förordningen (se avsnitt 5.2). Finansinspektionens verksamhet kommer att bestå i tillsyn över att bestämmelserna i DORA-förordningen och kompletteringslagen följs. Det är också inspektionen som ska besluta om vilka finansiella entiteter som ska genomgå hotbildsstyrda penetrationstester och hur ofta (se avsnitt 6.1). Därtill ska inspektionen utföra flera uppgifter inom ramen för samarbetet med de europeiska tillsynsmyndigheterna och andra behöriga myndigheter (se avsnitt 11).

Med nya arbetsuppgifter följer vanligtvis ökade kostnader, som kräver finansiering. Finansinspektionens verksamhet finansieras i dag dels via anslag i statens budget, dels via avgifter för prövning av ärenden.

De företag som är att anse som finansiella entiteter enligt DORA-förordningen står i dag under tillsyn hos Finansinspektionen och betalar årliga avgifter till inspektionen enligt förordningen (2007:1135) om årliga avgifter för finansiering av Finansinspektionens verksamhet. Sådana avgifter ska stå i proportion till de kostnader som inspektionen har haft för tillsynen och övriga kostnader som inte finansieras på annat sätt. Dessa avgifter får Finansinspektionen inte disponera, utan de ska redovisas mot inkomsttitel på statens budget. De årliga avgifterna ska i princip motsvara de medel som årligen anvisas Finansinspektionen på statsbudgeten. För att finansiera Finansinspektionens verksamhet enligt DORA-förordningen och kompletteringslagen bör Finansinspektionen få ta ut årliga avgifter av de finansiella entiteter som står under Finansinspektionens tillsyn. Som gäller enligt andra lagar på finansmarknadsområdet (se tex. 23 kap. 12 § första stycket och 15 § 6 lagen om värdepappersmarknaden) bör regeringen få meddela föreskrifter om avgifterna.

14.2 Riksbankens verksamhet

Promemorians förslag: Riksbanken ska få ta ut avgifter från de finansiella entiteter som genomgår hotbildsstyrd penetrationstestning.

Riksbanken ska få meddela föreskrifter om avgifterna.

Skälen för promemorians förslag: Riksbankens kommer, liksom Finansinspektionen, att få nya uppgifter i och med DORA-förordningen. Ovan föreslås att Riksbanken ska samordna och övervaka utförandet av den hotbildsstyrda penetrationstestningen (se avsnitt 6.1). Detta innebär att Riksbanken ska delta i planeringen och genomförandet av testningen genom att bl.a. validera vilka delar inom den finansiella entiteten som ska

omfattas av testningen och säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i DORA-förordningen. Riksbanken ska även utfärda intyg om att ett test har utförts i enlighet med kraven i förordningen.

De nya uppgifterna, som utgör myndighetsutövning mot enskilda, kommer att innebära nya kostnader för Riksbanken.

Inom den finansiella sektorn finansieras myndighetsutövning mot enskilda vanligtvis genom avgifter. Detta gäller tex. Riksbankens verksamhet som rör referensvärden (1 kap. 12 § andra stycket lagen om Sveriges riksbank). Också Riksbankens verksamhet som rör hotbildsstyrda penetrationstester enligt DORA-förordningen bör finansieras genom avgifter. Riksbanken bör därför få ta ut avgifter av de finansiella entiteter som ska genomföra testerna. Som gäller för referensvärden bör Riksbanken få meddela föreskrifter om avgifterna (jfr 13 kap. 1 § 1 lagen om Sveriges riksbank).

15 Överklagande och beslut som ska gälla omedelbart

15.1 Överklagande och verkställighet av Finansinspektionens beslut

Promemorians förslag: Finansinspektionens beslut om sanktionsföreläggande enligt lagen om tjänstepensionsföretag och kompletteringslagen ska inte få överklagas. Andra beslut som Finansinspektionen meddelar enligt kompletteringslagen och DORA-förordningen ska få överklagas till allmän förvaltningsdomstol. Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Finansinspektionen ska få bestämma att beslut om förbud, föreläggande och återkallelse enligt kompletteringslagen ska gälla omedelbart.

Promemorians bedömning: DORA-förordningens krav om att den behöriga myndigheten ska motivera sina beslut tillgodoses av gällande svensk rätt.

Skälen för promemorians förslag och bedömning

Motiveringsskyldighet och överklagbarhet för Finansinspektionens beslut

Enligt DORA-förordningen ska alla beslut om att ålägga administrativa sanktioner eller avhjälpande åtgärder vara vederbörligen motiverade och kunna överklagas (artikel 50.6).

Allmänna bestämmelser om krav på motivering av beslut finns i förvaltningslagen (32 §). De förvaltningsbeslut som kan aktualiseras till följd av DORA-förordningen och den kompletterande lagstiftningen är t.ex. Finansinspektionens beslut om ingripanden genom administrativa sanktioner eller åtgärder. För sådana beslut gäller alltså redan enligt gällande rätt ett krav på motivering. Därför krävs det ingen lagstiftnings-

åtgärd med anledning av DORA-förordningens krav på motivering av vissa beslut.

Finansinspektionen kan ingripa mot vissa finansiella entiteter som åsidosätter sina skyldigheter enligt DORA-förordningen, med stöd av bestämmelser i de rörelselagar på finansmarknadsområdet som reglerar verksamheten (se avsnitt 8.2.1). De beslut som Finansinspektionen fattar till följd av ett sådant ingripande kan överklagas med stöd av bestämmelser i respektive lag (se t.ex. 26 kap. 1 § lagen om värdepappersmarknaden och 17 kap. 1 § lagen om bank- och finansieringsrörelse). Möjligheten att överklaga sådana beslut följer således redan av rörelselagarna och kräver därför inte någon lagstiftningsåtgärd med anledning av DORA-förordningen.

Däremot behöver det införas bestämmelser om överklagande av de beslut som Finansinspektionen fattar med stöd av kompletteringslagen. Allmänt inom finansmarknadsområdet gäller att beslut av Finansinspektionen får överklagas och prövas av allmän förvaltningsdomstol, med krav på prövningstillstånd vid överklagande till kammarrätten. Detta bör även gälla för Finansinspektionens beslut enligt kompletteringslagen. En bestämmelse om rätt till överklagande av Finansinspektionens beslut bör införas i den lagen efter förebild av motsvarande bestämmelser i andra lagar på finansmarknadsområdet (se t.ex. 26 kap. 1 § lagen om värdepappersmarknaden).

Ett beslut om sanktionsföreläggande bör inte få överklagas

I avsnitt 8.3 föreslås att Finansinspektionens ingripande mot en fysisk person för en överträdelse av DORA-förordningen som en finansiell entitet har gjort sig skyldig till ska ske genom sanktionsföreläggande.

Ett sanktionsföreläggande innebär att den fysiska personen föreläggs att inom en viss tid godkänna ett ingripande som är bestämt till tid eller belopp. När föreläggandet har godkänts, gäller det som ett domstolsavgörande som fått laga kraft. Om ett sanktionsföreläggande inte har godkänts inom angiven tid, får Finansinspektionen ansöka hos domstol om att en sanktion ska beslutas. Ett beslut om sanktionsföreläggande är således i sig ett förberedande beslut. Ett överklagande av ett sådant beslut skulle kunna fördröja Finansinspektionens utredning i onödan. Ett förberedande beslut förhindrar inte heller en senare slutlig prövning i domstol.

Enligt andra lagar på finansmarknadsområdet där det finns möjlighet för Finansinspektionen att ingripa genom sanktionsföreläggande gäller att ett beslut om sanktionsföreläggande inte får överklagas (se t.ex. 26 kap. 1 § första stycket lagen om värdepappersmarknaden, 6 kap. 1 § första stycket lagen med kompletterande bestämmelser till EU:s marknadsmissbruksförordning och 10 kap. 1 § första stycket lagen om försäkringsdistribution). På samma sätt bör ett beslut om sanktionsföreläggande som Finansinspektionen fattar med stöd av lagen om tjänstepensionsföretag och den nya kompletteringslagen inte heller få överklagas. En fysisk person som har fått ett felaktigt sanktionsföreläggande meddelat mot sig, har möjlighet att ansöka om resning (se prop. 2016/17:162 s. 573–574).

Vissa beslut ska kunna gälla omedelbart

I rörelselagar och flera andra lagar på finansmarknadsområdet finns det bestämmelser om att Finansinspektionen får bestämma att ett beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart (se t.ex. 26 kap. 1 § fjärde stycket lagen om värdepappersmarknaden, 5 kap. 2 § lagen med kompletterande bestämmelser till EU:s förordning om referensvärden och 4 kap. 2 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering). Bestämmelser om att en myndighet i vissa fall kan verkställa ett beslut omedelbart om ett väsentligt allmänt eller enskilt intresse kräver det finns numera även i förvaltningslagen (35 §). Förvaltningslagen är subsidiär, vilket innebär att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från förvaltningslagen, tillämpas den bestämmelsen (4 §).

Omedelbar verkställighet är av särskild betydelse vid vissa typer av ingripanden eftersom en aktör annars kan fortsätta agera på ett sätt som Finansinspektionen anser strider mot kompletteringslagen eller DORA-förordningen. Det gäller framför allt vid beslut om att inom viss tid vidta en viss åtgärd eller upphöra med ett visst agerande eller om att en fysisk person under en viss tid inte får vara styrelseledamot eller verkställande direktör, eller ersättare för någon av dem, i en finansiell entitet. Också vid beslut om återkallelse av tillstånd kan omedelbar verkställighet vara särskild betydelse. Finansinspektionen bör därför få bestämma att dessa beslut ska gälla omedelbart. En bestämmelse om det bör införas i kompletteringslagen. Vid ingripanden mot de finansiella entiteter som omfattas av en rörelselag blir bestämmelserna i rörelselagarna om omedelbar verkställighet tillämpliga på Finansinspektionens beslut om förbud, föreläggande och återkallelse.

15.2 Överklagande av Riksbankens beslut

Promemorians förslag: Riksbankens beslut om föreläggande enligt kompletteringslagen och om utfärdande av intyg enligt artikel 26.7 i DORA-förordningen ska få överklagas till allmän förvaltningsdomstol.

Andra beslut som Riksbanken fattar med stöd av kompletteringslagen ska inte få överklagas.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Skälen för promemorians förslag: I avsnitt 6.1 föreslås Riksbanken få i uppgift att samordna och övervaka hotbildstyrda penetrationstester och utfärda intyg som bekräftar att testet genomförts i enlighet med kraven i DORA-förordningen. Riksbanken ska få förelägga finansiella entiteter att lämna de uppgifter som är nödvändiga för Riksbankens verksamhet med testning. Sådana föreläggandena ska även få förenas med vite (avsnitt 6.3).

Som vanligtvis gäller för en myndighets beslut som rör enskilda bör Riksbankens beslut att meddela förelägganden få överklagas till allmän förvaltningsdomstol. Detsamma gäller Riksbankens beslut om utfärdande av intyg enligt artikel 26.7 i förordningen. Det kan t.ex. avse ett beslut att inte utfärda ett intyg. Det bör även krävas prövningstillstånd vid överklagande till kammarrätten.

Under testprocessen torde Riksbanken även behöva fatta flera olika beslut. Riksbanken ska bl.a. säkerställa att den finansiella entiteten tillämpar den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen. Enligt DORA-förordningen ska Riksbanken också validera vilka kritiska eller viktiga funktioner som ska omfattas av testningen (artikel 26.2 tredje stycket) och säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i förordningen (artikel 27). Ett överklagande av dessa beslut skulle kunna fördröja testprocessen i onödan och bör därför inte få överklagas. Ett beslut kan likväl, om än i ett senare skede, komma att prövas av domstol. Detta antingen genom att Riksbanken fattar ett beslut om att inte utfärda ett intyg om att testningen har utförts i enlighet med kraven i DORA-förordningen. Andra beslut än de som avser förelägganden eller utfärdande av intyg bör därför inte få överklagas.

16 EU-direktiv på finansmarknadsområdet som ändras med anledning av DORA-förordningen

Promemorians förslag: Följande svenska bestämmelser ska ändras med anledning av ändringar i UCITS-direktivet, Solvens II-direktivet, AIFM-direktivet, kapitaltäckningsdirektivet, MiFID II, andra betaltjänstdirektivet och andra tjänstepensionsdirektivet:

– Bestämmelserna i lagen om värdepappersfonder om krav på organisation av verksamheten.

– Bestämmelsen i försäkringsrörelselagen om kontinuitet i verksamheten.

– Bestämmelsen i lagen om förvaltare av alternativa investeringsfonder om organisatoriska krav.

– Bestämmelsen i lagen om bank- och finansieringsrörelse om riskhantering.

– Bestämmelserna i lagen om värdepappersmarknaden om värdepappersbolags riskhantering, om värdepappersinstituts interna riktlinjer, rutiner och system, om krav för att värdepappersinstitut ska få bedriva algoritmisk handel och om allmänna verksamhetskrav för börser.

– Bestämmelserna i lagen om betaltjänster om betaltjänstleverantörers hantering av operativa risker.

– Bestämmelserna i lagen om tjänstepensionsföretag och lagen om tryggande av pensionsutfästelse m.m. om krav på kontinuitet i verksamheten.

Promemorians bedömning: Följande ändringar i EU-rättsliga bestämmelser tillgodoses av gällande svensk rätt och kräver inga lagstiftningsåtgärder:

– Ändringarna i kapitaltäckningsdirektivet om att de behöriga myndigheterna ska ha alla de informationsinsamlings- och undersökningsbefogenheter som myndigheterna behöver för att utöva sina

funktioner och om att de behöriga myndigheterna inom tillsynen ska utvärdera de risker som påvisats vid testning av digital operativ motståndskraft.

– Ändringarna i krishanteringsdirektivet om vad en återhämtningsplan ska innehålla och vilka uppgifter som resolutionsmyndigheter får begära in från institut för utarbetande och uppdatering av resolutionsplaner.

– Ändringarna i betaltjänstdirektivet om att direktivet inte är tillämpligt på tekniska stödtjänster och om utkontraktering av viktiga operativa funktioner.

Ändringar i EU-rättsliga bestämmelser som inte riktar sig till medlemsstaterna kräver inte några lagstiftningsåtgärder.

Skälen för promemorians förslag och bedömning

Ändringar i EU-direktiv på finansmarknadsområdet

Tillsammans med DORA-förordningen har Europaparlamentet och rådet beslutat om vissa ändringar i flera direktiv på finansmarknadsområdet. Genom ändringsdirektivet görs ändringar i:

– Europaparlamentet och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag), i det följande benämnt UCITS-direktivet.

– Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet, i det följande benämnt Solvens II-direktivet.

– Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010, i det följande benämnt AIFM-direktivet.

– kapitaltäckningsdirektivet.

– Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012, i det följande benämnt krishanteringsdirektivet.

– MiFID II,

– andra betaltjänstdirektivet.

– Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut, i det följande benämnt andra tjänstepensionsdirektivet.

Nedan behandlas vilken typ av ändringar det rör sig om i de olika EU-direktiven och behovet av lagstiftningsåtgärder.

Ändringar som inte riktar sig till medlemsstaterna

Flera ändringar i EU-direktiven rör bestämmelser som inte riktar sig till de enskilda medlemsstaterna. Detta gäller ändringarna i artikel 12.3 i UCITS-direktivet, artikel 50.1 i Solvens II-direktivet, artikel 18.2 i AIFM-direktivet, artikel 10.9 i krishanteringsdirektivet, artikel 17.7 och 48.12 i MiFID II och artikel 98.5 i andra betaltjänstdirektivet. Dessa ändringar kräver inte några lagstiftningsåtgärder.

Ändringar som kräver lagstiftningsåtgärder

En del ändringar i EU-direktiven kräver justeringar av de svenska bestämmelser som genomför direktiven. I huvudsak rör det bestämmelser om företagens riskhantering och att företagen framöver också ska uppfylla kraven i DORA-förordningen.

När det gäller fondbolag bör det förtydligas att ett fondbolags rutiner för drift och förvaltning av informationssystem ska uppfylla kraven i DORA-förordningen (2 kap. 17 § första stycket 3 lagen om värdepappersfonder). Motsvarande förtydligande bör göras för AIF-förvaltare (8 kap. 2 § första stycket 2 lagen om förvaltare av alternativa investeringsfonder).

För försäkringsföretag bör det förtydligas att företagets nätverks- och informationssystem ska uppfylla kraven i DORA-förordningen (10 kap. 3 § första stycket försäkringsrörelselagen). Också för kreditinstitut och vissa värdepappersbolag bör det förtydligas att deras nätverks- och informationssystem ska uppfylla kraven i DORA-förordningen (6 kap. 2 § första stycket lagen om bank- och finansieringsrörelse se även 8 kap. 1 c §lagen om värdepappersmarknaden).

Det bör även göras vissa förtydliganden för värdepappersinstitut. Ett värdepappersinstitut bör ha särskilda informations- och kommunikationstekniska system, vilka ska inrättas och förvaltas i enlighet det som anges i DORA-förordningen (8 kap. 10 § första stycket i lagen om värdepappersmarknaden). Ett värdepappersinstitut bör också ha sunda skyddsmekanismer för att, i enlighet med kraven i DORA-förordningen, säkerställa skyddet och autentiseringen vid informationsöverföring och för att minimera risken för dataförvanskning och obehörig åtkomst till informationen (8 kap. 10 § andra stycket lagen om värdepappersmarknaden). Värdepappersinstitut som bedriver algoritmisk handel bör ha system och riskkontroller som säkerställer att institutets handelssystem är motståndskraftiga och har tillräcklig kapacitet i enlighet med kraven i DORA-förordningen. Ett sådant värdepappersinstitutet bör också ha effektiva arrangemang för kontinuerlig drift av verksamheten för att hantera driftavbrott i sina handelssystem, inbegripet en informations- och kommunikationstekniks-kontinuitetspolicy och sådana kontinuitetsplaner samt därmed relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik som inrättas i enlighet med kraven i DORA-förordningen och ska se till att systemen är fullt testade och lämpligt övervakade för att säkerställa att de uppfyller kraven i förordningen (8 kap. 23 § första och tredje styckena lagen om värdepappersmarknaden).

För börser bör det förtydligas att arbetet med att identifiera och hantera de risker som kan uppstå i verksamheten också ska gälla informations- och kommunikationsteknikrisker i enlighet kraven i DORA-förordningen (13 kap. 1 § tredje stycket 1 lagen om värdepappersmarknaden). De till-

kommande kraven enligt DORA-förordningen gör att de särskilda kraven om att en börs ska vara utrustad så att systemets tekniska operationer hanteras korrekt och ha vidtagit effektiva kompletterande åtgärder för att hantera riskerna för systemavbrott är överflödiga (13 kap. 1 § tredje stycket 2 lagen om värdepappersmarknaden). Vidare bör det förtydligas att en börs ska inrätta och upprätthålla en operativ motståndskraft, i enlighet med kraven i DORA-förordningen, för att säkerställa att handelssystemen är motståndskraftiga, har tillräcklig kapacitet för att kunna hantera svåra påfrestningar på marknaden i fråga om order- och meddelandevolymer, kan upprätthålla ordnad handel vid förhållanden med påfrestningar på marknaden, är fullständigt testade och garanterar kontinuitet i verksamheten vid eventuella driftavbrott i handelssystemet. För kontinuiteten inbegriper detta en IKT-kontinuitetspolicy och IKT-planer samt IKT-relaterade åtgärds- och återställningsplaner i enlighet med DORA-förordningen (13 kap. 1 a § lagen om värdepappersmarknaden). När det gäller systemen och arrangemangen för att säkerställa att algoritmisk handel inte skapar eller bidrar till otillbörliga marknadsförhållanden bör det förtydligas att kraven om tester och miljöer för att underlätta tester ska gälla i enlighet med kraven i DORA-förordningen (13 kap. 1 d § lagen om värdepappersmarknaden).

Gällande betaltjänstleverantörer som omfattas av DORA-förordningen bör det förtydligas att de ska uppfylla dels kraven enligt lagen om betaltjänster, dels de tillkommande kraven enligt DORA-förordningen (5 b kap. 1 § lagen om betaltjänster). Dessa betaltjänstleverantörer bör dock bara incidentrapportera enligt DORA-regelverket (5 b kap. 2 § samma lag, se även artikel 19 i DORA-förordningen).

För tjänstepensionsföretag och pensionsstiftelser bör det förtydligas att de, i egenskap av tjänstepensionsinstitut, ska ha de nätverks- och informationssystem som följer av DORA-förordningen (9 kap. 2 § lagen om tjänstepensionsföretag och 16 g § lagen om tryggande av pensionsutfästelse m.m.).

Ändringar på annan nivå än lag

I några fall har bestämmelserna i EU-direktiven som ändras genom ändringsdirektivet genomförts i föreskrifter. Detta gäller artikel 85.2 i kapitaltäckningsdirektivet om krav på beredskaps- och kontinuitetspolicyer samt beredskaps- och kontinuitetsplaner (se prop. 2013/14:228 s. 642), artikel 10.7 och bilaga avsnitt C i krishanteringsdirektivet om vad en resolutionsplan ska innehålla och vilka omständigheter som ska läggas till grund för resolutionsmyndighetens prövning av en resolutionsplan (se prop. 2015/16:5 s. 237–240) och artikel 5.1 i andra betaltjänstdirektivet om hur en betaltjänstleverantörs system för hantering av operativa risker och säkerhetsrisker ska utformas (se prop. 2017/18:77 s. 223–224 och 684). Ändringarna i dessa bestämmelser bör, som de ursprungliga bestämmelserna, genomföras i föreskrifter. Detta kan ske med stöd av befintliga bemyndiganden (16 kap. 1 § 5 lagen om bank- och finansieringsrörelse, 29 kap. 2 § 1 lagen om resolution och 2 kap. 10 § lagen om betaltjänster).

Ändringar som ryms inom gällande svenska bestämmelser

Vissa ändringar som görs i de ursprungliga EU-direktiven är sådana att både äldre och ny lydelse ryms inom gällande svenska bestämmelser. Det krävs därför inte några lagstiftningsåtgärder för att uppfylla kraven enligt EU-rätten.

Detta gäller bestämmelserna i kapitaltäckningsdirektivet om

– att de behöriga myndigheterna ska ha alla de informationsinsamlings- och undersökningsbefogenheter som myndigheterna behöver för att utöva sina funktioner (artikel 65.3, se 13 kap. 6 § lagen om bank- och finansieringsrörelse, 23 kap. 2 och 3 §§ lagen om värdepappersmarknaden och 6 kap. 1 § lagen om särskild tillsyn över kreditinstitut och värdepappersbolag), och
– att de behöriga myndigheterna inom tillsynen ska utvärdera de risker som påvisats vid testning av digital operativ motståndskraft i enlighet med DORA-förordningen (artikel 97.1, se 9 § förordningen [2014:993] om särskild tillsyn och kapitalbuffertar).

Också bestämmelserna i krishanteringsdirektivet om vad en återhämtningsplan ska innehålla (bilaga avsnitt A 16, se 16 kap. 1 § 7 lagen om bank- och finansieringsrörelse, 5 kap. 2 § 9 förordningen (2004:329) om bank- och finansieringsrörelse och 3 § Finansinspektionens föreskrifter [FFFS 2016:6] om återhämtningsplaner, koncernåterhämtningsplaner och avtal om finansiellt stöd inom koncerner) och vilka uppgifter som resolutionsmyndigheter får begära från institut för utarbetande och uppdatering av resolutionsplaner (bilaga avsnitt B 14 och 14a, se 28 kap. 1 § lagen [2015:1016] om resolution) tillgodoses genom gällande rätt. Vidare gäller detta även bestämmelserna i andra betaltjänstdirektivet om att direktivet inte är tillämpligt på tekniska stödtjänster (artikel 3 j, se 1 kap. 6 § 4 lagen om betaltjänster) och om utkontraktering av viktiga operativa funktioner (artikel 19.6, se 3 kap. 28 § andra stycket lagen om betaltjänster).

17 Några andra frågor om överklaganden av Finansinspektionens beslut

17.1 Förordnande av sakkunnig i gränsöverskridande förfaranden

Promemorians förslag: Finansinspektionens beslut om förordnande av sakkunnig i ärenden om gränsöverskridande fusioner, delningar och ombildningar ska inte få överklagas.

Skälen för promemorians förslag: I aktiebolagslagen (2005:551) finns det bestämmelser om fusion, delning och gränsöverskridande ombildning. Såväl en fusion som en delning kan vara gränsöverskridande. För förfarandet gäller att det eller de bolag som vill genomföra ett gränsöverskridande förfarande ska ansöka hos Bolagsverket om tillstånd att

verkställa en fusions-, delnings- eller ombildningsplan (23 kap. 20 och 36 a §§, 24 kap. 22 § och 31 §§ samt 24 a kap. 22 § aktiebolagslagen). Bolagsverket ska pröva om förutsättningarna för att verkställa en plan är uppfyllda och i så fall utfärda ett intyg om att den del av förfarandet som regleras av svensk lag har genomförts på föreskrivet sätt. Om det vid handläggningen av en ansökan om ett gränsöverskridande förfarande uppkommer en fråga som kräver särskild fackkunskap, får Bolagsverket förordna en lämplig person som sakkunnig. Bolagsverket ska ersätta den sakkunnige för utfört arbete och sökanden ska i sin tur ersätta Bolagsverket för denna kostnad enligt ett beslut som verket fattar (23 kap. 45 b §, 24 kap. 47 § och 24 a kap. 24 § aktiebolagslagen).

Om ett finansiellt företag, dvs. ett företag som omfattas av lagen om bank- och finansieringsrörelse, försäkringsrörelselagen), eller lagen om tjänstepensionsföretag, vill genomföra ett gränsöverskridande förfarande finns det särskilda bestämmelser i de lagarna. I sådana fall är det Finansinspektionen som prövar en ansökan. Inspektionen kan, som Bolagsverket, förordna en sakkunnig vid handläggningen. Finansinspektionen ska i så fall också besluta om sökandens betalningsskyldighet för ersättning till en sakkunnig (jfr 10 kap. 1 § lagen om bank- och finansieringsrörelse, 11 kap. 1 § försäkringsrörelselagen och 10 kap. 1 § lagen om tjänstepensionsföretag).

Bolagsverkets beslut om betalningsskyldighet för ersättning till sakkunnig kan överklagas till allmän förvaltningsdomstol (31 kap. 2 § 5 aktiebolagslagen). Ett beslut om förordnande av sakkunnig kan dock inte överklagas. Frågan om en sakkunnig borde ha utsetts kan dock bli föremål för prövning i samband med överklagande av beslutet om fastställande av ersättning (prop. 2021/22:286 s. 202).

I 17 kap. 1 § tredje stycket lagen om bank- och finansieringsrörelse, i 21 kap. 3 § försäkringsrörelselagen och 17 kap. 1 § i lagen om tjänstepensionsföretag finns det generella bestämmelser om överklagande av Finansinspektionens beslut. Såväl beslut om förordnande av sakkunnig, som beslut om betalningsskyldighet för ersättning till sakkunnig kan överklagas till allmän förvaltningsdomstol.

Det saknas skäl för denna skillnad mellan Bolagsverkets och Finansinspektionens handläggning. Om ett beslut om förordnande av sakkunnig kan överklagas finns det också risk för att ärendet fördröjs. Finansinspektionens beslut om förordnande av sakkunnig i ärenden om gränsöverskridande fusioner, delningar och ombildningar bör därför, som gäller för motsvarande beslut av Bolagsverket, inte få överklagas.

17.2 Undantag från bosättningskrav

Promemorians förslag: Finansinspektionens beslut enligt lagen om bank- och finansieringsrörelse om undantag från bosättningskraven för styrelseledamöter, verkställande direktör och särskild firmatecknare ska få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Skälen för promemorians förslag: I aktiebolagslagen, finns det bestämmelser om bosättningskrav för styrelseledamöter, verkställande

direktör och särskilda firmatecknare. För styrelseledamöter gäller att minst hälften ska vara bosatta inom Europeiska ekonomiska samarbetsområdet (8 kap. 9 §). Den verkställande direktören ska vara bosatt inom Europeiska ekonomiska samarbetsområdet (8 kap. 30 §) Av de särskilda firmatecknarna ska minst en vara bosatt inom Europeiska ekonomiska samarbetsområdet (8 kap. 37 §). Bolagsverket får besluta om undantag från dessa bosättningskrav om det finns särskilda skäl. För företag som omfattas av lagen om bank- och finansieringsrörelse eller försäkringsrörelselagen får Finansinspektionen fatta ett motsvarande beslut om undantag (10 kap. 1 § andra stycket lagen om bank- och finansieringsrörelse och 11 kap. 1 § andra stycket försäkringsrörelselagen).

Bolagsverkets beslut om undantag från bosättningskraven enligt aktiebolagslagen överklagas till allmän förvaltningsdomstol. Samma gäller för motsvarande beslut som fattas av Finansinspektionen enligt försäkringsrörelselagen (21 kap. 2 § första stycket, se även prop. 2018/19:158 s. 653). Ett beslut om undantag enligt lagen om bank- och finansieringsrörelse överklagas dock till regeringen (17 kap. 1 § första stycket).

Som anförts i tidigare lagstiftningsärenden bör en överprövning av denna typ av ärenden lämpligen ske i domstol då det som regel inte torde finnas något behov av ett ställningstagande från regeringen, i dess egenskap av politiskt organ (prop. 2013/14:86 s. 63–64). Även om det är olika myndigheter som fattar det grundläggande beslutet bör det inte finnas skäl för skilda förfaranden för överklagande. Särskilt inte som beslut enligt försäkringsrörelselagen överklagas på samma sätt som ett motsvarande beslut enligt aktiebolagslagen. Ett beslut om undantag från bosättningskraven som Finansinspektionen fattar enligt lagen om bank- och finansieringsrörelse bör därför i fortsättningen överklagas till allmän förvaltningsdomstol. Liksom gäller vid överklagande av motsvarande beslut enligt aktiebolagslagen och försäkringsrörelselagen, bör prövningstillstånd krävas vid överklagande till kammarrätten av beslut enligt lagen om bank- och finansieringsrörelse (31 kap. 8 § aktiebolagslagen och 21 kap. 2 § andra stycket försäkringsrörelselagen).

17.3 Begränsad skyldighet att meddela trafikförsäkring

Promemorians förslag: Finansinspektionens beslut om begränsning av skyldigheten att meddela trafikförsäkring ska få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Skälen för promemorians förslag: Enligt trafikskadelagen (1975:1410) ska det som utgångspunkt finnas en trafikförsäkring för ett motordrivet fordon som är registrerat i vägtrafikregistret och inte är avställt samt för annat motordrivet fordon som brukas i trafik i Sverige (2 § första stycket). Trafikförsäkring får meddelas av en svensk försäkringsgivare med tillstånd enligt 2 kap. 4 § försäkringsrörelselagen, en försäkringsgivare från tredje land med tillstånd enligt 4 kap. 1 § lagen

(1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, eller en EES-försäkringsgivare som är verksam i Sverige med stöd av 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige (5 § första stycket trafikskadelagen).

En försäkringsgivare som får meddela trafikförsäkring i Sverige är även skyldig att på begäran meddela sådan försäkring, den s.k. kontraheringsplikten. I ett tillstånd att meddela försäkring enligt 2 kap. 4 § försäkringsrörelselagen eller 4 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige kan denna skyldighet begränsas till att gälla försäkring åt personer som tillhör en viss yrkesgrupp eller intressegrupp eller som är bosatta inom ett visst område. Finansinspektionen kan efter ansökan besluta om motsvarande begränsning för en försäkringsgivare som bedriver verksamhet i Sverige enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige. Ett sådant beslut får överklagas hos regeringen (5 § andra stycket trafikskadelagen).

Som anförs ovan för ett beslut om undantag från bosättningskraven (avsnitt 17.2) torde det inte heller för ett beslut som begränsar kontraheringsplikten finnas anledning att regeringen ska överpröva Finansinspektionens beslut. En motsvarande inskränkning för en svensk försäkringsgivare eller en försäkringsgivare från tredje land överklagas dessutom till allmän förvaltningsdomstol (21 kap. 3 § första stycket försäkringsrörelselagen och 10 kap. 4 § första stycket lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige). Denna typ av beslut bör i stället, som vanligtvis gäller för Finansinspektionens beslut, överklagas till allmän förvaltningsdomstol. Som också vanligtvis gäller för Finansinspektionens beslut, bör prövningstillstånd krävas vid överklagande till kammarrätten (se t.ex. 21 kap. 3 § andra stycket försäkringsrörelselagen och 10 kap. 4 § andra stycket lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige).

17.4 Tillsyn över Svenska skeppshypotekskassan

Promemorians förslag: Finansinspektionens beslut enligt lagen om Svenska skeppshypotekskassan ska få överklagas till allmän förvaltningsdomstol.

Prövningstillstånd ska krävas vid överklagande till kammarrätten.

Skälen för promemorians förslag: Bestämmelser om Svenska skeppshypotekskassan finns i lagen (1980:1097) om Svenska skeppshypotekskassan. Svenska skeppshypotekskassan har till ändamål att medverka vid finansiering av rederiverksamhet som bedrivs av svenskt rederi eller av en utländsk juridisk person där svenska fysiska eller juridiska personer har ett betydande inflytande eller intresse (1 §).

Svenska skeppshypotekskassan står under tillsyn av Finansinspektionen som i samband med tillsynen får meddela förelägganden eller förbud. Inspektionens beslut enligt lagen får överklagas hos regeringen (38 §).

I enlighet med vad som anförs och föreslås ovan (avsnitt 17.2 och 17.3), bör det inte heller för dessa beslut finnas anledning för en överprövning hos regeringen. De beslut som Finansinspektionen fattar enligt lagen om Svenska skeppshypotekskassan bör i stället överklagas till allmän förvaltningsdomstol. Vid ett överklagande bör, som vanligtvis gäller för Finansinspektionens beslut, prövningstillstånd krävas för överklagande till kammarrätten (se t.ex. 21 kap. 3 § andra stycket försäkringsrörelselagen).

18 Ikraftträdande- och övergångsbestämmelser

Promemorians förslag: Kompletteringslagen och övriga lagändringar ska träda i kraft den 17 januari 2025.

Äldre föreskrifter ska tillämpas för överklaganden av Finansinspektionens beslut enligt lagen om bank- och finansieringsrörelse om undantag från bosättningskrav, enligt trafikskadelagen om begränsad skyldighet att meddela försäkring och enligt lagen om Svenska skeppshypotekskassan om beslutet meddelats före ikraftträdandet.

Skälen för promemorians förslag

Ikraftträdande

DORA-förordningen ska tillämpas från och med den 17 januari 2025 (artikel 64 andra stycket). Även nationella bestämmelser som genomför de ändringar som görs genom ändringsdirektivet ska tillämpas från och med den 17 januari 2025 (artikel 9.1 andra stycket). Kompletteringslagen och övriga lagändringar som föranleds av DORA-förordningen och ändringsdirektivet bör därför träda i kraft vid denna tidpunkt.

De lagändringar som inte har samband med DORA-förordningen (se avsnitt 17) bör träda i kraft så snart det är möjligt. Detta bedöms också vara den 17 januari 2025.

Övergångsbestämmelser

Genom DORA-förordningen införs nya bestämmelser om digital operativ motståndskraft på finansmarknadsområdet. I huvudsak rör det sig om tillkommande bestämmelser och inte äldre bestämmelser som ändras. Det finns således inte någon tidigare lagstiftning att förhålla sig till. Inte heller finns det några övergångsbestämmelser i vare sig DORA-förordningen eller ändringsdirektivet. Det finns därmed inte något behov av övergångsbestämmelser till de lagändringar som nu föreslås.

Vissa beslut som tidigare har överklagats till regeringen ska överklagas till allmän förvaltningsdomstol. Detta gäller beslut enligt

– lagen om bank- och finansieringsrörelse om undantag från bosättningskraven (se avsnitt 17.1 och 17.2),

– trafikskadelagen om begränsad skyldighet att meddela trafikförsäkring (se avsnitt 17.3), och

– lagen om Svenska skeppshypotekskassan (se avsnitt 17.4).

I samtliga fall rör det sig om beslut som fattas av Finansinspektionen. För dessa beslut finns det anledning att införa en övergångsbestämmelse. Beslut som har meddelats före ikraftträdandet bör därför fortsatt överklagas till regeringen (jfr prop. 2013/14:86 s .86 och 87).

19 Konsekvensanalys

Promemorians bedömning: Genom förslagen tillgodoses DORA-förordningens krav när det gäller kompletterande reglering i svensk nationell rätt.

Eventuella ökade kostnader för Finansinspektionen, Riksbanken och andra myndigheter bedöms vara begränsade.

De flesta företag som bedriver verksamhet inom finansmarknadsområdet berörs av förslagen. Förslagen innebär i varierande omfattning ökade krav och kostnader för dem.

Enskilda berörs i den mån bestämmelserna leder till minskad risk för avbrott i finansiella tjänster och ökad säkerhet inom tjänsterna.

Skälen för promemorians bedömning

Förslagens syfte och alternativa lösningar

Förslagen har till syfte att komplettera DORA-förordningen. Förordningen förutsätter att det införs vissa nationella bestämmelser, t.ex. om testning av digital operativ motståndskraft (artikel 24–27). Enligt förordningen krävs det även nationella bestämmelser som ger den behöriga myndigheten nödvändiga utrednings-, tillsyns- och sanktionsbefogenheter (artikel 50.1). För att förordningen ska få genomslag i svensk rätt krävs således att Sverige inför bestämmelser i dessa avseenden.

Förslagen innebär att kompletterande bestämmelser till DORA-förordningen införs i en ny lag (se avsnitt 5.1). Genom förslagen tillgodoses förordningens krav avseende kompletterande reglering i nationell rätt. Förslagen går inte utöver vad som krävs för att uppfylla kraven i förordningen.

Det bedöms inte finnas några alternativa lösningar som skulle vara lämpliga när det gäller de åtgärder som är nödvändiga för att anpassa den svenska lagstiftningen till förordningen. Om Sverige inte gör anpassningar av lagstiftningen är det sannolikt att Europeiska kommissionen inleder ett förfarande om fördragsbrott. Att inte införa de bestämmelser som nu föreslås utgör alltså inte något alternativ.

Berörda aktörer

Förordningen berör de flesta företag som är verksamma inom finansmarknadsområdet, i DORA-förordningen benämnda finansiella entiteter. Som anges i avsnitt 4.3 rör det sig om flera olika typer av företag. Vissa företag kommer att beröras mer än andra. För företag som bedriver en begränsad verksamhet är det t.ex. tillräckligt med en förenklad riskhanteringsram (artikel 16). Andra företag omfattas fullt ut av förord-

ningens krav på hantering av IKT-risker (artikel 5–15). Några företag ska dessutom genomföra hotbildsstyrda penetrationstester (artikel 26).

Konsekvenser för Finansinspektionen

Finansinspektionen kommer att vara behörig myndighet enligt DORA-förordningen (se avsnitt 5.2). Som behörig myndighet kommer Finansinspektionen bl.a. att ansvara för tillsynen över att förordningen följs och inspektionen får därför vissa utrednings- och tillsynsbefogenheter, liksom befogenheter att ingripa med administrativa sanktioner och andra åtgärder vid överträdelser av förordningen (se förslagen i avsnitt 7 och 8). Som behörig myndighet ska Finansinspektionen också samarbeta med behöriga myndigheter i andra medlemsstater och med de europeiska tillsynsmyndigheterna, EBA, Esma och Eiopa (se avsnitt 11). Finansinspektionens ska även bestämma vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationsteser och hur ofta testerna ska genomföras (se avsnitt 6.1).

Ett nytt regelverk innebär i regel ökade kostnader. Detta gäller särskilt i ett inledande skede. Finansinspektionen behöver arbeta med att ta fram rutiner och mallar. Det bör också krävas vissa informationsinsatser. Den nya tillsynsstrukturen med den ledande tillsynsmyndigheten bör också kräva vissa arbetsinsatser (artikel 31–44 i DORA-förordningen).

I nuläget är det svårt att göra en bedömning av de ekonomiska konsekvenserna för Finansinspektionen. Inspektionens verksamhet avseende bl.a. regelgivning och tillsyn finansieras via anslag i statens budget. Detta gäller även Finansinspektionens avgifter till EU:s tillsynsmyndigheter. Kostnaderna för den verksamheten täcks genom avgifter som tas ut enligt förordningen om årliga avgifter för finansiering av Finansinspektionens verksamhet. Sådana avgifter ska uppgå till ett belopp som motsvarar kostnaden för den verksamhet som ska finansieras. Avgiftsintäkterna ska redovisas mot inkomsttitel på statens budget. Enligt förslagen ska Finansinspektionen få ta ut årliga avgifter av de aktörer som omfattas av det nya regelverket, de finansiella entiteterna, för att finansiera verksamheten med tillsyn enligt de nya reglerna (se avsnitt 14). Ändringar i förordningen om årliga avgifter för finansiering av Finansinspektionens verksamhet är därmed att vänta.

Ett stort antal av de företag som i dag står under tillsyn av Finansinspektionen kommer, som finansiella entiteter, att omfattas av kraven enligt DORA-förordningen. Europeiska kommissionen ska fastställa kriterier för bestämmande om ett företag ska omfattas fullt ut eller bara delvis av kraven i förordningen. Då arbetet med dessa kriterier fortfarande pågår är det svårt att avgöra hur många företag som kommer att omfattas av bestämmelserna i förordningen och i vilken mån och i och med det konsekvenserna för Finansinspektionens tillsynsarbete. Det torde inte röra sig om mer än ett 20-tal företag som omfattas fullt ut av förordningen och i och med det ska genomföra hotbildsstyrda penetrationstester. För andra företag innebär det i första hand skärpta krav på deras organisation och riskhantering. Finansinspektionen bör, till följd av den nuvarande tillsynen, ha en förhållandevis god kunskap om dessa företag. Nya krav bör i och för sig ställa högre krav på tillsynen. De flesta större företagen, t.ex. kreditinstitut och försäkringsföretag, omfattas dock redan i dag av bestäm-

melser med krav på dess organisation och riskhantering, vilket talar för begränsade konsekvenser för Finansinspektionen.

Sammantaget bedöms förslagen leda till ökade, om än begränsade, kostnader för Finansinspektionen.

Konsekvenser för Riksbanken

Riksbanken får genom förslagen nya uppgifter och befogenheter då myndigheten, i enlighet med DORA-förordningen, får uppgifter som rör testning av finansiella företags digitala operativa motståndskraft (avsnitt 6.1).

Riksbanken utför i dag liknande, om än frivilliga, tester inom ramen för TIBER-EU. Myndigheten har således en upparbetad kompetens för de nya uppgifterna. Detta gäller kunskap dels om själva testerna, dels om företagen som ska genomföra testerna.

Då det rör sig om en ny reglering bör det, på motsvarande sätt som för Finansinspektionen, krävas vissa informationsinsatser. Det bör också, som utvecklas ovan, bli något fler företag som ska genomföra tester när de nu blir obligatoriska. Riksbanken ska också få ta ut avgifter för verksamheten av de företag som ska genomföra testerna.

Sammantaget bedöms därmed konsekvenserna vara begränsade för Riksbanken.

Konsekvenser för företag

De flesta företag som bedriver verksamhet inom finansmarknadsområdet och står under tillsyn hos Finansinspektionen kommer att beröras av DORA-förordningen och kraven som anges i den. Nya krav är vanligtvis förenade med kostnader för enskilda företag. Detta gäller särskilt under den inledande fasen.

Utifrån de krav som anges i förordningen och utkasten till kommissionens delegerade akter bedöms det i första hand vara större kreditinstitut, enstaka försäkringsföretag, något eller några tjänstepensionsföretag, börser och värdepapperscentraler som kommer att omfattas fullt ut av förordningen och kraven om att genomföra hotbildsstyrda penetrationstester. Sammanlagt torde det röra sig om högst ett 20-tal svenska företag. Flera av dessa företag genomför dock redan motsvarande tester, dels i egen regi, dels inom ramen för TIBER-EU.

För de flesta företagen tillkommer krav på deras organisation och hantering av risker inom områdena för informations- och kommunikationssäkerhet. Det bör dock inte vara helt nya krav då de olika regelverken på finansmarknadsområdet i dag har närliggande, men mer generella och övergripande krav, tex. på kontinuitet och beredskapsplaner. Dessa delar av förordningen bör i första hand ses som förtydliganden och justeringar av redan gällande krav enligt de enskilda regelverken, vilket är i linje med de justeringar som görs i de grundläggande EU-rättsliga regelverken (se avsnitt 16). Genom förordningen tillkommer också krav på incidentrapportering. Dessa krav torde företagen kunna hantera utan större ändringar då de redan, enligt de olika regelverken på finansmarknadsområdet, har omfattande krav på regelbunden rapportering. Den nya tillsynen innebär dock ökade kostnader då såväl Finansinspektionen som Riksbanken ges möjlighet att ta ut avgifter (se avsnitt 14).

Syftet med DORA-förordningen är att öka motståndskraften och i förlängningen möjligheten för företagen att tillhandahålla sina tjänster utan avbrott. Driftsavbrott kan vara förenade med stora och oförutsedda kostnader både för de företag som drabbas och marknaden i stort. En hög driftssäkerhet bör för det enskilda företaget vara en konkurrensfördel. Genom förordningen fastställs enhetliga krav inom hela EU. Detta bör underlätta och påskynda företagens arbete med att öka sin egen motståndskraft i förhållande till om det är upp till varje medlemsstat eller enskilt företag att avgöra vilka krav som ska gälla. I ett längre perspektiv kan de nya kraven innebära kostnadsbesparingar för företagen och stärka allmänhetens förtroende både för företagen och för marknaden i dess helhet.

Finansinspektionens beslut om förordnande av sakkunnig i ett gränsöverskridande ärende ska enligt förslagen inte få överklagas (avsnitt 17.1). Även om ett beslut inte får överklagas särskilt kan det prövas i samband med överklagande av ett beslut om fastställande av ersättning till den sakkunnige. Ändringen bedöms därmed inte ha några negativa konsekvenser för företagen. Vidare föreslås att vissa beslut som Finansinspektionen fattar fortsättningsvis får överklagas till allmän förvaltningsdomstol (se avsnitt 17.2–17.4). Dessa beslut har hitintills överklagats till regeringen. Detta gäller vissa beslut om undantag från bosättningskrav för styrelseledamöter, verkställande direktörer och särskilda firmatecknare, beslut för försäkringsgivare från tredje land om undantag från kontraheringsplikten och beslut som rör Svenska skeppshypotekskassan. Detta är den överklagandeordning som normalt gäller för överklagande av Finansinspektionens beslut och bedöms därmed inte ha några negativa konsekvenser för företag.

Konsekvenser för domstolarna

De beslut som Finansinspektionen kommer att fatta enligt den nya lagen ska kunna överklagas till allmän förvaltningsdomstol (se avsnitt 15.1). Motsvarande gäller för de beslut som Riksbanken kommer att fatta (se avsnitt 15.2). Mål av nu aktuella slag kan i och för sig vara förhållandevis komplicerade och tidskrävande. Det är dock relativt få beslut från Finansinspektionen som överklagas. Sammanlagt torde det röra sig om ett begränsat antal beslut från myndigheterna per år och endast ett fåtal som överklagas.

Att vissa beslut framöver ska få överklagas till allmän förvaltningsdomstol i stället för till regeringen kan leda till en ökning av antalet ärenden hos de domstolarna (se avsnitt 17.2–17.4). Även i dessa fall torde det inte röra sig om annat än ett fåtal beslut per år om ens det.

Gränsöverskridande ombildningar är mindre vanliga vilket också torde gälla för beslut om förordnande av sakkunnig. Att förordnandebeslut inte ska få överklagas (se avsnitt 17.1) bör inte få annat än ringa påverkan hos domstolarna.

Sammantaget bör det röra sig om ett begränsat antal ärenden som tillkommer till domstolarna. Eventuella ökade kostnader för detta bedöms därför kunna hanteras inom befintliga ekonomiska ramar.

Konsekvenser för Kronofogdemyndigheten

Kronofogdemyndigheten berörs då beslut om viten enligt DORA-förordningen ska få verkställas på samma sätt som en svensk dom som har fått laga kraft (se avsnitt 7.5). Det föreslås också att Finansinspektionen och Riksbanken ska få förena vissa beslut med vite (se t.ex. avsnitt 6.3 och 7.2). Kronofogdemyndigheten berörs även genom att obetalda sanktionsavgifter ska lämnas till myndigheten för indrivning (se avsnitt 8.6). Antalet mål om obetalda viten och sanktionsavgifter förväntas bli mycket begränsat. Tillkommande kostnader med anledning av det för Kronofogdemyndigheten ska hanteras inom befintliga ekonomiska ramar.

Konsekvenser för enskilda

De krav som införs genom förordningen och den nya lagen riktar sig till företag, medlemsstateter och tillsynsmyndigheter. Kraven bör i förlängningen kunna komma de enskilda till nytta. Detta då förordningen har till syfte att öka säkerheten för finansiella tjänster genom att minska risken för dels driftsavbrott, dels att känsliga uppgifter kommer i orätta händer.

Inte heller de bestämmelser som i övrigt föreslås riktar sig direkt mot enskilda.

Ikraftträdande och särskilda informationsinsatser

Det föreslås att lagändringarna ska träda i kraft den 17 januari 2025. De övergångsbestämmelser som föreslås rör hanteringen av överklaganden (avsnitt 17). Sammantaget torde det inte finnas något behov av särskilda informationsinsatser med anledning av förslagen.

I övrigt kan förslagen i fråga om ikraftträdande inte anses medföra några sådana konsekvenser som behöver redovisas enligt förordningen (2007:1244) om konsekvensutredning vid regelgivning.

Övriga konsekvenser

Förslagen får inga konsekvenser för jämställdheten mellan kvinnor och män och har inga sociala konsekvenser. De har inte heller några konsekvenser för miljön.

Förenlighet med EU-rätten

Förslagen bedöms vara förenliga med EU-rätten.

20 Författningskommentar

20.1 Förslaget till lag med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn

1 kap. Inledande bestämmelser

Lagens syfte

1 § Denna lag kompletterar 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, i denna lag kallad EU-förordningen.

Termer och uttryck i denna lag har samma betydelse som i EU-förordning.

Paragrafen beskriver lagens innehåll. Hänvisningarna i lagen till DORA-förordningen är utformade på så sätt att de avser EU-förordningen i den vid varje tidpunkt gällande lydelsen, s.k. dynamisk hänvisning. Övervägandena finns i avsnitt 5.4.

I *första stycket* anges den EU-rättsakt som lagen kompletterar, dvs. DORA-förordningen.

I *andra stycket* klargörs att termer och uttryck i lagen har samma betydelse som i DORA-förordningen.

Behörig myndighet

2 § Av artikel 46 i EU-förordningen följer att Finansinspektionen är behörig myndighet enligt förordningen.

Paragrafen innehåller en upplysningsbestämmelse om behörig myndighet. Övervägandena finns i avsnitt 5.2.

Enligt DORA-förordningen (artikel 46) är behörig myndighet den myndighet som har utsetts som behörig myndighet i enlighet med vissa angivna EU-rättsakter. I Sverige är det i samtliga dessa fall Finansinspektionen som är behörig myndighet.

Avgifter till Finansinspektionen

3 § För att bekosta Finansinspektionens verksamhet enligt EU-förordningen och denna lag ska de företag som står under inspektionens tillsyn betala årliga avgifter.

Regeringen får meddela föreskrifter om avgifterna enligt första stycket.

Paragrafen innehåller bestämmelser om avgifter för finansiering av Finansinspektionens tillsynsverksamhet. Paragrafen är utformad efter förebild av bland annat 23 kap. 12 § första stycket och 15 § 6 lagen (2007:528) om värdepappersmarknaden. Bestämmelser om finansiering av Riksbankens testverksamhet finns i 3 kap. 5 §. Övervägandena finns i avsnitt 14.1.

I *första stycket* anges att Finansinspektionen får ta ut årliga avgifter av de företag som står under inspektionens tillsyn. Detta gäller de företag som

är finansiella entiteter enligt DORA-förordningen (se artikel 2.1). Dessa avgifter ska finansiera Finansinspektionens verksamhet enligt DORA-förordningen och denna lag.

I *andra stycket* finns ett bemyndigande för regeringen att meddela föreskrifter om avgifter. Regeringen får med stöd av bemyndigandet meddela föreskrifter för att bekosta Finansinspektionens verksamhet enligt förordningen och denna lag. Detta gäller årliga avgifter av de företag som står under tillsyn enligt förordningen.

2 kap. Hotbildsstyrda penetrationstester

Finansinspektionen

1 § Finansinspektionen ska besluta om vilka finansiella entiteter som ska genomföra hotbildsstyrd penetrationstestning enligt artikel 26 i EU-förordningen. Finansinspektionen ska också besluta om hur ofta en finansiell entitet ska genomföra sådan testning.

Paragrafen anger Finansinspektionens uppgifter för den hotbildsstyrda penetrationstestning som ska utföras enligt DORA-förordningen. Paragrafen införs till följd av artikel 26.10 i DORA-förordningen. Övervägandena finns i avsnitt 6.1.

Paragrafen innehåller en upplysning om att Finansinspektionen beslutar om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester. Enligt artikel 26.10 i DORA-förordningen ska den behöriga myndigheten ha befogenhet att välja ut vilka finansiella entiteter som är skyldiga att utföra hotbildsstyrd penetrationstestning om det inte har utsetts en enda offentlig myndighet inom finanssektorn som ska ansvara för frågor som rör hotbildsstyrd penetrationstestning. Kriterierna för att identifiera vilka finansiella entiteter som ska genomföra sådana tester finns i artikel 26.8 tredje stycket och kommer att preciseras ytterligare i en av Europeiska kommissionens genomförandeförordningar (artikel 26.11).

Riksbanken

2 § Riksbanken ska övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt artikel 26 och 27 i EU-förordningen.

Riksbanken ska utfärda sådana intyg som avses i artikel 26.7 i EU-förordningen.

Paragrafen anger Riksbankens uppgifter för den hotbildsstyrda penetrationstestning som ska genomföras enligt DORA-förordningen. Paragrafen införs till följd av artikel 26.10 i DORA-förordningen. Övervägandena finns i avsnitt 6.1.

Riksbanken ska enligt *första stycket* övervaka och samordna de hotbildsstyrda penetrationstester som ska genomföras enligt DORA-förordningen. Riksbanken har en övergripande roll vid testningen då det är de finansiella entiteterna som ska genomföra själva testerna (se artikel 26.1). I Riksbankens uppgifter ingår bl.a. att validera vilka kritiska eller viktiga funktioner som ska omfattas av testningen (artikel 26.2 tredje stycket) och säkerställa att den testare som anlitas för utförandet av testet uppfyller de krav som ställs i förordningen (artikel 27). Med att övervaka och samordna

avses även att säkerställa att den finansiella entiteten tillämpar den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen. De krav som ska gälla för testmetod och tillvägagångssätt kommer att preciseras ytterligare i en av kommissionens genomförandeförordningar (artikel 26.11).

I *andra stycket* anges att Riksbanken ska utfärda intyg om att ett test har utförts i enlighet med kraven i DORA-förordningen (artikel 26.7). Ett intyg ska bekräfta att ett hotbildsstyrt penetrationstest har genomförts i enlighet med kraven i förordningen och de krav som Riksbanken beslutat för det enskilda testet (första stycket), vilka ska framgå av intyget.

Samverkan

3 § Finansinspektionen ska ge Riksbanken tillfälle att yttra sig innan Finansinspektionen fattar beslut enligt 1 §.

Riksbanken ska ge Finansinspektionen tillfälle att yttra sig innan Riksbanken fattar beslut om hotbildsstyrd penetrationstestning som berör Finansinspektionens tillsynsverksamhet.

Finansinspektionen och Riksbanken ska lämna varandra de uppgifter som respektive myndighet behöver för samverkan.

Paragrafen innehåller bestämmelser om samverkan mellan Finansinspektionen och Riksbanken. Paragrafen är utformad efter förebild av 3 kap. 11 § lagen (2022:1568) om Sveriges riksbank. Övervägandena finns i avsnitt 6.2.

I *första stycket* anges att Finansinspektionen ska ge Riksbanken tillfälle att yttra sig när den avser att fatta beslut om vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och med vilken frekvens som respektive entitet ska genomföra testet, dvs. Finansinspektionens uppgifter enligt 1 §.

I *andra stycket* anges att Riksbanken ska ge Finansinspektionen tillfälle att yttra sig när den avser att fatta beslut som berör Finansinspektionens tillsynsverksamhet. Detta kan t.ex. gälla vilka funktioner hos den finansiella entiteten som ett test ska omfatta och att godkänna att den finansiella entiteten använder en intern testare. På motsvarande sätt som för Finansinspektionen knyts skyldigheten att samverka till de uppgifter som Riksbanken ska utföra enligt 2 §.

Enligt *tredje stycket* ska Finansinspektionen och Riksbanken till varandra lämna de uppgifter som myndigheterna behöver för att kunna samverka. Bestämmelsen är sekretessbrytande och möjliggör att myndigheterna inom den samverkan som ska ske enligt första och andra stycket kan dela uppgifter utan hinder av sekretess (10 kap. 28 § offentlighets- och sekretesslagen [2009:400]).

Uppgiftsskyldighet

4 § På begäran av Riksbanken ska finansiella entiteter lämna de uppgifter som är nödvändiga för Riksbankens verksamhet enligt detta kapitel och artikel 26 och 27 i EU-förordningen.

Paragrafen innehåller bestämmelser om uppgiftsskyldighet. Paragrafen är utformad efter förebild av 12 kap. 1 § lagen om Sveriges riksbank. Övervägandena finns i avsnitt 6.3.

I paragrafen finns bestämmelser om uppgiftsskyldighet för finansiella entiteter. Dessa är skyldiga att på begäran av Riksbanken lämna uppgifter till Riksbanken. Detta gäller dock bara uppgifter som är nödvändiga för Riksbankens verksamhet avseende hotbildsstyrda penetrationstester enligt DORA-förordningen, dvs. Riksbankens uppgifter enligt detta kapitel. Enligt artikel 26.3 i DORA-förordningen ska den finansiella entiteten som genomför testet ha det fulla ansvaret för att säkerställa att tredjepartsleverantörer av IKT-tjänster som omfattas av testet efterlever förordningens krav fullt ut. Om tredjepartsleverantörer av IKT-tjänster omfattas av den hotbildsstyrda penetrationstestningen omfattar den finansiella entitetens uppgiftsskyldighet därför även uppgifter som entiteten har tillgång till genom tredjepartsleverantören.

Förelägganden

5 § Riksbanken får besluta om de förelägganden som behövs för att en finansiell entitet ska följa uppgiftsskyldigheten i 4 §.

Ett beslut om föreläggande får förenas med vite.

Paragrafen innehåller bestämmelser om förelägganden. Paragrafen är utformad efter förebild av 12 kap. 2 § lagen om Sveriges riksbank. Övervägandena finns i avsnitt 6.3.

I *första stycket* finns bestämmelser om förelägganden kopplade till uppgiftsskyldigheten i 4 §. Riksbanken har genom bestämmelsen möjlighet att besluta om föreläggande mot en finansiell entitet som inte följer en begäran från Riksbanken att lämna uppgifter.

Av *andra stycket* framgår att ett beslut om föreläggande enligt paragrafen får förenas med vite. Allmänna bestämmelser om vite finns i lagen (1985:206) om viten.

Avgifter till Riksbanken

6 § Riksbanken får ta ut avgifter från de finansiella entiteter som genomför hotbildsstyrd penetrationstestning.

Riksbanken får meddela föreskrifter om avgifter enligt första stycket.

Paragrafen innehåller bestämmelser om avgifter för finansiering av Riksbankens verksamhet. Paragrafen är utformad efter förebild av 1 kap. 12 § andra stycket och 13 kap. 1 § 1 lagen om Sveriges riksbank. Bestämmelser om finansiering av Finansinspektionens tillsynsverksamhet finns i 1 kap. 4 §. Övervägandena finns i avsnitt 14.2.

I *första stycket* anges att Riksbanken får ta ut avgifter för utförandet av hotbildsstyrd penetrationstestning, dvs. de uppgifter som Riksbanken ska ansvara för enligt 2 §. För vilka uppgifter det rör sig om, se författningskommentaren till den paragrafen.

I *andra stycket* finns ett bemyndigande för Riksbanken att meddela föreskrifter om avgifter. Med stöd av bemyndigandet får Riksbanken meddela föreskrifter om avgifter för att bekosta dess verksamhet för den hotbildsstyrda penetrationstestningen som myndigheten ska ansvara för.

3 kap. Tillsyn

Tillsynens omfattning

1 § Finansinspektionen har tillsyn över att finansiella entiteter följer bestämmelserna i EU-förordningen och denna lag.

Paragrafen innehåller en bestämmelse om Finansinspektionens tillsyn över finansiella entiteter och vad tillsynen omfattar. Övervägandena finns i avsnitt 7.1.

Det följer även direkt av artikel 46 i DORA-förordningen att Finansinspektionen har tillsyn över finansiella entiteter och att tillsynen omfattar skyldigheterna enligt förordningen.

En konsekvens av att det i kompletteringslagen införs bestämmelser om Finansinspektionens utredningsbefogenheter är att det därigenom uppstår viss dubbelreglering. Det handlar framför allt om möjligheterna att inhämta uppgifter, hålla förhör och genomföra platsundersökningar. Finansinspektionen har då möjlighet att välja vilken bestämmelse som den ska lägga till grund för sin åtgärd.

Föreläggande om att lämna uppgifter

2 § För tillsynen enligt 1 § får Finansinspektionen förelägga

1. en fysisk eller juridisk person att tillhandahålla uppgifter, handlingar eller annat, och
2. den som förväntas kunna lämna upplysningar i saken att inställa sig till förhör på tid och plats som inspektionen bestämmer.

Första stycket gäller inte i den utsträckning uppgiftslämnandet skulle strida mot den i lag reglerade tystnadsplikten för advokater.

Paragrafen innehåller bestämmelser om Finansinspektionens befogenhet att begära uppgifter och kalla till förhör. Paragrafen införs till följd av artikel 50.2 i DORA-förordningen. Paragrafen är utformad efter förebild av bl.a. 23 kap. 3 § lagen om värdepappersmarknaden och 2 kap. 2 § lagen (2021:899) med kompletterande bestämmelser om gräsrotsfinansieringstjänster. Övervägandena finns i avsnitt 7.2.

Enligt *första stycket 1* får Finansinspektionen – för tillsynen enligt 1 § – förelägga både en fysisk och juridisk person att tillhandahålla uppgifter, handlingar eller annat. Med handling avses framställning i skrift eller bild och upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas bara med tekniska hjälpmedel (jfr 2 kap. 3 § första stycket tryckfrihetsförordningen).

Enligt *första stycket 2* får Finansinspektionen förelägga den som förväntas kunna lämna upplysningar i saken att inställa sig till förhör på tid och plats som inspektionen bestämmer. Skyldigheten att inställa sig till förhör innebär inte någon skyldighet att yttra sig vid förhöret, oavsett tystnadsplikt (se t.ex. prop. 2016/17:22 s. 142).

I *andra stycket* tydliggörs att ett föreläggande inte får beslutas om uppgiftslämnandet skulle strida mot den i lag reglerade tystnadsplikten för advokater (8 kap. 4 § rättegångsbalken). Att en begäran inte heller får framställas om uppgiftslämnandet skulle strida mot exempelvis anonymitetsskyddet och efterforskningsförbudet i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen följer redan av principen att grundlag har före-

träde framför vanlig lag. Med begreppet ”uppgiftslämnande” avses samtliga uppgifter som Finansinspektionen får begära att någon lämnar, dvs. såväl uppgifter som handlingar och annat.

Av 4 kap. 25 § följer att ett föreläggande får förenas med vite. Om ett föreläggande ändå inte följs får Finansinspektionen ingripa mot den finansiella entiteten (se 4 kap. 1 och 2 §§).

Platsundersökning

3 § Finansinspektionen får när det är nödvändigt för tillsynen enligt 1 § genomföra en undersökning i verksamhetslokalerna hos en finansiell entitet.

Paragrafen innehåller bestämmelser om platsundersökningar i verksamhetslokaler. Paragrafen införs till följd av artikel 50.2 i DORA-förordningen. Den är utformad efter förebild av bl.a. 23 kap. 4 § lagen (2007:528) om värdepappersmarknaden (prop. 2006/07:115 s. 630). Övervägandena finns i avsnitt 7.3.

Finansinspektionen får enligt paragrafen, om det är nödvändigt för tillsynen, genomföra en undersökning i en finansiell entitets verksamhetslokaler. Undersökningen kan endast avse den fysiska eller juridiska person som utreds och kan bara genomföras i den personens verksamhetslokaler. Finansinspektionen har inte någon möjlighet att tillgripa tvångsmedel om den person som är föremål för undersökningen inte medverkar till att undersökningen genomförs. En sådan vägran kan dock ligga till grund för ett ingripande mot den finansiella entiteten (se 4 kap. 1 och 2 §§). Med verksamhetslokal avses utrymmen som huvudsakligen används i verksamhet som medför eller kan antas medföra bokföringsskyldighet enligt bokföringslagen (1999:1078) eller som bedrivs av en annan juridisk person än ett dödsbo (jfr 3 kap. 18 § skatteförfarandelagen [2011:1244]). Att en undersökning endast får genomföras i verksamhetslokaler innebär att en lokal som enbart används som privatbostad inte får undersökas. Om verksamhet bedrivs i en privatbostad kan emellertid en undersökning genomföras där under vissa förutsättningar. För att en bostad ska kunna anses vara en verksamhetslokal krävs det att bostaden är den plats från vilken verksamheten i fråga huvudsakligen bedrivs. Att så är fallet kan t.ex. framgå genom att verksamheten är registrerad på samma adress som privatbostaden.

Verkställighet av beslut om viten

4 § Beslut om viten enligt EU-förordningen får verkställas enligt utsökningsbalken på samma sätt som en svensk dom som har fått laga kraft.

Paragrafen innehåller bestämmelser om verkställighet av beslut om viten enligt DORA-förordningen. Paragrafen införs till följd av artikel 35.9 i DORA-förordningen. Den är utformad efter förebild av bl.a. 2 kap. 5 § lagen (2019:1215) med kompletterande bestämmelser till EU:s förordning om värdepapperisering. Övervägandena finns i avsnitt 7.5.

Av paragrafen följer att beslut om viten är verkställbara enligt utsökningsbalken. Bestämmelsen innebär att den ledande tillsynsmyndighetens beslut om viten enligt DORA-förordningen är en utländsk exekutionstitel som får verkställas i Sverige (jfr 3 kap. 2 § utsökningsbalken).

Den ledande tillsynsmyndighetens beslut om viten ska därvid likställas med en svensk lagakraftvunnen dom. Beslut om viten enligt förordningen avser beslut som fattas av den ledande tillsynsmyndigheten inom ramen för dess tillsynsverksamhet avseende kritiska tredjepartsleverantörer. Kronofogdemyndigheten är den myndighet som ansvarar för den praktiska verkställigheten och dess beslut kan överklagas till allmän domstol. Vitet tillfaller den ledande tillsynsmyndigheten.

4 kap. Ingripanden

Ingripanden mot finansiella entiteter

1 § Finansinspektionen ska ingripa mot följande finansiella entiteter om de åsidosätter sina skyldigheter enligt EU-förordningen eller denna lag:

1. Svenska skeppshypotekskassan,
2. en leverantör av kryptotillgångstjänster,
3. en emittent av tillgångsanknutna token,
4. en pensionsstiftelse,
5. ett kreditvärderingsinstitut,
6. en administratör av kritiska referensvärden,
7. en leverantör av gräsrotsfinansieringstjänster,
8. ett värdepapperiseringsregister, och
9. ett transaktionsregister.

Paragrafen innehåller bestämmelser om ingripande mot överträdelser av DORA-förordningen och kompletteringslagen. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Övervägandena finns i avsnitt 5.1 och 8.2.2.

I paragrafen anges att Finansinspektionen ska ingripa mot en sådan finansiell entitet som anges i paragrafen, om entiteten åsidosätter sina skyldigheter enligt DORA-förordningen eller kompletteringslagen.

2 § Bestämmelser om ingripanden mot andra finansiella entiteter än de som anges i 1 § och som åsidosätter sina skyldigheter enligt EU-förordningen eller denna lag finns i de lagar som reglerar den berörda verksamheten.

Paragrafen innehåller en upplysningsbestämmelse om ingripande mot överträdelser av DORA-förordningen och kompletteringslagen. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Den är utformad efter förebild av bl.a. 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering (prop. 2019/20:37 s. 84). Övervägandena finns i avsnitt 8.2.1.

Paragrafen innehåller en upplysning om att det finns bestämmelser om ingripanden i andra lagar som är tillämpliga om en finansiell entitet, som inte anges i 1 §, åsidosätter sina skyldigheter enligt DORA-förordningen och kompletteringslagen.

Enligt artikel 46 i DORA-förordningen är det de behöriga myndigheter som har utsetts i medlemsstaterna enligt de i artikeln uppräknade EU-rättsakterna som ska utöva tillsynen över att finansiella entiteter uppfyller kraven i förordningen. I Sverige är det i samtliga dessa fall Finansinspektionen som är behörig myndighet. Det anges vidare i artikel 46 i förordningen att de behöriga myndigheterna ska utöva sin tillsyn i enlighet med

de befogenheter som dessa myndigheter har beviljats genom de uppräknade EU-rättsakterna. När de rättsakterna har genomförts i svensk rätt har det med vissa undantag gjorts i de rörelselagar som reglerar de aktuella verksamheterna. För kreditinstitut finns sådana bestämmelser i lagen (2004:297) om bank- och finansieringsrörelse (15 kap. 1 §), för betalningsinstitut och leverantörer av kontoinformationstjänster i lagen (2010:751) om betaltjänster (8 kap. 8 och 23 §§), för institut för elektroniska pengar och registrerade utgivare i lagen (2011:755) om elektroniska pengar (5 kap. 8 och 23 §§), för värdepappersföretag, som när de är svenska benämns värdepappersbolag, i lagen om värdepappersmarknaden (25 kap. 1 §), för värdepapperscentraler i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument (9 kap. 11 §), för centrala motparter i lagen (2007:527) om värdepappersmarknaden (1 kap. 1 a § första stycket och 25 kap. 1 §), för handelsplatser och leverantörer av datarapporteringstjänster i lagen om värdepappersmarknaden (25 kap. 1 §), för förvaltare av alternativa investeringsfonder (AIF-förvaltare) i lagen (2013:561) om förvaltare av alternativa investeringsfonder (14 kap. 1 §), för förvaltningsbolag, som i lagen (2004:46) om värdepappersfonder benämns fondbolag (10 kap 1 §), för försäkringsföretag (inklusive återförsäkringsbolag) i försäkringsrörelselagen (2010:2043) (18 kap. 1 §) och för tjänstepensionsföretag, i dess egenskap av tjänstepensionsinstitut, i lagen (2019:742) om tjänstepensionsföretag (15 kap. 1 §).

3 § Ett ingripande mot Svenska skeppshypotekskassan ska ske genom ett beslut om föreläggande att inom en viss tid vidta en åtgärd eller upphöra med ett visst agerande.

Paragrafen innehåller bestämmelser om hur Finansinspektionen får ingripa mot Svenska skeppshypotekskassan, om kassan har gjort sig skyldig till överträdelse av DORA-förordningen eller kompletteringslagen. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Övervägandena finns i avsnitt 8.2.2.

Ett ingripande genom ett föreläggande kan bara användas när det krävs för att få Svenska skeppshypotekskassan att vidta åtgärder för att rätta till något. Eftersom en överträdelse även kan bestå i underlåtenhet att uppfylla vissa krav, kan Finansinspektionen även ålägga den ansvarige att vidta en positiv åtgärd för att uppfylla kraven i DORA-förordningen. Ett föreläggande kan inte förenas med en sanktionsavgift (se 7 §). Ett föreläggande kan däremot förenas med vite enligt 25 §.

4 § Ett ingripande mot en emittent av tillgångsanknutna token, en pensionsstiftelse, ett kreditvärderingsinstitut, ett värdepapperiseringsregister eller ett transaktionsregister ska ske genom ett beslut om

1. föreläggande att inom en viss tid vidta en viss åtgärd eller upphöra med ett visst agerande, eller
2. anmärkning.

Paragrafen innehåller bestämmelser om hur Finansinspektionen får ingripa mot de finansiella entiteter som anges i paragrafen, om de har gjort sig skyldig till överträdelse av DORA-förordningen eller kompletteringslagen. Paragrafen införs till följd av artikel 50.4 i DORA-

förordningen. Den är utformad efter förebild av bl.a. 3 kap. 1 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering (prop. 2019/20:37 s. 84). Övervägandena finns i avsnitt 8.2.2.

Första stycket innehåller en uppräkning av de åtgärder och sanktioner som Finansinspektionen kan beslut om vid ett ingripande. I de fall en administrativ åtgärd eller sanktion ska påföras en juridisk person saknar det betydelse om verksamheten har överlåtits till någon annan efter det att den aktuella överträdelsen ägde rum (se t.ex. prop. 2003/04:121 s. 158–159). I 18 och 19 §§ anges omständigheter som ska beaktas vid valet av ingripande.

Föreläggande enligt *punkt 1* kan riktas mot de finansiella entiteter som anges i paragrafen. Ett ingripande genom ett föreläggande kan bara användas när det krävs för att få den finansiella entiteten i fråga att vidta åtgärder för att rätta till något. Eftersom en överträdelse även kan bestå i underlåtenhet att uppfylla vissa krav, kan Finansinspektionen även ålägga den ansvarige att vidta en positiv åtgärd för att uppfylla kraven i DORA-förordningen. Ett föreläggande kan inte förenas med en sanktionsavgift (se 7 §). Ett föreläggande kan däremot förenas med vite enligt 25 §.

En anmärkning enligt *punkt 2* bör användas när det inte finns något att åtgärda, men överträdelsen bör medföra en sanktion. Anmärkning kan förenas med sanktionsavgift enligt 7 §.

5 § Ett ingripande mot en leverantör av kryptotillgångstjänster, en administratör av kritiska referensvärden eller en leverantör av gräsrotsfinansieringstjänster ska ske genom ett beslut om

1. föreläggande att inom en viss tid vidta en viss åtgärd eller upphöra med ett visst agerande, eller
2. anmärkning.

Om överträdelsen är allvarlig får den finansiella entitetens auktorisation återkallas eller, om det är tillräckligt, en varning meddelas.

Paragrafen innehåller bestämmelser om hur Finansinspektionen får ingripa mot de finansiella entiteter som anges i paragrafen, om de har gjort sig skyldig till överträdelse av DORA-förordningen och kompletteringslagen. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 1 § andra stycket lagen om värdepappersmarknaden och 3 kap. 2 § lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering (prop. 2006/07:115 s. 636 och prop. 2020/21:206 s. 133–134). Övervägandena finns i avsnitt 8.2.2.

Första stycket innehåller en uppräkning av de åtgärder och sanktioner som Finansinspektionen kan beslut om vid ett ingripande. I de fall en administrativ åtgärd eller sanktion ska påföras en juridisk person saknar det betydelse om verksamheten har överlåtits till någon annan efter det att den aktuella överträdelsen ägde rum (se t.ex. prop. 2003/04:121 s. 158–159). I 18 och 19 §§ anges omständigheter som ska beaktas vid valet av ingripande.

Föreläggande enligt *punkt 1* kan riktas dels mot finansiella entiteter som är juridiska personer, dels mot administratörer av kritiska referensvärden som även kan vara fysiska personer. Ett ingripande genom ett föreläggande kan bara användas när det krävs för att få den finansiella entiteten i fråga att vidta åtgärder för att rätta till något. Eftersom en överträdelse även kan bestå i underlåtenhet att uppfylla vissa krav, kan Finansinspek-

tionen även ålägga den ansvarige att vidta en positiv åtgärd för att uppfylla kraven i DORA-förordningen. Ett föreläggande kan inte förenas med en sanktionsavgift (se 7 §). Ett föreläggande kan däremot förenas med vite enligt 25 §.

En anmärkning enligt *punkt 2* bör användas när det inte finns något att åtgärda, men överträdelsen bör medföra en sanktion. Anmärkning kan som föreläggande riktas både mot juridiska och fysiska personer. Anmärkning kan förenas med sanktionsavgift enligt 7 §.

Återkallelse av auktorisation enligt *andra stycket* bör vid valet av ingripandeåtgärd betraktas som den mest ingripande åtgärden. Auktorisationen för en leverantör av kryptotillgångstjänster, en administratör av kritiska referensvärden eller en leverantör av gräsrotsfinansieringstjänster får återkallas vid allvarliga överträdelser av DORA-förordningen. Att Finansinspektionen ”får ingripa” vid överträdelser av förordningen och kompletteringslagen påverkar inte inspektionens förutsättningar att ingripa mot finansiella entiteter i förhållande till andra lagar, där det anges att inspektionen ”ska ingripa” (se t.ex. 25 kap. 2 § lagen om värdepappersmarknaden). Om en sådan finansiell entitet gör sig skyldig till en allvarlig överträdelse där det inte är nödvändigt att återkalla auktorisationen, bör i stället en varning meddelas. En varning kan förenas med sanktionsavgift enligt 7 §.

6 § Ett ingripande enligt 3–5 §§ får inte ske om en överträdelse omfattas av ett föreläggande som har förenats med vite och en ansökan om utdömande av vitet har gjorts.

Paragrafen innehåller bestämmelser om hinder mot ingripande. Den är utformad efter förebild av bl.a. 3 kap. 2 § andra stycket lagen med kompletterande bestämmelser till EU:s förordning om gräsrotsfinansiering (prop. 2020/21:206 s. 75). Övervägandena finns i avsnitt 8.2.2.

I paragrafen regleras möjligheten till ingripande när Finansinspektionen redan har beslutat om ett föreläggande förenat med vite avseende samma överträdelse. Bestämmelsen syftar till att förhindra att någon prövas två gånger för samma sak på ett sätt som kan strida mot dubbelprövningsförbudet (artikel 4 i sjunde tilläggsprotokollet till den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna [Europakonventionen]). Om ett föreläggande har förenats med vite och föreläggandet inte följs, kan Finansinspektionen välja att ansöka om att vitet ska dömas ut. Det faktum att föreläggandet finns utgör inte något hinder mot ett ingripande enligt 3–5 §§. Den avgörande tidpunkten för när hindret uppkommer är tidpunkten då en domstolsprocess inleds om utdömande av vitet.

7 § Om ett beslut om anmärkning eller varning enligt 4 eller 5 § har meddelats, får Finansinspektionen besluta att den som har gjort sig skyldig till överträdelsen ska betala en sanktionsavgift.

Paragrafen innehåller bestämmelser om förutsättningarna för Finansinspektionen att besluta om sanktionsavgift mot en juridisk eller fysisk person. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Den är utformad efter förebild av bl.a. 3 kap. 3 § lagen med komplet-

terande bestämmelser till EU:s förordning om gräsrotsfinansiering (prop. 2020/21:206 s. 135). Övervägandena finns i avsnitt 8.2.2.

Bestämmelsen innebär att Finansinspektionen får besluta om sanktionsavgift mot en juridisk eller fysisk person bara om beslut om anmärkning eller varning har meddelats enligt 4 eller 5 §. Det är därmed inte möjligt att förena förelägganden eller beslut om återkallelse av tillståndet med sanktionsavgift. Avgiften kan uppgå till högst de belopp som anges i 14–16 §§.

8 § Om en auktorisation återkallas enligt 5 §, får Finansinspektionen bestämma hur verksamheten ska avvecklas

Ett beslut om återkallelse får förenas med förbud att fortsätta med hela eller delar av verksamheten.

Paragrafen innehåller bestämmelser om åtgärder vid återkallelse av auktorisation. Paragrafen är utformad efter förebild av bl.a. 25 kap. 6 § lagen om värdepappersmarknaden (prop. 2006/07:115 s. 639). Övervägandena finns i avsnitt 8.2.2.

Av *första stycket* följer att Finansinspektionen i sitt beslut om återkallelse av auktorisation kan ge anvisningar om hur verksamheten ska avvecklas. Hänsyn kan tas till individuella förhållanden hos det företag som beslutet avser.

Om Finansinspektionen meddelar ett beslut om återkallelse får den, enligt *andra stycket*, samtidigt meddela förbud för företaget att fortsätta verksamheten. Ett sådant förbud får förenas med vite enligt 25 §.

Ingripanden mot vissa företrädare för finansiella entiteter

9 § Finansinspektionen ska ingripa mot någon som ingår i styrelsen för en finansiell entitet som anges i 1 § eller är dess verkställande direktör, eller ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i EU-förordningen.

Ett ingripande enligt första stycket får ske bara om den finansiella entitetens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande ska ske genom en eller båda av följande sanktioner:

1. beslut att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en sådan finansiell entitet, eller ersättare för någon av dem, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om Finansinspektionens möjlighet att ingripa mot fysiska personer som ingår i företagets ledning när en finansiell entitet, som är en juridisk person, har åsidosatt sina skyldigheter. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Paragrafen är utformad efter förebild av bl.a. 25 kap. 1 c § lagen om värdepappersmarknaden (prop. 2016/17:162 s. 749–750). Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser som, om de överträds av en juridisk person som anges i 1 §, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig.

Finansinspektionen ska ingripa mot den som ingår i styrelsen för en finansiell entitet som anges i 1 §, är dess verkställande direktör, eller ersättare för någon av dem, om den finansiella entiteten har åsidosatt sina skyldigheter i något av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 10 § följer att frågor om ingripanden mot den fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande (se författningskommentaren till den paragrafen).

Ingripande sker enligt *tredje stycket* genom ett beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en sådan finansiell entitet som den fysiska personen ingår i ledningskretsen för eller ersättare för någon av dem (*punkt 1*), eller genom ett beslut om sanktionsavgift (*punkt 2)*. Dessa två sanktioner kan också kombineras. Bestämmelser om sanktionsavgift finns i 14–17 och 20 §§. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 18, 19 och 21 §§.

Sanktionsföreläggande

10 § Frågor om ingripande mot fysiska personer enligt 9 § tas upp av Finansinspektionen genom ett sanktionsföreläggande.

Ett sanktionsföreläggande innebär att den fysiska personen föreläggs att inom en viss tid godkänna en sanktion som är bestämd till tid eller belopp.

När ett sanktionsföreläggande har godkänts, gäller det som ett domstolsavgörande som fått laga kraft. Ett godkännande som görs efter den tid som angetts i föreläggandet är utan verkan.

Paragrafen reglerar, tillsammans med 11–13 §§, förfarandet för beslut om sanktioner genom ett sanktionsföreläggande. Paragrafen är utformad efter förebild av bl.a. 25 kap. 10 a § lagen om värdepappersmarknaden (prop. 2014/15:57 s. 72). Övervägandena finns i avsnitt 8.3.

Enligt *första stycket* ska ingripanden mot en fysisk person för överträdelse av en juridisk person, som anges i 2 §, tas upp av Finansinspektionen genom ett sanktionsföreläggande.

I *andra stycket* anges att ett sanktionsföreläggande innebär att den som bedöms vara ansvarig för en överträdelse föreläggs att inom en viss tid godkänna en sanktion som är bestämd till tid eller belopp. Tidsfristen bör vara så lång att personen i fråga får skäligt rådrum att ta ställning till Finansinspektionens påståenden.

Enligt *tredje stycket* gäller ett godkänt sanktionsföreläggande som ett domstolsavgörande som fått laga kraft. Ett godkänt sanktionsföreläggande som avser sanktionsavgift kan därmed verkställas enligt utsökningsbalkens bestämmelser (se 3 kap. 1 § första stycket 3 utsökningsbalken). Ett godkännande som görs efter den tid som angetts i sanktionsföreläggandet är utan verkan.

11 § Ett sanktionsföreläggande ska innehålla uppgift om
1. den fysiska person som föreläggandet avser,
2. överträdelsen och de omständigheter som behövs för att kännetecknа den,
3. de bestämmelser som är tillämpliga på överträdelsen, och
4. den sanktion som föreläggs personen.

Sanktionsföreläggandet ska också innehålla en upplysning om att ansökan om sanktion kan komma att ges in till domstol, om sanktionsföreläggandet inte godkänns inom den tid som Finansinspektionen anger.

Paragrafen anger vilka uppgifter ett sanktionsföreläggande ska innehålla. Paragrafen är utformad efter förebild av bl.a. 25 kap. 10 b § lagen om värdepappersmarknaden (prop. 2014/15:57 s. 73). Övervägandena finns i avsnitt 8.3.

För att kunna identifiera en överträdelse och avgränsa den mot andra förfaranden måste ett sanktionsföreläggande innehålla vissa specifika uppgifter.

I *första stycket* anges vilka uppgifter ett sanktionsföreläggande ska innehålla: den fysiska person som föreläggandet avser, överträdelsen och de omständigheter som behövs för att kännetecknа den, de bestämmelser som är tillämpliga på överträdelsen, och den sanktion som föreläggs personen. Med de omständigheter som behövs för att kännetecknа överträdelsen avses en beskrivning av vad som läggs den berörda fysiska personen till last. Genom Finansinspektionens uppgifter ska mottagaren av föreläggandet enkelt kunna förstå vad inspektionen hävdar att han eller hon har gjort sig skyldig till och därigenom kunna bedöma hur föreläggandet ska bemötas. Av föreläggandet bör det framgå under vilken tid och på vilken plats som överträdelsen har ägt rum samt vilken juridisk person som har begått den. Dessutom bör det framgå varför Finansinspektionen anser att den juridiska personens överträdelse är allvarlig och på vilka grunder inspektionen bedömer att den fysiska personen i fråga har orsakat överträdelsen uppsåtligen eller av grov oaktsamhet (jfr 9 § andra stycket). Bestämmelsen är uppbyggd på liknande sätt som 48 kap. 6 § rättegångsbalken, som avser strafföreläggande.

Enligt *andra stycket* ska sanktionsföreläggandet även innehålla en upplysning om att en ansökan om sanktion kan komma att ges in till domstol, om den fysiska personen i fråga inte godkänner sanktionsföreläggandet inom den tid som Finansinspektionen anger.

12 § Om ett sanktionsföreläggande inte har godkänts inom angiven tid, får Finansinspektionen ansöka hos domstol om att en sanktion ska beslutas. En sådan ansökan ska göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av Finansinspektionens beslut om ingripande mot den juridiska personen för samma överträdelse.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen anger det som gäller i fråga om domstolsprövning för det fall ett sanktionsföreläggande inte har godkänts. Paragrafen är utformad efter förebild av bl.a. 25 kap. 10 c § lagen om värdepappersmarknaden (prop. 2014/15:57 s. 73). Övervägandena finns i avsnitt 8.3.

Enligt *första stycket* får Finansinspektionen ansöka hos allmän förvaltningsdomstol om att en sanktion ska beslutas om ett sanktionsföreläggande inte har godkänts inom angiven tid. En sådan ansökan ska

göras hos den förvaltningsrätt som är behörig att pröva ett överklagande av Finansinspektionens beslut om ingripande mot den juridiska personen för samma överträdelse, dvs. Förvaltningsrätten i Stockholm.

I *andra stycket* anges att det krävs prövningstillstånd vid överklagande till kammarrätten.

13 § Ett sanktionsföreläggande enligt 10 § är utan verkan, om föreläggandet inte har delgetts den som det riktas mot inom två år från den tidpunkt då överträdelsen ägde rum. I ett sådant fall får inte heller någon sanktion enligt 12 § första stycket beslutas.

Paragrafen utgör en preskriptionsbestämmelse för sanktionsföreläggan-den. Paragrafen är utformad efter förebild av bl.a. 25 kap. 10 d § lagen om värdepappersmarknaden (prop. 2014/15:57 s. 73 och prop. 2022/23:124 s. 50–52). Övervägandena finns i avsnitt 8.3.

Av paragrafen följer att preskription kan ske när Finansinspektionen inte har utfärdat ett sanktionsföreläggande inom två år från tidpunkten för överträdelsen. Preskription kan även ske när Finansinspektionen har utfärdat ett sanktionsföreläggande, men utan att föreläggandet har blivit föremål för domstolsavgörande.

Vid delgivning av ett sanktionsföreläggande får det i normala fall anses vara olämpligt att använda kungörelsedelgivning och andra delgivningsformer enligt 3 § andra stycket, 34–38 och 47–51 §§ delgivningslagen (jfr 4 § den lagen).

Sanktionsavgifter

14 § Sanktionsavgiften för en finansiell entitet som anges i 2 § och som är en juridisk person ska som högst fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade en miljon euro,
2. tio procent av den finansiella entitetens omsättning närmast föregående räkenskapsår eller, i förekommande fall, motsvarande omsättning på koncernnivå, eller
3. tre gånger den vinst som den finansiella entiteten har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

Sanktionsavgiften får inte bestämmas till ett lägre belopp än 5 000 kronor.

Om en överträdelse har skett under den juridiska personens första verksamhetsår eller om uppgifter om omsättningen annars saknas eller är bristfälliga, får omsättningen uppskattas när den högsta sanktionsavgiften ska beräknas.

Paragrafen innehåller bestämmelser om storleken på sanktionsavgiften för en finansiell entitet, som anges i 2 §, som är en juridisk person. Paragrafen införs till följd av artikel 50.4 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 9 § lagen om värdepappersmarknaden (prop. 2006/07:115 s. 641 och prop. 2013/14:228 s. 319). Övervägandena finns i avsnitt 8.4.

I *första stycket* anges de olika beräkningsgrunderna för den högsta sanktionsavgift som får tas ut av en finansiell entitet som är en juridisk person för en överträdelse av DORA-förordningen.

Enligt *punkt 1* får sanktionsavgiften fastställas till ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 1 000 000 euro. Vid omräkning mellan euro och svenska kronor tillämpas den s.k. fixingkursen

som dagligen fastställs av Nasdaq Stockholm AB och publiceras på Riksbankens webbplats. Enligt fixingkursen den 16 januari 2023 motsvarade 1 euro 11,2691 svenska kronor.

Enligt *punkt 2* får sanktionsavgiften uppgå till tio procent av den finansiella entitetens omsättning närmast föregående räkenskapsår eller, i förekommande fall, motsvarande omsättning på koncernivå. Omsättningen på koncernnivå bör bestämmas utifrån den senast tillgängliga koncernredovisning som godkänts av ledningsorganet för det yttersta moderföretaget. Posterna för beräkningen av omsättningen på koncernnivå ska således hämtas ur koncernredovisningen för det yttersta moderföretaget.

Olika redovisningsregler kan dock gälla för företag inom en och samma koncern. För försäkringsföretag gäller reglerna i lagen (1995:1560) om årsredovisning i försäkringsföretag och för kreditinstitut och värdepappersbolag gäller reglerna i lagen (1995:1559) om årsredovisning i kreditinstitut och värdepappersbolag. För andra företag gäller reglerna i årsredovisningslagen (1995:1554).

Om den finansiella entitet som en sanktion ska riktas mot upprättar sin årsredovisning enligt årsredovisningslagen, är den omsättning som ska ligga till grund för sanktionsavgiften summan av nettoomsättningen och övriga rörelseintäkter. Om sanktionsavgiften ska beräknas på koncernnivå ska motsvarande årsomsättning, dvs. summan av nettoomsättningen och övriga rörelseintäkter, ligga till grund för beräkningen av sanktionsavgiften. För en beskrivning av vilka poster som ska anses utgöra omsättning i ett kreditinstitut eller ett försäkringsföretag, se prop. 2016/17:162 s. 764 och prop. 2022/23:7 s. 245.

Med ”motsvarande omsättning” avses det som utgör omsättning enligt de redovisningsregler som gäller för den juridiska personen som sanktionen riktas mot. Det är således denna omsättning inom koncernen som ska ligga till grund för beräkningen av den högsta möjliga sanktionsavgiften. Om den finansiella entitet som är föremål för ingripande också är ett försäkringsföretag ska således all omsättning från försäkringsverksamhet inom koncernen anses vara motsvarande omsättning på koncernnivå. Om företaget som en sanktion ska riktas mot i stället upprättar sin årsredovisning enligt årsredovisningslagen, är den omsättning som ska ligga till grund för sanktionsavgiften summan av nettoomsättningen och övriga rörelseintäkter inom koncernen (prop. 2016/17:162 s. 764–766).

I *punkt 3* anges att sanktionsavgiften får uppgå till tre gånger den vinst som den finansiella entiteten gjort till följd av överträdelsen, om beloppet går att fastställa. Med vinst som gjorts avses ett nettobelopp som omfattar de vinster som erhållits och de förluster som undvikits, dvs. den fördel som erhållits (jfr samma prop. s. 640).

Avgifterna i beräkningsmodellerna är maximibelopp, vilket innebär att Finansinspektionen har möjlighet att fastställa sanktionsavgiften till det högsta av de beräknade beloppen, eller ett lägre belopp.

I *andra stycket* anges att sanktionsavgiften inte får bestämmas till ett lägre belopp än 5 000 kronor.

I *tredje stycket* finns bestämmelser om att omsättningen för bestämmandet av den högsta sanktionsavgiften enligt första stycket 2 i vissa fall får uppskattas. Bestämmelsen är utformad efter förebild av bl.a. 25 kap. 9 § andra stycket lagen om värdepappersmarknaden och 4 kap. 7 § lagen med kompletterande bestämmelser till EU:s förordning om referens-

värden. Bestämmelsen är tillämplig om Finansinspektionen ska använda sig av den beräkningsmodell avseende sanktionsavgift som utgår ifrån en finansiell entitets (eller, i förekommande fall, koncernens) omsättning och sådana uppgifter saknas.

I 20 § finns bestämmelser om vilka omständigheter Finansinspektionen ska beakta när sanktionsavgiftens storlek fastställs, se författningskommentaren till den paragrafen.

15 § Sanktionsavgiften för en leverantör av gräsrotsfinansieringstjänster får inte vara så stor att leverantören därefter inte uppfyller kraven enligt artikel 11 i Europaparlamentets och rådets förordning (EU) 2020/1503 av den 7 oktober 2020 om europeiska leverantörer av gräsrotsfinansieringstjänster för företag och om ändring av förordning (EU) 2017/1129 och direktiv (EU) 2019/1937 eller andra bestämmelser om soliditet och likviditet som gäller för leverantören.

Paragrafen innehåller en särskild bestämmelse om storleken på en sanktionsavgift för en leverantör av gräsrotsfinansieringstjänster. Övervägandena finns i avsnitt 8.4.

I paragrafen finns en begränsning av hur stor en sanktionsavgift får vara för en leverantör av gräsrotsfinansieringstjänster. En sådan sanktionsavgift får inte bestämmas till ett belopp som är så stort att en leverantör av gräsrotsfinansieringstjänster därefter inte uppfyller försiktighetskraven i artikel 11 i förordning (EU) 2020/1503 eller andra bestämmelser om soliditet och likviditet som gäller för en sådan leverantören (t.ex. 8 kap. 3 § lagen om värdepappersmarknaden för det fall leverantören även har tillstånd att bedriva värdepappersrörelse). Avsikten med detta är att förhindra att uttaget av sanktionsavgiften får till följd att tillstånd att driva verksamhet enligt förordning (EU) 2020/1503 eller annan rörelselagstiftning måste återkallas (se prop. 2020/21:206 s. 141).

16 § Sanktionsavgiften för en fysisk person ska som högst fastställas till det högsta av

1. ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 500 000 euro, eller
2. tre gånger den vinst som den fysiska personen har gjort till följd av regelöverträdelsen, om beloppet går att fastställa.

Paragrafen innehåller bestämmelser om storleken på sanktionsavgiften för en fysisk person. Paragrafen införs till följd av artiklarna 50.4 och 50.5 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 9 a § lagen om värdepappersmarknaden (prop. 2016/17:162 s. 640–641). Övervägandena finns i avsnitt 8.4.

I paragrafen anges två beräkningsgrunder för beräkning av den högsta sanktionsavgiften för en fysisk person vid överträdelser av DORA-förordningen.

Enligt *punkt 1* får sanktionsavgiften uppgå till ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 500 000 euro. I fråga om vilken valutakurs som bör tillämpas vid omräkning mellan euro och svenska kronor, se författningskommentaren till 14 § första stycket 1.

Enligt *punkt 2* ska sanktionsavgiften kunna uppgå till tre gånger den vinst som den fysiska personen gjort till följd av överträdelsen, om belop-

pet går att fastställa. I fråga om termen vinst, se författningskommentaren till 14 § första stycket 3.

Avgifterna i beräkningsmodellerna är maximibelopp, vilket innebär att Finansinspektionen har möjlighet att fastställa sanktionsavgiften till det högsta av de beräknade beloppen, eller ett lägre belopp.

I 20 § finns bestämmelser om vilka omständigheter Finansinspektionen ska beakta när sanktionsavgiftens storlek fastställs.

17 § Sanktionsavgifter tillfaller staten.

Paragrafen innehåller en bestämmelse om vem sanktionsavgifter ska tillfalla. Övervägandena finns i avsnitt 8.4.

Finansinspektionen får i vissa fall besluta om sanktionsavgifter (se 7 §). I 14–16 §§ finns bestämmelser om sådana avgifter. Enligt paragrafen ska sanktionsavgifter tillfalla staten.

Val av ingripande

18 § Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått samt graden av ansvar hos den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen.

Paragrafen innehåller, tillsammans med 19–21 §§, bestämmelser om omständigheter som ska beaktas vid valet av ingripande. Paragrafen införs till följd av artikel 51.2 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 2 § första stycket lagen om värdepappersmarknaden (prop. 2016/17:162 s. 753). Övervägandena finns i avsnitt 8.5.

I paragrafen anges att Finansinspektionen vid valet av ingripande ska ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått (artikel 51.2 a i DORA-förordningen). Särskild hänsyn ska tas till överträdelsens art (jfr artikel 51. a.), överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått (artikel 50.2 e) samt graden av ansvar hos den fysiska eller juridiska person som har begått överträdelsen (artikel 51.2 b). Uppräkningen av omständigheter är inte uttömmande, utan en sammanvägd bedömning av alla relevanta omständigheter ska göras. Sanktionerna ska alltid vara proportionella i förhållande till överträdelsen och ligga på en sådan nivå att de är avskräckande. I fråga om varaktighet gäller att en överträdelse som har pågått under lång tid i allmänhet är mer klandervärd än en som har varat kortare tid.

Att graden av ansvar hos den som har begått överträdelsen ska beaktas innebär att en överträdelse som begås medvetet typiskt sett bör motivera en strängare sanktion än en överträdelse som begås av oaktsamhet. Att en överträdelse begås i vinningssyfte eller för att vilseleda bör i allmänhet inverka i försvårande riktning. I 19 § anges ytterligare några omständigheter som ska beaktas som försvårande respektive förmildrande. Bestämmelser om att Finansinspektionen i vissa fall får avstå från ingripande finns i 21 §. Finansinspektionen kan utifrån vad som är motiverat i det enskilda fallet välja att ingripa med en eller flera sanktionsåtgärder. Om flera åtgär-

der används, måste inspektionen se till att sanktionerna sammantaget är väl avvägda.

19 § Utöver det som anges i 18 § ska det i försvårande riktning beaktas om den som har begått överträdelsen tidigare har begått en överträdelse. Vid denna bedömning ska särskild vikt fästas vid om överträdelserna är likartade och den tid som har gått mellan de olika överträdelserna.

I förmildrande riktning ska det beaktas om den som har begått överträdelsen

1. i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och
2. snabbt upphört med överträdelsen eller snabbt verkat för att överträdelsen ska upphöra, sedan den anmälts till eller påtalats av Finansinspektionen.

Paragrafen innehåller, tillsammans med 18, 20 och 21 §§, bestämmelser om omständigheter som ska beaktas vid valet av ingripande. Paragrafen införs till följd av artikel 51.2 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 2 a § lagen om värdepappersmarknaden (prop. 2013/14:228 s. 319). Övervägandena finns i avsnitt 8.5.

Enligt *första stycket* ska Finansinspektionen, utöver det som anges i 18 §, i försvårande riktning beakta om den juridiska personen eller den fysiska personen tidigare har begått en överträdelse (artikel 51.2 g i DORA-förordningen). Vid denna bedömning ska särskild vikt fästas vid om överträdelserna är likartade och den tid som har gått mellan de olika överträdelserna.

Enligt *andra stycket 1* ska Finansinspektionen i förmildrande riktning beakta om den som har begått överträdelsen i väsentlig utsträckning genom ett aktivt samarbete har underlättat inspektionens utredning (jfr artikel 51.2 f i DORA-förordningen). Att en finansiell entitet eller dess företrädare endast medverkar i utredningen på Finansinspektionens begäran och svarar på inspektionens frågor är inte tillräckligt för att detta krav ska anses uppfyllt. Det krävs i stället att samarbetet i väsentlig utsträckning har underlättat utredningen. Det kan handla om att personen i fråga självmant för fram viktig information som Finansinspektionen inte redan har. Särskilt stort avseende bör fästas vid om det är personen själv som frivilligt anmäler överträdelsen till Finansinspektionen och det är först genom de uppgifter som personen lämnar som inspektionen får tillräckligt underlag för att ingripa mot överträdelsen. När det gäller en juridisk person bör det typiskt sett krävas att det är den juridiska personen som genom ställföreträdare eller ombud medverkar i utredningen. Att en enskild befattningshavare vid den juridiska personen anmäler en överträdelse bör alltså inte beaktas i förmildrande riktning enligt denna bestämmelse. Bestämmelsen ska inte tolkas motsatsvis på så sätt att den som förnekar en överträdelse eller försvårar utredningen drabbas av en hårdare sanktion än vad som annars hade blivit fallet.

Enligt *andra stycket 2* ska Finansinspektionen i förmildrande riktning även beakta om den som har begått överträdelsen snabbt upphört med densamma eller snabbt verkat för att överträdelsen ska upphöra, sedan den anmälts till eller påtalats av inspektionen.

Uppräkningen av omständigheter i paragrafen är inte uttömmande, utan en sammanvägd bedömning av alla relevanta omständigheter ska göras. Att en person har förlorat sin anställning eller ålagts att betala ett skade-

stånd på grund av överträdelsen bör t.ex. kunna beaktas i förmildrande riktning

20 § När sanktionsavgiftens storlek fastställs ska särskild hänsyn tas till sådana omständigheter som anges i 18 och 19 §§ samt till den berörda fysiska eller juridiska personens finansiella ställning och, om det går att bestämma, den vinst som personen gjort till följd av överträdelsen.

Paragrafen innehåller bestämmelser om vilka omständigheter som ska beaktas när sanktionsavgiftens storlek ska fastställas. Paragrafen införs till följd av artikel 51.2 c och d i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 10 § lagen om värdepappersmarknaden (prop. 2013/14:228 s. 319). Övervägandena finns i avsnitt 8.5.

Enligt paragrafen ska när sanktionsavgiftens storlek fastställs särskild hänsyn tas till sådana omständigheter som anges i 18 och 19 §§, samt till den juridiska eller den fysiska personens finansiella ställning (jfr artikel 51.2c i DORA-förordningen) och, om det går att bestämma, den vinst som den personen gjort till följd av överträdelsen (jfr artikel 51.2 d i förordningen). När det gäller begreppet vinst, se författningskommentaren till 14 § första stycket 3. Uppräkningen av omständigheter som ska beaktas är inte uttömmande.

21 § Finansinspektionen får avstå från ingripande, om

1. överträdelsen är ringa eller ursäktlig,
2. den fysiska eller juridiska personen i fråga gör rättelse,
3. den fysiska personen har verkat för att den juridiska personen gör rättelse, eller
4. någon annan myndighet eller något annat organ har vidtagit åtgärder mot den fysiska eller juridiska personen och dessa åtgärder bedöms tillräckliga.

Paragrafen innehåller bestämmelser om att Finansinspektionen får avstå från ingripande i vissa fall. Paragrafen är utformad efter förebild av bl.a. 25 kap. 2 § andra stycket lagen om värdepappersmarknaden (prop. 2016/17:162 s. 753–754). Övervägandena finns i avsnitt 8.5.

Enligt paragrafen får Finansinspektionen avstå från ingripande om en överträdelse är ringa eller ursäktlig (punkt 1), om den juridiska personen eller fysiska personen gör rättelse (punkt 2), den fysiska personen har verkat för att den juridiska personen ska göra rättelse (punkt 3) eller om någon annan myndighet eller något annat organ har vidtagit åtgärder mot den juridiska eller fysiska personen och dessa åtgärder bedöms tillräckliga (punkt 4).

Verkställighet av beslut om sanktionsavgift

22 § En sanktionsavgift ska betalas till Finansinspektionen inom 30 dagar efter det att ett beslut eller en dom om att ta ut avgiften har fått laga kraft eller ett sanktionsföreläggande har godkänts, eller efter den längre tid som anges i beslutet eller föreläggandet.

23 § Om sanktionsavgiften inte har betalats inom den tid som anges i 22 §, ska Finansinspektionen lämna avgiften för indrivning.

Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

24 § En sanktionsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet eller domen om att ta ut avgiften fick laga kraft eller sanktionsföreläggandet godkändes.

Paragraferna innehåller bestämmelser om verkställighet av beslut om sanktionsavgift. De motsvarar det som gäller beträffande verkställighet av beslut om sanktionsavgift enligt bl.a. 25 kap. 25–28 §§ lagen om värdepappersmarknaden (prop. 2006/07:115 s. 645 och prop. 2015/16:26 s. 150–151). Övervägandena finns i avsnitt 8.6.

I *22 §* anges inom vilken tid en sanktionsavgift ska betalas. När beslutet har fått laga kraft får det verkställas som en exekutionstitel (se 3 kap. 1 § första stycket 6 a och 20 § första stycket utsökningsbalken).

Om en avgift inte betalas i tid ska Finansinspektionen enligt *23 §* lämna den för indrivning.

Om verkställighet inte har skett inom fem år från det att beslutet eller domen om att ta ut avgiften fått laga kraft eller sanktionsföreläggandet godkändes faller sanktionsavgiften bort enligt preskriptionsbestämmelsen i *24 §*. Det som preskriberas är den del av avgiften som inte har drivits in när fem år har gått sedan beslutet eller domen fick laga kraft.

Vite

25 § Ett beslut om föreläggande eller förbud får förenas med vite.

Paragrafen innehåller en bestämmelse om att Finansinspektionen får förena ett beslut med vite. Paragrafen är utformad efter förebild av bl.a. 4 kap. 3 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering. Övervägandena finns i avsnitt 7.2, 8.2.2 och 8.3.

Finansinspektionen får förena ett beslut med vite. Det gäller såväl beslut om föreläggande som beslut om förbud. Till exempel kan ett beslut om att en finansiell entitet ska vidta viss åtgärd eller upphöra med visst agerande (3 § första stycket 1) förenas med vite. Även ett beslut om att en fysisk person inte får vara styrelseledamot, verkställande direktör eller ersättare för någon av dem (9 § tredje stycket 1) får förenas med vite. Dessutom får ett föreläggande om att tillhandahålla uppgifter, handlingar eller annat (3 kap. 2 § första stycket 1) förenas med vite.

Det är däremot inte möjligt att förena ett sanktionsföreläggande (10 §) med vite. Man kan således inte förelägga någon att svara på ett sanktionsföreläggande vid äventyr av vite (10 § andra stycket). Dock får sanktionen i sanktionsföreläggandet, dvs. själva ingripandet, förenas med vite (11 § första stycket 4).

Finansinspektionen har inte rätt att självt besluta om utdömande av vite. Ett utdömande sker i stället genom att inspektionen ansöker om detta hos allmän förvaltningsdomstol (6 § lagen [1985:206] om viten).

5 kap. Överklagande och beslut som ska gälla omedelbart

Överklagande av Finansinspektionens beslut

1 § Finansinspektionens beslut om sanktionsföreläggande enligt denna lag får inte överklagas.

Andra beslut som Finansinspektionen meddelar enligt denna lag och EU-förordningen får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av Finansinspektionens beslut. Paragrafen införs till följd av artikel 50.6 i DORA-förordningen. Den är utformad efter förebild av bl.a. 4 kap. 1 § lagen med kompletterande bestämmelser till EU:s förordning om värdepapperisering. Övervägandena finns i avsnitt 15.1.

Enligt *första stycket* får Finansinspektionens beslut om sanktionsföreläggande inte överklagas. Ett godkänt sanktionsföreläggande kan inte angripas med ordinära rättsmedel. I undantagsfall kan det dock vara möjligt att ansöka om resning enligt 37 b § förvaltningsprocesslagen (1971:291). Resning förutsätter att det på grund av något särskilt förhållande finns synnerliga skäl att pröva saken på nytt (prop. 2014/15:57 s. 64–65).

Enligt *andra stycket* får Finansinspektionens andra beslut enligt lagen och DORA-förordningen överklagas till allmän förvaltningsdomstol. Närmare bestämmelser om överklagande finns i förvaltningslagen (2017:900).

Enligt *tredje stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Överklagande av Riksbankens beslut

2 § Riksbankens beslut om föreläggande enligt 2 kap. 5 § och beslut om utfärdande av intyg enligt artikel 26.7 i EU-förordningen får överklagas till allmän förvaltningsdomstol.

Andra beslut som Riksbanken fattar enligt denna lag och EU-förordningen får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av Riksbankens beslut. Övervägandena finns i avsnitt 15.2.

I *första stycket* anges att Riksbankens beslut om föreläggande att lämna uppgifter enligt 2 kap. 5 § och beslut om intyg om godkänd hotbildsstyrd penetrationstestning enligt artikel 26.7 i DORA-förordningen får överklagas till allmän förvaltningsdomstol.

Enligt *andra stycket* får inte andra beslut som Riksbanken fattar enligt denna lag och förordningen överklagas. Det handlar om sådana delbeslut som Riksbanken fattar vid övervakningen och samordningen av den hotbildsstyrda penetrationstestningen enligt 2 kap. 2 §.

Enligt *tredje stycket* krävs prövningstillstånd vid överklagande till kammarrätten.

Beslut som kan gälla omedelbart

3 § Finansinspektionen får bestämma att ett beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart.

Paragrafen innehåller bestämmelser om att Finansinspektionen får bestämma att ett beslut av inspektionen ska gälla omedelbart. Den är utformad efter förebild av bl.a. 26 kap. 1 § fjärde stycket lagen om värdepappersmarknaden. Övervägandena finns i avsnitt 15.1.

Enligt paragrafen får Finansinspektionen bestämma att beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart. Möjligheten att bestämma att ett beslut om föreläggande, förbud eller återkallelse ska gälla omedelbart kan t.ex. användas om det behövs för att stoppa ett agerande eller se till att rättelse görs med omedelbar verkan (4 kap. 3§ 1 och 4 § första stycket 1), att återkalla ett tillstånd med omedelbar verkan (4 kap. andra stycket) eller att en fysisk person under viss tid inte får vara styrelseledamot eller verkställande direktör, eller ersättare för någon av dem i en finansiell entitet (4 kap. 9 § tredje stycket 1). När det gäller andra beslut av Finansinspektionen gäller förvaltningslagens bestämmelser om omedelbar verkställighet (35 § tredje stycket den lagen).

20.2 Förslaget till lag om ändring i lagen (1967:531) om tryggande av pensionsutfästelse m.m.

16 g § En pensionsstiftelse som avses i 9 a § andra eller tredje stycket ska upprätta och följa riktlinjer för

1. riskhantering,
2. internrevision, och
3. verksamhet som omfattas av uppdragsavtal.

Pensionsstiftelsen ska upprätta och vid behov följa en beredskapsplan som säkerställer att verksamheten kan bedrivas kontinuerligt. *Stiftelsen ska ha sådana nätverks- och informationssystem som avses i 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.*

Pensionsstiftelsen ska upprätta och följa en sund ersättningspolicy för personer som leder eller övervakar verksamheten eller på annat sätt kan påverka riskerna i verksamheten. Stiftelsen ska regelbundet offentliggöra relevant information om ersättningspolicyn.

Paragrafen innehåller bestämmelser om styrdokument (riktlinjer). Genom ändringen genomförs delvis artikel 21.5 i andra tjänstepensionsdirektivet, i lydelsen enligt artikel 8 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). En pensionsstiftelse som tryggar utfästelser om pension till minst 16 personer omfattas av DORA-förordningen i dess egenskap av tjänstepensionsinstitut och är i

och med det en finansiell entitet enligt förordningen (artikel 2.1 p och 2.2 i DORA-förordningen).

I *andra stycket* förtydligas att en pensionsstiftelse ska ha sådana nätverks- och informationssystem som avses i DORA-förordningen. Kraven på styrdokument och de tillkommande kraven gäller dock bara för pensionsstiftelser som tryggar utfästelser om pension till minst 100 personer (9 a §, se även prop. 2018/19:159 s. 34–37). De närmare kraven på nätverks- och informationssystemen och hur de ska utformas anges i DORA-förordningen. En motsvarande ändring görs för tjänstepensionsföretag i lagen (2019:742) om tjänstepensionsföretag (se 9 kap. 2 § och författningskommentaren till den paragrafen).

20.3 Förslaget till lag om ändring i trafikskadelagen (1975:1410)

5 § Trafikförsäkring får meddelas av

1. en försäkringsgivare som har fått tillstånd till det enligt 2 kap. 4 § försäkringsrörelselagen (2010:2043),
2. en försäkringsgivare som har fått tillstånd till det enligt 4 kap. 1 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, och
3. en EES-försäkringsgivare som är verksam i Sverige enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige.

En försäkringsgivare som får meddela trafikförsäkring är skyldig att på begäran meddela trafikförsäkring. I ett tillstånd enligt 2 kap. 4 § försäkringsrörelselagen eller 4 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige *får* dock skyldigheten begränsas till att gälla försäkring åt personer som tillhör en viss yrkesgrupp eller intressegrupp eller som är bosatta inom ett visst område. Finansinspektionen *får* efter ansökan besluta om motsvarande begränsning för försäkringsgivare som driver verksamhet här enligt 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige. Finansinspektionens beslut får överklagas *till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten.*

En försäkringsgivare som avser att meddela trafikförsäkring genom gränsöverskridande verksamhet med stöd av 2 kap. 1 § lagen om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige men som inte har fast driftställe i Sverige ska ha en representant här i landet. Representanten ska vara bosatt i Sverige eller vara en svensk juridisk person. Försäkringsgivaren ska utfärda en fullmakt för representanten att gentemot skadelidande företräda försäkringsgivaren och att själv eller genom någon annan tala och svara för denne angående försäkringsfall. Representanten ska även ha behörighet att företräda försäkringsgivaren vid kontroll av om det finns en giltig trafikförsäkring. Försäkringsgivaren ska informera försäkringstagarna om vem som är försäkringsgivarens representant och om dennes adress. Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om villkor för sådana representanter.

Paragrafen innehåller bestämmelser om meddelande av trafikförsäkring. Övervägandena finns i avsnitt 17.3.

En försäkringsgivare som får meddela trafikförsäkring har enligt *andra stycket* också en skyldighet att meddela sådan försäkring, den s.k. kontraheringsplikten. Finansinspektionen kan begränsa denna skyldighet till att

bara gälla försäkring åt personer som tillhör en viss yrkesgrupp eller intressegrupp eller som är bosatta inom ett visst område. Detta kan för svenska försäkringsgivare och försäkringsgivare från tredje land ske i det grundläggande tillståndet att meddela försäkring. En EES-försäkringsgivare, dvs en försäkringsgivare med hemvist i ett annat land inom EES, som inte behöver något särskilt tillstånd av Finansinspektionen för att meddela försäkringar i Sverige kan i stället ansöka hos Finansinspektionen om en motsvarande begränsning. Stycket ändras så att ett sådant beslut av Finansinspektionen får överklagas till allmän förvaltningsdomstol, i stället för som hittills gällt till regeringen. Prövningstillstånd krävs vid överklagande till kammarrätten. I stycket görs även språkliga ändringar. Inga ändringar i sak avses.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2025.
2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

Övervägandena finns i avsnitt 18.

I *punkt 1* anges när lagen träder i kraft.

Enligt *punkt 2* ska äldre föreskrifter gälla för överklagande av beslut som meddelats före ikraftträdandet. Det innebär att ett beslut om begränsad kontraheringsplikt för en EES-försäkringsgivare får överklagas till regeringen om Finansinspektionen har meddelat beslutet före ikraftträdandet.

20.4 Förslaget till lag om ändring i lagen (1980:1097) om Svenska skeppshypotekskassan

38 § Kassan står under tillsyn av Finansinspektionen.

Vid meddelande av föreläggande eller förbud i samband med tillsynen *får* Finansinspektionen förelägga vite.

Inspektionens beslut enligt denna lag får överklagas *till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätten*. Inspektionens beslut har omedelbar verkan, om inte annat beslutas.

Regeringen meddelar ytterligare föreskrifter om tillsynsverksamheten.

Paragrafen innehåller bestämmelser om tillsynen över Svenska skeppshypotekskassan. Övervägandena finns i avsnitt 17.4.

I *andra stycket* görs en språklig ändring. Ingen ändring avses i sak.

Tredje stycket ändras så att de beslut som Finansinspektionen fattar enligt lagen får överklagas till allmän förvaltningsdomstol, i stället för som hittills gällt till regeringen. Prövningstillstånd krävs vid överklagande till kammarrätten.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 17 januari 2025.
2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

Övervägandena finns i avsnitt 18.

I *punkt 1* anges när lagen träder i kraft.

Enligt *punkt 2* ska äldre föreskrifter gälla för överklagande av beslut som meddelats före ikraftträdandet. Det innebär att Finansinspektionens beslut enligt lagen får överklagas till regeringen om inspektionen har meddelat beslutet före ikraftträdandet.

20.5 Förslaget till lag om ändring i lagen (1998:1479) om värdepapperscentraler och kontoföring av finansiella instrument

9 kap.

12§ Finansinspektionen ska ingripa mot någon som ingår i en svensk värdepapperscentrals styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepapperscentralen

1. tillhandahåller tjänster enligt avsnitten A, B och C i bilagan till förordningen om värdepapperscentraler, i den ursprungliga lydelsen, i strid med artiklarna 16, 25 eller 54 i förordningen,
2. har fått auktorisationer som krävs enligt artikel 16 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen, genom osanna uppgifter eller andra olagliga metoder enligt artikel 20.1 b i förordningen,
3. låtit bli att uppfylla kapitalkravet i strid med artikel 47.1 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
4. låtit bli att uppfylla de organisatoriska kraven i strid med artiklarna 26–30 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
5. låtit bli att följa uppföranderegelerna i strid med artiklarna 32–35 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
6. låtit bli att uppfylla kraven för värdepapperscentraltjänster i strid med artiklarna 37–41 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
7. låtit bli att uppfylla stabilitetskraven i strid med artiklarna 43–47 i förordningen om värdepapperscentraler, i den ursprungliga lydelsen,
8. låtit bli att uppfylla kraven på länkar mellan värdepappers-centraler i strid med artikel 48 i förordningen om värdepappers-centraler, i den ursprungliga lydelsen,
9. utan giltig grund vägrat att bevilja olika typer av tillträde i strid med artiklarna 49–53 i förordningen om värdepappers-centraler, i den ursprungliga lydelsen, *eller*
10. *har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.*

Ett ingripande enligt första stycket får ske endast om värdepapperscentralens överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, eller, för upprepade allvarliga överträdelser, permanent inte får vara styrelseledamot, verkställande direktör eller ersättare för någon av dem i värdepapperscentralen, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om när Finansinspektionens ska ingripa mot någon som ingår i en svensk värdepapperscentrals styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepapperscentralen har gjort sig skyldig till en överträdelse. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 18.3.

Genom *första stycket 10*, som är ny, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för en värdepapperscentral om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen. Övriga ändringar i stycket är redaktionella.

I *andra stycket* görs en språklig ändring.

20.6 Förslaget till lag om ändring i lagen (2004:46) om värdepappersfonder

2 kap.

17 § Ett fondbolag ska ha sunda rutiner för

1. förvaltning av verksamheten och redovisning,
2. intern kontroll, och
3. drift och förvaltning av sina informationssystem.

Rutinerna enligt första stycket 3 ska uppfylla kraven i 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.

Fondbolaget ska särskilt

1. upprätta och tillämpa regler för styrelseledamöters och anställdas egna affärer med finansiella instrument,

2. dokumentera samtliga transaktioner som bolaget har genomfört för en värdepappersfonds räkning eller för ett sådant fondföretags räkning som avses i 12 § andra stycket eller 15 § andra stycket, och

3. ha en organisation som minskar risken för intressekonflikter som kan påverka fondandelsägares eller andra kunders intressen negativt.

Paragrafen innehåller bestämmelser om grundläggande krav på fondbolags organisation. Genom ändringen genomförs artikel 12.1 i UCITS-direktivet, i lydelsen enligt artikel 1.1 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). Ett fondbolag omfattas av DORA-förordningen i dess egenskap av förvaltningsbolag och

är i och med det en finansiell entitet enligt förordningen (artikel 2.1 l och 2.2 i DORA-förordningen).

I det nya *andra stycket* förtydligas kraven på ett fondbolags informationssystem (första stycket 3). Rutinerna för drift och förvaltning av dessa system ska uppfylla kraven i DORA-förordningen. De närmare kraven anges i DORA-förordningen. En motsvarande ändring görs för AIF-förvaltare i lagen (2013:561) om förvaltare av alternativa investeringsfonder (se 8 kap. 2 § och författningskommentaren till den paragrafen).

I det nya *tredje stycket*, hittillsvarande andra stycket, görs en redaktionell ändring då den tidigare strecklistan ändras till en punktlista.

12 kap.

1 a § Finansinspektionen ska ingripa mot någon som ingår i ett fondbolags styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om fondbolaget

1. har fått tillstånd att driva fondverksamhet genom att lämna falska uppgifter eller på annat otillbörligt sätt,
2. tillhandahåller diskretionär portföljförvaltning i strid med 1 kap. 4 §,
3. påbörjar marknadsföring av en av bolaget förvaltad värdepappersfond i ett annat land inom EES innan en underrättelse om detta gjorts hos Finansinspektionen i enlighet med 2 kap. 15 c §,
4. inte uppfyller grundläggande krav på organisation och drift av verksamheten enligt 2 kap. 17 eller 17 f § eller föreskrifter som har meddelats med stöd av 13 kap. 1 § 11 avseende dessa bestämmelser,
5. åsidosätter sina skyldigheter eller på annat sätt överträder det som anges om uppdragsavtal i någon av 4 kap. 4–6 §§ eller 7 § första stycket,
6. påbörjar förvaltning och marknadsföring av en värdepappersfond utan att fondbestämmelserna godkänts enligt 4 kap. 9 §,
7. vid upprepade tillfällen låter bli att upprätta eller tillhandahålla informationsbroschyr, faktablad, årsberättelse och halvårsberättelse i enlighet med 4 kap. 15–21 §§,
8. vid upprepade tillfällen placerar medel i en värdepappersfond i strid med det som anges i någon av 5 kap. 1, 3–22, 24 eller 25 §§ eller i föreskrifter som har meddelats med stöd av 13 kap. 1 § 21, 22, 24 och 25 avseende dessa bestämmelser,
9. inte uppfyller kraven på hantering av risker i 5 kap. 2 § första eller andra stycket eller i föreskrifter som har meddelats med stöd av 13 kap. 1 § 23 avseende dessa bestämmelser,
10. i strid med 11 kap. 5 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,
11. i strid med 11 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier i bolaget samt storleken på innehavet,
12. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen*, eller*

13. har åsidosatt sina skyldig-heter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Om en sådan person som anges i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 11 kap. 1 eller 4 § för förvärv eller avyttring av

aktier i bolaget, ska första stycket 10 och 11 inte gälla för den personen i fråga om dessa aktier.

Ett ingripande enligt första stycket får ske endast om bolagets överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, eller, för upprepade allvarliga överträdelser, permanent inte får vara styrelseledamot eller verkställande direktör i ett fondbolag, eller ersättare för någon av dem, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om när Finansinspektionens ska ingripa mot någon som ingår i ett fondbolags styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om fondbolaget har gjort sig skyldig till en överträdelse. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *första stycket 13*, som är ny, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för ett fondbolag om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen. Övriga ändringar i stycket är redaktionella.

I *tredje stycket* görs en språklig ändring.

20.7 Förslaget till lag om ändring i lagen (2004:297) om bank och finansieringsrörelse

6 kap.

3 § Ett kreditinstitut ska identifiera, mäta, styra, internt rapportera och ha kontroll över de risker som dess rörelse är förknippad med. *Nätverks- och informationssystem ska uppfylla kraven i 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.* Institutet ska se till att det har en tillfredsställande intern kontroll. Det ska också upprätta en återhämtningsplan eller koncernåterhämtningsplan enligt 6 a kap.

Ett kreditinstitut ska särskilt se till att dess kreditrisker, marknadsrisker, operativa risker och andra risker sammantagna inte medför att institutets förmåga att fullgöra sina förpliktelser äventyras. För att uppfylla detta krav ska det åtminstone ha metoder som gör det möjligt att fortlöpande värdera och upprätthålla ett kapital som till belopp, slag och fördelning är tillräckligt för att täcka arten och nivån på de risker som det är eller kan komma att bli exponerat för. Institutet ska utvärdera dessa metoder för att säkerställa att de är heltäckande.

Ett kreditinstitut ska på grundval av de metoder som avses i andra stycket fastställa tillräckliga kapitalbasnivåer.

Paragrafen innehåller bestämmelser om riskhantering. Genom ändringen genomförs delvis artikel 74.1 i kapitaltäckningsdirektivet, i lydelsen enligt artikel 4.2 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin

verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). Ett kreditinstitut omfattas av DORA-förordningen och är i och med det en finansiell entitet enligt förordningen (artikel 2.1 a och 2.2 i DORA-förordningen).

I *första stycket* förtydligas att ett kreditinstituts nätverks- och informationssystem ska uppfylla kraven i DORA-förordningen. De närmare kraven anges i DORA-förordningen. Bestämmelsen gäller även för de värdepappersbolag som ska tillämpa bestämmelserna om kapitaltäckning i lagen (8 kap. 1 c § lag [2007:528] om värdepappersmarknaden, se även prop. 2020/21:173 s. 134–142).

10 kap.

1 § För bankaktiebolag gäller föreskrifterna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller är särskilt föreskrivet. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag som gäller i stället för eller utöver bestämmelserna i aktiebolagslagen.

I fråga om bankaktiebolag ska det som anges om Bolagsverket i följande bestämmelser avse Finansinspektionen:

1. 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,
2. 23 kap. 45 b § aktiebolagslagen,
3. 24 kap. 47 § aktiebolagslagen, och
4. 24 a kap. 24 § aktiebolagslagen.

Av paragrafen framgår vilka associationsrättsliga regler som gäller för bankaktiebolag.

I *andra stycket* görs en redaktionell ändring då den tidigare strecklistan ändras till en punktlista.

15 kap.

1 a § Finansinspektionen ska ingripa mot någon som ingår i ett kreditinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om kreditinstitutet

1. har fått tillstånd att driva bank- eller finansieringsrörelse genom att lämna falska uppgifter eller på annat otillbörligt sätt,
2. i strid med 14 kap. 4 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,
3. i strid med 14 kap. 4 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier eller andelar i institutet samt storleken på innehaven,
4. inte uppfyller kraven i 6 kap. 1–3 c, 4, 4 a, 4 c eller 5 § eller i föreskrifter som har meddelats med stöd av 16 kap. 1 §5,
5. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om efterlevnaden av skyldigheten att uppfylla kapitalbaskraven enligt artikel 92 i tillsynsförordningen, i strid med artikel 430.1 i den förordningen,
6. låter bli att rapportera eller lämnar ofullständig eller felaktig information till Finansinspektionen när det gäller data som avses i artikel 430a i tillsynsförordningen,

7. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om en stor exponering i strid med artikel 394.1 i tillsynsförordningen,

8. låter bli att lämna information till Finansinspektionen eller lämnar ofullständig eller felaktig information om likviditet i strid med artikel 415.1 och 415.2 i tillsynsförordningen,

9. låter bli att lämna uppgifter till Finansinspektionen eller lämnar ofullständig eller felaktig information om sin bruttosoliditet i strid med artikel 430.1 och 430.2 i tillsynsförordningen,

10. vid upprepade tillfällen eller systematiskt låter bli att hålla likvida tillgångar i strid med artikel 412 i tillsynsförordningen,

11. utsätter sig för en exponering som överskrider gränserna enligt artikel 395 i tillsynsförordningen,

12. är exponerat för kreditrisken i en värdepapperiseringsposition utan att uppfylla villkoren i artikel 405 i tillsynsförordningen,

13. låter bli att lämna information eller lämnar ofullständig eller felaktig information i strid med någon av artiklarna 431.1–431.3 och 451.1 i tillsynsförordningen,

14. gör betalningar till innehavare av instrument som ingår i institutets kapitalbas i strid med 8 kap. 3 och 4 §§ lagen (2014:966) om kapitalbuffertar eller artikel 28, 51 eller 63 i tillsynsförordningen, när dessa artiklar förbjuder sådana betalningar till innehavare av instrument som ingår i kapitalbasen,

15. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen,

16. har befunnits ansvarigt för en allvarlig, upprepad eller systematisk överträdelse av Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtföljа överföringar av medel och om upphävande av förordning (EG) nr 1781/2006,

17. har tillåtit en styrelseledamot, verkställande direktören eller ersättare för någon av dem att åta sig ett sådant uppdrag i institutet eller kvarstå i institutet trots att kraven i 3 kap. 2 § första stycket 4 eller 5, 10 kap. 8 a–8 c §§ eller 12 kap. 6 a–6c §§ eller i föreskrifter som har meddelats med stöd av 16 kap. 1 § 3 inte är uppfyllda,

18. i strid med 6 a kap. 1 eller 2 § låter bli att upprätta eller lämna in en återhämtningsplan eller en koncernåterhämtningsplan,

19. i strid med 6 b kap. 11 § låter bli att anmäla att koncerninternt finansiellt stöd ska lämnas,

20. i strid med 13 kap. 4 a och 5 a §§ låter bli att underrätta Finansinspektionen om institutet fallerar eller sannolikt kommer att fallera,

21. inte uppfyller kravet på kapitalbas och kvalificerade skulder enligt 4 kap. lagen (2015:1016) om resolution eller i strid med 28 kap. 1 § samma lag låter bli att lämna begärda upplysningar till Riksgäldskontoret,

22. är ett moderföretag enligt artikel 4.1.15 i tillsynsförordningen och inte uppfyller kraven i del tre, fyra, sex eller sju i den förordningen eller 2 kap. 1 eller 2 § lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag på grupp- eller undergruppsnivå,

23. omfattas av tillståndsplikt enligt lagen (2003:1223) om utgivning av säkerställda obligationer och

a) har fått tillstånd att ge ut säkerställda obligationer genom att lämna falska uppgifter eller på något annat otillbörligt sätt,

b) driver verksamhet med säkerställda obligationer utan tillstånd,

c) ger ut säkerställda obligationer som inte uppfyller 3 kap. 1, 2, 3, 4, 5, 6, 7, 10, 11 eller 15 § eller 16 § andra stycket lagen om utgivning av säkerställda obligationer,

d) låter bli att lämna information eller lämnar ofullständig eller felaktig information i strid med 3 kap. 16 § första stycket lagen om utgivning av säkerställda obligationer, eller

e) vid upprepade tillfällen eller systematiskt låter bli att hålla likvida tillgångar i en sådan likviditetsbuffert som avses i 3 kap. 9 a § lagen om utgivning av säkerställda obligationer,

24. låter bli att lämna uppgifter om sin verksamhet med säkerställda obligationer till Finansinspektionen eller lämnar ofullständiga eller felaktiga uppgifter i strid med 13 kap. 3 §, *eller*

25. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Om en sådan person som anges i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 14 kap. 1 eller 3 § för förvärv eller avyttring av aktier eller andelar i institutet, ska första stycket 2 och 3 inte gälla för den personen i fråga om dessa aktier eller andelar.

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och *den fysiska* personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett kreditinstitut, eller ersättare för någon av dem, eller

2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om när Finansinspektionen ska ingripa mot någon som ingår i ett kreditinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om kreditinstitutet har gjort sig skyldig till en överträdelse. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *första stycket 25*, som är ny, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för ett kreditinstitut om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen. Övriga ändringar i stycket är redaktionella.

I *tredje stycket* görs en språklig ändring.

17 kap.

1 § Finansinspektionens beslut enligt 13 kap. 12 § och 15 kap. 9 a § och 18 § tredje stycket får inte överklagas. *Detsamma gäller för sådana beslut om förordnande av sakkunnig som avses i 10 kap. 1 § andra stycket 2–4.*

Andra beslut av Finansinspektionen enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Inspektionen får bestämma att ett beslut om förbud, föreläggande eller återkallelse ska gälla omedelbart.

Paragrafen innehåller bestämmelser om överklagande av Finansinspektionens beslut. Övervägandena finns i avsnitt 17.1 och 17.2.

Första stycket ändras så att ett beslut om förordnande av sakkunnig i ärenden om gränsöverskridande fusion, delning eller ombildning inte får överklagas. Finansinspektionen kan förordna en sakkunnig i denna typ av ärenden om det vid handläggningen uppkommer en fråga som kräver

särskild fackkunskap (se t.ex. 23 kap. 45 b § aktiebolagslagen [2005:551] och 10 kap. 1 § denna lag). Sökanden ska ersätta inspektionen för kostnaden för den sakkunniga i enlighet med ett beslut som inspektionen fattar. Beslutet om betalningsskyldighet kan överklagas enligt den allmänna överklagandebestämmelsen (andra stycket). Vid överklagande av ett sådant beslut kan, utöver det debiterade beloppets skälighet, även prövas huruvida det var motiverat att förordna en sakkunnig.

Det hittillsvarande *andra stycket* om att Finansinspektionens beslut om undantag från bosättningskravet för styrelseledamöter, verkställande direktörer och särskilda firmatecknare överklagas till regeringen utgår. I stället ska de allmänna bestämmelserna för överklaganden gälla, dvs nya andra stycket (hittillsvarande tredje stycket) och nya tredje stycket (hittillsvarande fjärde stycket). Ett beslut i dessa frågor ska således överklagas till allmän förvaltningsdomstol och prövningstillstånd krävs vid överklagande till kammarrätten.

Andra–fjärde styckena överensstämmer med hittillsvarande tredje–femte styckena.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 17 januari 2025.
2. Äldre föreskrifter gäller fortfarande för överklagande av beslut som har meddelats före den 17 januari 2025.

Övervägandena finns i avsnitt 18.

I *punkt 1* anges när lagen träder i kraft.

Enligt *punkt 2* ska äldre föreskrifter gälla för överklagande av beslut som meddelats före ikraftträdandet. Det innebär att Finansinspektionens beslut om undantag från bosättningskraven för styrelseledamöter, verkställande direktör och särskild firmatecknare får överklagas till regeringen om inspektionen har meddelat beslutet före ikraftträdandet.

20.8 Förslaget till lag om ändring i lagen (2007:528) om värdepappersmarknaden

8 kap.

10 § Ett värdepappersinstitut ska ha tillräckliga system, resurser och rutiner för att institutet ska kunna tillhandahålla investeringstjänster och utföra investeringsverksamhet kontinuerligt och regelbundet. *Informations- och kommunikationstekniksystem ska uppfylla kraven i 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.*

Ett värdepappersinstitut ska ha sunda skyddsmekanismer för att*, i enlighet med kraven i Europaparlamentets och rådets förordning (EU) 2022/2554,* säkerställa skyddet och autentiseringen vid informationsöverföring och för att minimera risken för dataförvanskning och obehörig åtkomst till informationen.

Paragrafen innehåller bl.a. bestämmelser om ett värdepappersinstituts skyddssystem. Genom ändringarna genomförs artikel 16.4 och delvis

artikel 16.5 i MiFID II, i lydelsen enligt artikel 6.1 a och 6.1 b i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Värdepappersinstut är ett vidare begrepp än värdepappersbolag (jfr 8 kap. 4 §) och omfattar också ett svenskt kreditinstitut som har fått tillstånd enligt lagen att driva värdepappersrörelse eller ett utländskt företag som driver värdepappersrörelse från filial i Sverige eller genom att använda anknutna ombud etablerade i Sverige (1 kap. 4 b §). Även värdepappersinstitut omfattas av DORA-förordningen i dess egenskap av värdepappersföretag och de är i och med det en finansiell entitet enligt förordningen (artikel 2.1 e). Som för andra finansiella entiteter införs det genom DORA-förordningen nya krav också för värdepappersinstitutens riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet).

I *första stycket* förtydligas att ett värdepappersinstituts informations- och kommunikationstekniksystem (s.k. IKT-system) ska uppfylla kraven i DORA-förordningen. De närmare kraven anges i DORA-förordningen.

I *andra stycket* förtydligas att det särskilda kravet om skydd för viss information också ska uppfylla kraven enligt DORA-förordningen. Också i detta fall anges de närmare kraven i DORA-förordningen.

11 § Ett värdepappersinstitut *ska*
1. tillämpa sunda rutiner för
a) förvaltning av verksamheten, och
b) redovisning,
2. ha rutiner för intern kontroll, *och*
3. ha effektiva metoder för riskbedömning.

Paragrafen innehåller bl.a. bestämmelser om ett värdepappersinstituts rutiner för verksamheten. Genom ändringen genomförs delvis artikel 16.5 i MiFID II, i lydelsen enligt artikel 6.1 b i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Hittillsvarande *punkt 4*, att ett värdepappersinstitut ska ha effektiv drift och förvaltning av sina informationssystem, utgår då motsvarande och mer detaljerade krav ska gälla enligt DORA-förordningen. I paragrafen görs också en språklig ändring.

23 § Ett värdepappersinstitut som bedriver algoritmisk handel ska ha effektiva system och riskkontroller som är anpassade för den verksamheten. Systemen och kontrollerna ska säkerställa att institutets handelssystem är motståndskraftiga och har tillräcklig kapacitet *i enlighet med kraven i kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554*, att de omfattas av lämpliga handelströsklar och handelslimiter och att de förhindrar att felaktiga order skickas eller att systemet på annat sätt fungerar så att det kan skapa eller bidra till en oordnad marknad.

Värdepappersinstitutet ska också ha effektiva system och åtgärder för riskkontroll för att säkerställa att handelssystemen inte kan användas för något ändamål som strider mot marknadsmissbruksförordningen eller mot reglerna på en handelsplats till vilken institutet är anslutet.

Värdepappersinstitutet ska ha inrättat effektiva arrangemang för kontinuerlig drift av verksamheten för att hantera driftavbrott i sina handelssystem*, inbegripet en IKT-kontinuitetspolicy och IKT-kontinuitetsplaner samt IKT-relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik*

som inrättas i enlighet med artikel 11 i Europaparlamentets och rådets förordning (EU) 2022/2554. Institutet ska se till att systemen är fullt testade och lämpligt övervakade för att säkerställa att de uppfyller kraven i första och andra styckena och kraven i kapitlen II och IV i Europaparlamentets och rådets förordning (EU) 2022/2554

Värdepappersinstitutet ska dokumentera de åtgärder som det har vidtagit enligt första–tredje styckena så att Finansinspektionen har möjlighet att övervaka att institutet har följt denna lag.

I paragrafen finns bestämmelser om allmänna krav för algoritmisk handel. Genom ändringarna genomförs artikel 17.1 i MiFID II, i lydelsen enligt artikel 6.2 a i ändringsdirektivet. Övervägandena finns i avsnitt 16.

I *första stycket* förtydligas att värdepappersinstitut som bedriver algoritmisk handel ska uppfylla de strängare kraven för handelssystem i fråga om IKT-risker som följer av DORA-förordningen. De närmare kraven anges i DORA-förordningen.

I *tredje stycket* förtydligas att ett värdepappersinstituts arrangemang för kontinuerlig drift av verksamheten ska uppfylla DORA-förordningens krav på IKT-kontinuitetspolicy och IKT-kontinuitetsplaner samt IKT-relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik. Det förtydligas även att ett institut ska se till att handelssystemen är fullt testade och lämpligt övervakade för att säkerställa att de uppfyller kraven i dels första och andra styckena, dels DORA-förordningen. I stycket görs även en redaktionell ändring.

13 kap.

1 § En börs ska driva sin verksamhet hederligt, rättvist och professionellt och på ett sätt så att allmänhetens förtroende för värdepappersmarknaden upprätthålls.

När börsen driver en reglerad marknad, ska den tillämpa principerna om

1. fritt tillträde, som innebär att var och en som uppfyller de krav som ställs i denna lag och av börsen får delta i handeln,
2. neutralitet, som innebär att börsens regler för den reglerade marknaden tillämpas på ett likformigt sätt gentemot alla som deltar i handeln, och
3. god genomlysning, som innebär att deltagarna får en snabb, samtidig och korrekt information om handeln och att allmänheten får tillfälle att ta del av sådan information.

En börs ska också

1. identifiera och hantera de risker*, inbegripet IKT-risker i enlighet med kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554,* som kan uppstå i verksamheten, och
2. identifiera och hantera de intressekonflikter som kan uppstå mellan börsens eller dess ägares intressen och intresset av att en reglerad marknad drivs i enlighet med första och andra styckena.

En börs får inte i sitt regelverk ställa oskäliga krav på emittenter och deltagare vid en reglerad marknad. Vad som utgör ett oskäligt krav ska bedömas med hänsyn till dess ändamål, *EU-rätten* och övriga omständigheter.

Paragrafen innehåller bestämmelser med allmänna krav på en börs verksamhet. Genom ändringarna genomförs artikel 47.1 b och 47.1 c i MiFID II, i lydelsen enligt artikel 6.3 a och 6.3 b i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). En börs omfattas av DORA-förordningen i dess egenskap av handelsplats och är i och med det en finansiell entitet enligt förordningen (artikel 2.1 i och 2.2 i DORA-förordningen).

I *tredje stycket 1* tydliggörs att en börs ska identifiera och hantera IKT-risker i enlighet med vad som anges i DORA-förordningen. De närmare kraven för detta anges i DORA-förordningen. Hittillsvarande *tredje stycket 2*, att en börs ska ha säkra tekniska system, utgår då motsvarande och mer detaljerade krav ska gälla enligt DORA-förordningen. Nya *tredje stycket 2*, om intressekonflikter, överensstämmer med hittillsvarande *tredje stycket 3*.

I *fjärde stycket* görs en språklig ändring. Ingen ändring avses i sak.

1 a § En börs ska inrätta *och upprätthålla en operativ motståndskraft i enlighet med kraven i kapitel II i Europaparlamentets och rådets förordning (EU) 2022/2554* för att säkerställa att handelssystemen

1. är motståndskraftiga,
2. har tillräcklig kapacitet för att kunna hantera svåra påfrestningar på marknaden i fråga om order- och meddelandevolymer,
3. kan upprätthålla ordnad handel vid förhållanden med påfrestningar på marknaden,
4. är fullständigt testade, och
5. garanterar kontinuitet i verksamheten vid eventuella driftavbrott i handelssystemet*, inbegripet en IKT-kontinuitetspolicy och IKT-planer samt IKT-relaterade åtgärds- och återställningsplaner i enlighet med artikel 11 i Europaparlamentets och rådets förordning (EU) 2022/2554*.

Paragrafen innehåller bestämmelser om att en börs ska inrätta system, förfaranden och arrangemang så att handelssystemen är motståndskraftiga, har tillräcklig kapacitet, kan säkerställa ordnad handel, är fullständigt testade och omfattas av effektiva arrangemang. Genom ändringarna genomförs artikel 48.1 i MiFID II, i lydelsen enligt artikel 6.4 a i ändringsdirektivet. Övervägandena finns i avsnitt 16.

I paragrafen förtydligas att en börs ska inrätta och upprätthålla en operativ motståndskraft för handelssystemen i enlighet med kraven i DORA-förordningen. Vidare förtydligas i *punkt 5* att en börs för ska ha en IKT-kontinuitetspolicy och IKT-planer samt IKT-relaterade åtgärds- och återställningsplaner i enlighet med vad som anges i DORA-förordningen. De närmare kraven för dessa områden anges i DORA-förordningen.

1 d § En börs ska inrätta effektiva system, förfaranden och arrangemang för att säkerställa att deltagare som använder algoritmiska handelssystem på en reglerad marknad som börsen driver inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden och för att kunna hantera eventuella otillbörliga marknadsförhållanden som kan uppstå till följd av användningen av sådana algoritmiska handelssystem.

I de förfaranden som avses i första stycket ska det ingå

1. krav på deltagarna att utföra lämpliga tester av algoritmer och att tillhandahålla miljöer för att underlätta sådana tester, *i enlighet med kraven i kapitlen II och IV i Europaparlamentets och rådets förordning (EU) 2022/2554,*

2. system för att begränsa andelen inte utförda order i förhållande till transaktionerna som kan läggas in i systemet av en deltagare,

3. system för att det ska vara möjligt att bromsa orderflödet om det finns en risk för att taket för systemkapaciteten uppnås, och

4. system för att begränsa och upprätthålla den minsta prisändring som får tillämpas på den reglerade marknaden.

Paragrafen innehåller bestämmelser om en börs att ha effektiva system, förfaranden och arrangemang när det gäller deltagare i handeln på en reglerad marknad som börsen driver som använder algoritmiska handelssystem. Genom ändringen genomförs artikel 48.6 i MiFID II, i lydelsen enligt artikel 6.4 b i ändringsdirektivet. Övervägandena finns i avsnitt 16.

I *andra stycket 1* förtydligas att kraven på lämpliga tester av algoritmer och miljöer för att underlätta sådana tester också omfattar kraven inom dessa områden enligt DORA-förordningen. De närmare kraven för detta anges i DORA-förordningen.

25 kap.

1 a § Finansinspektionen ska ingripa mot någon som ingår i ett svenskt värdepappersinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepappersinstitutet har åsidosatt sina skyldigheter enligt

1. 5 kap. 1, 3, 6 eller 7 §,

2. 6 kap. 1, 4 eller 6 §,

3. någon av 8 kap. 8 e eller 9–34 §§ eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 8 kap. 35 § 3–12,

4. någon av 9 kap. 1 §, 8 § tredje stycket, 9–12, 14–17 a, 19 a–41 eller 43 §§ eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 9 kap. 50 § 1, 3–9 eller 11,

5. någon av 11 kap. 1 §, 1 a § andra stycket, 1 b–4 a eller 12 §§ eller driver en tillväxtmarknad för små och medelstora företag trots att kraven i 13 § inte är uppfyllda,

6. någon av 13 kap. 1 a–1 j, 6 a eller 9 §§,

7. någon av 15 a kap. 7, 8 eller 10–14 §§,

8. 22 kap. 2 § andra stycket, 5 eller 6 § eller inte har följt ett beslut som meddelats av Finansinspektionen enligt 22 kap. 1 §, 2 § första stycket eller 3 §,

9. 23 kap. 2 § första stycket eller föreskrifter som meddelats med stöd av 23 kap. 15 § 1, eller inte har följt en begäran, ett föreläggande eller ett beslut som meddelats av Finansinspektionen enligt 23 kap. 2 § tredje stycket, 3 § första stycket, 3 a eller 3 b § eller har motsatt sig en undersökning enligt 23 kap. 4 §, *eller*

10. någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.

Paragrafen innehåller bestämmelser om när Finansinspektionen ska ingripa mot någon som ingår i ett värdepappersinstituts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om värdepappersinstitutet har gjort sig skyldig till en överträdelse. Paragrafen införs till

följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *första stycket 10*, som är ny, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för ett värdepappersinstitut om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen.

Övriga ändringar är redaktionella.

1 e § Finansinspektionen ska ingripa mot någon som ingår i en börs styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om börsen

1. har fått sitt tillstånd genom att lämna falska uppgifter eller på annat otillbörligt sätt,

2. har tillåtit en styrelseledamot, verkställande direktören eller ersättare för någon av dem att åta sig ett sådant uppdrag i företaget eller kvarstå i företaget trots att kraven i 12 kap. 2 § 4 eller 5 eller någon av 6 b–6 d §§ inte är uppfyllda,

3. har åsidosatt sina skyldigheter enligt

a) 8 kap. 21 § eller föreskrifter som meddelats med stöd av 8 kap. 35 § 12,

b) någon av 11 kap. 1 §, 1 a § andra stycket, 1 b–4 a eller 12 §§ eller driver en tillväxtmarknad för små och medelstora företag trots att kraven i 13 § inte är uppfyllda,

c) 12 kap. 6 e, 7 eller 10 § eller föreskrifter som meddelats med stöd av någon av bestämmelserna i 12 kap. 11 § 2–4,

d) någon av 13 kap. 1–2, 6–7 a eller 9 §§ eller 12 § femte stycket eller föreskrifter som meddelats med stöd av 13 kap. 17 § 1,

e) 14 kap. 1, 2 eller 3 §,

f) 15 kap. 1, 2, 5, 9 eller 10 §,

g) någon av 15 a kap. 7, 8 eller 10–12 §§,

h) 22 kap. 2 § andra stycket, 5 eller 6 § eller inte har följt ett beslut som meddelats av Finansinspektionen enligt 22 kap. 1 eller 3 §, eller

i) 23 kap. 2 § första stycket eller föreskrifter som meddelats med stöd av 23 kap. 15 § 1, eller inte har följt en begäran, ett föreläggande eller ett beslut som meddelats av Finansinspektionen enligt 23 kap. 2 § andra stycket, 3 § första stycket eller 3 b § eller har motsatt sig en undersökning enligt 23 kap. 4 §,

4. i strid med 24 kap. 5 § första stycket låter bli att till Finansinspektionen anmäla sådana förvärv och avyttringar som avses där,

5. i strid med 24 kap. 5 § tredje stycket låter bli att till Finansinspektionen anmäla namnen på de ägare som har ett kvalificerat innehav av aktier eller andelar i företaget samt storleken på innehaven*, eller*

6. har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.

Om en sådan person som avses i första stycket omfattas av tillstånds- eller underrättelseskyldighet enligt 24 kap. 1 eller 4 § för förvärv eller avyttring av aktier eller andelar i företaget, ska första stycket 4 och 5 inte gälla för den personen i fråga om dessa aktier eller andelar.

Paragrafen innehåller bestämmelser om när Finansinspektionens ska ingripa mot någon som ingår i en börs styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om börsen har gjort sig skyldig till en överträdelse. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *första stycket 6*, som är ny, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för en börs om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen.

Övriga ändringar är redaktionella.

1 i § Finansinspektionen ska ingripa mot någon som ingår i en central motparts styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om den centrala motparten har åsidosatt sina skyldigheter enligt förordningen om återhämtning och resolution av centrala motparter genom att inte

1. utarbeta, upprätthålla och uppdatera en återhämtningsplan (artikel 9),
2. tillhandahålla nödvändiga uppgifter för att utarbeta resolutionsplan (artikel 13), eller
3. underrätta Finansinspektionen om att den centrala motparten fallerar eller sannolikt kommer att fallera (artikel 70.1).

Finansinspektionen ska även ingripa mot en sådan fysisk person som avses i första stycket om den centrala motparten har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en central motpart, eller ersättare för någon av dem, eller
2. sanktionsavgift.

Ett ingripande enligt första *eller andra stycket* får ske bara om den centrala motpartens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Paragrafen innehåller bestämmelser om när Finansinspektionens ska ingripa mot någon som ingår i ledningen för en central motpart. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *andra stycket*, som är nytt, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för en central motpart om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen.

Tredje stycket överensstämmer med det hittillsvarande andra stycket.

I *fjärde stycket*, hittillsvarande tredje stycket, görs en följdändring med anledningen av att det införs ett nytt andra stycke i paragrafen.

1 j § *Finansinspektionen ska ingripa mot någon som ingår i en leverantör av datarapporteringstjänsters styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om leverantören har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.*

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en leverantör av datarapporteringstjänster, eller ersättare för någon av dem, eller

2. sanktionsavgift.

Ett ingripande får ske bara om Finansinspektionen har tillsyn över leverantören av datarapporteringstjänster.

Paragrafen, som är ny, innehåller bestämmelser om ingripande mot personer som ingår i ledningen för en leverantör av datarapporteringstjänster. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av 1 b och 1 d §§. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av en leverantör av datarapporteringstjänster, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i styrelsen för en leverantör av datarapporteringstjänster, är dess verkställande direktör, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Ett ingripande sker enligt *andra stycket* genom beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i leverantör av datarapporteringstjänster eller ersättare för någon av dem, eller genom ett beslut om sanktionsavgift. Dessa två sanktioner kan också kombineras. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 2 och 2 a §§ och bestämmelser om sanktionsavgift i 9 a och 10 §§.

Genom *tredje stycket* begränsas Finansinspektionens möjlighet att ingripa mot en företrädare för en leverantör av datarapporteringstjänster. Finansinspektionen får bara ingripa om inspektionen har tillsyn över leverantören av datarapporteringstjänster. Bestämmelser om Finansinspektionens tillsyn och dess omfattning finns i 23 kap. 1 §. Av den paragrafen framgår att Finansinspektionens tillsyn över leverantörer av datarapporteringstjänster bara omfattar sådana svenska APA-leverantörer och ARM-leverantörer för vilka inspektionen i egenskap av behörig myndighet ansvarar för tillståndsgivning och tillsyn enligt Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (se även prop. 2020/21:24 s. 40–41). Av 10 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

1 k § *Ett ingripande enligt 1 j § får ske bara om leverantören av datarapporteringstjänsters överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen.*

I paragrafen, som är ny, anges ett särskilt krav för att ett ingripande mot personer som ingår i ledningen för en leverantör av datarapporteringstjänster ska kunna komma i fråga. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av 1 c § första stycket och 1 g § första stycket. Övervägandena finns i avsnitt 8.3.

De grundläggande förutsättningarna för ett ingripande mot en fysisk person för en överträdelse av en leverantör av datarapporteringstjänster anges i 1 j § (se även författningskommentaren till den paragrafen). För att

ett ingripande ska kunna komma i fråga krävs, utöver det som anges i 1 j §, dels att leverantören av datarapporteringstjänsters överträdelse är allvarlig, dels att den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen. Detta motsvarar det som gäller enligt t.ex. 1 c § första stycket och 1 g § första stycket (se även prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542.

20.9 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

30 kap.

Verksamhet som rör digital operativ motståndskraft för finanssektorn

4 e § *Sekretess gäller i en statlig myndighets verksamhet enligt 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*

1. för uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser, om det kan antas att denne lider skada om uppgiften röjs, och

2. för uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser.

För uppgift i en allmän handling gäller sekretessen i högst tjugo år.

Paragrafen, som är ny, innehåller bestämmelser om sekretess i verksamhet som rör digital operativ motståndskraft för finanssektorn. Paragrafen införs för att tillgodose kraven i artikel 54 i DORA-förordningen. Övervägandena finns i avsnitt 9.

Genom paragrafen införs en ny grund för sekretess. Enligt *första stycket* ska sekretess gälla för statlig myndighets verksamhet enligt DORA-förordningen. Sekretessen kommer därmed att gälla för Finansinspektionens tillsynsverksamhet enligt förordningen (3 kap. 1 § i kompletteringslagen, se även avsnitt 7). Sekretessen är något vidare än sekretessen enligt 30 kap. 4 § offentlighets- och sekretesslagen, eftersom flera finansiella entiteter, t.ex. pensionsstiftelser, som inte bedriver verksamhet inom bank- och kreditväsendet, värdepappersmarknaden eller försäkringsväsendet omfattas. Sekretess kommer också att gälla för uppgifter i t.ex. rapporter om allvarliga IKT-relaterade incidenter och anmälningar av betydandet cyberhot (artikel 19 i DORA-förordningen och avsnitt 5.6). Genom bestämmelsen kommer sekretess även att gälla hos Riksbanken för uppgifter som förekommer i myndighetens övervakning och samordning av utförandet av hotbildsstyrda penetrationstester (2 kap. 2 § i kompletteringslagen, se även avsnitt 6.1). När det gäller vilka uppgifter som ska omfattas av sekretess och styrkan på sekretessen är bestämmelsen utformad efter förebild av den sekretess som gäller för en statlig myndighets verksamhet som består i tillståndsgivning eller tillsyn med avseende på bank- och kreditväsendet, värdepappersmarknaden eller försäkringsväsendet (jfr 30 kap. 4 § första stycket). Sekretess ska därmed gälla både för uppgift om affärs- eller driftförhållanden hos den som

myndighetens verksamhet avser (*första stycket 1)* och för uppgift om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser (*första stycket 2)*. För uppgift om affärs- eller driftförhållanden hos den som myndighetens verksamhet avser gäller sekretess bara om det kan antas att denne lider skada om uppgiften röjs. För tredjemansuppgifter, dvs uppgifter om ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser, gäller absolut sekretess.

I *andra stycket* anges att för uppgift i en allmän handling gäller sekretessen i högst tjugo år.

30 § Den tystnadsplikt som följer av 2 § första stycket första meningen, 4 § första stycket 2, 4 a § första stycket 2, 4 b § första stycket, *4 e § första stycket 2,* 6 b § första stycket, 12 § första stycket och andra stycket 2, 12 a § första stycket och andra stycket 2, 12 b § första stycket 2, 12 c § första stycket och andra stycket 2, 13 §, 15 § första stycket 2, 23 § första stycket 2, 23 a §, 23 b § och 27 § första stycket 2 och den tystnadsplikt som följer av ett förbehåll som gjorts med stöd av 9 § andra meningen, 14 § andra meningen, 26 § andra meningen eller 29 § andra meningen inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 24 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om andra ekonomiska eller personliga förhållanden än affärs- och driftförhållanden för den som trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Den tystnadsplikt som följer av 18 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om en enskilds personliga förhållanden vars röjande kan vålla allvarligt men.

Paragrafen innehåller bestämmelser om rätten att meddela och offentliggöra uppgifter, den s.k. meddelarfriheten. Övervägandena finns i avsnitt 9.

I *första stycket* anges de bestämmelser om sekretess och den tystnadsplikt som följer av dem som inskränker meddelarfriheten. I stycket görs ett tillägg för den sekretess för tredjemansuppgifter som ska gälla för verksamhet som rör digital operativ motståndskraft för finanssektorn (4 e §, se även författningskommentaren till den paragrafen). Rätten att meddela och offentliggöra uppgifter ska därmed inte gälla för uppgift i sådan verksamhet om den rör ekonomiska eller personliga förhållanden för annan som har trätt i affärsförbindelse eller liknande förbindelse med den som myndighetens verksamhet avser (4 e § första stycket 2).

20.10 Förslaget till lag om ändring i lagen (2010:751) om betaltjänster

5 b kap.

1 § En betaltjänstleverantör ska ha ett system med lämpliga åtgärder och kontrollmekanismer för att hantera operativa risker och säkerhetsrisker som är förknippade med de betaltjänster som den tillhandahåller. Inom ramen för detta system ska betaltjänstleverantören reglera hur incidenter ska hanteras.

För betaltjänstleverantörer som omfattas av 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 gäller även kapitel II i förordningen.

Paragrafen innehåller bestämmelser om en betaltjänstleverantörs system för hantering av operativa risker och säkerhetsrisker. Genom ändringen genomförs artikel 95.1 i betaltjänstdirektivet, i lydelsen enligt artikel 7.4 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). Vissa betaltjänstleverantörer omfattas av DORA-förordningen i dess egenskap som kreditinstitut, betalningsinstitut och institut för elektroniska pengar och är i och med det finansiella entiteter enligt förordningen (artikel 2.1 a, 2.1 b,2.1 d och 2.2 i DORA-förordningen).

I det nya *andra stycket* förtydligas att en betaltjänstleverantör som omfattas av DORA-förordningen även ska uppfylla kraven i DORA-förordningen om hanteringen av IKT-risker.

3 § En betaltjänstleverantör ska så snart det kan ske underrätta Finansinspektionen om en allvarlig operativ incident eller säkerhetsincident som uppkommit i verksamheten. Finansinspektionen ska så snart det kan ske informera Riksbanken, andra berörda svenska myndigheter, Europeiska bankmyndigheten och Europeiska centralbanken.

Om incidenten påverkar eller kan påverka betaltjänstanvändarnas ekonomiska intressen, ska betaltjänstleverantören så snart det kan ske informera användarna om incidenten och om de åtgärder som kan vidtas för att begränsa risken för skada.

Första och andra styckena gäller inte för betaltjänstleverantörer som omfattas av bestämmelserna i Europaparlamentets och rådets förordning (EU) 2022/2554.

Paragrafen innehåller bl.a. bestämmelser om att en betaltjänstleverantör i vissa falla ska underrätta Finansinspektionen och informera betaltjänstanvändarna om operativa incidenter eller säkerhetsincidenter. Genom ändringen genomförs artikel 96.7 i betaltjänstdirektivet, i lydelsen enligt artikel 7.5 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

I det nya *tredje stycket* förtydligas att bestämmelserna om underrättelser till Finansinspektionen och information till användarna inte ska gälla för betaltjänstleverantörer som omfattas av DORA-förordningen (se författningskommentaren till 5 b kap. 1 § för vilka betaltjänstleverantörer som omfattas av DORA-förordningen). För sådana betaltjänstleverantörer gäller i stället motsvarande bestämmelser om underrättelser och information i DORA-förordningen.

8 kap.

8 b § *Finansinspektionen ska ingripa mot någon som ingår i betalningsinstitutets styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om institutet har befunnits ansvarigt för en överträdelse av 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.*

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande får ske genom en eller båda av följande sanktioner: 1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, eller, för upprepade allvarliga överträdelser, permanent inte får upprätthålla en funktion som avses i första stycket hos ett betalningsinstitut, eller

2. beslut om sanktionsavgift.

Paragrafen, som är ny, innehåller bestämmelser om ingripanden mot personer som ingår i ledningen för ett betalningsinstitut. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av 8 a §. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av ett betalningsinstitut, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i betalningsinstitutets styrelse, är dess verkställande direkt, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 16 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

Ett ingripande sker enligt *tredje stycket* genom beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett betalningsinstitut eller ersättare för någon av dem, eller genom ett beslut om sanktionsavgift. Dessa två sanktioner kan också kombineras. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 9 och 9 a §§ och bestämmelser om sanktionsavgift i 15 b och 16 §§.

9 § Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

Finansinspektionen får avstå från ingripande enligt 8*,* 8 a *och 8 b* §§ om

1. en överträdelse är ringa eller ursäktlig,

2. betalningsinstitutet gör rättelse eller om den fysiska personen i betalningsinstitutets ledning verkat för att institutet gör rättelse, eller

3. någon annan myndighet har vidtagit åtgärder mot institutet eller den fysiska personen i betalningsinstitutets ledning som bedöms vara tillräckliga.

Paragrafen innehåller bestämmelser om omständigheter som ska beaktas vid valet av ingripande mot ett betalningsinstitut. Paragrafen införs till följd av artikel 51.2 i DORA-förordningen. Övervägandena finns i avsnitt 8.5.

Ändringen i *andra stycket* är en följd av att det genom den nya 8 kap. 8 b § införs bestämmelser om ingripande mot personer som ingår i ett betalningsinstituts ledning när institutet har överträtt vissa bestämmelser i DORA-förordningen.

16 a § Frågor om ingripanden mot fysiska personer enligt 8 a *och 8 b §§* ta upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

Paragrafen innehåller bestämmelser om att ingripande mot fysiska personer som ingår i ett betalningsinstituts ledning ska tas upp genom sanktionsföreläggande. Övervägandena finns i avsnitt 8.3.

Ändringen i *första stycket* är en följd av att det genom den nya 8 kap. 8 b § införs bestämmelser om ingripande mot personer som ingår i ett betalningsinstituts ledning när institutet har överträtt bestämmelser i DORA-förordningen.

23 b § Finansinspektionen ska ingripa mot en person som ingår i en registrerad betaltjänstleverantörs styrelse eller är dess verkställande direktör eller på motsvarande sätt företräder betaltjänstleverantören, eller är ersättare för någon av dem, om den registrerade betaltjänstleverantören har befunnits ansvarig för en överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen eller en överträdelse av förordning (EU) 2015/847.

Ett ingripande enligt första stycket får ske endast om överträdelsen är allvarlig, upprepad eller systematisk och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Finansinspektionen ska även ingripa mot någon som ingår i en registrerad betaltjänstleverantörs styrelse eller är dess verkställande direktör eller på motsvarande sätt företräder betaltjänstleverantören, eller är ersättare för någon av dem, om den registrerade betaltjänstleverantören har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt tredje stycket får ske endast om den registrerade betaltjänstleverantörens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i första stycket hos en registrerad betaltjänstleverantör, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om ingripande mot personer som ingår i ledningen i ledningen för en registrerad betaltjänstleverantör. Para-

grafen införs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *tredje stycket*, som är nytt, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för en registrerad betaltjänstleverantör om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen.

Av *fjärde stycket*, som är nytt, framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 23 c § följer att 15 b om sanktionsavgifter för fysiska personer och 16 a §§ om sanktionsföreläggande gäller vid beslut om ingripande och 18–20 §§ i fråga om verkställighet av beslut om sanktionsavgifter. Av 23 d § följer att Finansinspektionen, vid valet av åtgärd och sanktion, ska ta hänsyn till de omständigheter som anges i 9 § första stycket, 9 a och 16 §§.

Femte stycket överensstämmer med hittillsvarande tredje stycket.

20.11 Förslaget till lag om ändring i försäkringsrörelselagen (2010:2043)

10 kap.

3 § Ett försäkringsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna bedrivas med kontinuitet och i enlighet med gällande regler. *Nätverks- och informationssystem ska uppfylla kraven i 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.*

Ett försäkringsföretag ska ha en beredskapsplan.

Paragrafen innehåller bestämmelser om kontinuitet i verksamheten. Genom ändringen genomförs artikel 41.4 i Solvens II-direktivet, i lydelsen enligt artikel 2.1 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). Ett försäkringsföretag omfattas av DORA-förordningen och är i och med det en finansiell entitet enligt förordningen (artikel 2.1 n och 2.2 i DORA-förordningen).

I *första stycket* förtydligas att ett försäkringsföretags nätverks- och informationssystem ska uppfylla kraven i DORA-förordningen. De närmare kraven på nätverks- och informationssystemen och hur de ska utformas anges i DORA-förordningen.

11 kap.

1 § För försäkringsaktiebolag gäller föreskrifterna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller är särskilt föreskrivet. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag som gäller i stället för eller utöver bestämmelserna i aktiebolagslagen.

I fråga om försäkringsaktiebolag ska det som anges om Bolagsverket i följande bestämmelser avse Finansinspektionen:

1. 8 kap. 9 och 30 §§ samt 37 § andra stycket aktiebolagslagen,
2. 23 kap. 45 b § aktiebolagslagen,
3. 24 kap. 47 § aktiebolagslagen, och
4. 24 a kap. 24 § aktiebolagslagen.

Bestämmelserna i 32 kap. aktiebolagslagen om aktiebolag med särskild vinstutdelningsbegränsning gäller inte för försäkringsaktiebolag.

Av paragrafen framgår vilka associationsrättsliga regler som gäller för försäkringsaktiebolag.

I *andra stycket* görs en redaktionell ändring då den tidigare strecklistan ändras till en punktlista.

18 kap.

1 b § *Finansinspektionen ska ingripa mot någon som ingår i försäkringsföretagets styrelse eller är dess verkställande direktör, eller ersättare för någon av dem, om företaget har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.*

Ett ingripande enligt första stycket får ske endast om företagets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Paragrafen, som är ny, innehåller bestämmelser om ingripanden mot personer som ingår i ledningen för ett försäkringsföretag. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 1 a § i lagen om värdepappersmarknaden. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av ett försäkringsföretag, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i försäkringsföretagets styrelse, är dess verkställande direktör, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 18 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

2 a § Ingripande enligt 1 a *och 1 b §§* sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i 1 a § första stycket *och 1 b § första stycket* i ett försäkringsföretag, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om hur Finansinspektionen ska ingripa mot en fysisk person som ingår i ett försäkringsföretags ledning. Paragrafen införs till följd av artikel 51.2 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Ändringen i paragrafen är en följd av att det genom den nya 18 kap. 1 b § införs bestämmelser om ingripande mot personer som ingår i ett försäkringsföretags ledning när företaget har överträtt vissa bestämmelser i DORA-förordningen.

18 a § Frågor om ingripanden mot fysiska personer för överträdelser enligt 1 a *eller 1 b §* tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

Paragrafen innehåller bestämmelser om att ingripande mot fysiska personer som ingår i ett försäkringsföretags ledning ska tas upp genom sanktionsföreläggande. Övervägandena finns i avsnitt 8.3.

Ändringen i *första stycket* är en följd av att det genom den nya 18 kap. 1 b § införs bestämmelser om ingripande mot personer som ingår i ett försäkringsföretags ledning när företaget har överträtt vissa bestämmelser i DORA-förordningen.

21 kap.

1 § Finansinspektionens beslut i ärenden enligt 17 kap. 13 § första stycket och 18 kap. 25 § andra stycket får inte överklagas. *Detsamma gäller för sådana beslut om förordnande av sakkunnig som avses i 11 kap. 1 § andra stycket 2–4 och för beslut om sanktionsföreläggande.*

Paragrafen innehåller bestämmelser om att vissa beslut av Finansinspektionen inte får överklagas. Övervägandena finns i avsnitt 17.1.

Paragrafen ändras på så sätt att Finansinspektionens beslut om förordnande av sakkunnig i ärenden om gränsöverskridande fusion, delning eller ombildning inte får överklagas. Beslut om betalningsskyldighet för ersättning till sakkunnig kan överklagas enligt den allmänna överklagandebestämmelsen (3 §). Motsvarande ändring görs i lagen (2004:297) om bank- och finansieringsrörelse (se 17 kap. 1 § första stycket och författningskommentaren till den paragrafen).

20.12 Förslaget till lag om ändring i lagen (2011:755) om elektroniska pengar

5 kap.

8 b § *Finansinspektionen ska ingripa mot någon som ingår i styrelsen för institutet för elektroniska pengar eller är dess verkställande direktör, eller ersättare för någon av dem, om institutet har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i 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.*

Ett ingripande enligt första stycket får ske endast om institutets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ett ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett institut för elektroniska pengar, eller ersättare för någon av dem, eller

2. sanktionsavgift.

Paragrafen, som är ny, innehåller bestämmelser om ingripanden mot personer som ingår i ledningen för ett institut för elektroniska pengar. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av 8 a §. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av ett institut för elektroniska pengar, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i institutets styrelse, är dess verkställande direktör, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 16 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

Ett ingripande sker enligt *tredje stycket* genom beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett betalningsinstitut eller ersättare för någon av dem, eller genom ett beslut om sanktionsavgift. Dessa två sanktioner kan också kombineras. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 9 och 9 a §§ och bestämmelser om sanktionsavgift i 15 b och 16 §§.

9 § Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

Finansinspektionen får avstå från ingripande enligt 8, 8 a *och 8 b* §§ om

1. en överträdelse är ringa eller ursäktlig,
2. institutet för elektroniska pengar gör rättelse eller om den fysiska personen verkat för att institutet gör rättelse, eller
3. någon annan myndighet har vidtagit åtgärder mot institutet eller den fysiska personen som bedöms vara tillräckliga.

Paragrafen innehåller bestämmelser om omständigheter som ska beaktas vid valet av ingripande mot ett institut för elektroniska pengar. Ändringen görs till följd av artikel 51.2 i DORA-förordningen. Övervägandena finns i avsnitt 8.5.

Ändringen i *andra stycket* är en följd av att det genom den nya 5 kap. 8 b § införs bestämmelser om ingripande mot personer som ingår i ett instituts ledning när institutet har överträtt vissa bestämmelser i DORA-förordningen.

16 a § Frågor om ingripanden mot fysiska personer enligt 8 a *eller 8 b §* tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

Paragrafen innehåller bestämmelser om att ingripande mot fysiska personer som ingår i ledningen för ett institut för elektroniska pengar ska tas upp genom sanktionsföreläggande. Övervägandena finns i avsnitt 8.3.

Ändringen i *första stycket* är en följd av att det genom den nya 5 kap. 8 b § införs bestämmelser om ingripande mot personer som ingår i ledningen för ett institut för elektroniska pengar när institutet har överträtt vissa bestämmelser i DORA-förordningen.

23 b§ Finansinspektionen ska ingripa mot en person som ingår i den registrerade utgivarens styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om den registrerade utgivaren har befunnits ansvarig för överträdelse av lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism eller föreskrifter som har meddelats med stöd av den lagen eller en överträdelse av förordning (EU) 2015/847.

Ett ingripande enligt första stycket får ske endast om överträdelsen är allvarlig, systematisk eller upprepad och personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Finansinspektionen ska även ingripa mot någon som ingår i den registrerade utgivarens styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om den registrerade utgivaren, har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.

Ett ingripande enligt tredje stycket får ske endast om den registrerade utgivarens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande sker genom

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i första stycket hos en utgivare av elektroniska pengar, eller
2. beslut om sanktionsavgift.

Paragrafen innehåller bestämmelser om ingripande mot personer som ingår i ledningen i ledningen för en registrerad utgivare. Ändringen görs till följd av artikel 50.5 i DORA-förordningen. Övervägandena finns i avsnitt 8.3.

Genom *tredje stycket*, som är nytt, görs ett tillägg att Finansinspektionen kan ingripa mot en fysisk person i ledningen för en registrerad utgivare om den juridiska personen har åsidosatt sina skyldigheter i de angivna fallen i DORA-förordningen.

Av *fjärde stycket*, som är nytt, framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 23 c § följer att 15 b om sanktionsavgifter för fysiska personer och 16 a §§ om sanktionsföreläggande gäller vid beslut om ingripande och 18–20 §§ i fråga om verkställighet av beslut om sanktionsavgifter. Av 23 d § följer att Finansinspektionen, vid valet av åtgärd och sanktion, ska ta hänsyn till de omständigheter som anges i 9 § första stycket, 9 a och 16 §§.

Femte stycket överensstämmer med hittillsvarande tredje stycket.

20.13 Förslaget till lag om ändring i lagen (2013:561) om förvaltare av alternativa investeringsfonder

8 kap.

2 § En AIF-förvaltare ska ha sunda rutiner för

1. förvaltning av verksamheten och redovisning,
2. drift och förvaltning av sina informationssystem, och
3. intern kontroll.

Rutinerna enligt första stycket 2 ska uppfylla kraven i 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.

AIF-förvaltaren ska särskilt

1. upprätta och tillämpa regler för anställdas egna transaktioner,
2. upprätta och tillämpa regler för investeringar som görs för förvaltarens egen räkning,
3. ha rutiner för att kunna säkerställa att varje transaktion som genomförs för en alternativ investeringsfonds räkning är möjlig att rekonstruera i efterhand med avseende på dess ursprung, art, parter, tidpunkt och plats, samt
4. ha rutiner för att säkerställa att tillgångarna i de alternativa investeringsfonder som förvaltaren förvaltar investeras i enlighet med denna lag och andra författningar som reglerar verksamheten eller lagstiftningen i det land där fonden är etablerad samt fondbestämmelser, bolagsordning eller motsvarande regelverk.

Paragrafen innehåller bestämmelser om organisatoriska krav. Genom ändringen genomförs artikel 18.1 i AIFM-direktivet, i lydelsen enligt artikel 3 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ

motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). En AIF-förvaltare omfattas av DORA-förordningen och är i och med det en finansiell entitet enligt förordningen (artikel 2.1 k och 2.2 i DORA-förordningen).

I det nya *andra stycket* förtydligas kraven på en AIF-förvaltares informationssystem (första stycket 2). Rutinerna för drift och förvaltning av dessa system ska uppfylla kraven i DORA-förordningen. De närmare kraven anges i DORA-förordningen. En motsvarande ändring görs för fondbolag i lagen (2004:46) om värdepappersfonder (se 2 kap. 17 § och författningskommentaren till den paragrafen).

Den nya *tredje stycket* överensstämmer med hittillsvarande andra stycket.

14 kap.

1 b § *Finansinspektionen ska ingripa mot någon som ingår i en AIF-förvaltares ledning eller styrelse eller är förvaltarens verkställande direktör eller motsvarande, eller ersättare för någon av dem, om förvaltaren har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.*

Ett ingripande enligt första stycket får ske endast om AIF-förvaltarens överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

Ingripande får ske genom en eller båda av följande sanktioner:

1. att den fysiska personen under en viss tid, lägst tre och högst tio år,

inte får vara styrelseledamot eller verkställande direktör i en AIF-förvaltare, eller ersättare för någon av dem, eller

2. sanktionsavgift.

Paragrafen, som är ny, innehåller bestämmelser om ingripanden mot personer som ingår i en AIF-förvaltares ledning. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av 1 a §. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av en AIF-förvaltare, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i AIF-förvaltarens styrelse, är dess verkställande direktör, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 13 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

Ett ingripande sker enligt *tredje stycket* genom beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i en AIF-förvaltare eller ersättare för någon av dem, eller genom ett beslut om sanktionsavgift. Dessa två sanktioner kan också kombineras. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 2 och 2 a §§ och bestämmelser om sanktionsavgift i 12 a och 13 §§.

13 a § Frågor om ingripanden mot fysiska personer enligt 1 a*, 1 b* eller 9 a § tas upp av Finansinspektionen genom sanktionsföreläggande.

Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 12 kap. 9 a–9 d §§ lagen (2004:46) om värdepappersfonder.

Paragrafen innehåller bestämmelser om att ingripande mot fysiska personer som ingår i ledningen för en AIF-förvaltare ska tas upp genom sanktionsföreläggande. Övervägandena finns i avsnitt 8.3.

Ändringen i *första stycket* är en följd av att det genom den nya 14 kap. 1 b § införs bestämmelser om ingripande mot personer som ingår i ledningen för en AIF-förvaltare när AIF-förvaltaren har överträtt vissa bestämmelser i DORA-förordningen.

20.14 Förslaget till lag om ändring i lagen (2019:742) om tjänstepensionsföretag

9 kap.

2 § Ett tjänstepensionsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna drivas med kontinuitet och i enlighet med gällande regler. Ett tjänstepensionsföretag ska ha system, resurser och rutiner som är lämpliga för att verksamheten ska kunna drivas med kontinuitet och i enlighet med gällande regler. *Nätverks- och informationssystem ska uppfylla kraven i 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.*

Ett tjänstepensionsföretag ska ha en beredskapsplan.

Paragrafen innehåller bestämmelser om kontinuitet i verksamheten. Genom ändringen genomförs delvis artikel 21.5 i andra tjänstepensionsdirektivet, i lydelsen enligt artikel 8 i ändringsdirektivet. Övervägandena finns i avsnitt 16.

Genom DORA-förordningen införs nya krav på finansiella entiteters riskhantering. Finansiella entiteter ska, när det gäller digital operativ motståndskraft, vidta de åtgärder som är nödvändiga för att kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad (skäl 3 i ändringsdirektivet). Ett tjänstepensionsföretag omfattas av DORA-förordningen i dess egenskap av tjänstepensionsinstitut och är i och med det en finansiell entitet enligt förordningen (artikel 2.1 p och 2.2 i DORA-förordningen).

I *första stycket* förtydligas att ett tjänstepensionsföretags nätverks- och informationssystem ska uppfylla kraven i DORA-förordningen. De

närmare kraven på nätverks- och informationssystemen och hur de ska utformas anges i DORA-förordningen. En motsvarande ändring görs för pensionsstiftelser i lagen (1967:531) om tryggande av pensionsutfästelse m.m. (se 16 g § och författningskommentaren till den paragrafen).

10 kap.

1 § För tjänstepensionsaktiebolag gäller bestämmelserna för aktiebolag i allmänhet, om inte något annat följer av denna lag eller av sådana bestämmelser i försäkringsrörelselagen (2010:2043) som det hänvisas till i denna lag. Hänvisningar i aktiebolagslagen (2005:551) till bestämmelser i samma lag ska i de fall de förekommer avse de bestämmelser i denna lag eller i försäkringsrörelselagen som gäller i stället för eller utöver aktiebolagslagen.

I fråga om tjänstepensionsaktiebolag ska det som sägs om Bolagsverket i följande bestämmelser avse Finansinspektionen:

1. 8 kap. 9 och 30 §§ och 37 § andra stycket aktiebolagslagen,

2. 23 kap. 45 b § aktiebolagslagen,

3. 24 kap. 47 § aktiebolagslagen, och

4. 24 a kap. 24 § aktiebolagslagen.

Bestämmelserna i 32 kap. aktiebolagslagen om aktiebolag med särskild vinstutdelningsbegränsning gäller inte för tjänstepensionsaktiebolag.

Av paragrafen framgår vilka associationsrättsliga regler som gäller för tjänstepensionsaktiebolag.

I *andra stycket* görs en redaktionell ändring då den tidigare strecklistan ändras till en punktlista.

15 kap.

Ingripande mot tjänstepensionsföretag *och vissa fysiska personer*

1 a § *Finansinspektionen ska ingripa mot någon som ingår i tjänstepensionsföretagets styrelse eller är dess verkställande direktör, eller är ersättare för någon av dem, om företaget har åsidosatt sina skyldigheter enligt någon av artiklarna 5–10, 11.1–11.10, 12–14, 16.1, 16.2, 17, 18.1, 18.2, 19.1, 19.3, 19.4, 23–25, 26.1–26.8, 27, 28.1–28.8, 29, 30.1–30.4, 31.12 och 45 i Europaparlamentets och rådets förordning (EU) 2022/2554.*

Ett ingripande enligt första stycket får ske endast om företagets överträdelse är allvarlig och den fysiska personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen

Paragrafen, som är ny, innehåller bestämmelser om ingripanden mot personer som ingår i ledningen för ett tjänstepensionsföretag. Paragrafen införs till följd av artikel 50.5 i DORA-förordningen. Den är utformad efter förebild av bl.a. 25 kap. 1 a § i lagen om värdepappersmarknaden. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges de bestämmelser i DORA-förordningen som, om de överträds av ett tjänstepensionsföretag, ska kunna medföra ett ingripande från Finansinspektionen mot en fysisk person som kan hållas ansvarig. Finansinspektionen ska ingripa mot den som ingår i tjänstepensionsföretagets styrelse, är dess verkställande direktör, eller ersättare för någon av dem, om den juridiska personen har åsidosatt sina skyldigheter i ett av de angivna fallen.

Av *andra stycket* framgår förutsättningarna för att ett ingripande mot en fysisk person ska göras. Det krävs dels att den juridiska personens överträdelse är av allvarligt slag, dels att personen i fråga uppsåtligen eller av grov oaktsamhet har orsakat överträdelsen (se prop. 2014/15:57 s. 40–43 och prop. 2016/17:162 s. 540–542). Av 18 a § följer att frågor om ingripanden mot fysiska personen enligt denna paragraf tas upp av Finansinspektionen genom sanktionsföreläggande, se författningskommentaren till den paragrafen.

2 a § *Ingripande enligt 1 a § sker genom*

1. beslut att personen i fråga under en viss tid, lägst tre och högst tio år, inte får upprätthålla en funktion som avses i 1 a § första stycket i ett tjänstepensionsföretag, eller

2. beslut om sanktionsavgift.

Paragrafen, som är ny, innehåller bestämmelser om hur Finansinspektionen ska ingripa mot en fysisk person som ingår i tjänstepensionsföretags ledning. Paragrafen införs till följd av artikel 51.2 i DORA-förordningen. Den är utformad efter förebild av 18 kap. 2 a § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.3.

Ett ingripande sker genom beslut att den fysiska personen i fråga under en viss tid, lägst tre år och högst tio år, inte får vara styrelseledamot eller verkställande direktör i ett tjänstepensionsföretag eller ersättare för någon av dem, eller genom ett beslut om sanktionsavgift. Dessa två sanktioner kan också kombineras. Bestämmelser om omständigheter som ska beaktas vid valet av ingripande finns i 3 och 4 §§ och bestämmelser om sanktionsavgift i 17 a §, se författningskommentarerna till de paragraferna.

3 § Vid valet av ingripande ska Finansinspektionen ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till skador som har uppstått och graden av ansvar.

I försvårande riktning ska det beaktas om tjänstepensionsföretaget tidigare har begått en överträdelse *eller om den fysiska personen tidigare orsakat en sådan överträdelse.*

I förmildrande riktning ska det beaktas om

1. företaget *eller den fysiska personen* i väsentlig utsträckning genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och

2. företaget snabbt har upphört med överträdelsen*, eller den fysiska personen snabbt verkat för att överträdelsen ska upphöra,* sedan den anmälts till eller påtalats av Finansinspektionen.

Paragrafen innehåller bestämmelser om omständigheter som ska beaktas vid valet av ingripande mot ett tjänstepensionsföretag. Ändringen görs till följd av artikel 51.2 i DORA-förordningen. Den är utformad efter förebild av 18 kap. 3 a § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.5.

Ändringarna i paragrafen är en följd av att det genom den nya 15 kap. 1 a § införs bestämmelser om ingripande mot personer som ingår i ledningen för ett tjänstepensionsföretag när företaget har överträtt vissa bestämmelser i DORA-förordningen.

4 § Finansinspektionen får avstå från ingripande om

1. en överträdelse är ringa eller ursäktlig,
2. tjänstepensionsföretaget gör rättelse *eller om den fysiska personen verkat för att företaget gör rättelse,* eller
3. någon annan myndighet har vidtagit åtgärder mot företaget *eller den fysiska personen* och dessa åtgärder bedöms tillräckliga.

Paragrafen innehåller bestämmelser om Finansinspektionens möjligheter att avstå från ingripande. Paragrafen är utformad efter förebild av 18 kap. 3 a § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.5.

Ändringarna i paragrafen är en följd av att det genom den nya 15 kap. 1 a § införs bestämmelser om ingripande mot personer som ingår i ledningen för ett tjänstepensionsföretag när företaget har överträtt vissa bestämmelser i DORA-förordningen.

17 a § *En sanktionsavgift för en fysisk person ska som högst fastställas till det högsta av*

1. två gånger den vinst som den fysiska personen gjort till följd av regelöverträdelsen, om beloppet går att fastställa, eller

2. ett belopp som per den 16 januari 2023 i kronor motsvarade fem miljoner euro.

Avgiften tillfaller staten.

Paragrafen, som är ny, innehåller bestämmelser om storleken på den högsta sanktionsavgiften för en fysisk person. Paragrafen införs till följd av artiklarna 50.4 och 50.5 i DORA-förordningen. Den är utformad efter förebild av 18 kap. 17 b § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.4.

I paragrafen anges två beräkningsgrunder för beräkning av den högsta sanktionsavgiften för en fysisk person vid överträdelser av DORA-förordningen.

Enligt *punkt 1* ska sanktionsavgiften kunna uppgå till två gånger den vinst som den fysiska personen gjort till följd av överträdelsen, om beloppet går att fastställa. Med vinst som gjorts avses ett nettobelopp som omfattar de vinster som erhållits och de förluster som undvikits, dvs. den fördel som erhållits (jfr prop. 2016/17:162 s. 640).

Enligt *punkt 2* får sanktionsavgiften uppgå till ett belopp som per den 16 januari 2023 i svenska kronor motsvarade 5 000 000 euro. Vid omräkning mellan euro och svenska kronor tillämpas den s.k. fixingkursen som dagligen fastställs av Nasdaq Stockholm AB och publiceras på Riksbankens webbplats. Enligt fixingkursen den 16 januari 2023 motsvarade 1 euro 11,2691 svenska kronor.

Avgifterna i beräkningsmodellerna är maximibelopp, vilket innebär att Finansinspektionen har möjlighet att fastställa sanktionsavgiften till det högsta av de beräknade beloppen, eller ett lägre belopp.

I *andra stycket* anges att sanktionsavgiften tillfaller staten.

I 18 § finns bestämmelser om vilka omständigheter Finansinspektionen ska beakta när sanktionsavgiftens storlek fastställs.

18 § När sanktionsavgiftens storlek fastställs, ska särskild hänsyn tas till sådana omständigheter som anges i 3 § samt till tjänstepensionsföretagets *eller den fysiska*

personens finansiella ställning och, om det går att fastställa, den vinst som gjorts till följd av regelöverträdelsen.

Paragrafen innehåller bestämmelser om omständigheter som ska beaktas vid fastställande av sanktionsavgiftens storlek. Ändringen görs till följd av artikel 51.2 i DORA-förordningen. Den är utformad efter förebild av 18 kap. 18 § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.4.

Ändringen i paragrafen är en följd av att det genom den nya 15 kap. 1 a § införs bestämmelser om ingripande mot personer som ingår i ledningen för ett tjänstepensionsföretag när företaget har överträtt vissa bestämmelser i DORA-förordningen.

Sanktionsföreläggande

18 a § *Frågor om ingripanden mot fysiska personer för överträdelser enligt 1 a § tas upp av Finansinspektionen genom sanktionsföreläggande.*

Finansinspektionen ska då tillämpa bestämmelserna om sanktionsföreläggande i 15 kap. 9 a–9 d §§ lagen (2004:297) om bank- och finansieringsrörelse.

Paragrafen, som är ny, reglerar förfarandet för beslut om sanktioner genom ett sanktionsföreläggande. Paragrafen är utformad efter förebild av 18 kap. 18 a § försäkringsrörelselagen. Övervägandena finns i avsnitt 8.3.

Enligt *första stycket* ska ingripanden mot en fysisk person för överträdelse av ett tjänstepensionsföretag, som är en juridisk person, tas upp av Finansinspektionen genom sanktionsföreläggande.

Enligt *andra stycket* ska bestämmelserna om sanktionsföreläggande i 15 kap. 9 a–9 d §§ lagen om bank- och finansieringsrörelse tillämpas vid ett sådant ingripande.

20 § En sanktionsavgift eller förseningsavgift ska betalas till Finansinspektionen inom 30 dagar efter det att beslutet om den har fått laga kraft *eller sanktionsföreläggandet godkänts* eller inom den längre tid som anges i beslutet.

23 § En beslutad sanktionsavgift eller förseningsavgift faller bort i den utsträckning verkställighet inte har skett inom fem år från det att beslutet fick laga kraft *eller sanktionsföreläggandet godkändes*.

Paragraferna innehåller bestämmelse om verkställighet av bl.a. sanktionsavgifter. Paragraferna är utformade efter förebild av 18 kap. 20 och 23 §§ försäkringsrörelselagen. Övervägandena finns i avsnitt 8.6.

Ändringarna i paragraferna är en följd av att det genom den nya 15 kap. 1 a § införs bestämmelser om ingripande mot personer som ingår i ledningen för ett tjänstepensionsföretag när företaget har överträtt vissa bestämmelser i DORA-förordningen.

17 kap.

1 § *Finansinspektionens beslut om förordnande av sakkunnig som avses i 10 kap. 1 § andra stycket 2–4 och sanktionsföreläggande enligt 15 kap. 18 a § får inte överklagas.*

Andra beslut av Finansinspektionen enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen innehåller bestämmelser om överklagande av Finansinspektionens beslut. Övervägandena finns i avsnitt 15.1 och 17.1.

I *första stycket*, som är nytt, anges att ett beslut om förordnande av sakkunnig i ärenden om gränsöverskridande fusion, delning eller ombildning inte får överklagas. Ett beslut om betalningsskyldighet för ersättning till en sådan sakkunnig får överklagas enligt det nya andra stycket. Motsvarande ändringar görs i 17 kap. 1 § lagen (2004:297) om bank- och finansieringsrörelse och i 21 kap. 1 § försäkringsrörelselagen (2010:2043) (se de paragraferna och tillhörande författningskommentarer). Samma gäller för Finansinspektionens beslut om sanktionsföreläggande (se vidare författningskommentaren till 5 kap. 1 § i lagen med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn).

Anda beslut än de som avses i första stycket får enligt *andra stycket*, som är nytt, överklagas till allmän förvaltningsdomstol.

Tredje stycket överensstämmer med hittillsvarande andra stycket.

I

(Lagstiftningsakter)

FÖRORDNINGAR

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

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) I den digitala tidsåldern stöder informations- och kommunikationstekniken (IKT) komplexa system som används för dagliga aktiviteter. Den får våra ekonomier att fungera inom viktiga sektorer, inbegripet finanssektorn, och förbättrar den inre marknadens funktion. Ökad digitalisering och sammanlänkning ökar också IKT-risk och gör samhället som helhet – och i synnerhet det finansiella systemet – mer sårbart för cyberhot eller IKT-avbrott. Den allmänt utbredda användningen av IKT-system och hög digitalisering och konnektivitet är i dag centrala inslag i den verksamhet som bedrivs av unionens finansiella entiteter, men deras digitala motståndskraft måste fortfarande hanteras bättre och integreras i deras bredare operativa ramar.

(2) Användningen av IKT har under de senaste årtiondena fått en avgörande roll inom tillhandahållandet av finansiella tjänster och har nått den punkt där den i dag är avgörande för driften av alla finansiella entiteters vanliga dagliga funktioner. Digitaliseringen omfattar i dag t.ex. betalningar, som i allt högre grad har gått från kontanter och pappersbaserade metoder till användning av digitala lösningar, liksom clearing och avveckling av värdepapper, elektronisk och algoritmisk handel, utlåning och finansiering, peer-to-peer-finansiering, kreditvärdering, skadereglering och back-office-verksamhet. Försäkringssektorn har också omvandlats genom användningen av IKT,

([1]) EUT C 343, 26.8.2021, s. 1.
([2]) EUT C 155, 30.4.2021, s. 38.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.

från framväxten av försäkringsförmedlare som erbjuder sina tjänster online med hjälp av försäkringsteknik (insurtech), till digital försäkringsgarantiverksamhet. Hela finanssektorn har blivit till stor del digital, och digitaliseringen har också fördjupat sammanlänkningarna och beroendena inom finanssektorn och med tredjepartsinfrastruktur och tredjepartstjänsteleverantörer.

(3) Europeiska systemrisknämnden (ESRB) bekräftade i en rapport från 2020 om systemrisker på cyberområdet att den nuvarande höga graden av sammanlänkning mellan finansiella entiteter, finansmarknader och finansmarknadsinfrastrukturer, och särskilt det ömsesidiga beroendet mellan deras IKT-system, skulle kunna utgöra en systemsårbarhet, eftersom lokala cyberincidenter snabbt skulle kunna spridas från någon av de cirka 22 000 finansiella entiteterna i unionen till hela det finansiella systemet, utan hinder av geografiska gränser. Allvarliga IKT-relaterade överträdelser inom finanssektorn påverkar inte bara finansiella entiteter var för sig. De underlättar också spridning av lokaliserade sårbarheter i de finansiella överföringskanalerna och kan få negativa konsekvenser för stabiliteten i unionens finansiella system, t.ex. generera likviditetsrusningar och generellt leda till ett minskat förtroende för finansmarknaderna.

(4) På senare år har IKT-risk uppmärksammats av internationella, unionens och nationella beslutsfattare, tillsynsmyndigheter och standardiseringsorgan i ett försök att öka den digitala motståndskraften, fastställa standarder och samordna reglerings- eller tillsynsarbete. På internationell nivå har Baselkommittén för banktillsyn, kommittén för betalningar och marknadsinfrastruktur, rådet för finansiell stabilitet, Financial Stability Institute samt G7 och G20 som mål att förse behöriga myndigheter och marknadsoperatörer inom olika jurisdiktioner med verktyg för att stärka motståndskraften hos deras finansiella system. Det arbetet har också motiverats av behovet av att vederbörligen beakta IKT-risk i ett globalt finansiellt system som är starkt sammanlänkat och eftersträva större samstämmighet vad gäller relevant bästa praxis.

(5) Trots unionens och nationella riktade politiska initiativ och lagstiftningsinitiativ fortsätter IKT-risk att utgöra en utmaning för den operativa motståndskraften, prestandan och stabiliteten i unionens finansiella system. De reformer som följde på finanskrisen 2008 stärkte i första hand den finansiella motståndskraften hos unionens finanssektor och syftade till att skydda unionens konkurrenskraft och stabilitet ur ekonomiska och tillsynsmässiga perspektiv samt vad gäller marknadsbeteende. Även om IKT-säkerhet och digital motståndskraft ingår i de operativa riskerna har de inte uppmärksammats lika mycket i lagstiftningsagendan efter finanskrisen och har bara utvecklats inom vissa områden av unionens politik och regelverk för finansiella tjänster, eller endast i ett fåtal medlemsstater.

(6) I sitt meddelande av den 8 mars 2018 med titeln *Handlingsplanen för fintech: – ett viktigt steg mot en mer konkurrenskraftig europeisk finanssektor* betonade kommissionen att det är ytterst viktigt att göra unionens finanssektor mer motståndskraftig, inbegripet ur ett operativt perspektiv för att säkerställa dess tekniska säkerhet och goda funktion, och dess snabba återställning efter IKT-relaterade överträdelser och IKT-incidenter, så att finansiella tjänster i förlängningen kan tillhandahållas på ett effektivt och smidigt sätt i hela unionen, inbegripet i stressituationer, samtidigt som konsumenternas och marknadens förtroende bevaras.

(7) I april 2019 utfärdade gemensamt Europeiska tillsynsmyndigheten (Europeiska bankmyndigheten, EBA) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([4]), Europeiska tillsynsmyndigheten (Europeiska försäkrings- och tjänstepensionsmyndigheten, Eiopa) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1094/2010 ([5]), och Europeiska tillsynsmyndigheten (Europeiska värdepappers- och

([4]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

([5]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48).

marknadsmyndigheten, Esma) inrättad genom Europaparlamentets och rådets förordning (EU) nr 1095/2010 ([6]) (gemensamt kallade *de europeiska tillsynsmyndigheterna*) teknisk rådgivning och efterlyste ett enhetligt tillvägagångssätt för IKT-risk inom finanssektorn och rekommenderade en proportionell förstärkning av den digitala operativa motståndskraften i sektorn för finansiella tjänster genom ett sektorsspecifikt initiativ från unionen.

(8) Unionens finansiella sektor regleras genom ett enhetligt regelverk och styrs av ett europeiskt system för finansiell tillsyn. Icke desto mindre är bestämmelserna om digital operativ motståndskraft och IKT-säkerhet ännu inte fullständigt eller konsekvent harmoniserade, trots att den digitala operativa motståndskraften är avgörande för att säkerställa finansiell stabilitet och marknadsintegritet i den digitala tidsåldern, och inte mindre viktiga än t.ex. gemensamma standarder för tillsyn eller marknadsbeteenden. Det enhetliga regelverket och tillsynssystemet bör därför utvecklas så att de även omfattar digital operativ motståndskraft, genom att behöriga myndigheters mandat stärks så att de kan övervaka hanteringen av IKT-risk inom den finansiella sektorn i syfte att skydda den inre marknadens integritet och effektivitet samt för att främja dess korrekta funktion.

(9) Skillnader i lagstiftning och olika nationella reglerings- eller tillsynsstrategier för IKT-risk skapar hinder för den inre marknadens funktion för finansiella tjänster och hindrar ett smidigt utövande av etableringsfriheten och tillhandahållandet av tjänster för finansiella entiteter som bedriver gränsöverskridande verksamhet. Konkurrensen mellan samma typ av finansiella entiteter med verksamhet i olika medlemsstater skulle också kunna snedvridas. Detta gäller särskilt de områden där unionens harmonisering har varit mycket begränsad, såsom testning av digital operativ motståndskraft, eller saknas, såsom övervakning av IKT-tredjepartsrisk. Skillnader som härrör från den planerade utvecklingen på nationell nivå skulle kunna skapa ytterligare hinder för den inre marknadens funktion, till skada för marknadsaktörer och finansiell stabilitet.

(10) På grund av att bestämmelser i fråga om IKT-risk endast delvis behandlas på unionsnivå finns för närvarande luckor eller överlappningar på viktiga områden, t.ex. när det gäller IKT-relaterad incidentrapportering och testning av digital operativ motståndskraft, samt bristande konsekvens när skiljaktiga nationella regler utformas eller överlappande regler tillämpas på ett icke kostnadseffektivt sätt. Detta är särskilt skadligt för IKT-intensiva användare som finanssektorn, eftersom teknikrisker inte stannar vid nationsgränser och finanssektorn använder sina tjänster på bred gränsöverskridande basis inom och utanför unionen. Enskilda finansiella entiteter som bedriver gränsöverskridande verksamhet eller som innehar flera tillstånd (en finansiell entitet kan t.ex. ha tillstånd som bank, värdepappersföretag och betalningsinstitut, där varje tillstånd har utfärdats av olika behöriga myndigheter i en eller flera medlemsstater) ställs inför operativa utmaningar när det gäller att på egen hand hantera IKT-risk och mildra IKT-incidenters negativa effekter på ett samstämmigt och kostnadseffektivt sätt.

(11) Eftersom det enhetliga regelverket inte har åtföljts av en heltäckande IKT-ram eller ram för operativa risker krävs ytterligare harmonisering av viktiga krav på digital operativ motståndskraft för alla finansiella entiteter. Utvecklingen av IKT-kapacitet och övergripande motståndskraft hos finansiella entiteter baserat på dessa viktiga krav för att stå emot driftstörningar skulle bidra till att bevara stabiliteten och integriteten på unionens finansmarknader och därmed bidra till att säkerställa en hög skyddsnivå för investerare och konsumenter i unionen. Eftersom syftet med denna förordning är att bidra till att den inre marknaden fungerar friktionsfritt bör den baseras på artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), så som artikeln tolkats i Europeiska unionens domstols (domstolen) fasta rättspraxis.

(12) Denna förordning syftar till att konsolidera och uppgradera IKT-riskkraven som en del av de operativa riskkraven, vilka hittills har behandlats separat i olika unionsrättsakter. Även om dessa akter omfattade de huvudsakliga kategorierna av finansiell risk (t.ex. kreditrisk, marknadsrisk, motpartsrisk, likviditetsrisk och marknadsbeteenderisker), behandlades inte alla komponenter i den operativa motståndskraften på ett heltäckande sätt när dessa akter antogs. När reglerna rörande operativa risker närmare utformades i dessa unionsrättsakter föredrogs ofta en traditionell kvantitativ strategi för riskhantering (nämligen fastställande av ett kapitalkrav för att täcka IKT-risk) i stället för riktade kvalitativa regler avseende skydd, upptäckt, begränsning, återställning och avhjälpande av IKT-relaterade incidenter eller avseende rapporteringskapacitet och digital testkapacitet. Dessa akter var i första hand

([6]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84).

avsedda att omfatta och uppdatera grundläggande regler om tillsyn, marknadsintegritet eller marknadsbeteende. Genom att olika regler för IKT-risk konsolideras och uppgraderas bör alla bestämmelser om digitala risker inom finanssektorn för första gången samlas på ett enhetligt sätt i en enda rättsakt. Denna förordning täpper till luckorna eller avhjälper bristen på konsekvens i vissa av de tidigare rättsakterna, inbegripet i fråga om den terminologi som används i dem och som uttryckligen hänvisar till IKT-risk genom riktade regler om IKT-riskhanteringsförmåga, incidentrapportering, testning av operativ motståndskraft och övervakning av IKT-tredjepartsrisk. Denna förordning bör därför också öka medvetenheten om IKT-risk och understryka att IKT-incidenter och bristande operativ motståndskraft kan äventyra finansiella entiteters sundhet.

(13) Finansiella entiteter bör följa samma tillvägagångssätt och samma principbaserade regler i sin hantering av IKT-risk med beaktande av sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Enhetlighet bidrar till att öka förtroendet för det finansiella systemet och bevara dess stabilitet, särskilt i tider av starkt beroende av IKT-system, IKT-plattformar och IKT-infrastrukturer, vilket medför ökad digital risk. Iakttagande av grundläggande cyberhygien bör också leda till att det går att undvika höga kostnader för ekonomin, genom att effekterna av och kostnaderna för IKT-avbrott minimeras.

(14) En förordning bidrar till att minska lagstiftningens komplexitet, främjar konvergens i tillsynen och ökar rättssäkerheten, och bidrar också till att begränsa efterlevnadskostnaderna, särskilt för finansiella entiteter som bedriver gränsöverskridande verksamhet, och till att minska snedvridningen av konkurrensen. Därför är valet av en förordning för inrättandet av en gemensam ram för finansiella entiteters digitala operativa motståndskraft det lämpligaste sättet att garantera en enhetlig och samstämmig tillämpning av alla delar av IKT-riskhanteringen inom unionens finanssektor.

(15) Europaparlamentets och rådets direktiv (EU) 2016/1148 ([7]) var den första övergripande ramen för cybersäkerhet som antogs på unionsnivå och som också tillämpas på tre typer av finansiella entiteter, nämligen kreditinstitut, handelsplatser och centrala motparter. Eftersom det i direktiv (EU) 2016/1148 fastställdes en mekanism för identifiering på nationell nivå av leverantörer av samhällsviktiga tjänster, var det endast vissa kreditinstitut, handelsplatser och centrala motparter som identifierades av medlemsstaterna som inkluderades i direktivets tillämpningsområde i praktiken och därmed är skyldiga att uppfylla de rapporteringskrav i fråga om IKT-säkerhet och IKT-incidenter som fastställs i direktivet. I Europaparlamentets och rådets direktiv (EU) 2022/2555 ([8]) fastställs enhetliga kriterier för att avgöra vilka entiteter som omfattas av dess tillämpningsområde (storleksbaserad regel) samtidigt som de tre typerna av finansiella entiteter behålls inom dess tillämpningsområde.

(16) Eftersom denna förordning leder till en ökad harmonisering av de olika komponenterna av digital motståndskraft genom att det införs strängare krav på IKT-riskhantering och IKT-relaterad incidentrapportering än de som fastställs i den nuvarande unionsrätten avseende finansiella tjänster, innebär denna högre nivå en ökad harmonisering även jämfört med kraven i direktiv (EU) 2022/2555. Denna förordning utgör följaktligen *lex specialis* i förhållande till direktiv (EU) 2022/2555. Det är samtidigt mycket viktigt att upprätthålla en stark koppling mellan finanssektorn och unionens övergripande ram för cybersäkerhet, som för närvarande fastställs i direktiv (EU) 2022/2555 för att säkerställa överensstämmelse med de strategier för cybersäkerhet som antagits av medlemsstaterna och göra det möjligt för finansiella tillsynsmyndigheter att få kännedom om cyberincidenter som påverkar andra sektorer som omfattas av det direktivet.

([7]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

([8]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (se sidan 80 i detta nummer av EUT).

(17) I enlighet med artikel 4.2 i fördraget om Europeiska unionen och utan att det påverkar domstolens rättsliga prövning bör denna förordning inte påverka medlemsstaternas ansvar vad gäller väsentliga statliga funktioner rörande allmän säkerhet, försvar och skyddet av den nationella säkerheten, till exempel när det gäller tillhandahållande av information som står i strid med skyddet av den nationella säkerheten.

(18) För att möjliggöra sektorsövergripande lärande och effektivt ta vara på erfarenheter från andra sektorer när det gäller att hantera cyberhot bör de finansiella entiteter som avses i direktiv (EU) 2022/2555 fortsätta att ingå i ”ekosystemet” i det direktivet (t.ex. samarbetsgrupp samt nätverket av entiteter för hantering av it-säkerhetsincidenter (CSIRT-enheter)). De europeiska tillsynsmyndigheterna och de nationella behöriga myndigheterna bör kunna delta i de strategiska politiska diskussionerna och det tekniska arbetet i samarbetsgruppen enligt det direktivet och kunna utbyta information och samarbeta ytterligare med de gemensamma kontaktpunkter som har utsetts eller inrättats i enlighet med det direktivet. De behöriga myndigheterna enligt denna förordning bör också samråda och samarbeta med CSIRT-enheter. De behöriga myndigheterna bör också kunna begära teknisk rådgivning från de behöriga myndigheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555 samt inrätta samarbetsarrangemang i syfte att säkerställa effektiva och snabba samordningsmekanismer.

(19) Med tanke på de starka sambanden mellan finansiella entiteters digitala motståndskraft och fysiska motståndskraft krävs ett enhetligt tillvägagångssätt för kritiska entiteters motståndskraft i denna förordning och i Europaparlamentets och rådets direktiv (EU) 2022/2557 ([9]). Eftersom finansiella entiteters fysiska motståndskraft behandlas övergripande i de skyldigheter rörande IKT-riskhantering och rapportering som omfattas av denna förordning, bör de skyldigheter som fastställs i kapitlen III och IV i direktiv (EU) 2022/2557 inte tillämpas på finansiella entiteter som omfattas av tillämpningsområdet för det direktivet.

(20) Leverantörer av molntjänster är en kategori av leverantörer av digitala infrastrukturer som omfattas av direktiv (EU) 2022/2555. Den unionstillsynsram (*tillsynsramen*) som inrättas genom denna förordning är tillämplig på alla kritiska tredjepartsleverantörer av IKT-tjänster, inbegripet leverantörer av molntjänster som tillhandahåller IKT-tjänster till finansiella entiteter, och bör betraktas som ett komplement till den tillsyn som utförs enligt direktiv (EU) 2022/2555. Den tillsynsram som inrättas genom denna förordning bör dessutom omfatta leverantörer av molntjänster, i avsaknad av en unionsomfattande sektorsövergripande ram för inrättande av en digital tillsynsmyndighet.

(21) För att finansiella entiteter ska kunna upprätthålla full kontroll över IKT-risk måste de ha övergripande kapacitet som möjliggör en kraftfull och effektiv IKT-riskhantering, liksom särskilda mekanismer och riktlinjer för att hantera alla IKT-relaterade incidenter och rapportera allvarliga IKT-relaterade incidenter. På samma sätt bör finansiella entiteter ha inrättat strategier för testning av IKT-system, IKT-kontroller och IKT-processer samt för hantering av IKT-tredjepartsrisk. Referensnivån för digital operativ motståndskraft hos finansiella entiteter bör höjas och samtidigt möjliggöra en proportionell tillämpning av kraven för vissa finansiella entiteter, särskilt mikroföretag, liksom finansiella entiteter som är föremål för en förenklad IKT-riskhanteringsram. För att underlätta en effektiv tillsyn av tjänstepensionsinstitut som är proportionell och tillgodoser behovet att minska de behöriga myndigheternas administrativa bördor bör relevanta nationella tillsynsramar för sådana finansiella entiteter beakta deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser, även när de relevanta trösklar som fastställs i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/2341 ([10]) överskrids. Framför allt bör tillsynsverksamhet i första hand inriktas på behovet av att hantera allvarliga risker i samband med IKT-riskhantering i en särskild entitet.

([9]) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och upphävande av rådets direktiv 2008/114/EG (se sidan 164 i detta nummer av EUT).

([10]) Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut (EUT L 354, 23.12.2016, s. 37).

De behöriga myndigheterna bör också upprätthålla ett vaksamt men proportionellt tillvägagångssätt vad gäller tillsyn över tjänstepensionsinstitut som, i enlighet med artikel 31 i direktiv (EU) 2016/2341, utkontrakterar en betydande del av sin kärnverksamhet, till exempel kapitalförvaltning, försäkringstekniska beräkningar, redovisning och databehandling till tjänsteleverantörer.

(22) Tröskelvärden och taxonomier för rapportering av IKT-relaterade incidenter varierar avsevärt på nationell nivå. Även om en samsyn kan uppnås genom det relevanta arbete som utförs av Europeiska unionens cybersäkerhetsbyrå (Enisa), som inrättats genom Europaparlamentets och rådets förordning (EU) 2019/881 ([11]), och samarbetsgruppen enligt direktiv (EU) 2022/2555, kan det fortfarande förekomma eller växa fram olika strategier för tröskelvärden och taxonomier för andra finansiella entiteter. Dessa skillnader medför flera krav som finansiella entiteter måste uppfylla, särskilt när de är verksamma i flera medlemsstater och när de ingår i en finansiell koncern. Sådana skillnader kan dessutom hindra inrättandet av ytterligare enhetliga eller centraliserade mekanismer på unionsnivå som påskyndar rapporteringsprocessen och underlättar ett snabbt och smidigt informationsutbyte mellan behöriga myndigheter, vilket är avgörande för att hantera IKT-risk vid storskaliga attacker med eventuella konsekvenser för det finansiella systemet.

(23) För att minska den administrativa bördan och eventuellt dubbla rapporteringsskyldigheter för vissa finansiella entiteter bör kravet på incidentrapportering enligt Europaparlamentets och rådets direktiv (EU) 2015/2366 ([12]) upphöra att tillämpas för betaltjänstleverantörer som omfattas av tillämpningsområdet för denna förordning. Därför bör de kreditinstitut, institut för elektroniska pengar, betalningsinstitut och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i det direktivet, från och med tillämpningsdagen för denna förordning rapportera enligt denna förordning, alla betalningsrelaterade operativa incidenter eller säkerhetsincidenter som tidigare rapporterades enligt det direktivet, oavsett om sådana incidenter är IKT-relaterade.

(24) För att de behöriga myndigheterna ska kunna fullgöra tillsynsuppgifter genom att skaffa sig en fullständig överblick över IKT-relaterade incidenters art, frekvens, betydelse och inverkan och för att förbättra informationsutbytet mellan berörda offentliga myndigheter, inbegripet brottsbekämpande myndigheter och resolutionsmyndigheter, bör denna förordning fastställa regler för att uppnå ett stabilt rapporteringssystem för IKT-relaterade incidenter, där relevanta krav åtgärdar befintliga luckor i rätten avseende finansiella tjänster och undanröjer överlappningar och dubbleringar för att minska kostnaderna. Det är därför viktigt att harmonisera rapporteringssystemet för IKT-relaterade incidenter genom att kräva att alla finansiella entiteter rapporterar till sina behöriga myndigheter genom en harmoniserad ram i enlighet med denna förordning. Dessutom bör de europeiska tillsynsmyndigheterna ges befogenhet att närmare specificera relevanta delar i ramen för rapportering av IKT-relaterade incidenter, såsom taxonomi, tidsramar, datamängder, mallar och tillämpliga tröskelvärden. För att säkerställa fullständig överensstämmelse med direktiv (EU) 2022/2555 bör finansiella entiteter på frivillig basis tillåtas rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att cyberhotet är relevant för det finansiella systemet, tjänsteanvändare eller kunder.

(25) Krav på testning av digital operativ motståndskraft har utarbetats i vissa finansiella delsektorer med ramar som inte alltid är harmoniserade fullt ut. Detta leder till potentiellt dubbla kostnader för gränsöverskridande finansiella entiteter och gör ett ömsesidigt erkännande av testresultaten för digital operativ motståndskraft komplicerat, vilket i sin tur kan fragmentera den inre marknaden.

([11]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

([12]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

(26) I de fall där det inte krävs någon IKT-testning förblir dessutom sårbarheter oupptäckta och leder till att en finansiell entitet utsätts för IKT-risk, och skapar i förlängningen en högre risk för den finansiella sektorns stabilitet och integritet. Utan unionsåtgärder skulle testningen av digital operativ motståndskraft fortsätta att vara inkonsekvent och det skulle inte finnas något system för ömsesidigt erkännande av IKT-testresultat i olika jurisdiktioner. Eftersom det dessutom är osannolikt att andra finansiella delsektorer skulle anta testsystem i en meningsfull omfattning skulle de också gå miste om de potentiella fördelarna med en testram, t.ex. att avslöja IKT-sårbarheter och IKT-risker, och att testa försvarskapacitet och driftskontinuitet, vilket bidrar till att öka kundernas, leverantörernas och affärspartnernas förtroende. För att åtgärda dessa överlappningar, skillnader och luckor är det nödvändigt att fastställa regler som syftar till ett samordnat testsystem för finansiella entiteter, för att på så sätt underlätta ömsesidigt erkännande av avancerade tester för de finansiella entiteter som uppfyller de krav som fastställs i denna förordning.

(27) Finansinstitutens beroende av användningen av IKT-tjänster beror delvis på deras behov av att anpassa sig till en framväxande konkurrenskraftig digital global ekonomi, effektivisera sin verksamhet och tillgodose konsumenternas efterfrågan. Karaktären på och omfattningen av ett sådant beroende har utvecklats kontinuerligt under de senaste åren, vilket har drivit fram kostnadsminskningar inom finansiell förmedling, möjliggjort företagsexpansion och skalbarhet vid införandet av finansiell verksamhet och samtidigt gett tillgång till ett brett spektrum av IKT-verktyg för att hantera komplexa interna processer.

(28) Den omfattande användningen av IKT-tjänster framgår av komplexa kontraktsmässiga arrangemang, där finansiella entiteter ofta stöter på svårigheter med att förhandla om avtalsvillkor som är anpassade till de tillsynsstandarder eller andra lagstadgade krav som de omfattas av, eller på annat sätt hävda särskilda rättigheter, såsom åtkomsträtt eller revisionsrätt, även när dessa är inskrivna i deras kontraktsmässiga arrangemang. Många av de kontraktsmässiga arrangemangen innehåller dessutom inte tillräckliga skyddsåtgärder som möjliggör en fullständig övervakning av utkontrakteringsprocesser, vilket gör att den finansiella entiteten inte har möjlighet att bedöma dessa risker. Eftersom tredjepartsleverantörer av IKT-tjänster ofta tillhandahåller standardiserade tjänster till olika typer av kunder kan det dessutom hända att sådana kontraktsmässiga arrangemang inte alltid tillgodoser finansbranschaktörernas individuella eller särskilda behov.

(29) Även om unionsrätten avseende finansiella tjänster omfattar vissa allmänna regler om utkontraktering är övervakningen av avtalsdimensionen inte helt förankrad i unionsrätten. Tydliga och skräddarsydda unionsstandarder som är tillämpliga på de kontraktsmässiga arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster saknas, och därmed hanteras inte den externa IKT-riskkällan på ett heltäckande sätt. Det är därför nödvändigt att fastställa vissa nyckelprinciper för att vägleda finansiella entiteters hantering av IKT-tredjepartsrisker, vilka är särskilt viktiga när finansiella entiteter använder tredjepartsleverantörer av IKT-tjänster för att stödja kritiska eller viktiga funktioner. Dessa principer bör åtföljas av en uppsättning grundläggande avtalsenliga rättigheter i samband med flera aspekter av fullgörandet och avslutandet av kontraktsmässiga arrangemang i syfte att tillhandahålla vissa minimiskyddsåtgärder för att stärka finansiella entiteters förmåga att effektivt övervaka alla IKT-risker som uppstår på tredjepartstjänsteleverantörsnivå. De principerna kompletterar den sektorsrätt som är tillämplig på utkontraktering.

(30) Det är i dagsläget uppenbart att det råder en viss brist på homogenitet och konvergens vad gäller övervakningen av IKT-tredjepartsrisker och beroende av IKT-tredjeparter. Trots ansträngningarna för att hantera utkontraktering, t.ex. EBA:s riktlinjer för utkontraktering från 2019 och Esmas riktlinjer för utkontraktering till molntjänstleverantörer från 2021, behandlas den större frågan om att motverka systemrisker som kan utlösas av finanssektorns exponering mot ett begränsat antal kritiska tredjepartsleverantörer av IKT-tjänster inte i tillräcklig utsträckning i unionsrätten. Denna avsaknad av regler på unionsnivå förvärras av att det inte finns några nationella regler för mandat och verktyg som gör det möjligt för finansiella tillsynsmyndigheter att skaffa sig en god bild av beroendet av IKT-tredjeparter och att på lämpligt sätt övervaka risker som uppstår till följd av koncentration av beroenden av IKT-tredjeparter.

(31) Med hänsyn till de potentiella systemrisker som den ökade utkontrakteringen och koncentrationen av IKT-tredjeparter medför, och till de otillräckliga nationella mekanismer som ger finansiella tillsynsmyndigheter lämpliga verktyg för att kvantitativt och kvalitativt fastställa och åtgärda konsekvenserna av IKT-risk som uppstår hos kritiska tredjepartsleverantörer av IKT-tjänster, är det nödvändigt att inrätta en lämplig tillsynsram som möjliggör en kontinuerlig övervakning av verksamheten hos tredjepartsleverantörer av IKT-tjänster som är kritiska tredjepartsleverantörer av IKT-tjänster till finansiella entiteter, och samtidigt säkerställa konfidentialitet och säkerhet för kunder som inte är finansiella entiteter. Tillhandahållandet av IKT-tjänster inom en koncern medför specifika risker och fördelar, men det bör inte automatiskt anses mindre riskfyllt än tillhandahållande av IKT-tjänster från leverantörer utanför en finansiell koncern, och bör därför omfattas av samma regelverk. När IKT-tjänster tillhandahålls inom samma finansiella koncern kan dock finansiella entiteter ha större kontroll över koncerninterna leverantörer, vilket bör beaktas vid den övergripande riskbedömningen.

(32) I och med att IKT-risker blir alltmer komplexa och sofistikerade kommer effektiva åtgärder för att upptäcka och förebygga IKT-risk att i hög grad vara beroende av regelbundet utbyte mellan finansiella entiteter av underrättelser om hot och sårbarhet. Informationsutbyte bidrar till att skapa ökad medvetenhet om cyberhot. Detta ökar i sin tur finansiella entiteters förmåga att förhindra att cyberhot blir verkliga IKT-relaterade incidenter, och gör det möjligt för finansiella entiteter att på ett mer effektivt sätt begränsa IKT-relaterade incidenters inverkan och att återhämta sig snabbare. I avsaknad av vägledning på unionsnivå verkar flera faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerhet om förenligheten med dataskyddsregler, antitrustregler och ansvarsregler.

(33) Dessutom leder tveksamheter om vilken typ av information som kan delas med andra marknadsaktörer, eller med myndigheter som inte är tillsynsmyndigheter (t.ex. Enisa, för analytiskt underlag, eller Europol, för brottsbekämpande ändamål) till att användbar information inte lämnas ut. Omfattningen av och kvaliteten på informationsutbytet är därför i nuläget fortfarande begränsad och fragmenterad, med relevanta utbyten som oftast görs lokalt (via nationella initiativ) och inga enhetliga unionsomfattande arrangemang för informationsutbyte som är anpassade till behoven i ett integrerat finansiellt system. Det är därför viktigt att stärka dessa kommunikationskanaler.

(34) Finansiella entiteter bör därför uppmuntras att sinsemellan utbyta information och underrättelser om cyberhot, och kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt bedöma, övervaka, försvara och reagera på cyberhot genom att delta i arrangemang för informationsutbyte. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av mekanismer för frivilligt informationsutbyte som, när de genomförs i betrodda miljöer, skulle hjälpa finanssektorn att förebygga och kollektivt reagera på cyberhot genom att snabbt begränsa spridningen av IKT-risk och hindra potentiella spridningseffekter genom de finansiella kanalerna. Dessa mekanismer bör överensstämma med unionens tillämpliga konkurrensrättsliga regler som anges i kommissionens meddelande av den 14 januari 2011 med titeln *Riktlinjer för tillämpningen av artikel 101 i fördraget om Europeiska unionens funktionssätt på horisontella samarbetsavtal* samt med unionens dataskyddsregler, särskilt Europaparlamentets och rådets förordning (EU) 2016/679 ([13]). De bör fungera på grundval av en eller flera av de rättsliga grunder som fastställs i artikel 6 i den förordningen, till exempel i samband med sådan behandling av personuppgifter som är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, enligt artikel 6.1 f i den förordningen, liksom i samband med den behandling av personuppgifter som är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige, som är nödvändig för att utföra en uppgift i allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning, enligt artikel 6.1 c respektive e i den förordningen.

([13]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

(35) För att upprätthålla en hög nivå av digital operativ motståndskraft i hela den finansiella sektorn, och samtidigt hålla jämna steg med den tekniska utvecklingen, bör denna förordning hantera de risker som härrör från alla typer av IKT-tjänster. I det syftet bör definitionen av IKT-tjänster inom ramen för denna förordning ges en vid tolkning för att omfatta digitala tjänster och datatjänster som tillhandahålls fortlöpande genom IKT-system till en eller flera interna eller externa användare. Den definitionen bör till exempel omfatta s.k. over-the-top-tjänster, som omfattas av kategorin elektroniska kommunikationstjänster. Den bör endast utesluta den begränsade kategori av traditionella analoga telefonitjänster som räknas som tjänster inom det allmänna telefonnätet (PSTN), tjänster inom fasta nät, konventionella telefontjänster (POTS) eller telefonitjänster inom fasta nät.

(36) Trots den breda täckning som föreskrivs i denna förordning bör vid tillämpningen av reglerna om digital operativ motståndskraft beaktas betydande skillnader mellan finansiella entiteter i fråga om deras storlek och allmänna riskprofil. Som en allmän princip bör finansiella entiteter, när de fördelar resurser och kapacitet till genomförandet av IKT-riskhanteringsramen, på lämpligt sätt väga sina IKT-relaterade behov mot sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser medan de behöriga myndigheterna bör fortsätta att bedöma och se över tillvägagångssättet för en sådan fördelning.

(37) Leverantörer av kontoinformationstjänster, som avses i artikel 33.1 i direktiv (EU) 2015/2366, omfattas uttryckligen av denna förordnings tillämpningsområde, med hänsyn till den specifika arten av deras verksamhet och de risker som den ger upphov till. Dessutom omfattas institut för elektroniska pengar och betalningsinstitut och som är undantagna enligt artikel 9.1 i Europaparlamentets och rådets direktiv 2009/110/EG ([14]) och artikel 32.1 i direktiv (EU) 2015/2366 av tillämpningsområdet för denna förordning även om de inte har beviljats auktorisation i enlighet med direktiv 2009/110/EG att ge ut elektroniska pengar, eller om de inte har auktoriserats i enlighet med direktiv (EU) 2015/2366 att tillhandahålla och genomföra betaltjänster. De postgiroinstitut som avses i artikel 2.5.3 i Europaparlamentets och rådets direktiv 2013/36/EU ([15]) är dock undantagna från denna förordnings tillämpningsområde. Den behöriga myndigheten för betalningsinstitut som är undantagna enligt direktiv (EU) 2015/2366, institut för elektroniska pengar som är undantagna enligt direktiv 2009/110/EG och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366, bör vara den behöriga myndighet som utsetts i enlighet med artikel 22 i direktiv (EU) 2015/2366.

(38) Eftersom större finansiella entiteter skulle kunna ha mer omfattande resurser och snabbt kan använda medel för att utveckla styrningsstrukturer och inrätta olika företagsstrategier, bör endast finansiella entiteter som inte är mikroföretag i den mening som avses i denna förordning vara skyldiga att inrätta mer komplexa styrformer. Framför allt är sådana entiteter bättre rustade att inrätta särskilda ledningsfunktioner för att övervaka arrangemang med tredjepartsleverantörer av IKT-tjänster eller för att sköta krishantering, organisera sin IKT-riskhantering enligt modellen med tre försvarslinjer, eller inrätta en intern riskhanterings- och kontrollmodell och låta sin IKT-riskhanteringsram undergå interna revisioner.

(39) Vissa finansiella entiteter är undantagna från eller omfattas av ett mycket begränsat regelverk enligt relevant sektorsspecifik unionsrätt. Sådana finansiella entiteter omfattar förvaltare av alternativa investeringsfonder som avses i artikel 3.2 i Europaparlamentets och rådets direktiv 2011/61/EU ([16]), försäkrings- och återförsäkringsföretag som avses i artikel 4 i Europaparlamentets och rådets direktiv 2009/138/EG ([17]) samt tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 15 medlemmar. Mot bakgrund av dessa undantag

([14]) Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).

([15]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([16]) Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010 (EUT L 174, 1.7.2011, s. 1).

([17]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

skulle det inte vara proportionellt att inkludera sådana finansiella entiteter i denna förordnings tillämpningsområde. Denna förordning erkänner dessutom försäkringsförmedlingsmarknadens särdrag, vilket innebär att försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet och som räknas som mikroföretag eller som små eller medelstora företag inte bör omfattas av denna förordning.

(40) Eftersom de entiteter som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU är undantagna från det direktivets tillämpningsområde bör medlemsstaterna därför kunna välja att från denna förordning undanta sådana institut som är belägna inom deras respektive territorier.

(41) För att anpassa denna förordning till tillämpningsområdet för Europaparlamentets och rådets direktiv 2014/65/EU ([18]) är det också lämpligt att från denna förordnings tillämpningsområde utesluta de fysiska och juridiska personer som avses i artiklarna 2 och 3 i det direktivet och som får tillhandahålla investeringstjänster utan att behöva erhålla auktorisation enligt direktiv 2014/65/EU. Dock utesluts även enligt artikel 2 i direktiv 2014/65/EU från tillämpningsområdet för det direktivet entiteter som räknas som finansiella entiteter enligt denna förordning, till exempel värdepapperscentraler, företag för kollektiva investeringar eller försäkrings- och återförsäkringsföretag. Uteslutningen från denna förordnings tillämpningsområde för personer och entiteter som avses i artiklarna 2 och 3 i det direktivet bör inte omfatta dessa värdepapperscentraler, företag för kollektiva investeringar eller försäkrings- och återförsäkringsföretag.

(42) Enligt sektorsspecifik unionsrätt omfattas vissa finansiella entiteter av förenklade krav eller undantag av skäl som rör deras storlek eller de tjänster de tillhandahåller. Den kategorin av finansiella entiteter omfattar små och icke sammanlänkade värdepappersföretag, små tjänstepensionsinstitut som får uteslutas från tillämpningsområdet för direktiv (EU) 2016/2341 enligt de villkor som fastställs i artikel 5 i det direktivet av den berörda medlemsstaten och som har pensionsplaner som tillsammans inte omfattar fler än 100 personer totalt, liksom institut som är undantagna enligt direktiv 2013/36/EU. Det är därför lämpligt att, i enlighet med proportionalitetsprincipen och för att bevara andan av sektorsspecifik unionsrätt, låta de finansiella entiteterna omfattas av en förenklad IKT-riskhanteringsram enligt denna förordning. Den proportionella karaktären i den förenklade IKT-riskhanteringsram som omfattar dessa finansiella entiteter bör inte ändras av de lagstadgade tekniska standarder som ska utarbetas av de europeiska tillsynsmyndigheterna. I enlighet med proportionalitetsprincipen är det dessutom lämpligt att även låta de betalningsinstitut som avses i artikel 32.1 i direktiv (EU) 2015/2366 och de institut för elektroniska pengar som avses i artikel 9 i direktiv 2009/110/EG som är undantagna i enlighet med nationellt rätt som införlivar dessa unionsrättsakter omfattas av en förenklad IKT-riskhanteringsram enligt denna förordning, medan betalningsinstitut och institut för elektroniska pengar som inte har undantagits i enlighet med respektive nationell rätt som införlivar sektorsspecifik unionsrätt bör följa den allmänna ram som fastställs i denna förordning.

(43) På samma sätt bör finansiella entiteter som räknas som mikroföretag eller som omfattas av den förenklade IKT-riskhanteringsramen enligt denna förordning inte vara skyldiga att inrätta en funktion för att övervaka de arrangemang som de ingått med IKT-tredjepartsleverantörer för användning av IKT-tjänster; eller att utse en medlem av den högre ledningen till ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation; att överföra ansvaret för att hantera och övervaka IKT-risk till en kontrollfunktion och säkerställa en lämplig nivå av oberoende för den kontrollfunktionen för att undvika intressekonflikter; att minst en gång om året dokumentera och se över IKT-riskhanteringsramen; att regelbundet låta IKT-riskhanteringsramen undergå en internrevision; att göra djupgående bedömningar efter större förändringar i deras infrastruktur och processer för nätverks- och informationssystem; att regelbundet genomföra riskanalyser av befintliga IKT-system; att låta genomförandet av åtgärds- och återställningsplaner avseende IKT undergå oberoende interna granskningar; att inrätta en krishanteringsfunktion, att utöka testningen av driftskontinuitet och åtgärds- och återställningsplaner för att fånga upp överflyttningsscenarier mellan primär IKT-infrastruktur och reservanläggningar, att på begäran av de behöriga myndigheterna lämna en uppskattning av de totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter, att upprätthålla IKT-reservkapacitet; att till de nationella behöriga myndigheterna meddela

([18]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

vilka förändringar som genomfördes efter efterhandsöversyner av IKT-relaterade incidenter; att kontinuerligt övervaka relevant teknisk utveckling, att inrätta ett heltäckande program för testning av digital operativ motståndskraft som en integrerad del av den IKT-riskhanteringsram som föreskrivs i den här förordningen, eller att anta och regelbundet se över en strategi för IKT-tredjepartsrisk. Mikroföretag ska dessutom endast bedöma behovet av att upprätthålla sådan IKT-reservkapacitet med utgångspunkt i vilken riskprofil de har. Mikroföretag bör omfattas av ett mer flexibelt system vad gäller program för testning av digital operativ motståndskraft. När de överväger vilken typ och frekvens av testning som ska utföras bör de vederbörligen väga målet att upprätthålla en hög digital operativ motståndskraft, de tillgängliga resurserna och sin allmänna riskprofil. Mikroföretag och finansiella entiteter som omfattas av den förenklade IKT-riskhanteringsramen enligt denna förordning bör undantas från kravet på avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning, eftersom endast finansiella entiteter som uppfyller de krav som fastställs i denna förordning bör vara skyldiga att utföra sådan testning. Mot bakgrund av sin begränsade kapacitet bör mikroföretag kunna komma överens med tredjepartsleverantören av IKT-tjänster att delegera den finansiella entiteten rätt till tillgång, inspektion och revision till en oberoende tredje part som utsetts av tredjepartsleverantören av IKT-tjänster, under förutsättning att den finansiella entiteten, när som helst, kan begära all relevant information och försäkran om tredjepartsleverantörens prestanda från respektive oberoende tredje part.

(44) Eftersom endast de finansiella entiteter som har identifierats vid tillämpning av avancerad testning av digital motståndskraft bör vara skyldiga att utföra hotbildsstyrda penetrationstester, bör dessutom de administrativa processer och finansiella kostnader som genomförandet av sådana tester medför överföras till en liten andel av finansiella entiteter.

(45) För att säkerställa fullständig anpassning och övergripande konsekvens mellan finansiella entiteters affärsstrategier, å ena sidan, och genomförandet av IKT-riskhantering, å andra sidan, bör finansiella entiteters ledningsorgan vara skyldiga att ha en central och aktiv roll i styrningen och anpassningen av IKT-riskhanteringsramen och den övergripande strategin för digital operativ motståndskraft. Ledningsorganens strategi bör inte enbart vara inriktad på hur IKT-systemens motståndskraft säkerställs, utan även omfatta människor och processer genom en uppsättning strategier som, på varje företagsnivå och för all personal, främjar en stark känsla av medvetenhet om cyberrisker och ett åtagande att tillämpa en strikt cyberhygien på alla nivåer. Ledningsorganets yttersta ansvar för att hantera en finansiell entitets IKT-risk bör utgöra en övergripande princip för den heltäckande strategin och omsättas i ett fortlöpande engagemang hos ledningen för att kontrollera övervakningen av IKT-riskhanteringen.

(46) Principen om ledningsorganets fullständiga och slutgiltiga ansvar för hanteringen av IKT-risken för en finansiell entitet går hand i hand med behovet av att säkerställa en nivå för IKT-relaterade investeringar och en övergripande budget för den finansiella entiteten som skulle möjliggöra för den finansiella entiteten att uppnå en hög nivå av digital operativ motståndskraft.

(47) Med inspiration från relevanta internationella, nationella och branschspecifika bästa praxis, riktlinjer, rekommendationer och strategier för hantering av cyberrisker, förordas i denna förordning en uppsättning principer som underlättar den övergripande strukturering av IKT-riskhanteringen. Så länge finansiella entiteters huvudsakliga kapacitet uppfyller de olika funktionerna för IKT-riskhantering (identifiering, skydd och förebyggande, upptäckt, åtgärd och återställning, lärande och utveckling samt kommunikation) som anges i denna förordning, bör det följaktligen stå finansiella entiteter fritt att använda IKT-riskhanteringsmodeller som utformas eller kategoriseras på olika sätt.

(48) För att hålla jämna steg med den föränderliga cyberhotbilden bör finansiella entiteter upprätthålla uppdaterade IKT-system som är tillförlitliga och har kapacitet, inte bara för att garantera den behandling av data som krävs för deras tjänster, utan också för att säkerställa tillräcklig teknisk motståndskraft som gör det möjligt för dem att på ett adekvat sätt hantera ytterligare databehandlingsbehov på grund av stressade marknadsförhållanden eller andra ogynnsamma situationer.

(49) Effektiva kontinuitets- och återställningsplaner krävs för att finansiella entiteter snabbt ska kunna åtgärda IKT-relaterade incidenter, särskilt cyberangrepp, genom att begränsa skador och prioritera återupptagande av verksamhet och återställningsåtgärder i enlighet med sina beredskapsplaner. Ett sådant återupptagande bör dock inte på något sätt äventyra integriteten och säkerheten i nätverks- eller informationssystemen eller uppgifternas tillgänglighet, äkthet, integritet eller konfidentialitet.

(50) Denna förordning innebär att finansiella entiteter kan fastställa sina mål för återställningstid och återskapandepunkt på ett flexibelt sätt och därvid fullt ut ta hänsyn till den berörda funktionens egenskaper och kritikalitet och till eventuella särskilda verksamhetsbehov, men det bör också krävas att de gör en bedömning av den eventuella övergripande inverkan på marknadseffektiviteten när sådana mål fastställs.

(51) Spridare av cyberangrepp tenderar att eftersträva ekonomisk vinning direkt vid källan, vilket utsätter finansiella entiteter för betydande konsekvenser. I syfte att förhindra att IKT-system förlorar integritet eller blir otillgängliga, och därmed undvika dataintrång och skador för den fysiska IKT-infrastrukturen, bör finansiella entiteters rapportering av allvarliga IKT-relaterade incidenter avsevärt förbättras och förenklas. IKT-relaterad incidentrapportering bör harmoniseras genom införande av ett krav för alla finansiella entiteter att rapportera direkt till sina berörda behöriga myndigheter. Om en finansiell entitet är föremål för tillsyn av mer än en nationell behörig myndighet bör medlemsstaterna utse en enda behörig myndighet som mottagare av sådan rapportering. Kreditinstitut som klassificerats som betydande i enlighet med artikel 6.4 i rådets förordning (EU) nr 1024/2013 ([19]) bör förelägga de nationella behöriga myndigheterna sådan rapportering, och dessa bör därefter översända rapporten till Europeiska centralbanken (ECB).

(52) Direkt rapportering bör göra det möjligt för finansiella tillsynsmyndigheter att få omedelbar tillgång till information om allvarliga IKT-relaterade incidenter. Finansiella tillsynsmyndigheter bör i sin tur vidarebefordra närmare detaljer om allvarliga IKT-relaterade incidenter till offentliga icke-finansiella myndigheter (t.ex. behöriga myndigheter och gemensamma kontaktpunkter enligt direktiv (EU) 2022/2555, nationella dataskyddsmyndigheter och brottsbekämpande myndigheter för allvarliga IKT-relaterade incidenter av brottslig karaktär) för att öka dessa myndigheters medvetenhet om sådana incidenter, och vad gäller CSIRT-enheter, för att underlätta snabbt stöd som kan ges till finansiella entiteter när så är lämpligt. Dessutom bör medlemsstaterna kunna avgöra huruvida finansiella entiteter själva bör tillhandahålla sådan information till offentliga myndigheter utanför området för finansiella tjänster. Dessa informationsflöden bör göra det möjligt för finansiella entiteter att snabbt dra fördel av relevanta tekniska uppgifter, råd om åtgärder och uppföljning från sådana myndigheter. Informationen om allvarliga IKT-relaterade incidenter bör förmedlas ömsesidigt: de finansiella tillsynsmyndigheterna bör ge all nödvändig återkoppling eller vägledning till den finansiella entiteten, medan de europeiska tillsynsmyndigheterna bör dela anonymiserade uppgifter om cyberhot och sårbarheter i samband med en incident, till stöd för ett bredare kollektivt försvar.

(53) Även om det bör krävas att alla finansiella entiteter rapporterar incidenter förväntas inte det kravet påverka dem alla på samma sätt. Relevanta väsentlighetströsklar och rapporteringsfrister bör vederbörligen anpassas, inom ramen för delegerade akter grundade på tekniska standarder för tillsyn som utarbetas av de europeiska tillsynsmyndigheterna, med syftet att endast omfatta allvarliga IKT-relaterade incidenter. Dessutom bör finansiella entiteters särdrag beaktas när fristerna för rapporteringsskyldigheter fastställs.

(54) Denna förordning bör innehålla krav på att kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar rapporterar alla betalningsrelaterade operativa incidenter eller säkerhetsincidenter – som tidigare rapporterades enligt direktiv (EU) 2015/2366 – oavsett om incidenten är IKT-relaterad eller inte.

([19]) Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut (EUT L 287, 29.10.2013, s. 63).

(55) De europeiska tillsynsmyndigheterna bör få i uppdrag att bedöma genomförbarheten av och villkoren för en eventuell centralisering av IKT-relaterade incidentrapporter på unionsnivå. Sådan centralisering kan bestå av en gemensam EU-knutpunkt för rapportering av allvarliga IKT-relaterade incidenter, som antingen direkt tar emot relevanta rapporter och automatiskt underrättar nationella behöriga myndigheter, eller som enbart centraliserar relevanta rapporter från de nationella behöriga myndigheterna och därmed fyller en samordnande funktion. De europeiska tillsynsmyndigheterna bör få i uppdrag att i samråd med ECB och Enisa utarbeta en gemensam rapport om möjligheten att inrätta en gemensam EU-knutpunkt.

(56) För att uppnå en hög nivå av digital operativ motståndskraft, och i linje med både relevanta internationella standarder (t.ex. G7-gruppens Fundamental Elements for Threat-Led Penetration Testing), och med de ramar som tillämpas inom unionen, till exempel TIBER-EU bör finansiella entiteter regelbundet testa sina IKT-system och sin personal med IKT-ansvar med avseende på hur effektiv deras kapacitet är för förebyggande, upptäckt, åtgärd och återställning, för att upptäcka och åtgärda potentiella IKT-sårbarheter. För att återspegla de skillnader som finns mellan och inom de olika finansiella undersektorerna vad gäller nivån på finansiella entiteters cybersäkerhetsberedskap bör testerna omfatta ett brett spektrum av verktyg och åtgärder, alltifrån en bedömning av grundläggande krav (t.ex. sårbarhetsbedömningar och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, bristanalyser, fysiska säkerhetsgranskningar, frågeformulär och programvarulösningar för skanning, källkodsgranskningar när så är möjligt, scenariobaserade tester, kompatibilitetstester, prestandatester eller tester ändpunkt till ändpunkt (*end-to-end*)) till mer avancerade tester genom hotbildsstyrd penetrationstestning. Sådana avancerade tester bör krävas endast av finansiella entiteter som är tillräckligt mogna ur ett IKT-perspektiv för att utföra dem på ett rimligt sätt. Den testning av den digitala operativa motståndskraften som krävs enligt denna förordning bör därför vara mer krävande för de finansiella entiteterna som uppfyller de krav som fastställs i denna förordning (t.ex. stora, systematiska och IKT-mogna kreditinstitut, fondbörser, värdepapperscentraler och centrala motparter) än för andra finansiella entiteter. Samtidigt bör testning av digital operativ motståndskraft genom hotbildsstyrd penetrationstestning vara mer relevant för finansiella entiteter som är verksamma inom delsektorer för centrala finansiella tjänster och som har en central betydelse för systemet (t.ex. betalningar, bankverksamhet, och clearing och avveckling) och mindre relevant för andra delsektorer (t.ex. kapitalförvaltare och kreditvärderingsinstitut).

(57) Finansiella entiteter som bedriver gränsöverskridande verksamhet och som utövar friheten att etablera sig eller tillhandahålla tjänster inom unionen bör uppfylla en enda uppsättning avancerade testkrav (t.ex. hotbildsstyrd penetrationstestning) i sin hemmedlemsstat, vilka bör omfatta IKT-infrastrukturerna i alla jurisdiktioner i unionen där den gränsöverskridande finansiella koncernen bedriver verksamhet, vilket innebär att relaterade IKT-testningskostnader uppstår i endast en jurisdiktion för sådana gränsöverskridande finansiella koncerner.

(58) För att dra nytta av den expertis som redan förvärvats av vissa behöriga myndigheter, särskilt med avseende på genomförandet av TIBER-EU-ramen, bör denna förordning ge medlemsstaterna möjligheten att utse en enda offentlig myndighet med ansvar för den finansiella sektorn, på nationell nivå, för alla frågor som rör hotbildsstyrd penetrationstestning eller, om ingen sådan myndighet utsetts, för behöriga myndigheter att delegera uppgifter som rör hotbildsstyrd penetrationstestning till en annan nationell finansiell behörig myndighet.

(59) Eftersom denna förordning inte kräver att finansiella entiteter täcker alla kritiska eller viktiga funktioner i en enda hotbildsstyrd penetrationstestning, bör finansiella entiteter vara fria att avgöra vilka och hur många kritiska eller viktiga funktioner som bör omfattas av ett sådant test.

(60) Gemensam testning i den mening som avses i denna förordning – som inbegriper deltagande av flera finansiella entiteter i en hotbildsstyrd penetrationstestning och för vilken en tredjepartsleverantör av IKT-tjänster direkt kan ingå kontraktsmässiga arrangemang med en extern testare – bör endast tillåtas om kvaliteten eller säkerheten för de tjänster som utförs av tredjepartsleverantören av IKT-tjänster åt kunder som är entiteter utanför denna förordnings tillämpningsområde, eller för konfidentialiteten för data som är relaterade till sådana tjänster, rimligen kan förväntas påverkas negativt, gemensam testning bör också omfattas av skyddsåtgärder (under ledning av en utsedd finansiell entitet, med kalibrering av antalet deltagande finansiella entiteter) för att för de berörda finansiella entiteterna säkerställa ett strikt testutförande som uppfyller målen för den hotbildsstyrda penetrationstestningen enligt denna förordning.

(61) För att dra fördel av de interna resurser som är tillgängliga på företagsnivå, bör denna förordning tillåta användningen av interna testare i syfte att utföra hotbildsstyrd penetrationstestning, under förutsättning att tillsynsmyndigheten godkänner det, att inga intressekonflikter föreligger och att användningen av interna och externa testare alternerar periodiskt (vart tredje test), och samtidigt kräver att den som tillhandahåller underrättelser om hot för den hotbildsstyrda penetrationstestningen alltid är extern i förhållande till den finansiella entiteten. Ansvaret för att genomföra hotbildsstyrd penetrationstestning bör till fullo ligga kvar hos den finansiella entiteten. Intyg från myndigheterna bör användas enbart för ömsesidigt erkännande och bör inte utesluta några uppföljningsåtgärder som krävs för att hantera den IKT-risk som den finansiella entiteten är utsatt för, och inte heller betraktas som tillsynsmyndighetens godkännande av den finansiella entitetens kapacitet att hantera och begränsa IKT-risk.

(62) För att säkerställa en sund övervakning av IKT-tredjepartsrisk i den finansiella sektorn är det nödvändigt att fastställa en uppsättning principbaserade regler för att vägleda finansiella entiteter vid övervakning av risker som uppstår i samband med funktioner som utkontrakterats till tredjepartsleverantörer av IKT-tjänster, särskilt för IKT-tjänster som stöder kritiska eller viktiga funktioner, liksom mer allmänt inom ramen för alla IKT-tredjepartsberoenden.

(63) För att hantera komplexiteten i de olika källorna till IKT-risk, och samtidigt ta hänsyn till den mångfald av leverantörer av tekniska lösningar som möjliggör ett smidigt tillhandahållande av finansiella tjänster, bör denna förordning omfatta många olika tredjepartsleverantörer av IKT-tjänster, inbegripet leverantörer av molntjänster, programvara, dataanalystjänster och leverantörer av datacentraltjänster. Eftersom finansiella entiteter effektivt och konsekvent bör identifiera och hantera alla typer av risker, inbegripet i samband med IKT-tjänster som tillhandahålls inom en finansiell koncern, bör det på samma sätt klargöras att företag som ingår i en finansiell koncern och som tillhandahåller IKT-tjänster främst till sitt moderföretag, eller till dess dotterbolag eller filialer, liksom finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter, också bör betraktas som tredjepartsleverantörer av IKT-tjänster enligt denna förordning. Slutligen bör, mot bakgrund av att marknaden för betaltjänster blir mer och mer beroende av komplexa tekniska lösningar, och med beaktande av framväxande typer av betaltjänster och betalningsrelaterade lösningar, deltagare i ekosystemet för betaltjänster som tillhandahåller betalningshanteringstjänster, eller som driver betalningsinfrastrukturer, också anses som tredjepartsleverantörer av IKT-tjänster enligt denna förordning, med undantag för centralbankers hantering av betalningssystem eller system för värdepappersavveckling, samt offentliga myndigheters tillhandahållande av IKT-relaterade tjänster vid uppfyllandet av statliga funktioner.

(64) En finansiell entitet bör alltid ha det fulla ansvaret för att uppfylla sina skyldigheter enligt denna förordning. Finansiella entiteter bör tillämpa ett proportionellt tillvägagångssätt vid övervakningen av de risker som uppstår hos tredjepartsleverantörer av IKT-tjänster, genom att vederbörlig hänsyn tas till karaktären på och omfattningen av, komplexiteten hos och betydelsen av sina IKT-relaterade beroenden, kritikaliteten hos eller betydelsen av de tjänster, processer eller funktioner som omfattas av de kontraktsmässiga arrangemangen och, i förlängningen, på grundval av en noggrann bedömning av eventuella effekter på kontinuiteten och kvaliteten hos finansiella tjänster på individuell nivå och koncernnivå, beroende på vad som är lämpligt.

(65) Denna övervakning bör följa ett strategiskt tillvägagångssätt för IKT-tredjepartsrisker som inrättas formellt genom att den finansiella entitetens ledningsorgan antar en särskild strategi för IKT-tredjepartsrisker som bygger på en kontinuerlig granskning av alla beroenden av IKT-tredjeparter. För att öka tillsynsmyndigheternas medvetenhet om beroenden av IKT-tredjeparter och ytterligare stödja arbetet i samband med den tillsynsram som inrättas genom denna förordning, bör alla finansiella entiteter ha skyldighet att upprätthålla ett informationsregister med alla kontraktsmässiga arrangemang som rör användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster. Finansiella tillsynsmyndigheter bör kunna begära tillgång till hela registret eller be om särskilda avsnitt av registret, och därigenom få viktig information för en bredare förståelse av finansiella entiteters IKT-relaterade beroenden.

(66) En grundlig förhandsanalys bör underbygga och föregå formellt ingående av kontraktsmässiga arrangemang, särskilt genom fokusering på inslag som kritikalitet eller betydelse av de tjänster som understöds av det planerade IKT-kontraktet, nödvändiga godkännanden från tillsynsmyndigheter eller andra villkor, den eventuella koncentrationsrisk som detta medför, liksom due diligence-granskning i förfarandet för urval och bedömning av tredjepartsleverantörer av IKT-tjänster och bedömning av potentiella intressekonflikter. Vad gäller kontraktsmässiga arrangemang rörande kritiska eller viktiga funktioner bör finansiella entiteter beakta tredjepartsleverantörer av IKT-tjänsters användning av de senaste och högsta standarderna för informationssäkerhet. Uppsägning av kontraktsmässiga arrangemang kan föranledas av åtminstone ett antal omständigheter som visar på brister hos tredjepartsleverantören av IKT-tjänster,

särskilt betydande överträdelser av lagar eller avtalsvillkor, omständigheter som påvisar en potentiell förändring av prestandan i de funktioner som avses i de kontraktsmässiga arrangemangen, bevis på svagheter hos tredjepartsleverantören av IKT-tjänster i den övergripande hanteringen av IKT-risk, eller omständigheter som tyder på att den berörda behöriga myndigheten inte har förmåga att effektivt övervaka den finansiella entiteten.

(67) För att hantera systemeffekterna av koncentrationsrisken för IKT-tredjeparter främjar denna förordning en balanserad lösning genom en flexibel och gradvis strategi för sådana koncentrationsrisker, eftersom införandet av strikta tak eller strikta begränsningar kan hindra företagens affärsverksamhet och begränsa avtalsfriheten. Finansiella entiteter bör göra en grundlig bedömning av sina planerade kontraktsmässiga arrangemang för att fastställa sannolikheten för att en sådan risk uppstår, bland annat genom djupgående analyser av underleverantörsavtal, särskilt när de ingås med tredjepartsleverantörer av IKT-tjänster som är etablerade i ett tredjeland. I detta skede, och i syfte att uppnå en rimlig balans mellan kravet på att bevara avtalsfriheten och kravet på att garantera finansiell stabilitet, anses det inte lämpligt att fastställa regler för strikta tak och gränser för exponeringar mot IKT-tredjeparter. I samband med översynsramen bör en ledande tillsynsmyndighet, som utsetts enligt denna förordning, med avseende på kritiska tredjepartsleverantörer av IKT-tjänster ägna särskild uppmärksamhet åt att fullt ut förstå omfattningen av ömsesidiga beroenden, upptäcka specifika fall där en hög koncentration av kritiska tredjepartsleverantörer av IKT-tjänster i unionen sannolikt kommer att sätta press på stabiliteten och integriteten i unionens finansiella system och upprätthålla en dialog med kritiska tredjepartsleverantörer av IKT-tjänster där denna specifika risk har identifierats.

(68) För att regelbundet utvärdera och övervaka förmågan hos en tredjepartsleverantör av IKT-tjänster att säkert tillhandahålla tjänster till en finansiell entitet utan negativa effekter på den finansiella entitetens digitala operativa motståndskraft, bör flera centrala avtalsdelar med tredjepartsleverantörer av IKT-tjänster harmoniseras. En sådan harmonisering bör omfatta åtminstone de områden som är avgörande för att den finansiella entiteten ska kunna bedriva en fullständig övervakning av de risker som kan uppstå genom tredjepartsleverantören av IKT-tjänster, utifrån en finansiell entitets behov av att säkerställa sin digitala motståndskraft eftersom den är beroende av stabiliteten, funktionaliteten, tillgängligheten och säkerheten hos de IKT-tjänster som den använder.

(69) När de omförhandlar kontraktsmässiga arrangemang för att anpassa sig till kraven i denna förordning bör finansiella entiteter och tredjepartsleverantören av IKT-tjänster säkerställa att de viktiga avtalsbestämmelser som anges i denna förordning omfattas.

(70) Den definition av *kritisk eller viktig funktion* som anges i denna förordning omfattar de *kritiska funktioner* som anges i artikel 2.1.35 i Europaparlamentets och rådets direktiv 2014/59/EU ([20]). I enlighet med detta är de funktioner som anses vara kritiska enligt direktiv 2014/59/EU inbegripna i definitionen av kritiska funktioner i den mening som avses i denna förordning.

(71) Oavsett kritikaliteten hos eller betydelsen av den funktion som stöds av IKT-tjänsterna bör kontraktsmässiga arrangemang särskilt innehålla en specifikation med heltäckande beskrivningar av funktioner och tjänster, platser där sådana funktioner tillhandahålls och där uppgifterna kommer att behandlas, samt beskrivningar av servicenivån. Andra grundläggande delar för att möjliggöra en finansiell entitets övervakning av IKT-tredjepartsrisker är: avtalsbestämmelser som anger hur åtkomst, tillgänglighet, integritet, säkerhet och skydd av personuppgifter säkerställs av tredjepartsleverantören av IKT-tjänster, bestämmelser som fastställer relevanta garantier för att säkerställa åtkomst, återvinning och återlämnande av uppgifter vid insolvens, resolution eller nedläggning av affärsverksamheten hos tredjepartsleverantören av IKT-tjänster samt bestämmelser som kräver att tredjepartsleverantören av IKT-tjänster ger stöd vid IKT-incidenter i samband med de tjänster som tillhandahålls,

([20]) Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190).

utan ytterligare kostnad eller till en kostnad som fastställts på förhand, bestämmelser om skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella entiteten, samt bestämmelser om uppsägningsrätt och tillhörande minsta uppsägningstid för kontraktsmässiga arrangemang, i enlighet med de behöriga myndigheternas och resolutionsmyndigheternas förväntningar.

(72) Utöver sådana avtalsbestämmelser, och i syfte att säkerställa att finansiella entiteter behåller full kontroll över all utveckling som sker på tredjepartsnivå och som kan försämra deras IKT-säkerhet, bör avtalen om tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner också innehålla bestämmelser om fullständiga beskrivningar av servicenivån, med exakta kvantitativa och kvalitativa prestationsmål, för att utan onödigt dröjsmål möjliggöra lämpliga korrigerande åtgärder om de överenskomna servicenivåerna inte uppnås, relevanta tidsfrister för anmälan och rapporteringsskyldigheter för tredjepartsleverantören av IKT-tjänster för händelser som kan ha en väsentlig inverkan på tredjepartsleverantörens förmåga att effektivt tillhandahålla respektive IKT-tjänster, ett krav på att tredjepartsleverantören av IKT-tjänster ska genomföra och testa beredskapsplaner för verksamheten och införa IKT-säkerhetsåtgärder, IKT-verktyg och IKT-strategier som möjliggör ett säkert tillhandahållande av tjänster, samt delta och samarbeta fullt ut i den hotbildsstyrda penetrationstestningen som utförs av den finansiella entiteten.

(73) Avtalen om tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner bör också innehålla bestämmelser om den finansiella entitetens eller en utsedd tredjeparts rätt till åtkomst, inspektion och revision samt rätten att ta kopior som avgörande verktyg i finansiella entiteters fortlöpande övervakning av IKT-tredjepartsleverantörens prestanda, i kombination med att den sistnämnda samarbetar fullt ut under inspektionerna. På samma sätt bör den finansiella entitetens behöriga myndighet ha rätt att, på grundval av anmälningar, kontrollera och granska tredjepartsleverantören av IKT-tjänster, med förbehåll för sekretesskrav.

(74) Sådana kontraktsmässiga arrangemang bör också innehålla särskilda exitstrategier som i synnerhet möjliggör obligatoriska övergångsperioder under vilka tredjepartsleverantörer av IKT-tjänster bör fortsätta att tillhandahålla relevanta tjänster för att minska risken för avbrott på finansiell enhetsnivå eller göra det möjligt för den finansiella entiteten att på ett effektivt sätt byta till andra tredjepartsleverantörer av IKT-tjänster, eller byta till interna lösningar som är förenliga med den tillhandahållna IKT- tjänstens komplexitet. Dessutom bör finansiella entiteter som omfattas av direktiv 2014/59/EU säkerställa att relevanta avtal för IKT-tjänster är solida och kan hävdas i händelse av resolution av finansiella entiteter. I linje med resolutionsmyndigheternas förväntningar bör dessa finansiella entiteter därför säkerställa att relevanta avtal för IKT-tjänster är motståndskraftiga mot resolution. Så länge de fortsätter att uppfylla sina betalningsskyldigheter bör dessa finansiella entiteter bland annat säkerställa att relevanta avtal för IKT-tjänster innehåller klausuler om att de inte får sägas upp, inte får upphävas tillfälligt och inte ändras på grund av omstrukturering eller resolution.

(75) Dessutom kan frivillig användning av standardavtalsklausuler som offentliga myndigheter eller unionens institutioner har utarbetat, särskilt användningen av avtalsklausuler som kommissionen har utarbetat för molntjänster, underlätta ytterligare för finansiella entiteter och tredjepartsleverantörer av IKT-tjänster genom att öka rättssäkerheten avseende den finansiella sektorns användning av molntjänster, i fullständig överensstämmelse med de krav och förväntningar som fastställs i unionsrätten avseende finansiella tjänster. Utarbetandet av standardavtalsklausuler bygger på åtgärder som planerades redan i 2018 års handlingsplan för fintech, där kommissionen tillkännagav sin avsikt att uppmuntra och underlätta utarbetandet av standardavtalsklausuler för finansiella entiteters utkontraktering till molntjänster, genom att bygga på de branschöverskridande ansträngningar från molntjänstintressenternas sida som kommissionen redan har bidragit till med den finansiella sektorns medverkan.

(76) I syfte att främja konvergens och effektivitet när det gäller tillsynsstrategier för IKT-tredjepartsrisker i den finansiella sektorn, och för att stärka den digitala operativa motståndskraften hos finansiella entiteter som är beroende av kritiska tredjepartsleverantörer av IKT-tjänster för att tillhandahålla IKT-tjänster som stöder tillhandahållandet av finansiella tjänster, och därmed bidra till att bevara stabiliteten i unionens finansiella system och integriteten på den inre marknaden för finansiella tjänster, bör kritiska tredjepartsleverantörer av IKT-tjänster omfattas av en tillsynsram på unionsnivå. Inrättandet av tillsynsramen motiveras av mervärdet av att vidta åtgärder på unionsnivå

och av särdragen hos användningen av IKT-tjänster och den roll de spelar vid tillhandahållandet av finansiella tjänster, men det bör samtidigt erinras om att denna lösning endast förefaller vara lämplig inom ramen för denna förordning, som specifikt behandlar digital operativ motståndskraft inom finanssektorn. En sådan tillsynsram bör dock inte betraktas som en ny modell för unionstillsyn på andra områden av finansiella tjänster och finansiell verksamhet.

(77) Tillsynsramen bör endast tillämpas på kritiska tredjepartsleverantörer av IKT-tjänster. Det bör därför inrättas en klassificeringsmekanism för att ta hänsyn till omfattningen och arten av den finansiella sektorns beroende av sådana tredjepartsleverantörer av IKT-tjänster. Den mekanismen bör inbegripa en uppsättning kvantitativa och kvalitativa kriterier för att fastställa kritikalitetsparametrarna som en grund för inkludering i tillsynsramen. För att säkerställa att den bedömningen är korrekt, och oavsett företagsstrukturen hos tredjepartsleverantören av IKT-tjänster, bör sådana kriterier, när det gäller en tredjepartsleverantör av IKT-tjänster som ingår i en större koncern, beakta hela koncernstrukturen hos tredjepartsleverantören av IKT-tjänster. Å ena sidan bör kritiska tredjepartsleverantörer av IKT-tjänster som inte automatiskt utses genom tillämpning av dessa kriterier ha möjlighet att på frivillig basis delta i tillsynsramen, å andra sidan bör de tredjepartsleverantörer av IKT-tjänster som redan omfattas av tillsynsramar för fullgörandet av Europeiska centralbankssystemet uppgifter enligt artikel 127.2 i EUF-fördraget undantas.

(78) På samma sätt bör finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter, även om de tillhör kategorin tredjepartsleverantörer av IKT-tjänster enligt denna förordning, också undantas från tillsynsramen eftersom de redan omfattas av tillsynsmekanismer som inrättats genom relevant unionsrätt avseende finansiella tjänster. I tillämpliga fall bör de behöriga myndigheterna inom ramen för sin tillsynsverksamhet beakta den IKT-risk som finansiella entiteter som tillhandahåller IKT-tjänster utgör för finansiella entiteter. På samma sätt bör, på grund av de befintliga riskövervakningsmekanismerna på koncernnivå, samma undantag införas för tredjepartsleverantörer av IKT-tjänster som huvudsakligen tillhandahåller tjänster till entiteter i den egna koncernen. Tredjepartsleverantörer av IKT-tjänster som endast tillhandahåller IKT-tjänster i en medlemsstat till finansiella entiteter som endast är verksamma i den medlemsstaten bör också undantas från klassificeringsmekanismen på grund av sin begränsade verksamhet och avsaknad av gränsöverskridande inverkan.

(79) Digitaliseringen av finansiella tjänster har lett till en användning och ett beroende av IKT-tjänster som aldrig tidigare skådats. Eftersom det har blivit otänkbart att tillhandahålla finansiella tjänster utan användning av molntjänster, programvarulösningar och datarelaterade tjänster, har unionens finansiella ekosystem i sig blivit beroende av vissa IKT-tjänster som tillhandahålls av leverantörer av IKT-tjänster. Vissa av dessa leverantörer är innovatörer när det gäller att utveckla och tillämpa IKT-baserad teknik, och spelar en viktig roll i tillhandahållandet av finansiella tjänster eller har integrerats i värdekedjan för finansiella tjänster. De har därför blivit kritiska för stabiliteten och integriteten i unionens finansiella system. Detta utbredda beroende av tjänster som tillhandahålls av kritiska tredjepartsleverantörer av IKT-tjänster, i kombination med det ömsesidiga beroendet mellan olika marknadsoperatörers informationssystem, skapar en direkt och potentiellt allvarlig risk för unionens system för finansiella tjänster och för kontinuiteten i tillhandahållandet av finansiella tjänster, om kritiska tredjepartsleverantörer av IKT-tjänster skulle påverkas av operativa störningar eller allvarliga cyberincidenter. Cyberincidenter har en särskild förmåga att föröka sig och sprida sig i hela det finansiella systemet i en betydligt snabbare takt än andra typer av risker som övervakas inom finanssektorn och kan sträcka sig över sektorer och över geografiska gränser. De har potential att utvecklas till en systemkris där förtroendet för det finansiella systemet har urholkats på grund av störningar i funktioner som stöder realekonomin, eller betydande finansiella förluster som når en nivå som det finansiella systemet inte kan klara, eller som kräver omfattande åtgärder för att absorbera stora chocker. För att förhindra att dessa scenarier inträffar och därmed äventyrar unionens finansiella stabilitet och integritet, är det viktigt att skapa konvergens i tillsynspraxis för IKT-tredjepartsrisker inom finanssektorn, särskilt genom nya regler som möjliggör unionstillsyn av kritiska tredjepartsleverantörer av IKT-tjänster.

(80) Tillsynsramen är till stor del beroende av graden av samarbete mellan den ledande tillsynsmyndigheten och den kritiska tredjepartsleverantör av IKT-tjänster som levererar tjänster till finansiella entiteter som påverkar tillhandahållandet av finansiella tjänster. En framgångsrik tillsyn är beroende av bland annat den ledande tillsynsmyndighetens förmåga att effektivt genomföra övervakningsuppdrag och inspektioner för att bedöma de regler, kontroller och processer som används av kritiska tredjepartsleverantörer av IKT-tjänster, samt bedöma den potentiella kumulativa effekten av deras verksamhet på den finansiella stabiliteten och det finansiella systemets integritet. Samtidigt är det mycket viktigt att kritiska tredjepartsleverantörer av IKT-tjänster följer den ledande tillsynsmyndighetens rekommendationer och åtgärdar dess farhågor. Eftersom bristande samarbete från en kritisk tredjepartsleverantör av IKT-tjänster som tillhandahåller tjänster som påverkar tillhandahållandet av finansiella tjänster, såsom vägran att bevilja tillträde till sina lokaler eller att lämna information, i slutändan skulle beröva den ledande tillsynsmyndigheten dess grundläggande verktyg för att bedöma IKT-tredjepartsrisker och skulle kunna inverka negativt på det finansiella systemets stabilitet och integritet, är det nödvändigt att även föreskriva ett proportionellt sanktionssystem.

(81) Mot denna bakgrund bör den ledande tillsynsmyndighetens behov av att ålägga viten för att tvinga kritiska tredjepartsleverantörer av IKT-tjänster att uppfylla de skyldigheter rörande transparens och tillträde som fastställs i denna förordning inte äventyras av svårigheter som uppstår till följd av verkställandet av dessa viten i förhållande till kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i tredjeländer. För att säkerställa sådana sanktioners verkställbarhet, och för att möjliggöra ett snabbt införande av förfaranden som upprätthåller de kritiska IKT-tredjepartsleverantörernas rätt till försvar inom ramen för klassificeringsmekanismen och utfärdandet av rekommendationer, bör de kritiska tredjepartsleverantörerna av IKT-tjänster som tillhandahåller tjänster till finansiella entiteter som påverkar tillhandahållandet av finansiella tjänster vara skyldiga att upprätthålla en tillräcklig verksamhet i unionen. På grund av tillsynens karaktär och avsaknaden av jämförbara arrangemang i andra jurisdiktioner finns det inga lämpliga alternativa mekanismer som säkerställer detta mål genom ett effektivt samarbete med finansiella tillsynsmyndigheter i tredjeländer när det gäller övervakningen av effekterna av de digitala operativa risker som systemviktiga tredjepartsleverantörer av IKT-tjänster, vilka räknas som kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i tredjeländer, utgör. I syfte att fortsätta att tillhandahålla IKT-tjänster till finansiella entiteter i unionen bör därför en tredjepartsleverantör av IKT-tjänster som är etablerad i tredjeländer som klassificerats som kritisk i enlighet med denna förordning vidta, inom tolv månader efter en sådan klassificering, alla nödvändiga arrangemang för att säkerställa dess inkorporering i unionen genom att inrätta en filial, enligt unionens regelverk, närmare bestämt i Europaparlamentets och rådets direktiv 2013/34/EU ([21]).

(82) Kravet på att inrätta ett dotterbolag i unionen bör inte hindra den kritiska tredjepartsleverantören av IKT-tjänster från att tillhandahålla IKT-tjänster och tillhörande teknisk support från anläggningar och infrastruktur utanför unionen. Denna förordning inför inte någon datalokaliseringsplikt eftersom den inte kräver att datalagring eller databehandling ska utföras i unionen.

(83) Kritiska tredjepartsleverantörer av IKT-tjänster bör kunna tillhandahålla IKT-tjänster från vilken plats som helst i världen, och inte nödvändigtvis eller inte bara från lokaler som är belägna i unionen. Tillsynsverksamheten bör först genomföras i lokaler som är belägna i unionen och genom interaktion med entiteter som är belägna i unionen, inbegripet dotterbolag som inrättats av kritiska tredjepartsleverantörer av IKT-tjänster enligt denna förordning. Sådana åtgärder inom unionen kan dock vara otillräckliga för att den ledande tillsynsmyndigheten fullt ut och effektivt ska kunna utföra sina uppgifter enligt denna förordning. Den ledande tillsynsmyndigheten bör därför också kunna utöva sina relevanta tillsynsbefogenheter i tredjeländer. Utövandet av dessa befogenheter i tredjeländer bör göra det möjligt för den ledande tillsynsmyndigheten att undersöka de faciliteter från vilka IKT-tjänsterna eller teknisk supporttjänsterna faktiskt tillhandahålls eller förvaltas av den kritiska tredjepartsleverantören av IKT-tjänster och bör ge den ledande tillsynsmyndigheten en heltäckande och operativ förståelse av IKT-riskhanteringen hos den kritiska tredjepartsleverantören av IKT-tjänster. Möjligheten för den ledande tillsynsmyndigheten, i egenskap av unionsbyrå, att utöva befogenheter utanför unionens territorium bör vederbörligen avgränsas av relevanta villkor, särskilt samtycke från den berörda kritiska tredjepartsleverantören av IKT-tjänster. På samma sätt bör de berörda myndigheterna i tredjelandet informeras om, och inte ha invänt mot, utövandet av den ledande tillsynsmyndighetens verksamhet på tredjelandets eget territorium. För att säkerställa ett effektivt genomförande, och utan att det påverkar

([21]) Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG (EUT L 182, 29.6.2013, s. 19).

unionsinstitutionernas och medlemsstaternas respektive befogenheter, måste dock sådana befogenheter också vara fullt förankrade i ingåendet av avtal om administrativt samarbete med de relevanta myndigheterna i det berörda tredjelandet. Denna förordning bör därför göra det möjligt för de europeiska tillsynsmyndigheterna att ingå avtal om administrativt samarbete med relevanta myndigheter i tredjeländer, vilka inte på annat sätt bör skapa rättsliga skyldigheter för unionen och dess medlemsstater.

(84) För att underlätta kommunikationen med den ledande tillsynsmyndigheten och säkerställa lämplig representation bör kritiska tredjepartsleverantörer av IKT-tjänster som ingår i en koncern utse en juridisk person till sin samordningspunkt.

(85) Tillsynsramen bör inte påverka medlemsstaternas behörighet att utföra egna tillsyns- eller övervakningsuppdrag avseende tredjepartsleverantörer av IKT-tjänster som inte klassificeras som kritiska enligt denna förordning, men som anses vara viktiga på nationell nivå.

(86) För att utnyttja den flerskiktade institutionella strukturen på området finansiella tjänster bör de europeiska tillsynsmyndigheternas gemensamma kommitté fortsätta att säkerställa den övergripande sektorsövergripande samordningen i alla frågor som rör IKT-risk, i enlighet med sina uppgifter i fråga om cybersäkerhet. Detta arbete bör stödjas av en ny underkommitté (*tillsynsforumet*) som utför förberedande arbete både för de enskilda beslut som riktar sig till kritiska tredjepartsleverantörer av IKT-tjänster, och för utfärdande av kollektiva rekommendationer, särskilt i förhållande till riktmärkning av tillsynsprogram för kritiska tredjepartsleverantörer av IKT-tjänster, och fastställande av bästa praxis för hantering av IKT-koncentrationsrisker.

(87) För att säkerställa att kritiska tredjepartsleverantörer av IKT-tjänster lämpligt och effektivt övervakas på unionsnivå föreskriver denna förordning att var och en av de tre europeiska tillsynsmyndigheterna kan utses till ledande tillsynsmyndighet. Den enskilda tilldelningen av en kritisk tredjepartsleverantör av IKT-tjänster till en av de tre europeiska tillsynsmyndigheterna bör vara resultatet av en bedömning av den övervägande andelen finansiella entiteter som är verksamma inom de finansiella sektorer för vilka den europeiska tillsynsmyndigheten har ansvar. Detta tillvägagångssätt bör leda till en välavvägd fördelning av uppgifter och ansvar mellan de tre europeiska tillsynsmyndigheterna i samband med utövandet av tillsynsfunktionerna och bör på bästa sätt utnyttja de personalresurser och den tekniska expertis som finns i var och en av de tre europeiska tillsynsmyndigheterna.

(88) Ledande tillsynsmyndigheter bör tilldelas de befogenheter som krävs för att genomföra undersökningar, inspektioner på plats och på annan plats i kritiska tredjepartsleverantörer av IKT-tjänsters lokaler och platser och få fullständig och uppdaterad information. De befogenheterna bör göra det möjligt för den ledande tillsynsmyndigheten att få verklig inblick i typen, omfattningen och effekten av den IKT-tredjepartsrisk som finansiella entiteter och i förlängningen unionens finansiella system utsätts för. Att de europeiska tillsynsmyndigheterna anförtros den ledande tillsynsrollen är en förutsättning för att kunna få grepp om och ta itu med den systemrelaterade dimensionen av IKT-risk inom finanssektorn. Den inverkan som kritiska tredjepartsleverantörer av IKT-tjänster har på unionens sektor för finansiella tjänster och de potentiella problemen med den därmed förknippade IKT-koncentrationsrisken kräver en gemensam strategi på unionsnivå. Det samtidiga utförandet av ett stort antal revisioner och åtkomsträttigheter som utnyttjas separat av en mängd behöriga myndigheter med liten eller ingen samordning sinsemellan, skulle förhindra finansiella tillsynsmyndigheter från att erhålla en fullständig och övergripande överblick över IKT-tredjepartsriskerna inom unionen, och skulle samtidigt innebära redundans, börda och komplexitet för kritiska tredjepartsleverantörer av IKT-tjänster om dessa vore föremål för en mängd förfrågningar om övervakning och inspektion.

(89) På grund av den betydande inverkan som klassificeringen som kritisk har, bör denna förordning säkerställa att rättigheterna för kritiska tredjepartsleverantörer av IKT-tjänster respekteras inom hela genomförandet av tillsynsramen. Innan sådana leverantörer klassificeras som kritiska bör de t.ex. ha rätt att till den ledande tillsynsmyndigheten lämna in ett motiverat utlåtande med all information som är relevant för den bedömning som rör klassificeringen. Eftersom den ledande tillsynsmyndigheten bör ha befogenhet att lämna rekommendationer om IKT-riskfrågor och lämpliga åtgärder för hantering av dessa, vilket inbegriper befogenheten att motsätta sig vissa avtalsarrangemang som i slutändan påverkar stabiliteten i den finansiella entiteten eller det finansiella systemet, bör kritiska tredjepartsleverantörer av IKT-tjänster också, innan de rekommendationerna färdigställs, ges möjlighet att lämna förklaringar om vilka effekter de föreslagna lösningarna i rekommendationerna förväntas ha på kunder som är entiteter som faller utanför denna förordnings tillämpningsområde samt utarbeta lösningar för att minska riskerna. Kritiska tredjepartsleverantörer av IKT-tjänster som invänder mot rekommendationerna bör lämna en

motiverad förklaring gällande deras avsikt att inte godta rekommendationen. Om en sådan motiverad förklaring inte lämnas eller där den bedöms vara otillräcklig bör den ledande tillsynsmyndigheten utfärda ett offentligt meddelande med en kortfattad beskrivning av den bristande efterlevnaden.

(90) De behöriga myndigheterna bör vederbörligen låta uppgiften att kontrollera den faktiska efterlevnaden av rekommendationer som utfärdats av den ledande tillsynsmyndigheten ingå i deras uppdrag i fråga om tillsyn över finansiella entiteter. De behöriga myndigheterna bör kunna begära att finansiella entiteter vidtar ytterligare åtgärder för att hantera de risker som har identifierats i den ledande tillsynsmyndighetens rekommendationer, och bör i sinom tid utfärda meddelanden om detta. Om den ledande tillsynsmyndigheten riktar rekommendationer till kritiska tredjepartsleverantörer av IKT-tjänster som står under tillsyn enligt direktiv (EU) 2022/2555 bör de behöriga myndigheterna, på frivillig basis och innan ytterligare åtgärder antas, kunna samråda med de behöriga myndigheterna enligt det direktivet i syfte att främja en samordnad strategi för hantering av de berörda kritiska tredjepartsleverantörerna av IKT-tjänster.

(91) Utövandet av tillsyn bör styras av tre operativa principer som syftar till att säkerställa a) nära samordning mellan de europeiska tillsynsmyndigheterna i deras roller som ledande tillsynsmyndigheter, genom ett gemensamt tillsynsnätverk, b) överensstämmelse med den ram som inrättas genom direktiv (EU) 2022/2555 (genom frivilligt samråd med organ enligt det direktivet i syfte att undvika överlappning av åtgärder som är riktade till kritiska tredjepartsleverantörer av IKT-tjänster), och c) omsorg för att minimera den potentiella risken för avbrott i tjänster som kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller kunder som är entiteter som faller utanför denna förordnings tillämpningsområde.

(92) Tillsynsramen bör inte ersätta eller på något sätt eller i någon del användas i stället för kravet på att finansiella entiteter själva ska hantera de risker som är förknippade med användningen av tredjepartsleverantörer av IKT-tjänster, inbegripet deras skyldighet att upprätthålla en fortlöpande övervakning av avtal med kritiska tredjepartsleverantörer av IKT-tjänster. På motsvarande sätt bör tillsynsramen inte påverka finansiella entiteters fulla ansvar för att efterleva och uppfylla alla rättsliga skyldigheter som fastställs i denna förordning och i den relevanta rätten avseende finansiella tjänster.

(93) För att undvika dubbelarbete och överlappningar bör de behöriga myndigheterna avstå från att enskilt vidta åtgärder som syftar till att övervaka riskerna i samband med den kritiska tredjepartsleverantören av IKT-tjänster och bör i detta avseende förlita sig på den relevanta ledande tillsynsmyndighetens bedömning. Alla åtgärder bör under alla förhållanden i förväg samordnas och överenskommas med den ledande tillsynsmyndigheten vid fullgörandet av uppgifter inom tillsynsramen.

(94) För att främja konvergens på internationell nivå när det gäller användning av bästa praxis vid granskningen och övervakningen av den digitala riskhanteringen hos tredjepartsleverantörer av IKT-tjänster bör de europeiska tillsynsmyndigheterna uppmuntras att ingå samarbetsavtal med relevanta tillsynsmyndigheter och reglerande myndigheter i tredjeländer.

(95) För att dra nytta av den särskilda kompetensen, de tekniska färdigheterna och expertisen hos personal som är specialiserad på operativa risker och IKT-risk inom de behöriga myndigheterna bör de tre europeiska tillsynsmyndigheterna och, på frivillig basis, de behöriga myndigheterna enligt direktiv (EU) 2022/2555, den ledande tillsynsmyndigheten ta vara på nationell tillsynsförmåga och tillsynskunskap och inrätta särskilda granskningsgrupper för varje kritisk tredjepartsleverantör av IKT-tjänster, för att samla sektorsövergripande grupper till stöd för förberedelserna och genomförandet av tillsynsverksamhet, inbegripet allmänna utredningar och inspektioner av kritiska tredjepartsleverantörer av IKT-tjänster, samt för eventuell nödvändig uppföljning av dem.

(96) Medan kostnader som uppstår till följd av tillsynsuppgifter till fullo skulle finansieras genom avgifter som tas ut av kritiska tredjepartsleverantörer av IKT-tjänster, kommer de europeiska tillsynsmyndigheterna sannolikt, innan tillsynsramen börjar tillämpas, att ådra sig kostnader för genomförandet av särskilda IKT-system till stöd för den kommande tillsynen, eftersom särskilda IKT-system skulle behöva utvecklas och införas i förväg. I denna förordning föreskrivs därför en hybridfinansieringsmodell, enligt vilken själva tillsynsramen till fullo skulle finansieras genom avgifter, medan utvecklingen av de europeiska tillsynsmyndigheternas IKT-system skulle finansieras genom bidrag från unionen och nationella behöriga myndigheter.

(97) De behöriga myndigheterna bör ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att säkerställa ett korrekt fullgörande av sina skyldigheter enligt denna förordning. De bör i princip offentliggöra meddelanden om de administrativa sanktioner som de ålägger. Eftersom finansiella entiteter och tredjepartsleverantörer av IKT-tjänster kan vara etablerade i olika medlemsstater och övervakas av olika behöriga myndigheter bör tillämpningen av denna förordning underlättas, å ena sidan, av ett nära samarbete mellan de relevanta behöriga myndigheterna, inbegripet ECB när det gäller särskilda uppgifter som den tilldelas genom rådets förordning (EU) nr 1024/2013, och, å andra sidan, av samråd med de europeiska tillsynsmyndigheterna genom ömsesidigt informationsutbyte och bistånd inom ramen för den relevanta tillsynsverksamheten.

(98) För att ytterligare kvantitativt och kvalitativt fastställa kriterierna för klassificering av tredjepartsleverantörer av IKT-tjänster som kritiska och harmonisera tillsynsavgifterna bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen för att komplettera denna förordning med närmare specificering av den systempåverkan som ett fel eller en driftstörning hos en tredjepartsleverantör av IKT-tjänster skulle kunna ha på de finansiella entiteter som den levererar IKT-tjänster till, antalet globala systemviktiga institut, eller andra systemviktiga institut, som är beroende av respektive tredjepartsleverantör av IKT-tjänster, antalet tredjepartsleverantörer av IKT-tjänster som är verksamma på en viss marknad, kostnaderna för att migrera data och IKT-arbetsbelastningar till en annan tredjepartsleverantör av IKT-tjänster samt tillsynsavgifternas storlek och hur de ska betalas. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([22]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter bör Europaparlamentet och rådet erhålla alla handlingar samtidigt som medlemsstaternas experter, och deras experter bör ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(99) Tekniska standarder för tillsyn bör säkerställa en konsekvent harmonisering av kraven i denna förordning. De europeiska tillsynsmyndigheterna bör i sina roller som organ med högspecialiserad expertis utarbeta förslag till tekniska standarder för tillsyn som inte inbegriper några politiska val, och som ska läggas fram för kommissionen. Tekniska standarder för tillsyn bör utarbetas inom områdena IKT-riskhantering, rapportering av allvarliga IKT-relaterade incidenter och testning samt med avseende på nyckelkrav för en sund övervakning av IKT-tredjepartsrisker. Kommissionen och de europeiska tillsynsmyndigheterna bör säkerställa att dessa standarder och krav kan tillämpas av alla finansiella entiteter på ett sätt som står i proportion till deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Kommissionen bör ges befogenhet att anta dessa tekniska standarder för tillsyn genom delegerade akter i enlighet med artikel 290 i EUF-fördraget och i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

(100) För att göra det lättare att jämföra rapporter om allvarliga IKT-relaterade incidenter och allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, samt säkerställa insyn avseende avtalsarrangemang för användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster, bör de europeiska tillsynsmyndigheterna utarbeta förslag till tekniska standarder för genomförande där det fastställs standardiserade mallar, formulär och förfaranden för finansiella entiteter för rapportering av allvarliga IKT-relaterade incidenter och allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, samt standardiserade mallar för registrering av information. När de europeiska tillsynsmyndigheterna utarbetar dessa standarder bör de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser. Kommissionen bör ges befogenhet att anta dessa tekniska standarder för genomförande genom genomförandeakter i enlighet med artikel 291 i EUF-fördraget och i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

([22]) EUT L 123, 12.5.2016, s. 1.

(101) Eftersom ytterligare krav redan har specificerats genom delegerade akter och genomförandeakter baserade på tekniska standarder för tillsyn och genomförande i Europaparlamentets och rådets förordningar (EG) nr 1060/2009 ([23]), (EU) nr 648/2012 ([24]), (EU) nr 600/2014 ([25]) och (EU) nr 909/2014 ([26]) är det lämpligt att ge de europeiska tillsynsmyndigheterna i uppdrag att, antingen enskilt eller gemensamt genom den gemensamma kommittén, överlämna tekniska standarder för tillsyn och genomförande till kommissionen för antagande av delegerade akter och genomförandeakter för att överföra och uppdatera befintliga IKT-riskhanteringsregler.

(102) Eftersom denna förordning, tillsammans med Europaparlamentets och rådets direktiv (EU) 2022/2556 ([27]), innebär en konsolidering av IKT-riskhanteringsbestämmelser i flera förordningar och direktiv i unionens regelverk om finansiella tjänster, inbegripet förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014 samt Europaparlamentets och rådets förordning (EU) 2016/1011 ([28]), bör dessa förordningar ändras för att säkerställa fullständig enhetlighet och klargöra att de tillämpliga bestämmelserna om IKT-risker fastställs i den här förordningen.

(103) Följaktligen bör tillämpningsområdet för de relevanta artiklar som rör operativ risk, för vilka delegerade akter och genomförandeakter ska antas enligt befogenheterna i förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011, begränsas så att alla bestämmelser som omfattar aspekter av digital operativ motståndskraft och som i dag ingår i de förordningarna överförs till den här förordningen.

(104) Den potentiella systemrisk på cyberområdet som är förknippad med användningen av IKT-infrastrukturer som möjliggör drift av betalningssystem och tillhandahållande av betalningshantering bör vederbörligen hanteras på unionsnivå genom harmoniserade regler om digital motståndskraft. I detta syfte bör kommissionen snabbt bedöma behovet av en översyn av denna förordnings tillämpningsområde och samtidigt anpassa en sådan översyn till resultatet av den omfattande översyn som avses i direktiv (EU) 2015/2366. Många storskaliga attacker som genomförts under det senaste årtiondet visar hur betalningssystemen har blivit en ingång för cyberhot. Betalningssystem och betalningshantering, som ligger i centrum av betaltjänstkedjan och uppvisar en hög grad av sammanlänkning med det övergripande finansiella systemet, har fått en avgörande betydelse för unionens finansmarknaders funktion. Cyberangrepp mot sådana system kan orsaka allvarliga driftstörningar i verksamheten med direkta konsekvenser för viktiga ekonomiska funktioner, såsom underlättande av betalningar, och indirekta effekter på därmed sammanhängande ekonomiska processer. Till dess att ett harmoniserat system för och tillsyn över operatörer av betalningssystem och hanteringsentiteter har införts på unionsnivå, får medlemsstaterna, i syfte att tillämpa liknande marknadspraxis, hämta inspiration från de krav på digital operativ motståndskraft som fastställs i denna förordning när de tillämpar regler på operatörer av betalningssystem och hanteringsentiteter som står under tillsyn inom deras egna jurisdiktioner.

([23]) Europaparlamentets och rådets förordning (EG) nr 1060/2009 av den 16 september 2009 om kreditvärderingsinstitut (EUT L 302, 17.11.2009, s. 1).

([24]) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).

([25]) Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

([26]) Europaparlamentets och rådets förordning (EU) nr 909/2014 av den 23 juli 2014 om förbättrad värdepappersavveckling i Europeiska unionen och om värdepapperscentraler samt ändring av direktiv 98/26/EG och 2014/65/EU och förordning (EU) nr 236/2012 (EUT L 257, 28.8.2014, s. 1).

([27]) 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 (se sidan 153 i detta nummer av EUT).

([28]) Europaparlamentets och rådets förordning (EU) 2016/1011 av den 8 juni 2016 om index som används som referensvärden för finansiella instrument och finansiella avtal eller för att mäta investeringsfonders resultat, och om ändring av direktiven 2008/48/EG och 2014/17/EU och förordning (EU) nr 596/2014 (EUT L 171, 29.6.2016, s. 1).

(105) Eftersom målet för denna förordning, dvs. att uppnå en hög nivå av digital operativ motståndskraft för reglerade finansiella entiteter, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna eftersom det kräver harmonisering av en mängd olika regler i unionsrätten och nationell rätt, utan snarare, på grund av dess omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(106) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([29]) och avgav ett yttrande den 10 maj 2021 ([30]).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Innehåll

1. I syfte att uppnå en hög gemensam nivå av digital operativ motståndskraft fastställs i denna förordning enhetliga krav avseende säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser enligt följande:

a) Krav som är tillämpliga på finansiella entiteter i fråga om

   i) riskhantering inom informations- och kommunikationsteknik (IKT),

   ii) rapportering av allvarliga IKT-relaterade incidenter och underrättande om, på frivillig grund, betydande cyberhot till de behöriga myndigheterna,

   iii) rapportering av allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter till de behöriga myndigheterna av de finansiella entiteter som avses i artikel 2.1 a–d,

   iv) testning av digital operativ motståndskraft,

   v) utbyte av information och underrättelser i samband med cyberhot och cybersårbarheter,

   vi) åtgärder för en sund hantering av tredjepartsrelaterad IKT-risk.

b) Krav i samband med de kontraktsmässiga arrangemang som har ingåtts mellan tredjepartsleverantörer av IKT-tjänster och finansiella entiteter.

c) Regler för inrättandet och genomförandet av tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster när de tillhandahåller tjänster till finansiella entiteter.

d) Regler om samarbete mellan behöriga myndigheter och regler om behöriga myndigheters tillsyn och kontroll av efterlevnaden i alla frågor som omfattas av denna förordning.

2. När det gäller finansiella entiteter som har identifierats som leverantörer av väsentliga eller viktiga entiteter enligt nationella regler som införlivar artikel 3 i direktiv (EU) 2022/2555 ska denna förordning betraktas som en sektorsspecifik unionsrättsakt vid tillämpningen av artikel 4 i det direktivet.

3. Denna förordning påverkar inte medlemsstaternas ansvar vad gäller väsentliga statliga funktioner inom områdena allmän säkerhet, försvar och nationell säkerhet i enlighet med unionsrätten.

([29]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([30]) EUT C 229, 15.6.2021, s. 16.

Artikel 2

Tillämpningsområde

1. Utan att det påverkar tillämpningen av punkterna 3 och 4 är denna förordning tillämplig på följande entiteter:

a) Kreditinstitut.

b) Betalningsinstitut, inbegripet sådana betalningsinstitut som är undantagna enligt direktiv (EU) 2015/2366.

c) Leverantörer av kontoinformationstjänster.

d) Institut för elektroniska pengar, inbegripet sådana institut för elektroniska pengar som är undantagna enligt direktiv 2009/110/EG.

e) Värdepappersföretag.

f) Leverantörer av kryptotillgångstjänster, auktoriserade enligt en Europaparlamentets och rådets förordning om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 och direktiven 2013/36/EU och (EU) 2019/1937 (*förordningen om kryptotillgångar*) och emittenter av tillgångsanknutna token.

g) Värdepapperscentraler.

h) Centrala motparter.

i) Handelsplatser.

j) Transaktionsregister.

k) Förvaltare av alternativa investeringsfonder.

l) Förvaltningsbolag.

m) Leverantörer av datarapporteringstjänster.

n) Försäkrings- och återförsäkringsföretag.

o) Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet.

p) Tjänstepensionsinstitut.

q) Kreditvärderingsinstitut.

r) Administratörer av kritiska referensvärden.

s) Leverantörer av gräsrotsfinansieringstjänster.

t) Värdepapperiseringsregister.

u) Tredjepartsleverantörer av IKT-tjänster.

2. Vid tillämpningen av denna förordning ska de entiteter som avses i punkt 1 a–t tillsammans benämnas *finansiella entiteter*.

3. Denna förordning är inte tillämplig på

a) förvaltare av alternativa investeringsfonder som avses i artikel 3.2 i direktiv 2011/61/EU,

b) försäkrings- och återförsäkringsföretag som avses i artikel 4 i direktiv 2009/138/EG,

c) tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 15 medlemmar,

d) fysiska eller juridiska personer som är undantagna enligt artiklarna 2 och 3 i direktiv 2014/65/EU,

e) försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet som är mikroföretag eller små eller medelstora företag,

f) postgiroinstitut som avses i artikel 2.5.3 i direktiv 2013/36/EU.

4. Medlemsstaterna får från tillämpningsområdet för denna förordning utesluta sådana enheter som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU om de är belägna inom deras respektive territorier. Om en medlemsstat utnyttjar en sådan möjlighet ska den informera kommissionen om detta samt om eventuella senare ändringar av detta. Kommissionen ska offentliggöra informationen på sin webbplats eller på annat lättillgängligt vis.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *digital operativ motståndskraft*: en finansiell entitets förmåga att bygga upp, säkerställa och se över sin operativa integritet och tillförlitlighet genom att, direkt eller indirekt, med användning av tjänster från tredjepartsleverantörer av IKT-tjänster, säkerställa hela skalan av IKT-relaterad kapacitet som behövs för att hantera säkerheten i de nätverks- och informationssystem som en finansiell entitet använder och som stöder ett fortlöpande tillhandahållande av finansiella tjänster och deras kvalitet, inbegripet under avbrott.

2. *nätverks- och informationssystem*: ett nätverks- och informationssystem enligt definitionen i artikel 6.1 i direktiv (EU) 2022/2555.

3. *äldre IKT-system*: ett IKT-system som har nått slutet på sin livscykel, som inte lämpar sig för uppgraderingar eller justeringar, av tekniska eller kommersiella skäl, eller som inte längre stöds av leverantören eller av en tredjepartsleverantör av IKT-tjänster, men som fortfarande används och stöder den finansiella entitetens funktioner.

4. *säkerhet i nätverks- och informationssystem*: ett säkerhet i nätverks- och informationssystem enligt definitionen i artikel 6.2 i direktiv (EU) 2022/2555.

5. *IKT-risk*: varje rimligen identifierbar omständighet i samband med användningen av nätverks- och informationssystem som, om de inträffar, kan äventyra säkerheten i nätverks- och informationssystem, verktyg eller processer som är teknikberoende, funktioner och processer eller tillhandahållandet av tjänster genom att orsaka negativa effekter i den digitala eller fysiska miljön.

6. *informationstillgång*: en samling materiell eller immateriell skyddsvärd information.

7. *IKT-tillgång*: en programvaru- eller maskinvarutillgång i nätverks- och informationssystemen som används av den finansiella entiteten.

8. *IKT-relaterad incident*: en enskild händelse eller en serie sammankopplade händelser som inte planerats av den finansiella entiteten och som äventyrar säkerheten i nätverks- och informationssystemen och har negativ inverkan på tillgängligheten, äktheten, integriteten eller konfidentialiteten vad gäller datan eller de tjänster som tillhandahålls av den finansiella entiteten.

9. *betalningsrelaterad operativ incident eller säkerhetsincident*: en enskild händelse eller en serie sammankopplade händelser som inte planerats av de finansiella entiteter som avses i artikel 2.1 a–d och som kan vara IKT-relaterade men inte behöver vara det och har negativ inverkan på tillgängligheten, äktheten, integriteten eller konfidentialiteten vad gäller betalningsrelaterade data eller de betalningsrelaterade tjänster som tillhandahålls av den finansiella entiteten.

10. *allvarlig IKT-relaterad incident*: en IKT-relaterad incident som har stor negativ inverkan på nätverks- och informationssystem som stöder den finansiella entitetens kritiska eller viktiga funktioner.

11. *allvarlig betalningsrelaterad operativ incident eller säkerhetsincident*: en betalningsrelaterad operativ incident eller säkerhetsincident som har stor negativ inverkan på de betalningsrelaterade tjänster som tillhandahålls.

12. *cyberhot*: ett *cyberhot* enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

13. *betydande cyberhot*: ett cyberhot vars tekniska egenskaper indikerar att det potentiellt kan leda till en allvarlig IKT-relaterad incident eller allvarlig betalningsrelaterad operativ incident eller säkerhetsincident.

14. *cyberangrepp*: en skadlig IKT-relaterad incident orsakad av ett försök av en fientlig aktör att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller obehörigt utnyttja en tillgång.

15. *underrättelser om hot*: information som har sammanställts, omvandlats, analyserats, tolkats eller berikats för att skapa det sammanhang som krävs för beslutsfattande och som möjliggör relevant och tillräcklig förståelse för att mildra effekterna av en IKT-relaterad incident eller ett cyberhot, inbegripet de tekniska detaljerna om ett cyberangrepp, de ansvariga för attacken och deras tillvägagångssätt och motiv.

16. *sårbarhet*: en svaghet, mottaglighet eller brist hos en tillgång, ett system, en process eller en kontroll som kan utnyttjas.

17. *hotbildsstyrd penetrationstestning*: en ram som efterliknar den taktik, teknik och de förfaranden som används av verkliga fientliga aktörer, som uppfattas som ett genuint cyberhot och som ger ett kontrollerat, skräddarsytt, underrättelsestyrt (rött lag) test av de kritiska produktionssystem som är i drift hos den finansiella entiteten.

18. *IKT-tredjepartsrisk*: en IKT-risk som kan uppstå för en finansiell entitet i samband med dess användning av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster eller av underleverantörer till sådana leverantörer, inbegripet genom utkontrakteringsarrangemang.

19. *tredjepartsleverantör av IKT-tjänster*: ett företag som tillhandahåller IKT-tjänster.

20. *koncernintern IKT-tjänsteleverantör*: ett företag som ingår i en finansiell koncern och som huvudsakligen tillhandahåller IKT-tjänster till finansiella entiteter inom samma koncern eller till finansiella entiteter som tillhör samma institutionella skyddssystem, inbegripet till deras moderföretag, dotterföretag, filialer eller andra entiteter som står under samma ägarskap eller kontroll.

21. *IKT-tjänster*: digitala tjänster och datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare, inbegripet maskinvara som tjänst och maskinvarutjänster som inbegriper tillhandahållande av teknisk support genom uppdateringar av programvara eller fast programvara från maskinvaruleverantören, ej inbegripet traditionella analoga telefontjänster.

22. *kritisk eller viktig funktion*: en funktion vars avbrott väsentligt skulle försämra den finansiella entitetens finansiella resultat eller sundheten eller kontinuiteten i dess tjänster och verksamhet, eller om funktionens upphörande, brister eller misslyckande väsentligt skulle försämra en finansiell entitets fortsatta efterlevnad av villkoren och skyldigheterna i auktorisationen eller av dess övriga skyldigheter enligt tillämplig rätt avseende finansiella tjänster.

23. *kritisk tredjepartsleverantör av IKT-tjänster*: en tredjepartsleverantör av IKT-tjänster som har klassificerats som kritisk i enlighet med artikel 31.

24. *tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland*: en tredjepartsleverantör av IKT-tjänster som är en juridisk person som är etablerad i ett tredjeland och som har ingått ett kontraktsmässigt arrangemang med en finansiell entitet om tillhandahållande av IKT-tjänster.

25. *dotterföretag*: ett dotterföretag i den mening som avses i artiklarna 2.10 och 22 i direktiv 2013/34/EU.

26. *koncern*: en koncern enligt definitionen i artikel 2.11 i direktiv 2013/34/EU.

27. *moderföretag*: ett moderföretag i den mening som avses i artiklarna 2.9 och 22 i direktiv 2013/34/EU.

28. *IKT-underleverantör etablerad i ett tredjeland*: en IKT-underleverantör som är en juridisk person som är etablerad i ett tredjeland och som har ingått ett kontraktsmässigt arrangemang antingen med en tredjepartsleverantör av IKT-tjänster eller med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland.

29. *IKT-koncentrationsrisk*: exponering mot enskilda eller flera närstående kritiska tredjepartsleverantörer av IKT-tjänster som skapar ett visst beroende av sådana leverantörer, så att otillgänglighet, fel eller annan typ av brist hos sådana leverantörer kan komma att äventyra förmågan hos en finansiell entitet att tillhandahålla kritiska eller viktiga funktioner eller leda till andra typer av negativa effekter, inbegripet stora förluster, eller äventyra den finansiella stabiliteten i unionen som helhet.

30. *ledningsorgan*: ett ledningsorgan enligt definitionen i artikel 4.1.36 i direktiv 2014/65/EU, artikel 3.1.7 i direktiv 2013/36/EU, artikel 2.1 s i Europaparlamentets och rådets direktiv 2009/65/EG ([31]), artikel 2.1.45 i förordning (EU) nr 909/2014, artikel 3.1.20 i förordning (EU) 2016/1011 och i de relevanta bestämmelserna i förordningen om kryptotillgångar, eller motsvarande personer som i praktiken leder entiteten eller har nyckelfunktioner i enlighet med relevant unionsrätt eller nationell rätt.

31. *kreditinstitut*: ett kreditinstitut enligt definitionen i artikel 4.1.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([32]).

32. *institut undantaget enligt direktiv 2013/36/EU*: en sådan enhet som avses i artikel 2.5.4–2.5.23 i direktiv 2013/36/EU.

33. *värdepappersföretag*: ett värdepappersföretag enligt definitionen i artikel 4.1.1 i direktiv 2014/65/EU.

34. *litet och icke-sammanlänkat värdepappersföretag*: ett värdepappersföretag som uppfyller villkoren i artikel 12.1 i Europaparlamentets och rådets förordning (EU) 2019/2033 ([33]).

35. *betalningsinstitut*: ett betalningsinstitut enligt definitionen i artikel 4.4 i direktiv (EU) 2015/2366.

36. *betalningsinstitut undantaget enligt direktiv (EU) 2015/2366*: sådana betalningsinstitut som är undantagna enligt artikel 32.1 i direktiv (EU) 2015/2366.

37. *leverantör av kontoinformationstjänster*: sådana leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366.

38. *institut för elektroniska pengar*: ett institut för elektroniska pengar enligt definitionen i artikel 2.1 i Europaparlamentets och rådets direktiv 2009/110/EG.

39. *institut för elektroniska pengar undantaget enligt direktiv 2009/110/EG*: ett institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.

40. *central motpart*: en central motpart enligt definitionen i artikel 2.1 förordning (EU) nr 648/2012.

41. *transaktionsregister*: ett transaktionsregister enligt definitionen i artikel 2.2 i förordning (EU) nr 648/2012.

42. *värdepapperscentral*: en värdepapperscentral enligt definitionen i artikel 2.1.1 i förordning (EU) nr 909/2014.

43. *handelsplats*: en handelsplats enligt definitionen i artikel 4.1.24 i direktiv 2014/65/EU.

44. *förvaltare av alternativa investeringsfonder*: en förvaltare av alternativa investeringsfonder enligt definitionen i artikel 4.1 b i direktiv 2011/61/EU.

45. *förvaltningsbolag*: ett förvaltningsbolag enligt definitionen i artikel 2.1 b i direktiv 2009/65/EG.

46. *leverantör av datarapporteringstjänster*: en leverantör av datarapporteringstjänster i enlighet med vad som avses i artikel 2.1.34–36 i förordning (EU) nr 600/2014.

47. *försäkringsföretag*: ett försäkringsföretag enligt definitionen i artikel 13.1 i direktiv 2009/138/EG.

48. *återförsäkringsföretag*: ett återförsäkringsföretag enligt definitionen i artikel 13.4 i direktiv 2009/138/EG.

([31]) Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag) (EUT L 302, 17.11.2009, s. 32).

([32]) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

([33]) Europaparlamentets och rådets förordning (EU) 2019/2033 av den 27 november 2019 om tillsynskrav för värdepappersföretag och om ändring av förordningarna (EU) nr 1093/2010, (EU) nr 575/2013, (EU) nr 600/2014 och (EU) nr 806/2014 (EUT L 314, 5.12.2019, s. 1).

49. *försäkringsförmedlare*: en försäkringsförmedlare enligt definitionen i artikel 2.1.3 i Europaparlamentets och rådets direktiv (EU) 2016/97 ([34]).

50. *försäkringsförmedlare som bedriver förmedling som sidoverksamhet*: en försäkringsförmedlare som bedriver förmedling som sidoverksamhet enligt definitionen i artikel 2.1.4 i direktiv (EU) 2016/97.

51. *återförsäkringsförmedlare*: en återförsäkringsförmedlare enligt definitionen i artikel 2.1.5 i direktiv (EU) 2016/97.

52. *tjänstepensionsinstitut*: ett tjänstepensionsinstitut enligt definitionen i artikel 6.1 i direktiv (EU) 2016/2341.

53. *litet tjänstepensionsinstitut*: ett tjänstepensionsinstitut som förvaltar pensionsplaner som tillsammans inte har fler än totalt 100 medlemmar.

54. *kreditvärderingsinstitut*: ett kreditvärderingsinstitut enligt definitionen i artikel 3.1 b i förordning (EG) nr 1060/2009.

55. *leverantör av kryptotillgångstjänster*: en leverantör av kryptotillgångstjänster enligt definitionen i de relevanta bestämmelserna i förordningen om kryptotillgångar.

56. *emittent av tillgångsanknutna token*: en emittent av tillgångsanknutna token enligt definitionen i de relevanta bestämmelserna i förordningen om kryptotillgångar.

57. *administratör av kritiska referensvärden*: en administratör av *kritiska referensvärden* enligt definitionen i artikel 3.1.25 i förordning (EU) 2016/1011.

58. *leverantör av gräsrotsfinansieringstjänster*: en leverantör av gräsrotsfinansieringstjänster enligt definitionen i artikel 2.1 e i Europaparlamentets och rådets förordning (EU) 2020/1503 ([35]).

59. *värdepapperiseringsregister*: ett värdepapperiseringsregister enligt definitionen i artikel 2.23 i Europaparlamentets och rådets förordning (EU) 2017/2402 ([36]).

60. *mikroföretag*: en finansiell entitet, som inte är en handelsplats, en central motpart, ett transaktionsregister eller en värdepapperscentral, och som har färre än 10 anställda och en årsomsättning och/eller årlig balansomslutning som inte överstiger 2 miljoner EUR.

61. *ledande tillsynsmyndighet*: den europeiska tillsynsmyndighet som utses i enlighet med artikel 31.1 b i denna förordning.

62. *den gemensamma kommittén*: den kommitté som avses i artikel 54 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

63. *litet företag*: en finansiell entitet med tio eller fler anställda men färre än 50 anställda och en årsomsättning och/eller årlig balansomslutning som överstiger 2 miljoner EUR men som inte överstiger 10 miljoner EUR.

64. *medelstort företag*: en finansiell entitet som inte är ett litet företag och som har färre än 250 anställda och en årsomsättning som inte överstiger 50 miljoner EUR och/eller en årlig balansomslutning som inte överstiger 43 miljoner EUR.

65. *offentlig myndighet*: alla statliga entiteter eller andra entiteter inom offentlig förvaltning, inbegripet nationella centralbanker.

([34]) Europaparlamentets och rådets direktiv (EU) 2016/97 av den 20 januari 2016 om försäkringsdistribution (EUT L 26, 2.2.2016, s. 19).

([35]) Europaparlamentets och rådets förordning (EU) 2020/1503 av den 7 oktober 2020 om europeiska leverantörer av gräsrotsfinansieringstjänster för företag och om ändring av förordning (EU) 2017/1129 och direktiv (EU) 2019/1937 (EUT L 347, 20.10.2020, s. 1).

([36]) Europaparlamentets och rådets förordning (EU) 2017/2402 av den 12 december 2017 om ett allmänt ramverk för värdepapperisering och om inrättande av ett särskilt ramverk för enkel, transparent och standardiserad värdepapperisering samt om ändring av direktiven 2009/65/EG, 2009/138/EG och 2011/61/EU och förordningarna (EG) nr 1060/2009 och (EU) nr 648/2012 (EUT L 347, 28.12.2017, s. 35).

Artikel 4

Proportionalitetsprincipen

1. Finansiella entiteter ska genomföra reglerna i kapitel II i enlighet med proportionalitetsprincipen, och med beaktande av sin storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, sin verksamhet och sina insatser.

2. Dessutom ska finansiella entiteters tillämpning av kapitlen III, IV och V, avsnitt I, stå i proportion till deras storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i sina tjänster, verksamhet och insatser, i enlighet med vad som specificeras i de relevanta reglerna i dessa kapitel.

3. De behöriga myndigheterna ska beakta finansiella entiteters tillämpning av proportionalitetsprincipen när de ser över enhetligheten i IKT-riskhanteringsramen baserat på de rapporter som lämnats in på begäran av de behöriga myndigheterna enligt artiklarna 6.5 och 16.2.

KAPITEL II

IKT-riskhantering

Avsnitt I

Artikel 5

Styrning och organisation

1. Finansiella entiteter ska ha en intern styrnings- och kontrollram som säkerställer en effektiv och ansvarsfull hantering av IKT-risk i enlighet med artikel 6.4, i syfte att åstadkomma en hög nivå av digital operativ motståndskraft.

2. Den finansiella entitetens ledningsorgan ska fastställa, godkänna, övervaka och ansvara för genomförandet av alla arrangemang som rör den IKT-riskhanteringsram som avses i artikel 6.1.

Vid tillämpning av det första stycket ska ledningsorganet

a) ha det slutliga ansvaret för att hantera den finansiella entitetens IKT-risk,

b) införa strategier som syftar till att säkerställa bibehållandet av höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet för data,

c) fastställa tydliga roller och ansvarsområden för alla IKT-relaterade funktioner och inrätta lämpliga styrformer för att säkerställa kommunikation, samarbete och samordning på ett effektivt och skyndsamt sätt mellan dessa funktioner,

d) ha det övergripande ansvaret för att fastställa och godkänna strategin för digital operativ motståndskraft enligt artikel 6.8, inbegripet fastställandet av en lämplig risktoleransnivå för IKT-risk för den finansiella entiteten, enligt vad som avses i artikel 6.8 b,

e) godkänna, övervaka och regelbundet se över genomförandet av den IKT-kontinuitetspolicy och de åtgärds- och återställningsplaner avseende IKT för den finansiella entiteten som avses i artikel 11.1 respektive 11.3, vilka kan antas som särskilda specifika planer och utgöra integrerade delar av den finansiella entitetens övergripande kontinuitetsplan och åtgärds- och återställningsplan,

f) godkänna och regelbundet se över den finansiella entitetens IKT-internrevisionsplaner, IKT-revisioner och väsentliga ändringar av dessa,

g) anslå och regelbundet se över den lämpliga budgeten för att uppfylla den finansiella entitetens behov av digital operativ motståndskraft när det gäller alla typer av resurser, inbegripet relevanta program för medvetenhet om IKT-säkerhet och sådan utbildning om digital operativ motståndskraft som avses i artikel 13.6 och IKT-färdigheter för all personal,

h) godkänna och regelbundet se över den finansiella entitetens riktlinjer för arrangemang vad gäller användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster,

i) på verksamhetsnivå etablera rapporteringskanaler som gör det möjligt att vederbörligen informeras om

i) arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster,

ii) alla relevanta planerade väsentliga ändringar som rör tredjepartsleverantörerna av IKT-tjänster,

iii) den potentiella effekten av sådana ändringar på de kritiska eller viktiga funktioner som omfattas av dessa arrangemang, inbegripet en sammanfattning av riskanalysen för att bedöma effekterna av dessa ändringar och åtminstone allvarliga IKT-relaterade incidenter och deras inverkan liksom åtgärder, återställande och korrigerande åtgärder.

3. Andra finansiella entiteter än mikroföretag ska inrätta en funktion för att övervaka de arrangemang som har ingåtts med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster, eller utse en medlem av den verkställande ledningen som ansvarig för att övervaka den åtföljande riskexponeringen och relevant dokumentation.

4. Medlemmarna i den finansiella entitetens ledningsorgan ska aktivt upprätthålla tillräckliga och aktuella kunskaper och färdigheter för att förstå och bedöma IKT-risk och deras inverkan på den finansiella entitetens verksamhet, inbegripet genom att regelbundet genomgå särskild utbildning som står i proportion till den IKT-risk som hanteras.

Avsnitt II

Artikel 6

IKT-riskhanteringsram

1. Finansiella entiteter ska ha en sund, heltäckande och väldokumenterad IKT-riskhanteringsram som en del av sitt övergripande riskhanteringssystem och den ska göra det möjligt för dem att snabbt, effektivt och heltäckande hantera IKT-risk och säkerställa en hög nivå av digital operativ motståndskraft.

2. IKT-riskhanteringsramen ska omfatta åtminstone de strategier, riktlinjer, förfaranden, IKT-protokoll och IKT-verktyg som är nödvändiga för att på ett vederbörligt och adekvat sätt skydda alla informations- och IKT-tillgångar, inbegripet datorprogramvara, datormaskinvara och servrar, och skydda alla relevanta fysiska komponenter och infrastrukturer, såsom lokaler, datacentraler och känsliga angivna områden, för att säkerställa att alla informations- och IKT-tillgångar är tillräckligt skyddade mot risker, inbegripet skada och obehörig åtkomst eller användning.

3. I enlighet med sin IKT-riskhanteringsram ska finansiella entiteter minimera effekterna av IKT-risk genom att införa lämpliga strategier, riktlinjer, förfaranden, IKT-protokoll och verktyg. De ska tillhandahålla fullständig och uppdaterad information om IKT-risk och om sin IKT-riskhanteringsram till de behöriga myndigheterna när dessa begär det.

4. Andra finansiella entiteter än mikroföretag ska överföra ansvaret för att hantera och övervaka IKT-risk till en kontrollfunktion och säkerställa en lämplig nivå av oberoende för den kontrollfunktionen för att undvika intressekonflikter. Finansiella entiteter ska säkerställa lämplig åtskillnad mellan och lämpligt oberoende för riskhanteringsfunktioner, kontrollfunktioner och interna revisionsfunktioner avseende IKT, enligt modellen med tre försvarslinjer eller en intern riskhanterings- och kontrollmodell.

5. IKT-riskhanteringsramen ska dokumenteras och ses över minst en gång per år, eller regelbundet när det gäller mikroföretag, liksom vid uppkomsten av allvarliga IKT-relaterade incidenter, och i enlighet med tillsynsinstruktioner eller slutsatser från relevanta testnings- eller revisionsprocesser för digital operativ motståndskraft. Ramen ska förbättras fortlöpande baserat på erfarenheterna från genomförande och övervakning. En rapport om översynen av IKT-riskhanteringsramen ska överlämnas till den behöriga myndigheten på dess begäran.

6. IKT-riskhanteringsramen hos andra finansiella entiteter än mikroföretag ska vara föremål för en internrevision av revisorer på regelbunden basis och i enlighet med finansiella entiteters revisionsplan. Dessa revisorer ska ha tillräckliga kunskaper, färdigheter och expertis om IKT-risker, samt ha en lämplig nivå av oberoende. IKT-revisionernas frekvens och inriktning ska stå i proportion till den finansiella entitetens IKT-risk.

7. Finansiella entiteter ska baserat på slutsatserna från den interna revisionsrapporten inrätta en formell uppföljningsprocess, inbegripet regler för snabb kontroll och snabbt åtgärdande av kritiska resultat från IKT-revisionen.

8. IKT-riskhanteringsramen ska omfatta en strategi för digital operativ motståndskraft där det anges hur ramen ska genomföras. För detta ändamål ska strategin för digital operativ motståndskraft inbegripa metoder för att hantera IKT-risk och uppnå specifika IKT-mål på följande sätt:

a) Förklara hur IKT-riskhanteringsramen stöder den finansiella entitetens affärsstrategi och mål.

b) Fastställa risktoleransnivån för IKT-risk i enlighet med den finansiella entitetens riskbenägenhet och analysera toleransen mot effekterna av IKT-avbrott.

c) Fastställa tydliga informationssäkerhetsmål, inbegripet nyckelprestationsindikatorer och viktiga riskmått.

d) Förklara IKT-referensarkitekturen och eventuella förändringar som krävs för att uppnå specifika verksamhetsmål.

e) Beskriva de olika mekanismer som har införts för att upptäcka IKT-relaterade incidenter, förebygga deras effekter och ge skydd däremot.

f) Lägga fram bevis för den befintliga situationen vad gäller digital operativ motståndskraft baserat på antalet rapporterade allvarliga IKT-relaterade incidenter och de förebyggande åtgärdernas effektivitet.

g) Genomföra tester av den digitala operativa motståndskraften, i enlighet med kapitel IV i denna förordning.

h) Beskriva en kommunikationsstrategi vid IKT-relaterade incidenter; vars offentliggörande föreskrivs i artikel 14.

9. Finansiella entiteter får, när det gäller den strategi för digital operativ motståndskraft som avses i punkt 8, utforma en holistisk strategi med flera olika leverantörer av IKT-tjänster på koncern- eller entitetsnivå som visar de viktigaste beroendena av tredjepartsleverantörer av IKT-tjänster och förklarar logiken bakom upphandlingsmixen av tredjepartsleverantörer av IKT-tjänster.

10. Finansiella entiteter får, i enlighet med unionsrätten och den nationella rätten på området utkontraktera uppgiften att kontrollera efterlevnaden av IKT-riskhanteringskraven till koncerninterna eller externa företag. Vid sådan utkontraktering bär den finansiella entiteten det fulla ansvaret för kontrollen av efterlevnaden av IKT-riskhanteringskraven.

Artikel 7

IKT-system, IKT-protokoll och IKT-verktyg

Finansiella entiteter ska för att åtgärda och hantera IKT-risk använda och upprätthålla uppdaterade IKT-system, IKT-protokoll och IKT-verktyg som

a) är lämpliga med hänsyn till omfattningen hos de transaktioner som ligger till grund för deras verksamhet, i enlighet med den proportionalitetsprincip som anges i artikel 4,

b) är tillförlitliga,

c) har tillräcklig kapacitet för att korrekt behandla de uppgifter som krävs för att bedriva verksamheten och skyndsamt tillhandahålla tjänster, och vid behov hantera toppar i order-, meddelande- eller transaktionsvolymer, även vid införande av ny teknik,

d) är tekniskt motståndskraftiga för att på lämpligt sätt hantera ytterligare informationsbehandlingsbehov när detta krävs under stressade marknadsförhållanden eller andra ogynnsamma situationer.

Artikel 8

Identifiering

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter identifiera, klassificera och på lämpligt sätt dokumentera alla IKT-stödda affärsfunktioner, roller och ansvarsområden, de informationstillgångar och IKT-tillgångar som stöder dessa funktioner och deras roller och beroenden i förhållande till IKT-risk. Finansiella entiteter ska vid behov, och minst en gång per år, granska lämpligheten i denna klassificering och i all relevant dokumentation.

2. Finansiella entiteter ska fortlöpande identifiera alla källor till IKT-risk, särskilt riskexponeringen mot och från andra finansiella entiteter, och bedöma cyberhot och IKT-sårbarheter som är relevanta för deras IKT-stödda affärsfunktioner, informationstillgångar och IKT-tillgångar. Finansiella entiteter ska regelbundet och minst en gång per år se över de riskscenarier som påverkar dem.

3. Andra finansiella entiteter än mikroföretag ska göra en riskbedömning vid varje större förändring av nätverks- och informationssystemets infrastruktur, av de processer eller förfaranden som påverkar deras IKT-stödda affärsfunktioner, informationstillgångar eller IKT-tillgångar.

4. Finansiella entiteter ska identifiera alla informationstillgångar och IKT-tillgångar, inbegripet sådana på fjärrplatser, nätverksresurser och maskinvaruutrustning, och kartlägga de som anses vara kritiska. De ska kartlägga informationstillgångarnas och IKT-tillgångarnas konfiguration samt länkarna och det ömsesidiga beroendet mellan de olika informationstillgångarna och IKT-tillgångarna.

5. Finansiella entiteter ska identifiera och dokumentera alla processer som är beroende av tredjepartsleverantörer av IKT-tjänster och identifiera kopplingar till de tredjepartsleverantörer av IKT-tjänster som tillhandahåller tjänster som stöder kritiska eller viktiga funktioner.

6. Vid tillämpning av punkterna 1, 4 och 5 ska finansiella entiteter upprätthålla relevanta inventeringar och uppdatera dem regelbundet och varje gång en sådan större förändring som avses i punkt 3 inträffar.

7. Andra finansiella entiteter än mikroföretag ska regelbundet, och minst en gång per år, genomföra en särskild IKT-riskbedömning av alla äldre IKT-system, och i varje fall före och efter sammanlänkning av tekniker, tillämpningar eller system.

Artikel 9

Skydd och förebyggande

1. För att skydda IKT-system på lämpligt sätt och organisera motåtgärder ska finansiella entiteter kontinuerligt övervaka och kontrollera IKT-systemens och IKT-verktygens säkerhet och funktion och ska minimera effekterna av IKT-risk på IKT-system genom att införa lämpliga verktyg, riktlinjer och förfaranden för IKT-säkerhet.

2. Finansiella entiteter ska utforma, upphandla och genomföra IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som syftar till att säkerställa IKT-systemens motståndskraft, kontinuitet och tillgänglighet, i synnerhet för de system som stöder kritiska eller viktiga funktioner, och upprätthålla höga standarder för tillgänglighet, äkthet, integritet och konfidentialitet avseende data, oberoende av om de är i vila, i bruk eller under överföring.

3. För att uppnå de mål som avses i punkt 2 ska finansiella entiteter använda IKT-lösningar och IKT-processer som är lämpliga i enlighet med artikel 4. Dessa IKT-lösningar och IKT-processer ska

a) säkerställa skyddet vid dataöverföring,

b) minimera risken för förvanskning eller förlust av uppgifter, obehörig åtkomst och tekniska brister som kan hindra affärsverksamheten,

c) förhindra bristen på tillgänglighet, försvagandet av äkthet och integritet, överträdelserna av konfidentialitet, och förlusten av data,

d) säkerställa att uppgifterna skyddas mot risker som uppstår från datahanteringen, inbegripet bristfällig förvaltning, processrelaterade risker och den mänskliga faktorn.

4. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter

a) utarbeta och dokumentera riktlinjer för informationssäkerhet där det fastställs regler för att skydda tillgängligheten, äktheten, integriteten och konfidentialiteten hos data, informationstillgångar och IKT-tillgångar, inbegripet hos deras kunder, när så är tillämpligt,

b) enligt en riskbaserad strategi upprätta en sund struktur för förvaltning av nätverk och infrastruktur med hjälp av lämpliga tekniker, metoder och protokoll, vilket kan inbegripa införande av automatiserade mekanismer för att isolera berörda informationstillgångar vid cyberangrepp,

c) genomföra strategier för att begränsa den fysiska eller logiska åtkomsten till informationstillgångar och IKT-tillgångar till enbart det som krävs för legitima och godkända funktioner och verksamheter, och för detta ändamål fastställa en uppsättning strategier, förfaranden och kontroller för åtkomsträttigheter och säkerställa en sund förvaltning av dessa,

d) genomföra strategier och protokoll för starka äkthetsmekanismer, baserade på relevanta standarder och särskilda kontrollsystem, samt skyddsåtgärder för kryptografiska nycklar där data krypteras baserat på resultat från godkända processer för klassificering och IKT-riskbedömning,

e) genomföra dokumenterade strategier, förfaranden och kontroller för hantering av IKT-förändringar, inbegripet ändringar av programvara, maskinvara, fasta programvarukomponenter, system eller säkerhetsparametrar, som bygger på en riskbedömningsmetod och är en integrerad del av den finansiella entitetens övergripande förändringshanteringsprocess, för att säkerställa att alla ändringar av IKT-system registreras, testas, bedöms, godkänns, genomförs och verifieras på ett kontrollerat sätt,

f) ha lämpliga och heltäckande dokumenterade strategier för programfixar och uppdateringar.

Vid tillämpning av första stycket led b ska finansiella entiteter utforma infrastrukturen för nätanslutning på ett sätt som gör att den omedelbart kan avskiljas eller segmenteras i syfte att minimera och förhindra spridning, särskilt för sammanlänkade finansiella processer.

Vid tillämpning av första stycket led e ska processen för hantering av IKT-förändringar godkännas av lämpliga ledningsnivåer och ska ha särskilda protokoll på plats

Artikel 10

Upptäckt

1. Finansiella entiteter ska ha mekanismer för att snabbt upptäcka onormal verksamhet i enlighet med artikel 17, inbegripet frågor som rör IKT-nätverkens prestanda och IKT-relaterade incidenter, och för att identifiera potentiella väsentliga systemkritiska felpunkter (*single points of failure*).

Alla upptäcktsmekanismer som avses i första stycket ska testas regelbundet i enlighet med artikel 25.

2. De upptäcktsmekanismer som avses i punkt 1 ska möjliggöra flera kontrollnivåer, innehålla fastställda varningströskelvärden och varningskriterier för att utlösa och inleda processer för hantering av IKT-relaterade incidenter, inbegripet automatiska varningsmekanismer för relevant personal med ansvar för hantering av IKT-relaterade incidenter.

3. Finansiella entiteter ska avsätta tillräckligt med resurser och kapacitet för att övervaka användarnas verksamhet, förekomsten av IKT-avvikelser och IKT-relaterade incidenter, särskilt cyberangrepp.

4. Leverantörer av datarapporteringstjänster ska dessutom ha system som på ett effektivt sätt gör det möjligt att kontrollera handelsrapporters fullständighet, hitta fall av utelämnad information och uppenbara fel och begära omsändning av dessa rapporter.

Artikel 11

Åtgärder och återställande

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 och baserat på identifieringskraven i artikel 8 ska finansiella entiteter införa en heltäckande IKT-kontinuitetspolicy, vilken kan antas som en särskild specifik plan och utgöra en integrerad del av den finansiella entitetens övergripande kontinuitetsplan.

2. Finansiella entiteter ska genomföra IKT-kontinuitetspolicyn genom särskilda, lämpliga och dokumenterade arrangemang, planer, förfaranden och mekanismer som syftar till att

a) säkerställa kontinuiteten i den finansiella entitetens kritiska eller viktiga funktioner,

b) snabbt, lämpligt och effektivt reagera på och lösa alla IKT-relaterade incidenter på ett sätt som begränsar skador och prioriterar återupptagandet av verksamhet och återställningsåtgärder,

c) utan dröjsmål aktivera särskilda planer som möjliggör begränsningsåtgärder, processer och teknik som är anpassade till varje typ av IKT-relaterad incident och som förhindrar ytterligare skador, samt skräddarsydda åtgärds- och återställningsförfaranden som har fastställts i enlighet med artikel 12,

d) beräkna preliminära effekter, skador och förluster,

e) fastställa kommunikations- och krishanteringsinsatser som säkerställer att uppdaterad information överförs till all berörd intern personal och alla externa berörda parter i enlighet med artikel 14 och rapportera till behöriga myndigheter i enlighet med artikel 19.

3. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter genomföra åtföljande åtgärds- och återställningsplaner avseende IKT som, när det gäller andra finansiella entiteter än mikroföretag, ska bli föremål för oberoende interna granskningar.

4. Finansiella entiteter ska införa, upprätthålla och regelbundet testa lämpliga IKT-kontinuitetsplaner, särskilt när det gäller kritiska eller viktiga funktioner som har utkontrakterats eller kontrakterats genom arrangemang med tredjepartsleverantörer av IKT-tjänster.

5. Finansiella entiteter ska som en del av sin övergripande IKT-kontinuitetspolicy genomföra en verksamhetskonsekvensanalys av hur exponerade de är mot allvarliga störningar i verksamheten. I verksamhetskonsekvensanalysen ska finansiella entiteter bedöma vilka potentiella följder som allvarliga störningar i verksamheten kan få genom kvantitativa och kvalitativa kriterier och med hjälp av interna och externa data och scenarioanalys, beroende på vad som är lämpligt. I verksamhetskonsekvensanalysen ska hänsyn tas till kritikaliteten i de identifierade och kartlagda affärsfunktionerna, stödprocesserna, tredjepartsberoendena och informationstillgångarna, samt deras ömsesidiga beroende. Finansiella entiteter ska säkerställa att IKT-tillgångarna och IKT-tjänsterna är utformade och används i full samstämmighet med verksamhetskonsekvensanalysen, särskilt vad gäller att i tillräcklig utsträckning säkerställa reservkapaciteten för alla kritiska komponenter.

6. Som en del av sin övergripande IKT-riskhantering ska finansiella entiteter

a) testa IKT-kontinuitetsplanerna och åtgärds- och återställningsplanerna avseende IKT för de IKT-system som stöder alla funktioner minst en gång per år samt i samband med omfattande ändringar av de IKT-system som stöder kritiska eller viktiga funktioner,

b) testa de kriskommunikationsplaner som har upprättats i enlighet med artikel 14.

Vid tillämpning av första stycket led a ska andra finansiella entiteter än mikroföretag i testplanerna inkludera scenarier för cyberangrepp och byten mellan den primära IKT-infrastrukturen och den reservkapacitet, de säkerhetskopior och reservanläggningar som krävs för att uppfylla de skyldigheter som anges i artikel 12.

Finansiella entiteter ska regelbundet se över sin IKT-kontinuitetspolicy och sina åtgärds- och återställningsplaner avseende IKT med hänsyn till resultatet av tester som har utförts i enlighet med första stycket och rekommendationer från revisionskontroller eller tillsynsgranskningar.

7. Andra finansiella entiteter än mikroföretag ska ha en krishanteringsfunktion som, om deras IKT-kontinuitetsplaner eller åtgärds- och återställningsplaner avseende IKT aktiveras, bland annat ska innehålla tydliga förfaranden för hantering av intern och extern kriskommunikation i enlighet med artikel 14.

8. Finansiella entiteter ska ha lättillgänglig dokumentation om den verksamhet som pågår före och under avbrott när deras IKT-kontinuitetsplaner och åtgärds- och återställningsplaner avseende IKT aktiveras.

9. Värdepapperscentraler ska förse de behöriga myndigheterna med kopior av resultatet av IKT-kontinuitetstesterna eller liknande övningar.

10. Andra finansiella entiteter än mikroföretag ska på begäran till de behöriga myndigheterna lämna en uppskattning av de totala årliga kostnader och förluster som orsakas av allvarliga IKT-relaterade incidenter.

11. I enlighet med artikel 16 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 ska de europeiska tillsynsmyndigheterna genom den gemensamma kommittén senast den 17 juli 2024 utarbeta gemensamma riktlinjer om uppskattningen av de totala årliga kostnaderna och förlusterna som avses i punkt 10.

Artikel 12

Strategier och förfaranden för säkerhetskopiering och förfaranden och metoder för återskapande och återställning

1. För att säkerställa att IKT-system och data kan återställas med minsta möjliga driftstopp, begränsade avbrott och förluster ska finansiella entiteter som en del i sin IKT-riskhanteringsram utarbeta och dokumentera

a) strategier och förfaranden för säkerhetskopiering där de anger omfattningen av de data som ska säkerhetskopieras och minimifrekvensen för säkerhetskopieringen, baserat på informationens kritikalitet eller uppgifternas konfidentialitetsnivå,

b) förfaranden och metoder för återskapande och återställning.

2. Finansiella entiteter ska skapa säkerhetskopieringssystem som kan aktiveras i enlighet med strategierna och förfarandena för säkerhetskopiering samt med förfarande och metoder för återskapande och återställning. Aktiveringen av säkerhetskopieringssystem får inte äventyra säkerheten i nätverks- och informationssystemen eller datans tillgänglighet, äkthet, integritet eller konfidentialitet. Testning av säkerhetskopieringsförfarandena och förfarande och metoder för återskapande och återställning och metoderna ska genomföras regelbundet.

3. När finansiella entiteter återställer säkerhetskopierade data med hjälp av egna system ska de använda IKT-system som är fysiskt och logiskt segregerade från det IKT-system som är källan. IKT-systemen ska ha ett säkert skydd mot obehörig åtkomst eller IKT-förvanskning och medge ett snabbt återupptagande av tjänster, med hjälp av säkerhetskopior av data och system efter behov.

För centrala motparter ska återställningsplanerna göra det möjligt att återställa alla transaktioner så som de var vid tidpunkten för avbrottet, så att den centrala motpartens verksamhet är fortsatt säker och avvecklingen kan fullföljas vid fastställd tidpunkt.

Leverantörer av datarapporteringstjänster ska dessutom ha tillräckliga resurser och ha anläggningar för säkerhetskopiering och återskapande, så att de alltid kan erbjuda och upprätthålla sina tjänster.

4. Andra finansiella entiteter än mikroföretag ska upprätthålla IKT-reservkapacitet med resurser, förmåga och funktioner som är adekvata för att säkerställa verksamhetens behov. Mikroföretag ska bedöma behovet av att upprätthålla sådan IKT-reservkapacitet med utgångspunkt i vilken riskprofil de har.

5. Värdepapperscentraler ska ha minst ett sekundärt driftsställe med adekvata resurser, kapacitet, funktioner och personalarrangemang för att säkerställa verksamhetens behov.

Det sekundära driftsstället ska

a) vara beläget på ett geografiskt avstånd från det primära driftsstället som gör det möjligt för det sekundära driftsstället att ha en åtskild riskprofil och hindrar det från att påverkas av den händelse som påverkar det primära driftsstället,

b) kunna säkra driftskontinuiteten i kritiska eller viktiga funktioner som är identiska med det primära driftsstället eller tillhandahålla den servicenivå som är nödvändig för att säkerställa att den finansiella entiteten kan bedriva sin kritiska verksamhet inom ramen för återställningsmålen,

c) vara omedelbart tillgängligt för den finansiella entitetens personal i syfte att säkra driftskontinuitet i dess kritiska eller viktiga funktioner om det primära driftsstället inte är tillgängligt.

6. När finansiella entiteter fastställer återställningstid och återställningspunktmål för varje funktion ska de ta hänsyn till huruvida det är en kritisk eller viktig funktion och den eventuella övergripande inverkan på marknadseffektiviteten. Tidsmålen ska säkerställa att de överenskomna servicenivåerna uppnås i extrema scenarier.

7. När finansiella entiteter återställer verksamheten efter en IKT-relaterad incident ska de göra nödvändiga kontroller, inbegripet flera kontroller och avstämningar, för att säkerställa att dataintegriteten håller högsta nivå. Dessa kontroller ska också utföras när data från externa berörda parter rekonstrueras för att säkerställa att alla data stämmer överens mellan systemen.

Artikel 13

Lärande och utveckling

1. Finansiella entiteter ska ha lämplig kapacitet och personal för att samla in information om sårbarheter och cyberhot, IKT-relaterade incidenter, särskilt cyberangrepp, och analysera vilken inverkan de kan förmodas ha på den digitala operativa motståndskraften.

2. Finansiella entiteter ska införa efterhandsöversyner av IKT-relaterade incidenter efter det att en allvarlig IKT-relaterad incident medför ett avbrott i kärnverksamheten, så att orsakerna till avbrotten kan analyseras och nödvändiga förbättringar av IKT-verksamheten eller i den IKT-kontinuitetspolicy som avses i artikel 11 identifieras.

Andra finansiella entiteter än mikroföretag ska på begäran till de behöriga myndigheterna meddela vilka ändringar som genomfördes efter de efterhandsöversyner av IKT-relaterade incidenter som avses i första stycket.

De efterhandsöversyner av IKT-relaterade incidenter som avses i första stycket ska fastställa om de fastställda förfarandena följdes och om de åtgärder som vidtogs var effektiva, bl.a. när det gäller

a) svarstiden för att reagera på säkerhetsvarningar och fastställa konsekvenserna av IKT-relaterade incidenter och deras allvarlighetsgrad,

b) kvalitet och snabbhet i utförandet av kriminaltekniska analyser, om så är lämpligt,

c) incidenteskaleringens effektivitet inom den finansiella entiteten,

d) effektiviteten i intern och extern kommunikation.

3. Lärdomar av den testning av digital operativ motståndskraft som har utförts i enlighet med artiklarna 26 och 27 och av verkliga IKT-relaterade incidenter, särskilt cyberangrepp, samt utmaningar i samband med aktivering av IKT-kontinuitetsplaner och åtgärds- och återställningsplaner avseende IKT och relevant information som har utväxlats med motparter och bedömts under tillsynsgranskningar, ska införlivas fortlöpande i IKT-riskbedömningsprocessen. Dessa resultat ska utgöra en grund för lämpliga översyner av relevanta delar i den IKT-riskhanteringsram som avses i artikel 6.1.

4. Finansiella entiteter ska övervaka effektiviteten i genomförandet av den strategi för digital operativ motståndskraft som anges i artikel 6.8. De ska kartlägga IKT-riskens utveckling över tid, analysera IKT-relaterade incidenters frekvens, typ, omfattning och utveckling, särskilt cyberangrepp och deras mönster, i syfte att förstå graden av IKT-riskexponering, särskilt när det gäller kritiska eller viktiga funktioner, och öka den finansiella entitetens cybermognad och cyberberedskap.

5. Senior IKT-personal ska minst en gång per år rapportera till ledningsorganet om de resultat som avses i punkt 3 och lägga fram rekommendationer.

6. Finansiella entiteter ska utarbeta program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft som obligatoriska moduler i sina personalutbildningsprogram. Dessa program och utbildningar ska gälla för alla anställda och personer i ledande ställning, och deras komplexitet ska motsvara behörigheten för personens roll. När så är lämpligt ska finansiella entiteter också inkludera tredjepartsleverantörer av IKT-tjänster i sina relevanta utbildningar, i enlighet med artikel 30.2 i.

7. Andra finansiella entiteter än mikroföretag ska kontinuerligt övervaka relevant teknisk utveckling, även i syfte att förstå vilka konsekvenser införandet av sådan ny teknik kan få för IKT-säkerhetskraven och den digitala operativa motståndskraften. De ska hålla sig uppdaterade om de senaste IKT-riskhanteringsprocesserna för att effektivt bekämpa nuvarande eller nya former av cyberangrepp.

Artikel 14

Kommunikation

1. Som en del av den IKT-riskhanteringsram som avses i artikel 6.1 ska finansiella entiteter ha kriskommunikationsplaner som gör det möjligt att på ett ansvarsfullt sätt informera kunder och motparter samt allmänheten om åtminstone allvarliga IKT-relaterade incidenter eller sårbarheter, beroende på vad som är lämpligt.

2. Som en del av IKT-riskhanteringsramen ska finansiella entiteter genomföra kommunikationsstrategier för intern personal och externa berörda parter. I sina kommunikationsstrategier för personalen ska hänsyn tas till behovet av att skilja mellan personal som deltar i IKT-riskhantering, framför allt personalen med ansvar för åtgärder och återställande, och personal som behöver information.

3. Minst en person i den finansiella entiteten ska ha i uppgift att genomföra kommunikationsstrategin för IKT-relaterade incidenter och fungera som talesperson gentemot allmänheten och medierna i detta syfte.

Artikel 15

Ytterligare harmonisering av verktyg, metoder, processer och strategier för IKT-riskhantering

De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa), utarbeta gemensamma förslag till tekniska standarder för tillsyn i syfte att

a) närmare specificera delar som ska ingå i de IKT-relaterade säkerhetsstrategier, förfaranden, protokoll och verktyg som avses i artikel 9.2 i syfte att säkerställa säkerheten i nätverk, möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av uppgifter, bevara uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet, inbegripet krypteringsmetoder, och garantera en korrekt och snabb dataöverföring utan allvarliga avbrott och onödiga dröjsmål,

b) utveckla ytterligare komponenter i den hantering av kontroll av åtkomsträttigheter som avses i artikel 9.4 c och tillhörande personalpolitik där det specificeras åtkomsträttigheter, förfaranden för beviljande och återkallande av rättigheter, övervakning av onormalt beteende i förhållande till IKT-risk genom lämpliga indikatorer, inbegripet mönster för nätanvändning, tidpunkter, it-verksamhet och okänd utrustning,

c) vidareutveckla de mekanismer som anges i artikel 10.1 för att möjliggöra en snabb upptäckt av onormal verksamhet och de kriterier som fastställs i artikel 10.2 som utlöser processer för upptäckt och hantering av IKT-relaterade incidenter,

d) närmare specificera komponenterna i den IKT-kontinuitetspolicy som avses i artikel 11.1,

e) närmare specificera de tester av IKT-kontinuitetsplaner som avses i artikel 11.6 för att säkerställa att det vid sådan testning tas tillräckligt stor hänsyn till scenarier där kvaliteten på tillhandahållandet av en kritisk eller viktig funktion försämras till en oacceptabel nivå eller tillhandahållandet avbryts, och till de potentiella konsekvenserna av insolvens eller andra fel hos en relevant tredjepartsleverantör av IKT-tjänster och, i förekommande fall, de politiska riskerna i respektive leverantörers jurisdiktioner,

f) närmare specificera komponenterna i de åtgärds- och återställningsplaner avseende IKT som avses i artikel 11.3,

g) närmare specificera innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som avses i artikel 6.5.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de beakta den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser, samtidigt som vederbörlig hänsyn tas till eventuella särdrag som härrör från den särskilda karaktären på verksamheten i olika sektorer för finansiella tjänster.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 16

Förenklad IKT-riskhanteringsram

1. Artiklarna 5–15 i denna förordning ska inte tillämpas på små och icke-sammanlänkade värdepappersföretag, betalningsinstitut undantagna enligt direktiv (EU) 2015/2366, institut undantagna enligt direktiv 2013/36/EU och för vilka medlemsstaterna har beslutat att inte tillämpa den möjlighet som anges i artikel 2.4 i denna förordning; institut för elektroniska pengar undantagna enligt direktiv 2009/110/EG och små tjänstepensionsinstitut.

Utan att det påverkar tillämpningen av första stycket ska de enheter som förtecknas i första stycket

a) inrätta och upprätthålla en sund och dokumenterad IKT-riskhanteringsram som specificerar de mekanismer och åtgärder som syftar till att ge en snabb, effektiv och heltäckande hantering av IKT-risk, inbegripet vad gäller skyddet av relevanta fysiska komponenter och infrastrukturer,

b) kontinuerligt övervaka alla IKT-systems säkerhet och funktion,

c) minimera effekterna av IKT-risk genom användningen av sunda, motståndskraftiga och uppdaterade IKT-system, IKT-protokoll och IKT-verktyg som lämpar sig för att stödja utförandet av verksamheten och tillhandahållandet av tjänster och på ett tillräckligt sätt skydda konfidentialitet, tillgänglighet, integritet eller äkthet hos datan i nätverks- och informationssystemen,

d) göra det möjligt att snabbt identifiera och upptäcka IKT-risk och avvikelser i nätverks- och informationssystemen och att snabbt hantera IKT-relaterade incidenter,

e) identifiera de viktigaste beroendena av tredjepartsleverantörer av IKT-tjänster,

f) säkerställa kontinuiteten för kritiska eller viktiga funktioner genom kontinuitetsplaner och åtgärds- och återställnings-åtgärder, vilket bland annat innefattar säkerhetskopiering och återskapande,

g) regelbundet testa de planer och åtgärder som avses i led f, samt effektiviteten i de kontroller som genomförts i enlighet med leden a och c,

h) i enlighet med vad som är lämpligt genomföra relevanta operativa slutsatser som härrör från de test som avses i led g och från efteranalyser av incidenter i IKT-riskbedömningsprocessen, och utifrån behoven och IKT-riskprofilen utarbeta program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft för personal och ledning.

2. Den IKT-riskhanteringsram som avses i punkt 1 andra stycket a, ska dokumenteras och ses över regelbundet och vid uppkomsten av allvarliga IKT-relaterade incidenter, i enlighet med tillsynsinstruktionerna. Ramen ska förbättras fortlöpande baserat på erfarenheterna från genomförande och övervakning. En rapport om översynen av IKT-riskhanteringsramen ska överlämnas till den behöriga myndigheten på dess begäran.

3. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Enisa, utarbeta gemensamma förslag till tekniska standarder för tillsyn i syfte att

a) närmare specificera vilka komponenter som ska ingå i den IKT-riskhanteringsram som avses i punkt 1 andra stycket a,

b) närmare specificera komponenterna i förhållande till system, protokoll och verktyg för att minimera effekterna av IKT-risk som avses i punkt 1 andra stycket c, i syfte att säkerställa säkerheten i nätverken, möjliggöra lämpliga skyddsåtgärder mot intrång och missbruk av data och bevara datans tillgänglighet, äkthet, integritet och konfidentialitet,

c) närmare specificera komponenterna i de IKT-kontinuitetsplaner som avses i punkt 1 andra stycket f,

d) närmare specificera reglerna för testningen av kontinuitetsplanerna och säkerställa att de kontroller som avses i punkt 1 andra stycket g är effektiva, och säkerställa att det vid sådan testning tas tillräckligt stor hänsyn till scenarier där kvaliteten på tillhandahållandet av en kritisk eller viktig funktion försämras till en oacceptabel nivå eller tillhandahållandet avbryts,

e) närmare specificera innehållet i och formatet för den rapport om översynen av IKT-riskhanteringsramen som avses i punkt 2.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

KAPITEL III

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

Artikel 17

Process för hantering av IKT-relaterade incidenter

1. Finansiella entiteter ska fastställa, inrätta och genomföra en process för hantering av IKT-relaterade incidenter för att upptäcka, hantera och rapportera IKT-relaterade incidenter.

2. Finansiella entiteter ska registrera alla IKT-relaterade incidenter och betydande cyberhot. Finansiella entiteter ska inrätta lämpliga förfaranden och processer för att säkerställa en konsekvent och integrerad övervakning, hantering och uppföljning av IKT-relaterade incidenter, för att säkerställa att grundorsakerna identifieras, dokumenteras och åtgärdas i syfte att förhindra att sådana incidenter inträffar.

3. Den process för hantering av IKT-relaterade incidenter som avses i punkt 1 ska

a) införa indikatorer för tidig varning,

b) innehålla fastställda förfaranden för att identifiera, spåra, logga, kategorisera och klassificera IKT-relaterade incidenter enligt deras prioritetsordning och allvar och enligt de berörda tjänsternas kritikalitet i enlighet med de kriterier som fastställs i artikel 18.1,

c) innehålla en fördelning av roller och ansvarsområden som behöver aktiveras för olika IKT-relaterade incidenttyper och scenarier,

d) innehålla planer för kommunikation till personal, externa berörda parter och medier i enlighet med artikel 14 och för anmälan till kunder, för interna eskaleringsförfaranden, inbegripet IKT-relaterade kundklagomål, samt för tillhandahållande av information till finansiella entiteter som fungerar som motparter, beroende på vad som är lämpligt,

e) säkerställa att åtminstone allvarliga IKT-relaterade incidenter rapporteras till relevant senior ledning och att ledningsorganet informeras om åtminstone allvarliga IKT-relaterade incidenter, med en förklaring av effekter, åtgärder och ytterligare kontroller som ska fastställas till följd av sådana IKT-relaterade incidenter,

f) innehålla fastställda förfaranden för åtgärder vid IKT-relaterade incidenter för att mildra effekterna och säkerställa att tjänsterna snabbt kan tas i drift och är säkra.

Artikel 18

Klassificering av IKT-relaterade incidenter och cyberhot

1. Finansiella entiteter ska klassificera IKT-relaterade incidenter och fastställa deras inverkan baserat på följande kriterier:

a) Antalet och/eller betydelsen av kunder eller finansiella motparter som påverkas, och i tillämpliga fall, mängden eller antalet transaktioner som påverkas av den IKT-relaterade incidenten, och om anseendet har påverkats av den IKT-relaterade incidenten.

b) Den IKT-relaterade incidentens varaktighet, inklusive driftstopp.

c) Den geografiska spridningen med avseende på de områden som påverkas av den IKT-relaterade incidenten, särskilt om den påverkar fler än två medlemsstater.

d) De dataförluster som den IKT-relaterade incidenten medför, vad gäller tillgänglighet, äkthet, integritet eller konfidentialitet vad gäller datan

e) De berörda tjänsternas kritikalitet, inbegripet den finansiella entitetens transaktioner och verksamhet.

f) De ekonomiska effekterna, särskilt direkta och indirekta kostnader och förluster, av den IKT-relaterade incidenten i absoluta och relativa tal.

2. Finansiella entiteter ska klassificera cyberhot som betydande baserat på de hotade tjänsternas kritikalitet, inbegripet den finansiella entitetens transaktioner och verksamhet, antalet och/eller betydelsen av kunder eller finansiella motparter som hotas och den geografiska spridningen av de hotade områdena.

3. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med ECB och Enisa, utarbeta gemensamma förslag till tekniska standarder för tillsyn som ytterligare specificerar följande:

a) De kriterier som anges i punkt 1, inbegripet väsentlighetströsklar för att fastställa allvarliga IKT-relaterade incidenter eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, som omfattas av rapporteringsskyldigheten i artikel 19.1.

b) De kriterier som de behöriga myndigheterna ska tillämpa för att bedöma allvarliga IKT-relaterade incidenters eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenters eller säkerhetsincidenters relevans för de relevanta behöriga myndigheterna i andra medlemsstater och de detaljer i rapporter om allvarliga IKT-relaterade incidenter eller, i tillämpliga fall, allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter som ska delas med andra behöriga myndigheter enligt artikel 19.6 och 19.7.

c) De kriterier som anges i punkt 2 i denna artikel, inbegripet höga väsentlighetströsklar för att fastställa betydande cyberhot.

4. När de europeiska tillsynsmyndigheterna utarbetar de gemensamma förslag till tekniska standarder för tillsyn som avses i punkt 3 i denna artikel ska de ta hänsyn till kriterierna i artikel 4.2 samt internationella standarder, riktlinjer och specifikationer som har utarbetats och offentliggjorts av Enisa, inbegripet, när så är lämpligt, specifikationer för andra ekonomiska sektorer. Vid tillämpningen av kriterierna i artikel 4.2 ska de europeiska tillsynsmyndigheterna vederbörligen beakta behovet av att mikroföretag och små och medelstora företag mobiliserar tillräckliga resurser och tillräcklig kapacitet för att säkerställa att IKT-relaterade incidenter hanteras snabbt.

De europeiska tillsynsmyndigheterna ska överlämna dessa gemensamma förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i punkt 3 i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 19

Rapportering av allvarliga IKT-relaterade incidenter och frivillig anmälan av betydande cyberhot

1. Finansiella entiteter ska rapportera allvarliga IKT-relaterade incidenter till den relevanta behöriga myndighet som avses i artikel 46 i enlighet med punkt 4 i den här artikeln.

Om en finansiell entitet är föremål för tillsyn av mer än en sådan nationell behörig myndighet som avses i artikel 46 ska medlemsstaterna utse en enda behörig myndighet till relevant behörig myndighet med ansvar för att utföra de funktioner och skyldigheter som föreskrivs i denna artikel.

Kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 ska rapportera allvarliga IKT-relaterade incidenter till den relevanta nationella behöriga myndighet som utsetts i enlighet med artikel 4 i direktiv 2013/36/EU, och myndigheten ska omedelbart översända den rapporten till ECB.

Vid tillämpning av första stycket ska finansiella entiteter, efter att ha samlat in och analyserat all relevant information, utarbeta den första anmälan och de rapporter som avses i punkt 4 i denna artikel med hjälp av de mallar som avses i artikel 20 och överlämna dem till den behöriga myndigheten. Om det visar sig vara tekniskt omöjligt att överföra den första anmälan med hjälp av mallen ska finansiella entiteter anmäla till den behöriga myndigheten på annat vis.

Den första anmälan och de rapporter som avses i punkt 4 ska innehålla all information som är nödvändig för att den behöriga myndigheten ska kunna fastställa betydelsen av den allvarliga IKT-relaterade incidenten och bedöma eventuella gränsöverskridande konsekvenser.

Utan att det påverkar den finansiella entitetens rapportering enligt första stycket till den relevanta behöriga myndigheten får medlemsstaterna även besluta att vissa eller alla finansiella entiteter dessutom till den första anmälan och de rapporter som avses i punkt 4 i denna artikel ska använda de mallar som avses i artikel 20 när de överlämnar anmälan och rapporterna till de behöriga myndigheterna eller de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

2. Finansiella entiteter får på frivillig basis rapportera betydande cyberhot till den relevanta behöriga myndigheten, när de anser att hotet är relevant för det finansiella systemet, tjänsteanvändarna eller kunderna. Den relevanta behöriga myndigheten får lämna sådan information till de andra relevanta myndigheter som avses i punkt 6.

Kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 får på frivillig basis rapportera betydande cyberhot till den relevanta nationella behöriga myndighet som utsetts i enlighet med artikel 4 i direktiv 2013/36/EU, och myndigheten ska omedelbart översända den anmälan till ECB.

Medlemsstaterna får fastställa att de finansiella entiteter som rapporterar på frivillig basis i enlighet med första stycket också får vidarebefordra den anmälan till de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

3. Om en allvarlig IKT-relaterad incident inträffar och påverkar kunders ekonomiska intressen ska finansiella entiteter utan onödigt dröjsmål så snart de blir medvetna om den informera sina kunder om den allvarliga IKT-relaterade incidenten och om de åtgärder som har vidtagits för att mildra de negativa effekterna av en sådan incident.

I händelse av ett betydande cyberhot ska finansiella entiteter, i tillämpliga fall, informera de kunder som kan påverkas om alla lämpliga skyddsåtgärder som de sistnämnda kan överväga att vidta.

4. Finansiella entiteter ska, inom de tidsfrister som ska fastställas i enlighet med artikel 20 första stycket a ii, lämna följande till den relevanta behöriga myndigheten:

a) En första anmälan.

b) En delrapport efter den första anmälan som avses i led a, så snart statusen för den ursprungliga incidenten har förändrats avsevärt eller hanteringen av den allvarliga IKT-relaterade incidenten har förändrats på grund av ny tillgänglig information, när så är lämpligt åtföljd av uppdaterade anmälningar varje gång en relevant statusuppdatering finns tillgänglig, samt på särskild begäran av den behöriga myndigheten.

c) En slutrapport, när analysen av grundorsakerna har slutförts, oavsett om begränsande åtgärder redan har vidtagits, och när de faktiska påverkanssiffrorna finns tillgängliga för att ersätta uppskattningar.

5. Finansiella entiteter får i enlighet med unionsrätten och nationell rätt på området utkontraktera rapporteringsskyldigheterna enligt denna artikel till en tredjepartsleverantör av tjänster. Vid sådan utkontraktering bär den finansiella entiteten det fulla ansvaret för efterlevnaden av incidentrapporteringskraven.

6. Efter mottagandet av den första anmälan och av varje rapport som avses i punkt 4 ska den behöriga myndigheten skyndsamt lämna närmare uppgifter om den allvarliga IKT-relaterade incidenten till följande mottagare, i tillämpliga fall på grundval av deras respektive behörigheter:

a) EBA, Esma eller Eiopa,

b) ECB när det gäller de finansiella entiteter som avses i artikel 2.1 a, b och d,

c) de behöriga myndigheter, de gemensamma kontaktpunkter eller de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555,

d) de resolutionsmyndigheter som avses i artikel 3 i direktiv 2014/59/EU och den gemensamma resolutionsnämnden när det gäller sådana enheter som avses i artikel 7.2 i Europaparlamentets och rådets förordning (EU) nr 806/2014 ([37]) och när det gäller sådana enheter och koncerner som avses i artikel 7.4 b och 7.5 i förordning (EU) nr 806/2014 om sådana detaljer gäller incidenter som utgör en risk för säkerställandet av kritiska funktioner i den mening som avses i artikel 2.1.35 i direktiv 2014/59/EU, och

e) andra relevanta offentliga myndigheter enligt nationell rätt.

7. Efter att ha mottagit information i enlighet med punkt 6 ska EBA, Esma eller Eiopa och ECB, i samråd med Enisa och i samarbete med den relevanta behöriga myndigheten, bedöma huruvida den allvarliga IKT-relaterade incidenten är relevant för behöriga myndigheter i andra medlemsstater. Efter denna bedömning ska EBA, Esma eller Eiopa så snart som möjligt underrätta de relevanta behöriga myndigheterna i andra medlemsstater i ärendet. ECB ska underrätta medlemmarna i Europeiska centralbankssystemet om frågor som är relevanta för betalningssystemet. Baserat på denna underrättelse ska de behöriga myndigheterna vid behov vidta alla nödvändiga åtgärder för att skydda det finansiella systemets omedelbara stabilitet.

([37]) Europaparlamentets och rådets förordning (EU) nr 806/2014 av den 15 juli 2014 om fastställande av enhetliga regler och ett enhetligt förfarande för resolution av kreditinstitut och vissa värdepappersföretag inom ramen för en gemensam resolutionsmekanism och en gemensam resolutionsfond och om ändring av förordning (EU) nr 1093/2010 (EUT L 225, 30.7.2014, s. 1).

8. Den anmälan som Esma ska göra enligt punkt 7 i denna artikel ska inte påverka den behöriga myndighetens skyldighet att skyndsamt översända uppgifterna om den allvarliga IKT-relaterade incidenten till den relevanta myndigheten i värdmedlemsstaten, om en värdepapperscentral har betydande gränsöverskridande verksamhet i värdmedlemsstaten, om den allvarliga IKT-relaterade incidenten sannolikt kommer att medföra allvarliga konsekvenser för finansmarknaderna i värdmedlemsstaten och om det finns samarbetsarrangemang mellan behöriga myndigheter som gäller tillsynen av finansiella entiteter.

Artikel 20

Harmonisering av rapporteringsinnehåll och mallar

De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med Enisa och ECB, utarbeta

a) gemensamma förslag till tekniska standarder för tillsyn för att

   i) fastställa innehållet i rapporterna om allvarliga IKT-relaterade incidenter, för att återspegla de kriterier som fastställts i artikel 18.1 och införliva ytterligare beståndsdelar, såsom detaljerna för att fastställa huruvida rapporteringen är relevant för andra medlemsstater och huruvida det utgör en allvarliga betalningsrelaterad operativ incident eller säkerhetsincident eller inte,

   ii) fastställa tidsfristerna för den första anmälan och för varje rapport som avses i artikel 19.4,

   iii) fastställa innehållet i anmälan om betydande cyberhot.

   Vid utarbetandet av dessa förslag till tekniska standarder för tillsyn ska de europeiska tillsynsmyndigheterna ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil samt karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser, särskilt för att säkerställa att olika tidsfrister för tillämpningen av detta stycke led a ii, beroende på vad som är lämpligt, kan återspegla de finansiella sektorernas särdrag, utan att det påverkar upprätthållandet av en enhetlig strategi för IKT-relaterad incidentrapportering enligt denna förordning och i direktiv (EU) 2022/2555. De europeiska tillsynsmyndigheterna ska, beroende på vad som är tillämpligt, lämna en motivering när de avviker från de metoder som tillämpas inom ramen för det direktivet.

b) gemensamma förslag till tekniska standarder för genomförande i syfte att fastställa standardformulär, mallar och förfaranden för finansiella entiteter för rapportering av en allvarlig IKT-relaterad incident eller anmälan av ett betydande cyberhot.

De europeiska tillsynsmyndigheterna ska överlämna de gemensamma förslag till tekniska standarder för tillsyn som avses i första stycket a och de gemensamma förslag till tekniska genomförandestandarder som avses i första stycket b till kommissionen senast den 17 juli 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de gemensamma tekniska standarder för tillsyn som avses i första stycket a i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Kommissionen ges befogenhet att anta de gemensamma tekniska standarder för genomförande som avses i första stycket b i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 21

Centralisering av rapportering av allvarliga IKT-relaterade incidenter

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och i samråd med ECB och Enisa, utarbeta en gemensam rapport med en bedömning av genomförbarheten av ytterligare centralisering av incidentrapporteringen genom inrättandet av en gemensam EU-knutpunkt för finansiella entiteters rapportering av allvarliga IKT-relaterade incidenter. Den gemensamma rapporten ska innehålla en undersökning av olika sätt att underlätta flödet av IKT-relaterad incidentrapportering, minska de därmed sammanhängande kostnaderna och underbygga tematiska analyser i syfte att öka konvergensen i tillsynen.

2. Den gemensamma rapport som avses i punkt 1 ska innehålla minst följande:

a) Förutsättningar för att inrätta en gemensam EU-knutpunkt.

b) Fördelar, begränsningar och risker, inbegripet risker förknippade med hög koncentration av känslig information.

c) Nödvändig kapacitet för att säkerställa interoperabilitet med andra relevanta rapporteringssystem.

d) Inslag i den operativa förvaltningen.

e) Villkor för medlemskap.

f) Tekniska arrangemang för att finansiella entiteter och nationella behöriga myndigheter ska få tillgång till den gemensamma EU-knutpunkten.

g) En preliminär bedömning av de finansiella kostnaderna för inrättandet av den operativa plattformen till stöd för den gemensamma EU-knutpunkten, inklusive den sakkunskap som krävs.

3. De europeiska tillsynsmyndigheterna ska överlämna den rapport som avses i punkt 1 till Europaparlamentet, rådet och kommissionen senast den 17 januari 2025.

Artikel 22

Återkoppling från tillsynsmyndigheterna

1. Utan att det påverkar de tekniska uppgifterna, råden eller åtgärderna och efterföljande uppföljning, som i tillämpliga fall kan tillhandahållas i enlighet med nationell rätt, av CSIRT-enheterna enligt direktiv (EU) 2022/2555, ska den behöriga myndigheten, efter mottagandet av den första anmälan och av varje rapport som avses i artikel 19.4, bekräfta mottagandet och får, när så är möjligt, skyndsamt tillhandahålla relevant och proportionell återkoppling eller vägledning på hög nivå till den finansiella entiteten, särskilt genom att göra tillgänglig all eventuell relevant anonymiserad information och underrättelser om liknande hot, och får diskutera åtgärder som tillämpas på finansiell entitetsnivå, och sätt att minimera och mildra de negativa effekterna i den finansiella sektorn. Utan att det påverkar den återkoppling som mottagits från tillsynsmyndigheterna ska finansiella entiteter förbli fullt ansvariga för hanteringen av och konsekvenserna av IKT-relaterade incidenter som rapporteras enligt artikel 19.1.

2. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén årligen lämna anonymiserade och aggregerade rapporter om allvarliga IKT-relaterade incidenter, vars detaljer ska komma från behöriga myndigheter i enlighet med artikel 19.6, med angivande av åtminstone antalet allvarliga IKT-relaterade incidenter och deras art, inverkan på finansiella entiteters eller kunders verksamhet, vidtagna avhjälpande åtgärder och uppkomna kostnader.

De europeiska tillsynsmyndigheterna ska utfärda varningar och ta fram statistik på hög nivå till stöd för IKT-hot- och sårbarhetsbedömningar.

Artikel 23

Betalningsrelaterade operativa incidenter eller säkerhetsincidenter som gäller kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar

De krav som fastställs i detta kapitel ska också tillämpas på betalningsrelaterade operativa incidenter eller säkerhetsincidenter och på allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, om de gäller kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar.

KAPITEL IV

Testning av digital operativ motståndskraft

Artikel 24

Allmänna krav för testning av digital operativ motståndskraft

1. För att bedöma beredskapen för hantering av IKT-relaterade incidenter, identifiera svagheter, brister och luckor i den digitala operativa motståndskraften och snabbt genomföra korrigerande åtgärder ska andra finansiella entiteter än mikroföretag, med hänsyn till de kriterier som fastställs i artikel 4.2, inrätta, upprätthålla och se över ett sunt och heltäckande program för testning av digital operativ motståndskraft som en integrerad del av den IKT-riskhanteringsram som avses i artikel 6.

2. Programmet för testning av digital operativ motståndskraft ska omfatta en rad bedömningar, tester, metoder, praxis och verktyg som ska tillämpas i enlighet med artiklarna 25 och 26.

3. När andra finansiella entiteter än mikroföretag genomför det testprogram för digital operativ motståndskraft som avses i punkt 1 i denna artikel ska de följa en riskbaserad metod med hänsyn tagen till kriterierna i artikel 4.2 med vederbörligt beaktande av IKT-riskens utveckling, eventuella specifika risker som den berörda finansiella entiteten är eller kan bli exponerad för, kritikaliteten hos informationstillgångar och tillhandahållna tjänster samt varje annan faktor som den finansiella entiteten anser lämplig.

4. Andra finansiella entiteter än mikroföretag ska se till att testerna utförs av oberoende parter, oavsett om de är interna eller externa. När tester utförs av en intern testare ska finansiella entiteter avsätta tillräckliga resurser och säkerställa att intressekonflikter kan undvikas under testets utformning och genomförande.

5. Andra finansiella entiteter än mikroföretag ska fastställa förfaranden och strategier för prioritering, klassificering och åtgärdande av alla problem som visar sig under genomförandet av testerna och ska införa interna valideringsmetoder för att säkerställa att alla identifierade svagheter, brister eller luckor åtgärdas fullt ut.

6. Andra finansiella entiteter än mikroföretag ska säkerställa, åtminstone årligen, att lämpliga tester utförs på alla IKT-system och IKT-tillämpningar som stöder kritiska eller viktiga funktioner.

Artikel 25

Testning av IKT-verktyg och IKT-system

1. Det program för testning av digital operativ motståndskraft som avses i artikel 24 ska, i enlighet med kriterierna i artikel 4.2, innehålla bestämmelser om utförande av lämpliga tester, såsom sårbarhetsanalyser och skanningar, analyser av öppen källkod, nätverkssäkerhetsbedömningar, gapanalyser, fysiska säkerhetsgranskningar, frågeformulär och programvarulösningar för skanning, källkodsgranskningar när så är möjligt, scenariobaserade tester, kompatibilitetstester, prestandatester, tester ändpunkt till ändpunkt (end-to-end) och penetrationstester.

2. Värdepapperscentraler och centrala motparter ska utföra sårbarhetsbedömningar före eventuellt införande eller återinförande av nya eller befintliga tillämpningar och infrastrukturkomponenter, och IKT-tjänster som stöder den finansiella entitetens kritiska eller viktiga funktioner,.

3. Mikroföretag ska utföra de tester som avses i punkt 1 genom att kombinera en riskbaserad metod med strategisk planering av IKT-testning, genom att vederbörligen beakta behovet av att upprätthålla en balans mellan å ena sidan omfattningen av de resurser och den tid som ska avsättas för IKT-testning som föreskrivs i denna artikel och å andra sidan skyndsamheten, typen av risk, kritikaliteten hos informationstillgångarna och de tillhandahållna tjänsterna samt alla andra relevanta faktorer, inbegripet den finansiella entitetens förmåga att ta beräknade risker.

Artikel 26

Avancerad testning av IKT-verktyg, IKT-system och IKT-processer baserad på hotbildsstyrd penetrationstestning

1. Andra finansiella entiteter än de entiteter som avses i artikel 16.1 första stycket och mikroföretag, vilka har identifierats i enlighet med punkt 8 tredje stycket i den här artikeln ska minst vart tredje år genomföra avancerade tester med hjälp av hotbildsstyrd penetrationstestning. Baserat på den finansiella entitetens riskprofil och med beaktande av de operativa omständigheterna får den behöriga myndigheten vid behov begära att den finansiella entiteten minskar eller ökar denna frekvens.

2. Varje hotbildsstyrt penetrationstest ska omfatta flera eller alla av en finansiell entitets kritiska eller viktiga funktioner och ska utföras på produktionssystem i drift som stöder sådana funktioner.

Finansiella entiteter ska identifiera alla relevanta underliggande IKT-system, IKT-processer och IKT-tekniker som stöder kritiska eller viktiga funktioner och IKT-tjänster, inbegripet de som stöder de kritiska eller viktiga funktioner som har utkontrakterats eller kontrakterats till tredjepartsleverantörer av IKT-tjänster.

Finansiella entiteter ska bedöma vilka kritiska eller viktiga funktioner som behöver omfattas av den hotbildsstyrda penetrationstestningen. Resultatet av denna bedömning ska fastställa den exakta omfattningen av den hotbildsstyrda penetrationstestningen och ska valideras av de behöriga myndigheterna.

3. Om tredjepartsleverantörer av IKT-tjänster omfattas av den hotbildsstyrda penetrationstestningen ska den finansiella entiteten vidta nödvändiga åtgärder och skyddsåtgärder för att säkerställa att sådana tredjepartsleverantörer av IKT-tjänster deltar i den hotbildsstyrda penetrationstestningen och ska alltid ha fullt ansvar för att säkerställa att denna förordning efterlevs.

4. Utan att det påverkar tillämpningen av punkt 2 första och andra styckena får den finansiella entiteten och en tredjepartsleverantör av IKT-tjänster, om tredjepartsleverantörens deltagande i den hotbildsstyrda penetrationstestningen som avses i punkt 3 kan förväntas få negativ inverkan på kvaliteten eller säkerheten för de tjänster som tredjepartsleverantören av IKT-tjänster tillhandahåller till kunder som är entiteter som inte omfattas av denna förordning, eller för konfidentialiteten för data som är relaterade till sådana tjänster, skriftligen enas om att tredjepartsleverantören av IKT-tjänster ingår avtal med en extern testare i syfte att, under ledning av en utsedd finansiell entitet, genomföra en gemensam hotbildsstyrd penetrationstestning med flera finansiella entiteter (gemensam testning) till vilka tredjepartsleverantören av IKT-tjänster tillhandahåller IKT-tjänster.

Den gemensamma testningen ska omfatta det relevanta spektrum av IKT-tjänster som stöder kritiska eller viktiga funktioner som de finansiella entiteterna har ingått avtal om med respektive tredjepartsleverantör av IKT-tjänster. Den gemensamma testningen ska betraktas som hotbildsstyrd penetrationstestning utförd av de finansiella entiteter som deltar i den gemensamma testningen.

Antalet finansiella entiteter som deltar i den gemensamma testningen ska vederbörligen kalibreras med beaktande av de berörda tjänsternas komplexitet och typ.

5. De finansiella entiteterna ska, i samarbete med tredjepartsleverantörer av IKT-tjänster och andra berörda parter, inbegripet testarna men exklusive de behöriga myndigheterna, tillämpa effektiva riskhanteringskontroller för att minska riskerna för möjliga effekter på data, skador på tillgångar och avbrott i kritiska eller viktiga funktioner, tjänster eller transaktioner hos den finansiella entiteten själv, dess motpart eller den finansiella sektorn.

6. När testet har avslutats och efter det att rapporter och åtgärdsplaner har godkänts ska den finansiella entiteten och, i tillämpliga fall, de externa testarna förse den myndighet som utsetts i enlighet med punkt 9 eller 10 med en sammanfattning av de relevanta resultaten, åtgärdsplanerna och dokumentation som visar att den hotbildsstyrda penetrationstestningen har utförts i enlighet med kraven.

7. Myndigheter ska förse finansiella entiteter med ett intyg som bekräftar att testet genomfördes i enlighet med kraven, vilket ska framgå av dokumentationen, i syfte att möjliggöra ömsesidigt erkännande av hotbildsstyrd penetrationstestning mellan behöriga myndigheter. Den finansiella entiteten ska underrätta den relevanta behöriga myndigheten om intyget, sammanfattningen av de relevanta resultaten och åtgärdsplanerna.

Utan att det påverkar tillämpligheten av ett sådant intyg ska de finansiella entiteterna alltid ha det fulla ansvaret för effekterna av de tester som avses i punkt 4.

8. Finansiella entiteter ska anlita testare i syfte att genomföra hotbildsstyrd penetrationstestning i enlighet med artikel 27. Om finansiella entiteter använder interna testare för att genomföra hotbildsstyrd penetrationstestning ska de anlita externa testare vid vart tredje test.

De kreditinstitut som klassificeras som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013 ska endast använda externa testare i enlighet med artikel 27.1 a–e.

De behöriga myndigheterna ska identifiera de finansiella entiteter som är skyldiga att genomföra hotbildsstyrd penetrationstestning med beaktande av kriterierna i artikel 4.2, baserat på en bedömning av följande:

a) Påverkansfaktorer, särskilt i vilken utsträckning de tjänster som tillhandahålls och den verksamhet som bedrivs av den finansiella entiteten påverkar den finansiella sektorn.

b) Eventuella farhågor om den finansiella stabiliteten, inbegripet den finansiella entitetens betydelse för systemet som helhet på unionsnivå eller nationell nivå, beroende på vad som är tillämpligt.

c) Den berörda finansiella entitetens specifika IKT-riskprofil, IKT-mognadsgrad och tekniska funktioner.

9. Medlemsstaterna får utse en enda offentlig myndighet inom finanssektorn som ska ansvara för frågor som rör hotbildsstyrd penetrationstestning inom den finansiella sektorn på nationell nivå och ska ge myndigheten alla befogenheter och uppgifter i detta syfte.

10. Om det inte har utsetts någon myndighet i enlighet med punkt 9 i denna artikel, och utan att det påverkar befogenheten att välja ut vilka finansiella entiteter som är skyldiga att utföra hotbildsstyrd penetrationstestning, får en behörig myndighet delegera vissa eller alla av de uppgifter som avses i denna artikel och artikel 27 till en annan nationell myndighet inom den finansiella sektorn.

11. De europeiska tillsynsmyndigheterna ska, i samförstånd med ECB, utarbeta gemensamma förslag till tekniska standarder för tillsyn i enlighet med TIBER-EU-ramen i syfte att närmare specificera

a) de kriterier som används för tillämpningen av punkt 8 andra stycket,

b) kraven och standarderna för användning av interna testare

c) kraven i fråga om

   i) omfattningen av den hotbildsstyrda penetrationstestning som avses i punkt 2,

   ii) den testmetod och det tillvägagångssätt som ska följas för varje specifik fas i testprocessen,

   iii) testningens resultat och avslutnings- och åtgärdsfaser,

d) den typ av tillsynssamarbete och annat relevant samarbete som krävs för genomförandet av hotbildsstyrd penetrationstestning och för underlättande av det ömsesidiga erkännandet av sådan testning när det gäller finansiella entiteter som är verksamma i mer än en medlemsstat, för att det ska gå att införa lämplig nivå av tillsynsengagemang och ett flexibelt genomförande i syfte att ta hänsyn till särdragen hos finansiella delsektorer eller lokala finansmarknader.

När de europeiska tillsynsmyndigheterna utvecklar dessa förslag till tekniska standarder för tillsyn ska de ta vederbörlig hänsyn till eventuella särdrag som härrör från den särskilda karaktären på verksamheten i olika sektorer för finansiella tjänster.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 27

Krav för testare vid utförandet av hotbildsstyrd penetrationstestning

1. Finansiella entiteter ska endast utföra sådana testare för att utföra hotbildsstyrd penetrationstestning som

a) är allra bäst lämpade och har högst anseende,

b) har teknisk och organisatorisk kapacitet och uppvisar särskild sakkunskap om underrättelser om hot, penetrationstestning och red-team-testning,

c) har certifierats av ett ackrediteringsorgan i en medlemsstat eller ansluter sig till formella uppförandekoder eller etiska ramar,

d) lämnar en oberoende försäkran eller en revisionsberättelse om sund riskhantering i samband med utförandet av hotbildsstyrd penetrationstestning, inbegripet relevant skydd av den finansiella entitetens konfidentiella information och ersättning för den finansiella entitetens affärsrisker,

e) har en relevant och heltäckande ansvarsförsäkring som omfattar risker för fel och försummelser i yrkesutövningen.

2. Vid användandet av interna testare ska finansiella entiteter säkerställa att, utöver villkoren i punkt 1, följande villkor är uppfyllda:

a) Sådan användning av dem har godkänts av den relevanta behöriga myndigheten eller av den enda offentliga myndighet som utsetts i enlighet med artikel 26.9 och 26.10.

b) Den relevanta behöriga myndigheten har verifierat att den finansiella entiteten har avsatt tillräckliga resurser och säkerställt att intressekonflikter kan undvikas under testets utformning och genomförande.

c) Leverantören av underrättelser om hot är extern i förhållande till den finansiella entiteten.

3. Finansiella entiteter ska se till att avtal som ingås med externa testare innehåller krav på en sund förvaltning av resultaten av den hotbildsstyrda penetrationstestningen och att all databehandling av dem, inbegripet generering, lagring, aggregering, utkast, rapportering, kommunikation eller förstörelse, inte skapar risker för den finansiella entiteten.

KAPITEL V

Hantering av IKT-tredjepartsrisker

Avsnitt I

Huvudprinciper för en sund hantering av IKT-tredjepartsrisker

Artikel 28

Allmänna principer

1. Finansiella entiteter ska hantera IKT-tredjepartsrisker som en integrerad del av IKT-risken inom sin IKT-riskhanteringsram som avses i artikel 6.1, och i enlighet med följande principer:

a) De finansiella entiteter som har ingått ett kontraktsmässigt arrangemang om användningen av IKT-tjänster för att bedriva sin affärsverksamhet ska alltid ha det fulla ansvaret för uppfyllandet och fullgörandet av alla skyldigheter enligt denna förordning och tillämplig rätt avseende finansiella tjänster.

b) Finansiella entiteters hantering av IKT-tredjepartsrisker ska genomföras med hänsyn till proportionalitetsprincipen, med beaktande av

i) IKT-relaterade beroendens karaktär, omfattning, komplexitet och betydelse,

ii) de risker som uppstår till följd av kontraktsmässiga arrangemang om användningen av IKT-tjänster som har ingåtts med tredjepartsleverantörer av IKT-tjänster, med hänsyn till den kritikaliteten eller betydelsen av respektive tjänst, process eller funktion, och den potentiella inverkan på kontinuiteten och tillgängligheten hos finansiella tjänster och verksamheter, på individuell nivå och på koncernnivå.

2. Som en del av sin IKT-riskhanteringsram ska andra finansiella entiteter än de enheter som avses i artikel 16.1 första stycket och mikroföretag anta och regelbundet se över en strategi för IKT-tredjepartsrisk, med beaktande av den strategi för flera olika leverantörer som avses i artikel 6.9 i tillämpliga fall. Strategin för IKT-tredjepartsrisk ska omfatta riktlinjer för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster och ska tillämpas individuellt och, i förekommande fall, på undergrupps- och gruppnivå. Ledningsorganet ska, baserat på en bedömning av den finansiella entitetens allmänna riskprofil samt omfattningen av och komplexiteten i entitetens affärstjänster, regelbundet se över de risker som har identifierats vad gäller kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner.

3. Som en del av sin IKT-riskhanteringsram ska finansiella entiteter upprätthålla och uppdatera ett register med information på entitetsnivå, undergrupps- och gruppnivå om alla kontraktsmässiga arrangemang som rör användningen av IKT-tjänster som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.

De kontraktsmässiga arrangemang som avses i första stycket ska dokumenteras på lämpligt sätt, varvid åtskillnad ska göras mellan de kontraktsmässiga arrangemang som omfattar kritiska eller viktiga funktioner och de som inte gör det.

Finansiella entiteter ska minst en gång per år rapportera till de behöriga myndigheterna om antalet nya arrangemang för användningen av IKT-tjänster, kategorierna av tredjepartsleverantörer av IKT-tjänster, typen av kontraktsmässigt arrangemang och de IKT-tjänster och funktioner som tillhandahålls.

Finansiella entiteter ska på begäran ge den behöriga myndigheten tillgång till det fullständiga registret eller angivna avsnitt av registret, tillsammans med all information som anses nödvändig för att möjliggöra en effektiv tillsyn av den finansiella entiteten.

Finansiella entiteter ska i god tid informera den behöriga myndigheten om eventuella planerade kontraktsmässiga arrangemang för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner samt när en funktion har blivit kritisk eller viktig.

4. Innan finansiella entiteter ingår ett kontraktsmässigt arrangemang om användning av IKT-tjänster ska de

a) bedöma om det kontraktsmässiga arrangemanget omfattar användningen av IKT-tjänster som stöder en kritisk eller viktig funktion,

b) bedöma om tillsynsvillkoren för utkontraktering är uppfyllda,

c) identifiera och bedöma alla relevanta risker i samband med det kontraktsmässiga arrangemanget, inbegripet möjligheten att sådana kontraktsmässiga arrangemang kan bidra till att förstärka IKT-koncentrationsrisken enligt artikel 29,

d) genomföra all due diligence-granskning av potentiella tredjepartsleverantörer av IKT-tjänster och under urvals- och bedömningsprocesserna se till att tredjepartsleverantören av IKT-tjänster är lämplig,

e) identifiera och bedöma intressekonflikter som det kontraktsmässiga arrangemanget kan orsaka.

5. Finansiella entiteter får endast ingå kontraktsmässiga arrangemang med tredjepartsleverantörer av IKT-tjänster som uppfyller lämpliga standarder för informationssäkerhet. När dessa kontraktsmässiga arrangemang gäller kritiska eller viktiga funktioner ska finansiella entiteter, innan de ingår arrangemangen, vederbörligen beakta huruvida tredjepartsleverantörerna av IKT-tjänster använder de senaste och mest högkvalitativa standarderna för informationssäkerhet.

6. När finansiella entiteter utövar åtkomst-, inspektions- och revisionsrättigheter gentemot tredjepartsleverantören av IKT-tjänster ska de baserat på en riskbaserad metod på förhand fastställa frekvensen för revisioner och inspektioner samt de områden som ska granskas genom att följa allmänt accepterade revisionsstandarder i enlighet med eventuella tillsynsinstruktioner om användning och införlivande av sådana revisionsstandarder.

Om kontraktsmässiga arrangemang som ingås med tredjepartsleverantörer av IKT-tjänster om användningen av IKT-tjänster medför hög teknisk komplexitet ska den finansiella entiteten kontrollera att revisorer, oavsett om de är interna eller externa eller ingår i en pool av revisorer, har lämpliga färdigheter och kunskaper för att effektivt kunna utföra de relevanta revisionerna och bedömningarna.

7. Finansiella entiteter ska se till att kontraktsmässiga arrangemang om användning av IKT-tjänster kan avslutas under någon av följande omständigheter:

a) Tredjepartsleverantören av IKT-tjänster bryter på ett betydande sätt mot tillämpliga lagar, förordningar eller avtalsvillkor.

b) Omständigheter har identifierats under övervakningen av IKT-tredjepartsrisker som bedöms kunna ändra prestandan hos de funktioner som tillhandahålls genom det kontraktsmässiga arrangemanget, inbegripet väsentliga förändringar som påverkar arrangemanget eller situationen för tredjepartsleverantören av IKT-tjänster.

c) IKT-tredjepartsleverantören har påvisade svagheter vad gäller sin övergripande IKT-riskhantering och i synnerhet det sätt på vilket den säkerställer tillgänglighet, äkthet, integritet och konfidentialitet för data, oavsett om det är personuppgifter eller på annat sätt känsliga uppgifter eller icke-personuppgifter.

d) Om den behöriga myndigheten inte längre effektivt kan utöva tillsyn över den finansiella entiteten till följd av villkoren i eller omständigheter relaterade till respektive kontraktsmässiga arrangemang.

8. När det gäller IKT-tjänster som stöder kritiska eller viktiga funktioner ska finansiella entiteter införa exitstrategier. Exitstrategierna ska ta hänsyn till risker som kan uppstå hos tredjepartsleverantörerna av IKT-tjänster, i synnerhet eventuella fel hos dessa, försämring av kvaliteten på de IKT-tjänster som tillhandahålls, eventuella avbrott i verksamheten på grund av olämpligt eller misslyckat tillhandahållande av IKT-tjänster eller eventuella väsentliga risker som uppstår i samband med en lämplig och kontinuerlig användning av respektive IKT-tjänst, eller uppsägning av kontraktsmässiga arrangemang med tredjepartsleverantörer av IKT-tjänster under någon av de omständigheter som anges i punkt 7.

Finansiella entiteter ska säkerställa att de kan säga upp kontraktsmässiga arrangemang utan

a) avbrott i sin affärsverksamhet,

b) begränsning av efterlevnaden av lagstadgade krav,

c) skada på kontinuiteten och kvaliteten hos de tjänster som tillhandahålls kunder.

Exitplanerna ska vara heltäckande och dokumenterade och de ska, i enlighet med kriterierna i artikel 4.2, vara tillräckligt testade och ska regelbundet ses över.

Finansiella entiteter ska identifiera alternativa lösningar och utarbeta övergångsplaner som gör det möjligt för dem att avlägsna de kontrakterade IKT-tjänsterna och relevanta data från tredjepartsleverantören av IKT-tjänster och på ett säkert och fullständigt sätt överföra dem till alternativa leverantörer eller återintegrera dem internt.

Finansiella entiteter ska ha lämpliga beredskapsåtgärder på plats för att upprätthålla kontinuiteten i verksamheten vid uppkomst av de omständigheter som avses i första stycket.

9. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för genomförande för att fastställa standardmallar för det register över uppgifter som avses i punkt 3, inbegripet uppgifter som är gemensamma för alla kontraktsmässiga arrangemang om användning av IKT-tjänster. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för genomförande till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att anta de tekniska standarder för genomförande som avses i första stycket i enlighet med artikel 15 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

10. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera det detaljerade innehållet i de riktlinjer som avses i punkt 2 i fråga om de kontraktsmässiga arrangemangen för användningen av IKT-tjänster som stöder kritiska eller viktiga funktioner och som tillhandahålls av tredjepartsleverantörer av IKT-tjänster.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 januari 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 29

Preliminär bedömning av IKT-koncentrationsrisker på entitetsnivå

1. När finansiella entiteter utför den identifiering och bedömning av risk som avses i artikel 28.4 c ska de även ta hänsyn till om det planerade ingåendet av ett kontraktsmässigt arrangemang avseende IKT-tjänster som stöder kritiska eller viktiga funktioner skulle leda till något av följande:

a) Avtal med en tredjepartsleverantör av IKT-tjänster som inte är lätt utbytbar.

b) Flera kontraktsmässiga arrangemang gällande tillhandahållande av IKT-tjänster som stöder kritiska eller viktiga funktioner med samma tredjepartsleverantör av IKT-tjänster eller med nära anknutna tredjepartsleverantörer av IKT-tjänster.

Finansiella entiteter ska väga fördelarna och kostnaderna med alternativa lösningar, t.ex. användning av olika tredjepartsleverantörer av IKT-tjänster, med hänsyn till om och hur planerade lösningar motsvarar de affärsbehov och mål som anges i deras strategi för digital motståndskraft.

2. Om de kontraktsmässiga arrangemangen om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner inbegriper möjligheten att en tredjepartsleverantör av IKT-tjänster lägger ut IKT-tjänster som stöder kritisk eller viktig funktion på underentreprenad till andra tredjepartsleverantörer av IKT-tjänster, ska finansiella entiteter väga de fördelar och risker som kan uppstå i samband med en sådan underentreprenad, särskilt när det gäller en IKT-underleverantör som är etablerad i ett tredjeland.

Om de kontraktsmässiga arrangemangen gäller IKT-tjänster som stöder kritiska eller viktiga funktioner ska finansiella entiteter vederbörligen ta hänsyn till de insolvensrättsliga bestämmelser som skulle vara tillämpliga om IKT-tjänsteleverantören går i konkurs samt eventuella begränsningar som kan uppstå när det gäller skyndsam återställning av den finansiella entitetens data.

Om kontraktsmässiga arrangemang om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner ingås med en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland ska finansiella entiteter utöver de hänsynstaganden som avses i andra stycket även beakta överensstämmelsen med unionens dataskyddsregler och den faktiska efterlevnaden av rätten i det tredjelandet.

Om de kontraktsmässiga arrangemangen om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner medger underentreprenad, ska finansiella entiteter bedöma om och hur potentiellt långa eller komplexa underentreprenadskedjor kan påverka deras förmåga att till fullo övervaka de avtalade funktionerna och den behöriga myndighetens förmåga att effektivt övervaka den finansiella entiteten i detta avseende.

Artikel 30

Viktiga avtalsbestämmelser

1. Rättigheterna och skyldigheterna för den finansiella entiteten och tredjepartsleverantören av IKT-tjänster ska vara tydligt fördelade och skriftligen angivna. Det fullständiga avtalet ska omfatta servicenivåavtalen och dokumenteras i ett skriftligt dokument som parterna ska ha tillgång till på papper eller i ett dokument med ett annat nedladdningsbart, varaktigt och tillgängligt format.

2. De kontraktsmässiga arrangemangen för användning av IKT-tjänster ska innehålla åtminstone följande delar:

a) En tydlig och fullständig beskrivning av alla funktioner och IKT-tjänster som ska tillhandahållas av tredjepartsleverantören av IKT-tjänster, med uppgift om huruvida underentreprenad av en IKT-tjänst som stöder en kritisk eller viktig funktion eller väsentliga delar därav, är tillåten och, när så är fallet, de villkor som gäller för sådan underentreprenad.

b) De platser, nämligen regioner eller länder, där de funktioner och IKT-tjänster som har utkontrakterats eller lagts ut på underentreprenad ska tillhandahållas och var uppgifterna ska behandlas, inklusive lagringsplatsen, och ett krav på att tredjepartsleverantören av IKT-tjänster på förhand ska underrätta den finansiella entiteten om den planerar att ändra sådana platser.

c) Bestämmelser om tillgänglighet, äkthet, integritet och konfidentialitet vad gäller skydd av data, inbegripet personuppgifter.

d) Bestämmelser om säkerställande av åtkomst, återställande och återlämnande i ett lättillgängligt format av personuppgifter och andra uppgifter än personuppgifter som behandlas av den finansiella entiteten i händelse av insolvens, resolution eller nedläggning av verksamheten vad avser tredjepartsleverantören av IKT-tjänster, eller i händelse av uppsägning av de kontraktsmässiga arrangemangen.

e) Beskrivningar av servicenivå, inbegripet uppdateringar och revideringar av dessa.

f) Skyldigheten för tredjepartsleverantören av IKT-tjänster att tillhandahålla assistans till den finansiella entiteten utan extra kostnad, eller till en kostnad som fastställs på förhand, när en IKT-incident med anknytning till den IKT-tjänst som tillhandahålls den finansiella entiteten inträffar.

g) Skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut med de behöriga myndigheterna och resolutionsmyndigheterna för den finansiella entiteten, inbegripet personer som har utsetts av dem.

h) Uppsägningsrätt och tillhörande minsta uppsägningstid för uppsägning av det kontraktsmässiga arrangemanget, i enlighet med de behöriga myndigheternas och resolutionsmyndigheternas förväntningar.

i) Villkoren för deltagande av tredjepartsleverantörer av IKT-tjänster i finansiella entiteters program för medvetenhet om IKT-säkerhet och utbildning om digital operativ motståndskraft i enlighet med artikel 13.6.

3. De kontraktsmässiga arrangemangen om användning av IKT-tjänster som stöder kritiska eller viktiga funktioner ska, utöver de delar som avses i punkt 2, innehålla åtminstone följande:

a) Beskrivningar av fullständig servicenivå, inklusive uppdateringar och revideringar av dessa, med exakta kvantitativa och kvalitativa prestationsmål inom de överenskomna servicenivåerna för att göra det möjligt för den finansiella entiteten att effektivt övervaka IKT-tjänster och göra det möjligt att utan onödigt dröjsmål vidta lämpliga korrigerande åtgärder när överenskomna servicenivåer inte uppnås.

b) Anmälningsperioder och rapporteringsskyldigheter för tredjepartsleverantören av IKT-tjänster till den finansiella entiteten, inbegripet underrättelse om varje händelse som kan ha en väsentlig inverkan på IKT-tredjepartsleverantörens förmåga att effektivt tillhandahålla IKT-tjänster som stöder kritiska eller viktiga funktioner i linje med överenskomna servicenivåer.

c) Krav på att tredjepartsleverantören av IKT-tjänster ska genomföra och testa beredskapsplaner för verksamheten och ha infört IKT-säkerhetsåtgärder, IKT-verktyg och IKT-strategier som ger en lämplig säkerhetsnivå vid tillhandahållande av tjänster från den finansiella entitetens sida i enlighet med dess regelverk.

d) Skyldigheten för tredjepartsleverantören av IKT-tjänster att delta och fullt ut samarbeta i den finansiella entitetens hotbildsstyrda penetrationstestning enligt artiklarna 26 och 27.

e) Rätten att fortlöpande övervaka prestandan hos tredjepartsleverantören av IKT-tjänster, vilket omfattar följande:

i) Obegränsad rätt till tillgång till, inspektion och revision för den finansiella entiteten eller en utsedd tredjepart, och för den behöriga myndigheten, och rätt att ta kopior av relevant dokumentation på plats om de är kritiska för verksamheten hos tredjepartsleverantören av IKT-tjänster, vars faktiska utövande inte hindras eller begränsas av andra kontraktsmässiga arrangemang eller strategier för genomförande.

ii) Rätten att komma överens om alternativa garantinivåer om andra kunders rättigheter påverkas.

iii) Skyldigheten för tredjepartsleverantören av IKT-tjänster att samarbeta fullt ut under de inspektioner och revisioner på plats som utförs av de behöriga myndigheterna, den ledande tillsynsmyndigheten, den finansiella entiteten eller en utsedd tredjepart.

iv) Skyldigheten att tillhandahålla närmare uppgifter om omfattningen, de förfaranden som ska följas och frekvensen för sådana inspektioner och revisioner.

f) Exitstrategier, särskilt inrättande av en obligatorisk lämplig övergångsperiod

i) under vilken tredjepartsleverantören av IKT-tjänster kommer att fortsätta att tillhandahålla respektive funktioner eller IKT-tjänster i syfte att minska risken för avbrott hos den finansiella entiteten, eller säkerställa en effektiv resolution och omstrukturering av denna,

ii) som gör det möjligt för den finansiella entiteten att migrera till en annan tredjepartsleverantör av IKT-tjänster eller byta till interna lösningar som är förenliga med komplexiteten hos den tillhandahållna tjänsten.

Genom undantag från led e får tredjepartsleverantören av IKT-tjänster och en finansiell entitet som är ett mikroföretag komma överens om att den finansiella entitetens rätt till tillgång, inspektion och revision kan delegeras till en oberoende tredjepart som utsetts av tredjepartsleverantören av IKT-tjänster, och att den finansiella entiteten när som helst kan begära information och försäkran om IKT-tredjepartsleverantörens prestanda från den tredje parten.

4. När finansiella entiteter och tredjepartsleverantörer av IKT-tjänster förhandlar om kontraktsmässiga arrangemang ska de överväga att använda standardavtalsklausuler som har utarbetats av offentliga myndigheter för specifika tjänster.

5. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att närmare specificera de delar som avses i punkt 2 a och som en finansiell entitet måste fastställa och bedöma när den lägger ut IKT-tjänster som stöder kritiska eller viktiga funktioner på underentreprenad.

När de europeiska tillsynsmyndigheterna utarbetar dessa förslag till tekniska standarder för tillsyn ska de ta hänsyn till den finansiella entitetens storlek och allmänna riskprofil, och karaktären på, omfattningen av och komplexiteten i dess tjänster, verksamhet och insatser.

De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i första stycket i enlighet med artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Avsnitt II

Tillsynsram för kritiska tredjepartsleverantörer av IKT-tjänster

Artikel 31

Klassificering av tredjepartsleverantörer av IKT-tjänster som kritiska

1. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och på rekommendation av det tillsynsforum som har inrättats enligt artikel 32.1,

a) klassificera tredjepartsleverantörer av IKT-tjänster som kritiska för finansiella entiteter, efter en bedömning som tar hänsyn till de kriterier som anges i punkt 2,

b) utse till ledande tillsynsmyndighet för varje kritisk tredjepartsleverantör av IKT-tjänster den europeiska tillsynsmyndighet som är ansvarig enligt förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 eller (EU) nr 1095/2010 för de finansiella entiteter som tillsammans har den största andelen av de totala tillgångarna av värdet av de totala tillgångarna hos alla finansiella entiteter som utnyttjar tjänster från den relevanta kritiska tredjepartsleverantören av IKT-tjänster, i enlighet med vad som framgår av summan av dessa finansiella entiteters enskilda balansräkningar.

2. Den klassificering som avses i punkt 1 a ska baseras på samtliga följande kriterier när det gäller IKT-tjänster som tillhandahålls av tredjepartsleverantören av IKT-tjänster:

a) Systempåverkan på stabiliteten, kontinuiteten eller kvaliteten på tillhandahållandet av finansiella tjänster om den berörda tredjepartsleverantören av IKT-tjänster skulle drabbas av ett omfattande driftsavbrott i tillhandahållandet av tjänster, med tanke på antalet finansiella entiteter och det totala värdet av tillgångarna hos de finansiella entiteter som den berörda tredjepartsleverantören av IKT-tjänster tillhandahåller tjänster till.

b) Påverkan på eller betydelsen för systemet av de finansiella entiteter som är beroende av den berörda tredjepartsleverantören av IKT-tjänster, bedömt enligt följande parametrar:

   i) Antalet globala systemviktiga institut eller andra systemviktiga institut som är beroende av respektive tredjepartsleverantör av IKT-tjänster.

   ii) Det ömsesidiga beroendet mellan de globala systemviktiga institut eller andra systemviktiga institut som avses i led i och andra finansiella entiteter, inbegripet situationer där de globala systemviktiga instituten eller andra systemviktiga instituten tillhandahåller finansiella infrastrukturtjänster till andra finansiella entiteter.

c) Finansiella entiteters beroende av de tjänster som tillhandahålls av den berörda tredjepartsleverantören av IKT-tjänster i förhållande till kritiska eller viktiga funktioner hos de finansiella entiteter som i sista hand involverar samma tredjepartsleverantör av IKT-tjänster, oavsett om finansiella entiteter direkt eller indirekt är beroende av dessa tjänster, med hjälp av eller genom underleverantörsavtal.

d) Graden av utbytbarhet hos tredjepartsleverantören av IKT-tjänster, med beaktande av följande parametrar:

   i) Avsaknad av verkliga alternativ, även delvis, på grund av det begränsade antalet tredjepartsleverantörer av IKT-tjänster som är verksamma på en viss marknad, eller marknadsandelen för den berörda tredjepartsleverantören av IKT-tjänster, eller den tekniska komplexiteten eller avancerade karaktären, inbegripet i förhållande till eventuell proprietär teknik, eller särdragen hos IKT-tredjepartsleverantörens organisation eller verksamhet.

   ii) Svårigheter när det gäller att helt eller delvis migrera relevanta data och arbetsbelastningar från den berörda tredjepartsleverantören av IKT-tjänster till en annan tredjepartsleverantör av IKT-tjänster, på grund av betydande finansiella kostnader, tidsåtgång eller andra resurser som migrationsprocessen kan medföra, eller på grund av ökad IKT-risk eller andra operativa risker som den finansiella entiteten kan utsättas för genom sådan migration.

3. Om tredjepartsleverantören av IKT-tjänster ingår i en koncern ska de kriterier som avses i punkt 2 beaktas vad avser de IKT-tjänster som koncernen som helhet tillhandahåller.

4. Kritiska tredjepartsleverantörer av IKT-tjänster som ingår i en koncern ska utse en juridisk person till samordningspunkt för att säkerställa lämplig representation och kommunikation med den ledande tillsynsmyndigheten.

5. Den ledande tillsynsmyndigheten ska underrätta tredjepartsleverantören av IKT-tjänster om resultatet av den bedömning som leder till den klassificering som avses i punkt 1 a. Inom sex veckor från dagen för anmälan får tredjepartsleverantören av IKT-tjänster lämna in ett motiverat uttalande till den ledande tillsynsmyndigheten med all relevant information för bedömningen. Den ledande tillsynsmyndigheten ska beakta det motiverade uttalandet och får begära att ytterligare information lämnas inom 30 kalenderdagar efter mottagandet av ett sådant uttalande.

Efter att ha klassificerat en tredjepartsleverantör av IKT-tjänster som kritisk ska de europeiska tillsynsmyndigheterna, genom den gemensamma kommittén, underrätta tredjepartsleverantören av IKT-tjänster om klassificeringen och från och med vilket datum tredjepartsleverantören faktiskt kommer att omfattas av tillsynsverksamhet. Detta startdatum ska inträffa senast en månad efter anmälan. Tredjepartsleverantören av IKT-tjänster ska underrätta de finansiella entiteter som den tillhandahåller tjänster om att den klassificeras som kritisk.

6. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 57 för att komplettera denna förordning genom att närmare specificera kriterierna i punkt 2 i den här artikeln senast den 17 juli 2024.

7. Den klassificering som avses i punkt 1 a får inte användas förrän kommissionen har antagit en delegerad akt i enlighet med punkt 6.

8. Den klassificering som avses i punkt 1 a får inte tillämpas på följande:

i) Finansiella entiteter som tillhandahåller IKT-tjänster till andra finansiella entiteter.

ii) Tredjepartsleverantörer av IKT-tjänster som omfattas av tillsynsramar som har inrättats till stöd för de uppgifter som avses i artikel 127.2 i fördraget om Europeiska unionens funktionssätt.

iii) Koncerninterna IKT-tjänsteleverantörer.

iv) Tredjepartsleverantörer av IKT-tjänster som endast tillhandahåller IKT-tjänster i en medlemsstat till finansiella entiteter som endast är verksamma i den medlemsstaten.

9. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén upprätta, offentliggöra och årligen uppdatera förteckningen över kritiska tredjepartsleverantörer av IKT-tjänster på unionsnivå.

10. Vid tillämpning av punkt 1 a ska de behöriga myndigheterna årligen och i aggregerad form översända de rapporter som avses i artikel 28.3 tredje stycket till det tillsynsforum som har inrättats enligt artikel 32. Tillsynsforumet ska bedöma finansiella entiteters IKT-beroende gentemot tredjepart baserat på den information som har mottagits från de behöriga myndigheterna.

11. De tredjepartsleverantörer av IKT-tjänster som inte ingår i den förteckning som avses i punkt 9 får begära att bli klassificerade som kritiska i enlighet med punkt 1 a.

Vid tillämpning av första stycket ska tredjepartsleverantören av IKT-tjänster lämna in en motiverad ansökan till EBA, Esma eller Eiopa, som genom den gemensamma kommittén ska besluta huruvida den tredjepartsleverantören av IKT-tjänster ska klassificeras som kritisk i enlighet med punkt 1 a.

Det beslut som avses i andra stycket ska antas och meddelas tredjepartsleverantören av IKT-tjänster inom sex månader från mottagandet av ansökan.

12. Finansiella entiteter ska endast använda sig av de tjänster som en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland och som har klassificerats som kritisk i enlighet med punkt 1 a erbjuder om den har etablerat ett dotterföretag i unionen inom tolv månader efter klassificeringen.

13. Den kritiska tredjepartsleverantör av IKT-tjänster som avses i punkt 12 ska underrätta den ledande tillsynsmyndigheten om eventuella ändringar av ledningsstrukturen för det dotterföretag som är etablerat i unionen.

Artikel 32

Tillsynsramens struktur

1. Den gemensamma kommittén ska i enlighet med artikel 57.1 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010, inrätta tillsynsforumet som en underkommitté för att stödja arbetet i den gemensamma kommittén och i den ledande tillsynsmyndighet som avses i artikel 31.1 b inom området för IKT-tredjepartsrisker i alla finansiella sektorer. Tillsynsforumet ska utarbeta utkast till gemensamma ståndpunkter och utkast till gemensamma akter från den gemensamma kommittén på detta område.

Tillsynsforumet ska regelbundet diskutera relevant utveckling när det gäller IKT-risk och IKT-sårbarheter och främja en konsekvent strategi för övervakning av IKT-tredjepartsrisk på unionsnivå.

2. Tillsynsforumet ska årligen göra en gemensam bedömning av resultaten och slutsatserna av den tillsynsverksamhet som genomförts för alla kritiska tredjepartsleverantörer av IKT-tjänster och främja samordningsåtgärder för att öka finansiella entiteters digitala operativa motståndskraft, främja bästa praxis för hantering av IKT-koncentrationsrisker och undersöka riskreducerande åtgärder för sektorsövergripande risköverföring.

3. Tillsynsforumet ska lägga fram heltäckande referensvärden för kritiska tredjepartsleverantörer av IKT-tjänster som ska antas av den gemensamma kommittén i form av gemensamma ståndpunkter från de europeiska tillsynsmyndigheterna i enlighet med artikel 56.1 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

4. Tillsynsforumet ska bestå av följande:

a) Ordförandena för de europeiska tillsynsmyndigheterna.

b) En företrädare på hög nivå för den tjänstgörande personalen på den relevanta behöriga myndighet som avses i artikel 46 i varje medlemsstat.

c) De verkställande direktörerna för varje europeisk tillsynsmyndighet och en företrädare för kommissionen, ESRB, ECB och Enisa som observatörer.

d) När så är lämpligt, ytterligare en företrädare från en behörig myndighet som avses i artikel 46 i varje medlemsstat som observatör.

e) I tillämpliga fall, en företrädare från de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster som observatör.

Tillsynsforumet får, när så är lämpligt, rådfråga oberoende experter som utsetts i enlighet med punkt 6.

5. Varje medlemsstat ska utse den relevanta behöriga myndighet vars anställde ska vara den företrädare på hög nivå som avses i punkt 4 första stycket b, och ska informera den ledande tillsynsmyndigheten om detta.

De europeiska tillsynsmyndigheterna ska på sin webbplats offentliggöra förteckningen över de företrädare på hög nivå från den befintliga personalen vid den relevanta behöriga myndigheten som utsetts av medlemsstaterna.

6. De oberoende experter som avses i punkt 4 andra stycket ska utses av tillsynsforumet bland en pool av experter som väljs ut efter ett offentligt och transparent ansökningsförfarande.

De oberoende experterna ska utses baserat på sin sakkunskap om finansiell stabilitet, digital operativ motståndskraft och IKT-säkerhet. De ska handla oberoende och objektivt och uteslutande i hela unionens intresse och varken begära eller ta emot instruktioner från unionens institutioner eller organ, regeringen i någon medlemsstat eller något annat offentligt eller privat organ.

7. I enlighet med artikel 16 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 ska de europeiska tillsynsmyndigheterna senast den 17 juli 2024 vid tillämpningen av detta avsnitt utfärda riktlinjer för samarbetet mellan de europeiska tillsynsmyndigheterna och de behöriga myndigheterna som omfattar detaljerade förfaranden och villkor för fördelningen och utförandet av uppgifter mellan behöriga myndigheter och de europeiska tillsynsmyndigheterna och närmare uppgifter om det informationsutbyte som är nödvändiga för att de behöriga myndigheterna ska kunna säkerställa uppföljningen av de rekommendationer som riktas till kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 35.1 d.

8. De krav som fastställs i detta avsnitt ska inte påverka tillämpningen av direktiv (EU) 2022/2555 och andra unionsregler om tillsyn som är tillämpliga på leverantörer av molntjänster.

9. De europeiska tillsynsmyndigheterna ska, genom den gemensamma kommittén och på grundval av det förberedande arbete som utförs av tillsynsforumet, varje år lägga fram en rapport om tillämpningen av detta avsnitt för Europaparlamentet, rådet och kommissionen.

Artikel 33

Den ledande tillsynsmyndighetens uppgifter

1. Den ledande tillsynsmyndigheten, som utsetts i enlighet med artikel 31.1 b, ska utöva tillsyn över de kritiska tredjepartsleverantörer av IKT-tjänster som den tilldelats och ska, när det gäller alla frågor som rör tillsynen, vara den huvudsakliga kontaktpunkten för dessa kritiska tredjepartsleverantörer av IKT-tjänster.

2. Vid tillämpning av punkt 1 ska den ledande tillsynsmyndigheten bedöma huruvida varje kritisk tredjepartsleverantör av IKT-tjänster har infört heltäckande, sunda och effektiva regler, förfaranden, mekanismer och arrangemang för att hantera den IKT-risk som den kan medföra för finansiella entiteter.

Den bedömning som avses i första stycket ska huvudsakligen inriktas på IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantör av IKT-tjänster som stöder finansiella entiteters kritiska eller viktiga funktioner. Om det är nödvändigt för att hantera alla relevanta risker ska den bedömningen även omfatta IKT-tjänster som stöder andra funktioner än de som är kritiska eller viktiga.

3. Den bedömning som avses i punkt 2 ska omfatta:

a) IKT-krav för att i synnerhet säkerställa säkerhet, tillgänglighet, kontinuitet, skalbarhet och kvalitet hos de tjänster som den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller finansiella entiteter, samt förmåga att alltid upprätthålla höga standarder för tillgänglighet, äkthet, integritet eller konfidentialitet.

b) Den fysiska säkerhet som bidrar till att säkerställa IKT-säkerheten, inbegripet säkerheten i lokaler, anläggningar och datacenter.

c) Riskhanteringsprocesser, inbegripet IKT-riskhanteringsstrategier, IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT.

d) Styrformer, inbegripet en organisationsstruktur med tydliga, transparenta och konsekventa regler för ansvar och ansvarsskyldighet som möjliggör en effektiv IKT-riskhantering.

e) Identifiering, övervakning och snabb rapportering av väsentliga IKT-relaterade incidenter till finansiella entiteter, hantering och avhjälpande av dessa incidenter, särskilt cyberangrepp.

f) Mekanismer för dataportabilitet, tillämpningsportabilitet och interoperabilitet, som säkerställer att finansiella entiteter effektivt kan utöva sin uppsägningsrätt.

g) Testning av IKT-system, IKT-infrastruktur och IKT-kontroller.

h) IKT-revisioner.

i) Användning av relevanta nationella och internationella standarder som är tillämpliga på tillhandahållandet av leverantörens IKT-tjänster till finansiella entiteter.

4. Baserat på den bedömning som avses i punkt 2, och i samordning med det gemensamma tillsynsnätverk som avses i artikel 34.1, ska den ledande tillsynsmyndigheten anta en tydlig, detaljerad och motiverad individuell tillsynsplan med en beskrivning av de årliga tillsynsmålen och de huvudsakliga tillsynsinsatser som planeras för varje kritisk tredjepartsleverantör av IKT-tjänster. Planen ska varje år meddelas den kritiska tredjepartsleverantören av IKT-tjänster.

Innan tillsynsplanen antas ska den ledande tillsynsmyndigheten överlämna utkastet till tillsynsplan till den kritiska tredjepartsleverantören av IKT-tjänster.

Vid mottagandet av utkastet till tillsynsplan får den kritiska tredjepartsleverantören av IKT-tjänster lämna in ett motiverat uttalande inom 15 kalenderdagar som dels styrker den förväntade inverkan på de kunder som är entiteter som faller utanför denna förordnings tillämpningsområde och dels, i förekommande fall, formulerar lösningar för att minska riskerna.

5. När de årliga tillsynsplaner som avses i punkt 4 har antagits och anmälts till de kritiska tredjepartsleverantörerna av IKT-tjänster får de behöriga myndigheterna vidta åtgärder avseende sådana kritiska tredjepartsleverantörer av IKT-tjänster endast i samförstånd med den ledande tillsynsmyndigheten.

Artikel 34

Operativ samordning mellan ledande tillsynsmyndigheter

1. För att säkerställa ett konsekvent tillvägagångssätt för tillsynsverksamheten och i syfte att möjliggöra samordnade allmänna tillsynsstrategier och sammanhängande operativa tillvägagångssätt och arbetsmetoder, ska de tre ledande tillsynsmyndigheter som utsetts i enlighet med artikel 31.1 b inrätta ett gemensamt tillsynsnätverk för att sinsemellan samordna de förberedande faserna och samordna genomförandet av tillsynsverksamheten för de respektive kritiska tredjepartsleverantörer av IKT-tjänster som de granskar, samt inom ramen för eventuella åtgärder som kan behövas enligt artikel 42.

2. Vid tillämpning av punkt 1 ska de ledande tillsynsmyndigheterna utarbeta ett gemensamt tillsynsprotokoll som anger de detaljerade förfaranden som ska följas för den dagliga samordningen och för att säkerställa snabba utbyten och reaktioner. Protokollet ska regelbundet ses över för att återspegla de operativa behoven, särskilt utvecklingen av arrangemangen för den praktiska tillsynen.

3. De ledande tillsynsmyndigheterna får från fall till fall uppmana ECB och Enisa att tillhandahålla teknisk rådgivning, dela med sig av praktiska erfarenheter eller delta i specifika samordningsmöten för det gemensamma tillsynsnätverket.

Artikel 35

Den ledande tillsynsmyndighetens befogenheter

1. För att fullgöra de uppgifter som anges i detta avsnitt ska den ledande tillsynsmyndigheten vad gäller de kritiska tredjepartsleverantörerna av IKT-tjänster ha befogenhet att

a) begära all relevant information och dokumentation i enlighet med artikel 37,

b) genomföra allmänna utredningar och inspektioner i enlighet med artiklarna 38 respektive 39,

c) efter det att tillsynsverksamheten har slutförts begära rapporter med angivande av de åtgärder som har vidtagits eller de avhjälpande åtgärder som har vidtagits av de kritiska tredjepartsleverantörerna av IKT-tjänster i samband med de rekommendationer som avses i led d i denna punkt,

d) utfärda rekommendationer på de områden som avses i artikel 33.3, särskilt

   i) om tillämpning av specifika IKT-säkerhets- och kvalitetskrav eller IKT-processer, särskilt i samband med införandet av programfixar, uppdateringar, kryptering och andra säkerhetsåtgärder som den ledande tillsynsmyndigheten anser vara relevanta för att säkerställa IKT-säkerheten för tjänster som tillhandahålls till finansiella entiteter,

   ii) om användning av villkor, inbegripet deras tekniska genomförande, enligt vilka kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller IKT-tjänster till finansiella entiteter, som den ledande tillsynsmyndighetens bedömer är relevanta för att förhindra uppkomsten av felkritiska systemdelar (*single points of failure*) eller en förstärkning av dessa eller för att minimera de eventuella systemeffekterna inom unionens finansiella sektor i händelse av IKT-koncentrationsrisk,

   iii) om eventuell planerad underentreprenad, när den ledande tillsynsmyndigheten bedömer att ytterligare underentreprenad, inbegripet underentreprenadsavtal som de kritiska tredjepartsleverantörerna av IKT-tjänster planerar att ingå med tredjepartsleverantörer av IKT-tjänster eller med IKT-underleverantörer som är etablerade i ett tredjeland, kan utlösa risker för den finansiella entitetens tillhandahållande av tjänster eller risker för den finansiella stabiliteten, på grundval av granskningen av den information som samlas in i enlighet med artiklarna 37 och 38,

   iv) om att avstå från att ingå ytterligare underleverantörsavtal, om följande kumulativa villkor är uppfyllda, nämligen

      — den planerade underleverantören är en tredjepartsleverantör av IKT-tjänster eller en IKT-underleverantör som är etablerad i ett tredjeland,

      — underentreprenaden avser kritiska eller viktiga funktioner hos den finansiella entiteten, och

— den ledande tillsynsmyndigheten anser att användningen av sådan underentreprenad utgör en klar och allvarlig risk för unionens finansiella stabilitet eller för finansiella entiteter, inbegripet finansiella entiteters förmåga att uppfylla tillsynskraven.

Vid tillämpning av led iv i detta led ska tredjepartsleverantörer av IKT-tjänster, med hjälp av den mall som avses i artikel 41.1 b, överföra informationen om underentreprenad till den ledande tillsynsmyndigheten.

2. Vid utövandet av de befogenheter som avses i denna artikel ska den ledande tillsynsmyndigheten

a) säkerställa regelbunden samordning inom det gemensamma tillsynsnätverket, och i synnerhet eftersträva konsekventa tillvägagångssätt, när så är lämpligt, vad gäller tillsynen av kritiska tredjepartsleverantörer av IKT-tjänster,

b) ta vederbörlig hänsyn till den ram som fastställs i direktiv (EU) 2022/2555 och vid behov samråda med de relevanta behöriga myndigheter som utsetts eller inrättats i enlighet med det direktivet, för att undvika överlappning av tekniska och organisatoriska åtgärder som skulle kunna tillämpas på kritiska tredjepartsleverantörer av IKT-tjänster enligt det direktivet,

c) sträva efter att i möjligaste mån minimera risken för avbrott i tjänster som kritiska tredjepartsleverantörer av IKT-tjänster tillhandahåller kunder som är entiteter som faller utanför denna förordnings tillämpningsområde.

3. Den ledande tillsynsmyndigheten ska samråda med tillsynsforumet innan den utövar de befogenheter som avses i punkt 1.

Innan den ledande tillsynsmyndigheten utfärdar rekommendationer i enlighet med punkt 1 d ska den ge tredjepartsleverantören av IKT-tjänster möjlighet att inom 30 kalenderdagar tillhandahålla relevant information som dels styrker den förväntade inverkan på de kunder som är entiteter som faller utanför denna förordnings tillämpningsområde och dels, i förekommande fall, formulerar lösningar för att minska riskerna.

4. Den ledande tillsynsmyndigheten ska informera det gemensamma tillsynsnätverket om resultatet av utövandet av de befogenheter som avses i punkt 1 a och b. Den ledande tillsynsmyndigheten ska utan onödigt dröjsmål översända de rapporter som avses i punkt 1 c till det gemensamma tillsynsnätverket och till de behöriga myndigheterna för de finansiella entiteter som använder de IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantören av IKT-tjänster.

5. Kritiska tredjepartsleverantörer av IKT-tjänster ska samarbeta lojalt med den ledande tillsynsmyndigheten och bistå den vid fullgörandet av dess uppgifter.

6. Den ledande tillsynsmyndigheten ska, vid helt eller delvis bristande efterlevnad av de åtgärder som ska vidtas enligt utövandet av befogenheterna i punkt 1 a, b och c och efter utgången av en period på minst 30 kalenderdagar från den dag då den kritiska tredjepartsleverantören av IKT-tjänster mottog anmälan om åtgärderna, anta ett beslut om föreläggande av vite för att tvinga den kritiska tredjepartsleverantören av IKT-tjänster att efterleva dessa åtgärder.

7. Det vite som avses i punkt 6 ska åläggas dagligen till dess att efterlevnad har uppnåtts och i högst sex månader efter det att beslutet om vite har anmälts till den kritiska tredjepartsleverantören av IKT-tjänster.

8. Vitesbeloppet, beräknat från det datum som anges i beslutet om föreläggande av vitet, ska vara upp till 1 % av den genomsnittliga globala omsättningen per dag för den kritiska tredjepartsleverantören av IKT-tjänster under det föregående räkenskapsåret. Den ledande tillsynsmyndigheten ska när den fastställer vitesbeloppet beakta följande kriterier för bristande efterlevnad av de åtgärder som avses i punkt 6:

a) Den bristande efterlevnadens allvarlighetsgrad och varaktighet.

b) Huruvida den bristande efterlevnaden är uppsåtlig eller beror på oaktsamhet.

c) Viljan hos tredjepartsleverantören av IKT-tjänster att samarbeta med den ledande tillsynsmyndigheten.

Vid tillämpning av första stycket ska den ledande tillsynsmyndigheten samråda inom det gemensamma tillsynsnätverket för att säkerställa en konsekvent strategi.

9. Vitet ska vara av administrativ karaktär och ska vara verkställbart. Verkställigheten ska följa de civilprocessrättsliga regler som gäller i den medlemsstat inom vars territorium inspektionerna och åtkomsten ska genomföras. Domstolarna i den berörda medlemsstaten ska vara behöriga att pröva klagomål som rör oegentligheter i verkställigheten. De belopp som åläggs i form av viten ska tillfalla Europeiska unionens allmänna budget.

10. Den ledande tillsynsmyndigheten ska offentliggöra alla viten som har förelagts utom i de fall då offentliggörandet skulle skapa allvarlig oro på de finansiella marknaderna eller orsaka de berörda parterna oproportionellt stor skada.

11. Innan ett vite åläggs enligt punkt 6 ska den ledande tillsynsmyndigheten ge företrädarna för den kritiska tredjepartsleverantör av IKT-tjänster som är föremål för förfarandet möjlighet att höras om de omständigheter som tillsynsmyndigheterna har påtalat, och den ska grunda sina beslut endast på omständigheter som den kritiska tredjepartsleverantören av IKT-tjänster som är föremål för förfarandet har haft möjlighet att yttra sig över.

Rätten till försvar för personer som är föremål för förfarandet ska iakttas fullt ut under förfarandet. Den kritiska tredjepartsleverantör av IKT-tjänster som är föremål för förfarandet ska ha rätt att få tillgång till ärendehandlingarna, med förbehåll för andra personers berättigade intresse av att deras affärshemligheter skyddas. Tillgången till ärendehandlingarna ska inte omfatta konfidentiella uppgifter eller ledande tillsynsmyndighetens interna förberedande handlingar.

Artikel 36

Den ledande tillsynsmyndighetens utövande av befogenheter utanför unionen

1. Om tillsynsmålen inte kan uppnås genom samverkan med det dotterföretag som har etablerats i enlighet med artikel 31.12 eller genom utövande av tillsynsverksamhet i lokaler som är belägna i unionen, får den ledande tillsynsmyndigheten utöva de befogenheter som anges i följande bestämmelser i alla lokaler som är belägna i ett tredjeland och som ägs eller på något sätt används av en kritisk tredjepartsleverantör av IKT-tjänster i syfte att tillhandahålla tjänster till finansiella entiteter i unionen i samband med dess affärsverksamhet, funktioner eller tjänster, inbegripet alla administrativa kontor, företagslokaler eller driftställen, anläggningar, mark, byggnader eller annan egendom:

a) I artikel 35.1 a.

b) I artikel 35.1 b, i enlighet med artikel 38.2 a, b och d, artikel 39.1 och 39.2 a.

De befogenheter som avses i första stycket får utövas om samtliga följande villkor är uppfyllda:

i) Den ledande tillsynsmyndigheten anser att en inspektion i ett tredjeland är nödvändig för att den fullt ut och på ett ändamålsenligt sätt ska kunna utföra sina uppgifter enligt denna förordning.

ii) Inspektionen i ett tredjeland har ett direkt samband med tillhandahållandet av IKT-tjänster till finansiella entiteter i unionen.

iii) Den berörda kritiska tredjepartsleverantören av IKT-tjänster samtycker till att en inspektion genomförs i ett tredjeland.

iv) Den relevanta myndigheten i det berörda tredjelandet har underrättats officiellt av den ledande tillsynsmyndigheten och har inte gjort några invändningar mot detta.

2. Utan att det påverkar unionsinstitutionernas och medlemsstaternas befogenheter ska EBA, Esma eller Eiopa vid tillämpningen av punkt 1 ingå arrangemang för administrativt samarbete med den relevanta myndigheten i det tredjelandet för att göra det möjligt för den ledande tillsynsmyndigheten och den grupp som den har utsett för uppdraget i det berörda tredjelandet att på ett smidigt sätt genomföra inspektioner i det tredjelandet. Dessa samarbetsarrangemang får inte medföra några rättsliga skyldigheter för unionen och dess medlemsstater eller hindra medlemsstaterna och deras behöriga myndigheter från att ingå bilaterala eller multilaterala arrangemang med dessa tredjeländer och deras relevanta myndigheter.

I dessa samarbetsarrangemang ska åtminstone följande anges:

a) Förfarandena för samordning av den tillsynsverksamhet som genomförs enligt denna förordning och all motsvarande övervakning av IKT-tredjepartsrisker i den finansiella sektorn som utövas av den relevanta myndigheten i det berörda tredjelandet, inbegripet uppgifter för översändande av den sistnämndas samtycke så att den ledande tillsynsmyndigheten och dess utsedda grupp kan genomföra allmänna utredningar och inspektioner på plats enligt punkt 1 första stycket på det territorium som omfattas av dess jurisdiktion.

b) Mekanismen för översändande av relevant information mellan EBA, Esma eller Eiopa och den relevanta myndigheten i det berörda tredjelandet, särskilt i samband med information som den ledande tillsynsmyndigheten kan begära enligt artikel 37.

c) Mekanismerna för omedelbar anmälan till EBA, Esma eller Eiopa från den relevanta myndigheten i det berörda tredjelandet av fall där en tredjepartsleverantör av IKT-tjänster som är etablerad i ett tredjeland och har klassificerats som kritisk i enlighet med artikel 31.1 a anses ha åsidosatt de krav som den enligt det berörda tredjelandets tillämpliga rätt är skyldig att följa när den tillhandahåller tjänster till finansiella institut i det tredjelandet samt de avhjälpande åtgärder och sanktioner som tillämpas.

d) Regelbundet översändande av uppdateringar om utvecklingen på reglerings- eller tillsynsområdet när det gäller övervakningen av IKT-tredjepartsrisker för finansiella institut i det berörda tredjelandet.

e) Uppgifter som vid behov gör det möjligt för en företrädare för den relevanta myndigheten i det berörda tredjelandet att delta i de inspektioner som den ledande tillsynsmyndigheten och den utsedda gruppen genomför.

3. När den ledande tillsynsmyndigheten inte kan genomföra sådan tillsynsverksamhet utanför unionen som avses i punkterna 1 och 2, ska den ledande tillsynsmyndigheten

a) utöva sina befogenheter enligt artikel 35 på grundval av alla sakförhållanden som den känner till och dokument som den har tillgång till,

b) dokumentera och förklara eventuella konsekvenser av att den inte är i stånd att genomföra den planerade tillsynsverksamhet som avses i denna artikel.

De potentiella konsekvenser som avses i led b i denna punkt ska beaktas i den ledande tillsynsmyndighetens rekommendationer, som utfärdas enligt artikel 35.1 d.

Artikel 37

Begäran om information

1. Den ledande tillsynsmyndigheten får genom en enkel begäran eller genom ett beslut kräva att de kritiska tredjepartsleverantörerna av IKT-tjänster tillhandahåller all information som är nödvändig för att den ledande tillsynsmyndigheten ska kunna utföra sina uppgifter enligt denna förordning, inbegripet alla relevanta affärshandlingar och operativa dokument, avtal, strategier, dokumentation, rapporter från IKT-säkerhetsgranskningar, IKT-relaterade incidentrapporter samt all information som rör parter till vilka den kritiska tredjepartsleverantören av IKT-tjänster har utkontrakterat operativa funktioner eller verksamheter.

2. När den ledande tillsynsmyndigheten skickar en enkel begäran om information enligt punkt 1 ska den

a) hänvisa till denna artikel som rättslig grund för begäran,

b) ange syftet med begäran,

c) specificera vilka uppgifter som begärs,

d) ange en tidsfrist inom vilken uppgifterna ska lämnas,

e) underrätta företrädaren för den kritiska tredjepartsleverantör av IKT-tjänster av vilken uppgifterna begärs om att den inte är skyldig att lämna informationen, men att den information som lämnas vid ett frivilligt svar på begäran inte får vara oriktig eller vilseledande.

3. När den ledande tillsynsmyndigheten begär uppgifter genom ett beslut enligt punkt 1 ska den

a) hänvisa till denna artikel som rättslig grund för begäran,

b) ange syftet med begäran,

c) specificera vilka uppgifter som begärs,

d) ange en tidsfrist inom vilken uppgifterna ska lämnas,

e) ange de viten som föreskrivs i artikel 35.6 om den begärda informationen är ofullständig eller om informationen inte tillhandahålls inom den tidsfrist som anges i led d i den här punkten,

f) informera om rätten att överklaga beslutet till de europeiska tillsynsmyndigheternas överklagandenämnd och att få beslutet prövat av Europeiska unionens domstol (domstolen) i enlighet med artiklarna 60 och 61 i förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

4. Företrädarna för de kritiska tredjepartsleverantörerna av IKT-tjänster ska tillhandahålla den begärda informationen. I behörig ordning befullmäktigade advokater får lämna de begärda uppgifterna på sina huvudmäns vägnar. Den kritiska tredjepartsleverantören av IKT-tjänster förblir ansvarig fullt ut om de lämnade uppgifterna är ofullständiga, oriktiga eller vilseledande.

5. Den ledande tillsynsmyndigheten ska utan dröjsmål översända en kopia av beslutet om tillhandahållande av information till de behöriga myndigheterna för de finansiella entiteter som använder berörd kritisk tredjepartsleverantörs IKT-tjänster och till det gemensamma tillsynsnätverket.

Artikel 38

Allmänna utredningar

1. För att fullgöra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av den gemensamma undersökningsgrupp som avses i artikel 40.1, vid behov genomföra utredningar av kritiska tredjepartsleverantörer av IKT-tjänster.

2. Den ledande tillsynsmyndigheten ska ha befogenhet att

a) granska handlingar, uppgifter, rutiner och allt annat material av relevans för utförandet av dess uppgifter oberoende av i vilken form de föreligger,

b) ta eller erhålla bestyrkta kopior av, eller utdrag ur, sådana handlingar, uppgifter, dokumenterade förfaranden och allt annat material,

c) kalla till sig företrädare för den kritiska tredjepartsleverantören av IKT-tjänster och be dem om muntliga eller skriftliga förklaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren,

d) höra varje annan fysisk eller juridisk person som går med på att höras i syfte att samla in information om föremålet för utredningen,

e) begära in uppgifter om tele- och datatrafik.

3. De tjänstemän och andra personer som av den ledande tillsynsmyndigheten har bemyndigats att genomföra sådana utredningar som avses i punkt 1 ska utöva sina befogenheter mot uppvisande av ett skriftligt tillstånd där utredningens föremål och syfte anges.

I tillståndet ska även anges de viten som föreskrivs i artikel 35.6 om den dokumentation, de uppgifter, de dokumenterade förfaranden eller annat material som krävs eller svaren på frågor till företrädare för tredjepartsleverantören av IKT-tjänster inte tillhandahålls eller är ofullständiga.

4. Företrädarna för kritiska tredjepartsleverantörer av IKT-tjänster är skyldiga att underkasta sig utredningarna på grundval av ett beslut av den ledande tillsynsmyndigheten. Beslutet ska ange föremålet för och syftet med utredningen, de viten som föreskrivs i artikel 35.6, de rättsmedel som finns tillgängliga enligt förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 samt rätten att få beslutet prövat av domstolen.

5. Den ledande tillsynsmyndigheten ska i god tid innan utredningen inleds underrätta de behöriga myndigheterna för de finansiella entiteter som använder de IKT-tjänster som tillhandahålls av den kritiska tredjepartsleverantören av IKT-tjänster om den planerade utredningen och namnge de bemyndigade personerna.

Den ledande tillsynsmyndigheten ska underrätta det gemensamma tillsynsnätverket om all information som översänds enligt första stycket.

Artikel 39

Inspektioner

1. För att utföra sina uppgifter enligt denna förordning får den ledande tillsynsmyndigheten, med bistånd av de gemensamma undersökningsgrupper som avses i artikel 40.1, inleda och genomföra alla nödvändiga inspektioner på plats i företagslokaler, på mark eller egendom som tillhör tredjepartsleverantörerna av IKT-tjänster, såsom huvudkontor, driftscentrum och sekundära lokaler, samt genomföra skrivbordsinspektioner.

Vid utövandet av de befogenheter som avses i första stycket ska den ledande tillsynsmyndigheten samråda med det gemensamma tillsynsnätverket.

2. Tjänstemän och andra personer som av den ledande tillsynsmyndigheten har bemyndigats att genomföra en inspektion på plats ska ha befogenhet att

a) bereda sig tillträde till företagslokaler, mark eller egendom och att

b) försegla sådana företagslokaler, räkenskaper eller affärshandlingar under den tid och i den utsträckning som krävs för inspektionen.

Tjänstemän och andra personer som har bemyndigats av den ledande tillsynsmyndigheten ska utöva sina befogenheter mot uppvisande av ett skriftligt tillstånd som anger inspektionens föremål och syften liksom de viten som föreskrivs i artikel 35.6 om företrädarna för de berörda kritiska tredjepartsleverantörerna av IKT-tjänster inte underkastar sig inspektionen.

3. Den ledande tillsynsmyndigheten ska i god tid innan inspektionen inleds informera de behöriga myndigheterna för de finansiella entiteter som använder denna tredjepartsleverantör av IKT-tjänster.

4. Inspektionerna ska omfatta alla relevanta IKT-system, nätverk, anordningar, information och data som används för eller bidrar till tillhandahållandet av IKT-tjänster till finansiella entiteter.

5. Före en planerad inspektion på plats ska den ledande tillsynsmyndigheten i rimlig tid underrätta de kritiska tredjepartsleverantörerna av IKT-tjänster, såvida detta inte är omöjligt på grund av en nöd- eller krissituation, eller om det skulle leda till en situation där inspektionen eller revisionen inte längre skulle vara effektiv.

6. Den kritiska tredjepartsleverantören av IKT-tjänster ska underkasta sig inspektioner på plats som har beordrats genom beslut av den ledande tillsynsmyndigheten. Beslutet ska ange föremålet för och syftet med inspektionen, fastställa den dag då inspektionen ska inledas och ange de viten som föreskrivs i artikel 35.6, de rättsmedel som finns tillgängliga enligt förordning (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010 samt rätten att få beslutet prövat av domstolen.

7. Om de tjänstemän och andra personer som har bemyndigats av den ledande tillsynsmyndigheten finner att en kritisk tredjepartsleverantör av IKT-tjänster motsätter sig en inspektion som har beordrats enligt denna artikel, ska den ledande tillsynsmyndigheten informera den kritiska tredjepartsleverantören av IKT-tjänster om konsekvenserna av att den motsätter sig kontrollen, inbegripet möjligheten för de berörda finansiella entiteternas behöriga myndigheter att kräva att de finansiella entiteterna säger upp de kontraktsmässiga arrangemang som har ingåtts med den kritiska tredjepartsleverantören av IKT-tjänster.

Artikel 40

Fortlöpande tillsyn

1. Vid tillsynsverksamhet, särskilt allmänna utredningar eller inspektioner ska den ledande tillsynsmyndigheten bistås av en gemensam undersökningsgrupp som har inrättats för varje kritisk tredjepartsleverantör av IKT-tjänster.

2. Den gemensamma undersökningsgrupp som avses i punkt 1 ska bestå av personal från

a) de europeiska tillsynsmyndigheterna,

b) de relevanta behöriga myndigheter som utövar tillsyn över de finansiella entiteter till vilka den kritiska tredjepartsleverantören av IKT-tjänster tillhandahåller IKT-tjänster,

c) den nationella behöriga myndighet som avses i artikel 32.4 e, på frivillig basis,

d) en nationell behörig myndighet från den medlemsstat där den kritiska tredjepartsleverantören av IKT-tjänster är etablerad, på frivillig basis.

Medlemmar i den gemensamma undersökningsgruppen ska ha sakkunskap om IKT-frågor och om operativa risker. Den gemensamma undersökningsgruppen ska samordnas av en utsedd anställd vid den ledande tillsynsmyndigheten (*den ledande tillsynsmyndighetens samordnare*).

3. Inom tre månader efter slutförandet av en utredning eller inspektion ska den ledande tillsynsmyndigheten, efter samråd med tillsynsforumet, anta rekommendationer som ska riktas till den kritiska tredjepartsleverantören av IKT-tjänster enligt de befogenheter som avses i artikel 35.

4. De rekommendationer som avses i punkt 3 ska omedelbart meddelas den kritiska tredjepartsleverantören av IKT-tjänster och de behöriga myndigheterna för de finansiella entiteter till vilka den tillhandahåller IKT-tjänster.

För att genomföra tillsynsverksamheten får den ledande tillsynsmyndigheten ta hänsyn till relevanta tredjepartscertifieringar och interna eller externa IKT-revisionsrapporter som den kritiska tredjepartsleverantören av IKT-tjänster har gjort tillgängliga.

Artikel 41

Harmonisering av villkor som möjliggör genomförandet för tillsynsverksamheten

1. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén utarbeta förslag till tekniska standarder för tillsyn för att specificera

a) den information som ska tillhandahållas av en tredjepartsleverantör av IKT-tjänster i ansökan om frivillig begäran om att bli klassificerad som kritisk enligt artikel 31.11,

b) innehållet, strukturen och formatet avseende den information som tredjepartsleverantörerna av IKT-tjänster ska lämna in, offentliggöra eller rapportera enligt artikel 35.1, inbegripet mallen för tillhandahållande av information om underleverantörsavtal,

c) kriterierna för fastställande av den gemensamma undersökningsgruppens sammansättning, vilka säkerställer ett balanserat deltagande av personal från de europeiska tillsynsmyndigheterna och från de relevanta behöriga myndigheterna samt deras utseende, uppgifter och arbetsmetoder,

d) närmare uppgifter om de behöriga myndigheternas bedömning av de åtgärder som har vidtagits av kritiska tredjepartsleverantörer av IKT-tjänster på grundval av rekommendationerna från den ledande tillsynsmyndigheten enligt artikel 42.3.

2. De europeiska tillsynsmyndigheterna ska överlämna dessa förslag till tekniska standarder för tillsyn till kommissionen senast den 17 juli 2024.

Kommissionen ges befogenhet att komplettera denna förordning genom att anta de tekniska standarder för tillsyn som avses i punkt 1 i enlighet med det förfarande som fastställs i artiklarna 10–14 i förordningarna (EU) nr 1093/2010, (EU) nr 1094/2010 och (EU) nr 1095/2010.

Artikel 42

Behöriga myndigheters uppföljning

1. Inom 60 kalenderdagar från mottagandet av de rekommendationer som har utfärdats av den ledande tillsynsmyndigheten enligt artikel 35.1 d ska kritiska tredjepartsleverantörer av IKT-tjänster antingen underrätta den ledande tillsynsmyndigheten om sin avsikt att följa rekommendationerna eller lämna en motiverad förklaring till varför de inte följer sådana rekommendationer. Den ledande tillsynsmyndigheten ska omedelbart vidarebefordra denna information till de berörda finansiella entiteternas behöriga myndigheter.

2. Den ledande tillsynsmyndigheten ska offentliggöra fall där en kritisk tredjepartsleverantör av IKT-tjänster underlåter att underrätta den ledande tillsynsmyndigheten i enlighet med punkt 1 eller där den förklaring som lämnats av den kritiska tredjepartsleverantören av IKT-tjänster inte bedöms vara tillräcklig. Den offentliggjorda informationen ska avslöja identiteten på den kritiska tredjepartsleverantören av IKT-tjänster samt information om typen och arten av den bristande efterlevnaden. Sådan information ska begränsas till vad som är relevant och proportionellt för att säkerställa allmänhetens medvetenhet, såvida inte ett sådant offentliggörande skulle kunna orsaka de berörda parterna oproportionellt stor skada eller allvarligt skulle kunna äventyra finansmarknadernas korrekta funktion och integritet eller stabiliteten i hela eller delar av unionens finansiella system.

Den ledande tillsynsmyndigheten ska underrätta tredjepartsleverantören av IKT-tjänster om detta offentliggörande.

3. De behöriga myndigheterna ska informera de berörda finansiella entiteterna om de risker som har identifierats i rekommendationerna till kritiska tredjepartsleverantörer av IKT-tjänster i enlighet med artikel 35.1 d.

Finansiella entiteter ska när de hanterar IKT-tredjepartsrisker ta hänsyn till de risker som avses i första stycket.

4. Om en behörig myndighet bedömer att en finansiell entitet i sin hantering av IKT-tredjepartsrisker inte tar hänsyn till eller i tillräcklig utsträckning hanterar de specifika risker som identifierats i rekommendationerna, ska den underrätta den finansiella entiteten om att det inom 60 kalenderdagar efter mottagandet av en sådan underrättelse kan fattas ett beslut enligt punkt 6 i avsaknad av lämpliga kontraktsmässiga arrangemang för hantering av sådana risker.

5. De behöriga myndigheterna får efter att ha mottagit de rapporter som avses i artikel 35.1 c, och innan de fattar ett beslut som avses i punkt 6 i den här artikeln, på frivillig basis samråda med de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet, som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster.

6. De behöriga myndigheterna får, som en sista utväg efter underrättelsen och i förekommande fall samrådet enligt punkterna 4 och 5 i denna artikel, i enlighet med artikel 50 fatta ett beslut om att finansiella entiteter tillfälligt, helt eller delvis, ska avbryta användningen eller införandet av en tjänst som tillhandahålls av den kritiska tredjepartsleverantörer av IKT-tjänster till dess att de risker som identifieras i rekommendationerna till kritiska tredjepartsleverantörer av IKT-tjänster har åtgärdats. Vid behov får de kräva att finansiella entiteter helt eller delvis ska avsluta de relevanta kontraktsmässiga arrangemang som har ingåtts med de kritiska tredjepartsleverantörerna av IKT-tjänster.

7. Om en kritisk tredjepartsleverantör av IKT-tjänster vägrar att godta rekommendationer baserat på en annan strategi än den som den ledande tillsynsmyndigheten rekommenderar och en sådan annan strategi kan inverka negativt på ett stort antal finansiella entiteter eller en betydande del av den finansiella sektorn, och enskilda varningar från de behöriga myndigheterna inte har lett till konsekventa strategier som minskar den potentiella risken för den finansiella stabiliteten, får den ledande tillsynsmyndigheten efter samråd med tillsynsforumet när så är lämpligt utfärda icke-bindande och icke-offentliga yttranden till behöriga myndigheter för att främja konsekventa och samstämmiga uppföljningsåtgärder avseende tillsyn.

8. Efter att ha mottagit de rapporter som avses i artikel 35.1 c ska de behöriga myndigheterna när de fattar ett beslut som avses i punkt 6 i den här artikeln ta hänsyn till typen och omfattningen av den risk som inte hanteras av den kritiska tredjepartsleverantören av IKT-tjänster, samt hur allvarlig den bristande efterlevnaden är, med beaktande av följande kriterier:

a) Den bristande efterlevnadens allvarlighetsgrad och varaktighet.

b) Huruvida den bristande efterlevnaden har påvisat allvarliga brister i den kritiska tredjepartsleverantörens förfaranden, ledningssystem, riskhantering eller interna kontroller.

c) Huruvida ekonomisk brottslighet har underlättats eller orsakats av eller på annat sätt tillskrivs den bristande efterlevnaden.

d) Huruvida den bristande efterlevnaden är uppsåtlig eller beror på oaktsamhet.

e) Huruvida det tillfälliga upphävandet eller uppsägningen av de kontraktsmässiga arrangemangen hotar kontinuiteten i den finansiella entitetens affärsverksamhet trots den finansiella entitetens ansträngningar att undvika avbrott i tillhandahållandet av tjänster.

f) I tillämpliga fall, det yttrande som på frivillig basis har inhämtats i enlighet med punkt 5 i denna artikel från de behöriga myndigheter som i enlighet med direktiv (EU) 2022/2555 har utsetts eller inrättats till ansvariga för tillsynen av en väsentlig eller viktig entitet om inte annat följer av det direktivet, som har klassificerats som kritisk tredjepartsleverantör av IKT-tjänster.

De behöriga myndigheterna ska ge finansiella entiteter den tid som krävs för att de ska kunna anpassa sina kontraktsmässiga arrangemang med kritiska tredjepartsleverantörer av IKT-tjänster i syfte att undvika negativa effekter på den digitala operativa motståndskraften och för att de ska kunna införa sådana exitstrategier och övergångsplaner som avses i artikel 28.

9. Det beslut som avses i punkt 6 i denna artikel ska meddelas medlemmarna i det tillsynsforum som avses i artikel 32.4 a, b och c och det gemensamma tillsynsnätverket.

De kritiska tredjepartsleverantörer av IKT-tjänster som påverkas av de beslut som avses i punkt 6 ska samarbeta fullt ut med de berörda finansiella entiteterna, särskilt i samband med tillfälligt upphävande eller uppsägning av deras kontraktsmässiga arrangemang.

10. De behöriga myndigheterna ska regelbundet informera den ledande tillsynsmyndigheten om de metoder och åtgärder som de har vidtagit i sina tillsynsuppgifter när det gäller finansiella entiteter samt om de kontraktsmässiga arrangemang som finansiella entiteter har ingått om kritiska tredjepartsleverantörer av IKT-tjänster helt eller delvis inte har godtagit rekommendationerna till dem från den ledande tillsynsmyndigheten.

11. Den ledande tillsynsmyndigheten får på begäran lämna ytterligare klargöranden om de utfärdade rekommendationerna för att ge de behöriga myndigheterna vägledning i uppföljningsåtgärderna.

Artikel 43

Tillsynsavgifter

1. Den ledande tillsynsmyndigheten ska i enlighet med den delegerade akt som avses i punkt 2 i denna artikel från de kritiska tredjepartsleverantörerna av IKT-tjänster ta ut avgifter som till fullo täcker den ledande tillsynsmyndighetens nödvändiga utgifter i samband med fullgörandet av tillsynsuppgifter enligt denna förordning, inbegripet ersättning för eventuella kostnader som kan uppstå till följd av arbete som utförs av den gemensamma undersökningsgrupp som avses i artikel 40 samt kostnaderna för den rådgivning som tillhandahålls av de oberoende experter som avses i artikel 32.4 andra stycket i frågor som omfattas av direkt tillsynsverksamhet.

Det avgiftsbelopp som tas ut av en kritisk tredjepartsleverantör av IKT-tjänster ska täcka alla kostnader för fullgörandet av de uppgifter som anges i detta avsnitt och stå i proportion till leverantörens omsättning.

2. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 57 för att komplettera denna förordning genom att senast den 17 juli 2024 fastställa avgiftsbeloppen och hur de ska betalas.

Artikel 44

Internationellt samarbete

1. Utan att det påverkar tillämpningen av artikel 36 får EBA, Esma och Eiopa, i enlighet med artikel 33 i förordningarna (EU) nr 1093/2010, (EU) nr 1095/2010 och (EU) nr 1094/2010, ingå administrativa arrangemang med tredjeländers reglerings- och tillsynsmyndigheter för att främja internationellt samarbete om IKT-tredjepartsrisker inom olika finansiella sektorer, särskilt genom att utveckla bästa praxis för översyn av IKT-riskhanteringsmetoder och IKT-kontroller, begränsningsåtgärder och incidenthantering.

2. De europeiska tillsynsmyndigheterna ska genom den gemensamma kommittén vart femte år lämna en gemensam konfidentiell rapport till Europaparlamentet, rådet och kommissionen med en sammanfattning av resultaten av de relevanta diskussioner som har förts med de myndigheter i tredjeländer som avses i punkt 1, med fokus på utvecklingen av IKT-tredjepartsrisker och konsekvenserna för den finansiella stabiliteten, marknadsintegriteten, investerarskyddet och den inre marknadens funktion.

KAPITEL VI

Arrangemang för informationsutbyte

Artikel 45

Arrangemang för utbyte av information och underrättelser om cyberhot

1. Finansiella entiteter får sinsemellan utbyta information och underrättelser om cyberhot, inbegripet indikatorer på äventyrad säkerhet, taktiker, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, i den mån sådant utbyte av information och underrättelser

a) syftar till att förbättra finansiella entiteters digitala operativa motståndskraft, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra cyberhotens spridningsförmåga, varvid försvarsförmåga, metoder för att upptäcka hot, begränsningsstrategier eller åtgärds- och återställningsfaser stöds,

b) äger rum inom betrodda grupper av finansiella entiteter,

c) genomförs genom arrangemang för informationsutbyte som skyddar den potentiellt känsliga karaktären hos den information som utbyts och som styrs av uppföranderegler med full respekt för affärshemligheter, skydd av personuppgifter i enlighet med förordning (EU) 2016/679 och riktlinjer för konkurrenspolitiken.

2. Vid tillämpning av punkt 1 c ska arrangemangen för informationsutbyte innehålla fastställda villkor för deltagande och, när så är lämpligt, närmare uppgifter om offentliga myndigheters deltagande och på vilket sätt dessa kan knytas till arrangemangen för informationsutbyte, om deltagandet av tredjepartsleverantörer av IKT-tjänster och om operativa delar, inbegripet användningen av särskilda it-plattformar.

3. Finansiella entiteter ska underrätta de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte som avses i punkt 1, när deras medlemskap har godkänts eller, i tillämpliga fall, när medlemskapet upphör, så snart så har skett.

KAPITEL VII

Behöriga myndigheter

Artikel 46

Behöriga myndigheter

Utan att det påverkar tillämpningen av de bestämmelser om tillsynsramen för kritiska tredjepartsleverantörer av IKT-tjänster som avses i kapitel V avsnitt II i denna förordning ska efterlevnaden av denna förordning säkerställas av följande behöriga myndigheter i enlighet med de befogenheter som tilldelats genom respektive rättsakt:

a) För kreditinstitut och för institut undantagna enligt direktiv 2013/36/EU: den behöriga myndighet som har utsetts i enlighet med artikel 4 i det direktivet. För kreditinstitut som har klassificerats som betydande i enlighet med artikel 6.4 i förordning (EU) nr 1024/2013: ECB i enlighet med de befogenheter och uppgifter som har tilldelats genom den förordningen.

b) För betalningsinstitut, inbegripet betalningsinstitut undantagna enligt direktiv (EU) 2015/2366, institut för elektroniska pengar, inbegripet de som är undantagna enligt direktiv 2009/110/EG, och leverantörer av kontoinformationstjänster som avses i artikel 33.1 i direktiv (EU) 2015/2366: den behöriga myndighet som har utsetts i enlighet med artikel 22 i direktiv (EU) 2015/2366.

c) För värdepappersföretag: den behöriga myndighet som har utsetts i enlighet med artikel 4 i Europaparlamentets och rådets direktiv (EU) 2019/2034 ([38]).

d) För leverantörer av kryptotillgångstjänster som har auktoriserats enligt förordningen om kryptotillgångar och emittenter av tillgångsanknutna token: den behöriga myndighet som har utsetts i enlighet med de relevanta bestämmelserna i den förordningen.

e) För värdepapperscentraler: den behöriga myndighet som har utsetts i enlighet med artikel 11 i förordning (EU) nr 909/2014.

f) För centrala motparter: den behöriga myndighet som har utsetts i enlighet med artikel 22 i förordning (EU) nr 648/2012.

g) För handelsplatser och leverantörer av datarapporteringstjänster: den behöriga myndighet som har utsetts i enlighet med artikel 67 i direktiv 2014/65/EU och den behöriga myndigheten enligt definitionen i artikel 2.1.18 i förordning (EU) nr 600/2014.

h) För transaktionsregister: den behöriga myndighet som har utsetts i enlighet med artikel 22 i förordning (EU) nr 648/2012.

i) För förvaltare av alternativa investeringsfonder: den behöriga myndighet som har utsetts i enlighet med artikel 44 i direktiv 2011/61/EU.

j) För förvaltningsbolag: den behöriga myndighet som har utsetts i enlighet med artikel 97 i direktiv 2009/65/EG.

k) För försäkrings- och återförsäkringsföretag: den behöriga myndighet som har utsetts i enlighet med artikel 30 i direktiv 2009/138/EG.

l) För försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet: den behöriga myndighet som har utsetts i enlighet med artikel 12 i direktiv (EU) 2016/97.

m) För tjänstepensionsinstitut: den behöriga myndighet som har utsetts i enlighet med artikel 47 i direktiv (EU) 2016/2341.

n) För kreditvärderingsinstitut: den behöriga myndighet som har utsetts i enlighet med artikel 21 i förordning (EG) nr 1060/2009.

o) För administratörer av kritiska referensvärden: den behöriga myndighet som har utsetts i enlighet med artiklarna 40 och 41 i förordning (EU) 2016/1011.

([38]) Europaparlamentets och rådets direktiv (EU) 2019/2034 av den 27 november 2019 om tillsyn av värdepappersföretag och om ändring av direktiven 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU och 2014/65/EU (EUT L 314, 5.12.2019, s. 64).

p) För leverantörer av gräsrotsfinansieringstjänster: den behöriga myndighet som har utsetts i enlighet med artikel 29 i förordning (EU) 2020/1503.

q) För värdepapperiseringsregister: den behöriga myndighet som har utsetts i enlighet med artiklarna 10 och artikel 14.1 i förordning (EU) 2017/2402.

Artikel 47

Samarbete med strukturer och myndigheter som har inrättats genom direktiv (EU) 2022/2555

1. För att främja samarbete och möjliggöra tillsynsutbyten mellan de behöriga myndigheter som har utsetts enligt denna förordning och den samarbetsgrupp som har inrättats genom artikel 14 i direktiv (EU) 2022/2555 får de europeiska tillsynsmyndigheterna och de behöriga myndigheterna delta i samarbetsgruppens verksamhet i frågor som rör deras tillsynsverksamhet i samband med finansiella entiteter. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna får begära att bli inbjudna att delta i samarbetsgruppens verksamhet i väsentliga eller viktiga frågor som rör entiteter om inte annat följer av direktiv (EU) 2022/2555 och som har klassificerats som kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 31 i denna förordning.

2. De behöriga myndigheterna får när så är lämpligt samråda och utbyta information med den gemensamma kontaktpunkten och de CSIRT-enheter som utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555.

3. De behöriga myndigheterna får när så är lämpligt begära relevant teknisk rådgivning och tekniskt stöd från de behöriga myndigheter som har utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555 och ingå samarbetsarrangemang som gör det möjligt att inrätta effektiva och snabba samordningsmekanismer.

4. De arrangemang som avses i punkt 3 i denna artikel kan bland annat ange förfarandena för samordning av tillsynsverksamheten i samband med väsentliga eller viktiga entiteter om inte annat följer av] direktiv (EU) 2022/2555 och som har klassificerats som kritiska tredjepartsleverantörer av IKT-tjänster enligt artikel 31 i denna förordning, bl.a. för genomförande av utredningar och inspektioner på plats i enlighet med nationell rätt och för mekanismer för informationsutbyte mellan de behöriga myndigheterna enligt denna förordning och de behöriga myndigheter som har utsetts eller inrättats i enlighet med det direktivet, inbegripet tillgång till information som de senare myndigheterna har begärt.

Artikel 48

Samarbete mellan myndigheter

1. De behöriga myndigheterna ska ha ett nära samarbete sinsemellan och, i tillämpliga fall, med den ledande tillsynsmyndigheten.

2. De behöriga myndigheterna och den ledande tillsynsmyndigheten ska i god tid ömsesidigt utbyta all relevant information om kritiska tredjepartsleverantörer av IKT-tjänster som är nödvändig för att de ska kunna utföra sina respektive uppgifter enligt denna förordning, särskilt om identifierade risker, strategier och åtgärder som vidtas som en del av den ledande tillsynsmyndighetens tillsynsuppgifter.

Artikel 49

Övningar, kommunikation och samarbete mellan finansiella sektorer

1. De europeiska tillsynsmyndigheterna får, genom den gemensamma kommittén och i samarbete med behöriga myndigheter, resolutionsmyndigheter som avses i artikel 3 i direktiv 2014/59/EU, ECB, Gemensamma resolutionsnämnden, när det gäller information som rör entiteter som omfattas av tillämpningsområdet för förordning (EU) nr 806/2014, ESRB och Enisa, när så är lämpligt, inrätta mekanismer för att möjliggöra utbyte av effektiv praxis mellan olika finansiella sektorer för att öka situationsmedvetenheten och identifiera gemensamma sårbarheter och risker på it-området.

De får utveckla krishanterings- och beredskapsövningar som inbegriper cyberangrepp i syfte att utveckla kommunikationskanaler och gradvis möjliggöra en effektiv samordnad reaktion på unionsnivå i händelse av en allvarlig gränsöverskridande IKT-relaterad incident eller därmed sammanhängande hot som har en systempåverkan på unionens finansiella sektor som helhet.

Dessa övningar kan när så är lämpligt även innefatta test av den finansiella sektorns beroendeförhållanden till andra ekonomiska sektorer.

2. De behöriga myndigheterna, de europeiska tillsynsmyndigheterna och ECB ska ha ett nära samarbete och utbyta information för att fullgöra sina uppgifter enligt artiklarna 47–54. De ska nära samordna sin tillsyn för att identifiera och åtgärda överträdelser av denna förordning, utarbeta och främja bästa praxis, underlätta samarbete, främja en konsekvent tolkning och tillhandahålla bedömningar över jurisdiktionsgränserna om det uppstår meningsskiljaktigheter.

Artikel 50

Administrativa sanktioner och avhjälpande åtgärder

1. De behöriga myndigheterna ska ha alla tillsyns-, utrednings- och sanktionsbefogenheter som krävs för att de ska kunna fullgöra sina skyldigheter enligt denna förordning.

2. De befogenheter som avses i punkt 1 ska omfatta åtminstone följande befogenheter:

a) Få tillgång till alla dokument eller uppgifter i vilken form som helst som enligt den behöriga myndigheten är relevanta för fullgörandet av dess uppgifter och få eller ta en kopia av dem.

b) Utföra kontroller eller inspektioner på plats, som ska omfatta men inte vara begränsade till att

   i) kalla till sig företrädare för finansiella entiteter och be dem om muntliga eller skriftliga förklaringar angående sakförhållanden eller dokument som rör föremålet för och syftet med utredningen samt nedteckna svaren,

   ii) höra vilken annan fysisk eller juridisk person som helst som går med på att höras i syfte att samla in information om föremålet för utredningen.

c) Kräva korrigerande och avhjälpande åtgärder vid överträdelser av kraven i denna förordning.

3. Utan att det påverkar medlemsstaternas rätt att ålägga straffrättsliga påföljder i enlighet med artikel 52 ska medlemsstaterna fastställa regler om lämpliga administrativa sanktioner och avhjälpande åtgärder vid överträdelser av denna förordning och säkerställa att de genomförs effektivt.

Sådana sanktioner och åtgärder ska vara effektiva, proportionella och avskräckande.

4. Medlemsstaterna ska ge behöriga myndigheter befogenhet att tillämpa åtminstone följande administrativa sanktioner eller avhjälpande åtgärder vid överträdelser av denna förordning:

a) Utfärda ett föreläggande enligt vilket det krävs att den fysiska eller juridiska personen upphör med det agerande som strider mot denna förordning och inte upprepar detta agerande.

b) Kräva att varje praxis eller beteende som den behöriga myndigheten anser strider mot bestämmelserna i denna förordning tillfälligt eller permanent upphör och förhindra en upprepning av denna praxis eller detta beteende.

c) Vidta vilken typ av åtgärd som helst, även av ekonomisk art, för att säkerställa att finansiella entiteter fortsätter att uppfylla rättsliga krav.

d) Kräva tillgång till, i den mån det är tillåtet enligt nationell rätt, befintliga uppgifter om datatrafik som innehas av en teleoperatör om det föreligger en rimlig misstanke om överträdelse av denna förordning och om dessa uppgifter kan vara relevanta för en utredning av överträdelser av denna förordning.

e) Utfärda offentliga meddelanden, inbegripet offentliga uttalanden, med uppgift om den fysiska eller juridiska personens identitet och överträdelsens art.

5. Om punkt 2 c och punkt 4 är tillämpliga på juridiska personer ska medlemsstaterna ge de behöriga myndigheterna befogenhet att tillämpa administrativa sanktioner och avhjälpande åtgärder, med förbehåll för de villkor som föreskrivs i nationell rätt, på medlemmar i ledningsorganet och på andra personer som enligt nationell rätt är ansvariga för överträdelsen.

6. Medlemsstaterna ska säkerställa att alla beslut om att ålägga administrativa sanktioner eller avhjälpande åtgärder enligt punkt 2 c är vederbörligen motiverade och kan överklagas.

Artikel 51

Utövande av befogenheten att ålägga administrativa sanktioner och avhjälpande åtgärder

1. De behöriga myndigheterna ska utöva sina befogenheter att ålägga de administrativa sanktioner och avhjälpande åtgärder som avses i artikel 50 i enlighet med sina nationella rättsliga ramar, när så är lämpligt, på något av följande sätt:

a) Direkt.

b) I samarbete med andra myndigheter.

c) På eget ansvar genom delegering till andra myndigheter.

d) Genom hänvändelse till de behöriga rättsliga myndigheterna.

2. De behöriga myndigheterna ska, när de fastställer typen av och nivån på en administrativ sanktion eller avhjälpande åtgärd som ska åläggas enligt artikel 50, ta hänsyn till i vilken utsträckning överträdelsen är avsiktlig eller beror på försummelse och till alla andra relevanta omständigheter, bland annat följande, när så är lämpligt:

a) Överträdelsens väsentlighet, svårighetsgrad och varaktighet.

b) Graden av ansvar hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen.

c) Den finansiella styrkan hos den fysiska eller juridiska person som gjort sig skyldig till överträdelsen.

d) Omfattningen av de vinster som erhållits eller av förluster som undvikits av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen, i den mån de kan bestämmas.

e) Förluster för tredje parter orsakade av överträdelsen, i den mån de kan fastställas.

f) Viljan hos den ansvariga fysiska eller juridiska person att samarbeta med den behöriga myndigheten, utan att det påverkar behovet av att säkerställa återföring av den vinst som den fysiska eller juridiska personen gjort eller de förluster som denne undvikit.

g) Tidigare överträdelser av den fysiska eller juridiska person som har gjort sig skyldig till överträdelsen.

Artikel 52

Straffrättsliga påföljder

1. Medlemsstaterna får besluta att inte fastställa regler för administrativa sanktioner eller avhjälpande åtgärder för överträdelser som omfattas av straffrättsliga påföljder i deras nationella rätt.

2. Om medlemsstaterna har valt att fastställa straffrättsliga påföljder för överträdelser av denna förordning, ska de säkerställa att lämpliga åtgärder har vidtagits så att de behöriga myndigheterna har alla nödvändiga befogenheter att samarbeta med rättsliga myndigheter, åklagarmyndigheter eller straffrättsliga myndigheter inom sin jurisdiktion för att få specifik information om brottsutredningar eller straffrättsliga förfaranden som har inletts på grund av överträdelser av denna förordning, och att lämna samma information till andra behöriga myndigheter samt EBA, Esma eller Eiopa för att uppfylla sina skyldigheter att samarbeta enligt denna förordning.

Artikel 53

Underrättelseskyldigheter

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

Artikel 54

Offentliggörande av administrativa sanktioner

1. De behöriga myndigheterna ska utan onödigt dröjsmål på sina officiella webbplatser offentliggöra alla beslut om att ålägga en administrativ sanktion som inte kan överklagas efter det att sanktionens adressat har underrättats om beslutet.

2. Det offentliggörande som avses i punkt 1 ska innehålla information om överträdelsens typ och art, de ansvariga personernas identitet och ålagda sanktioner.

3. Om den behöriga myndigheten efter en bedömning av det enskilda fallet anser att ett offentliggörande av de juridiska personernas identitet eller av de fysiska personernas identitet och personuppgifter är oproportionellt, inbegripet riskerna när det gäller skyddet av personuppgifter, kan hota stabiliteten på de finansiella marknaderna eller äventyra en pågående brottsutredning eller, i den mån detta kan bestämmas, vålla den berörda personen oproportionell skada, ska den behöriga myndigheten vidta någon av följande åtgärder i fråga om beslutet om att ålägga en administrativ sanktion:

a) Skjuta upp offentliggörandet av beslutet tills det inte längre finns någon anledning att inte offentliggöra det.

b) Offentliggöra beslutet på anonym grund på ett sätt som överensstämmer med nationell rätt.

c) Avstå från att offentliggöra beslutet om de alternativ som anges i leden a och b inte anses vara tillräckliga för att säkerställa att det inte innebär något hot mot finansmarknadernas stabilitet eller om offentliggörandet inte är proportionellt när det gäller mindre stränga sanktioner.

4. Vid ett beslut om att offentliggöra en administrativ sanktion på anonym grund i enlighet med punkt 3 b får offentliggörandet av de relevanta uppgifterna skjutas upp.

5. Om en behörig myndighet offentliggör ett beslut om åläggande av en administrativ sanktion som överklagas till de relevanta rättsliga myndigheterna, ska de behöriga myndigheterna omedelbart på sin officiella webbplats lägga till denna information och i senare skeden all efterföljande tillhörande information om resultatet av ett sådant överklagande. Varje rättsligt beslut om ogiltigförklaring av ett beslut om åläggande av en administrativ sanktion ska också offentliggöras.

6. De behöriga myndigheterna ska säkerställa att alla offentliggöranden som avses i punkterna 1–4 finns kvar på deras officiella webbplats endast under den tidsperiod som är nödvändig vid tillämpning av denna artikel. Denna period får inte överstiga fem år efter offentliggörandet.

Artikel 55

Tystnadsplikt

1. All konfidentiell information som är föremål för mottagande, utbyte eller förmedling enligt denna förordning ska omfattas av de villkor för tystnadsplikt som föreskrivs i punkt 2.

2. Tystnadsplikten ska tillämpas för alla personer som arbetar eller har arbetat för de behöriga myndigheterna enligt denna förordning, eller för en myndighet eller ett marknadsföretag eller en fysisk eller juridisk person som dessa behöriga myndigheter har delegerat sina befogenheter till, inbegripet revisorer och experter som arbetar på den behöriga myndighetens uppdrag.

3. Information som omfattas av tystnadsplikt, inbegripet informationsutbyte mellan behöriga myndigheter enligt denna förordning och behöriga myndigheter som har utsetts eller inrättats i enlighet med direktiv (EU) 2022/2555, får inte lämnas ut till någon annan person eller myndighet utom när detta föreskrivs i unionsrätt eller nationell rätt.

4. All information som utbyts mellan de behöriga myndigheterna enligt denna förordning och som avser affärs- eller driftsförhållanden och andra ekonomiska eller personliga förhållanden ska anses vara konfidentiell och omfattas av tystnadsplikt, utom när den behöriga myndigheten vid den tidpunkt då informationen lämnas anger att informationen får lämnas ut eller om det är nödvändigt att lämna ut informationen i samband med rättsliga förfaranden.

Artikel 56

Dataskydd

1. De europeiska tillsynsmyndigheterna och de behöriga myndigheterna får endast behandla personuppgifter om det är nödvändigt för att de ska kunna fullgöra sina respektive skyldigheter och uppgifter enligt denna förordning, särskilt när det gäller utredning, inspektion, begäran om information, kommunikation, offentliggörande, utvärdering, verifiering, bedömning och utarbetande av tillsynsplaner. Personuppgifterna ska behandlas i enlighet med förordning (EU) 2016/679 eller förordning (EU) 2018/1725, beroende på vilken som är tillämplig.

2. Utom där annat föreskrivs i andra sektorsspecifika rättsakter ska de personuppgifter som avses i punkt 1 lagras till dess att de tillämpliga tillsynsuppgifterna fullgjorts och under alla omständigheter i högst 15 år, utom i fall av pågående domstolsförfaranden som kräver ytterligare lagring av sådana uppgifter.

KAPITEL VIII

Delegerade akter

Artikel 57

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 31.6 och 43.2 ska ges till kommissionen för en period på fem år från och med den 17 januari 2024. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 31.6 och 43.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning* eller vid ett senare, i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artiklarna 31.6 och 43.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

KAPITEL IX

Övergångs- och slutbestämmelser

Avsnitt I

Artikel 58

Översynsklausul

1. Senast den 17 januari 2028 ska kommissionen, efter samråd med de europeiska tillsynsmyndigheterna och ESRB, när så är lämpligt, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet, när så är lämpligt åtföljd av ett lagstiftningsförslag. Översynen ska minst omfatta följande:

a) Kriterierna för att klassificera tredjepartsleverantörer av IKT-tjänster som kritiska i enlighet med artikel 31.2.

b) Den frivilliga karaktären hos den anmälan av betydande cyberhot som avses i artikel 19.

c) Den ordning som avses i artikel 31.12 och de befogenheter för den ledande tillsynsmyndigheten som föreskrivs i artikel 35.1 d iv första strecksatsen, i syfte att utvärdera om dessa bestämmelser är ändamålsenliga för att säkerställa en effektiv tillsyn av kritiska tredjepartsleverantörer av IKT-tjänster som är etablerade i ett tredjeland och om det är nödvändigt att etablera ett dotterföretag i unionen.

   Vid tillämpning av första stycket i detta led ska översynen omfatta en analys av den ordning som avses i artikel 31.12, inbegripet vad gäller åtkomst för finansiella entiteter i unionen till tjänster från tredjeländer och tillgång till sådana tjänster på marknaden i unionen, och den ska ta hänsyn till den fortsatta utvecklingen på marknaderna för de tjänster som omfattas av denna förordning, finansiella entiteters och de finansiella tillsynsmyndigheternas praktiska erfarenheter av tillämpningen respektive tillsynen av den ordningen samt all relevant utveckling inom reglering och tillsyn som äger rum på internationell nivå.

d) Lämpligheten i att i tillämpningsområdet för denna förordning inkludera sådana finansiella entiteter som avses i artikel 2.3 e som använder automatiska försäljningssystem, mot bakgrund av den framtida marknadsutvecklingen när det gäller användningen av sådana system.

e) Det gemensamma tillsynsnätverkets funktion och ändamålsenlighet när det gäller att stödja konsekvens i tillsynen och effektivitet i informationsutbytet inom tillsynsramen.

2. I samband med översynen av direktiv (EU) 2015/2366 ska kommissionen bedöma behovet av ökad cyberresiliens i betalningssystem och betalningshantering och lämpligheten i att utvidga tillämpningsområdet för denna förordning till att även omfatta betalningssystemsoperatörer och enheter som deltar i betalningshantering. Mot bakgrund av denna bedömning ska kommissionen, som en del av översynen av direktiv (EU) 2015/2366, lägga fram en rapport för Europaparlamentet och rådet senast den 17 juli 2023.

Baserat på den översynsrapporten och efter samråd med de europeiska tillsynsmyndigheterna, ECB och ESRB får kommissionen, när så är lämpligt och som en del av det lagstiftningsförslag som den får anta i enlighet med artikel 108 andra stycket i direktiv (EU) 2015/2366, lägga fram ett förslag för att säkerställa att alla betalningssystemsoperatörer och entiteter som deltar i betalningshantering är föremål för lämplig tillsyn, samtidigt som hänsyn tas till den befintliga tillsynen av centralbanken.

3. Senast den 17 januari 2026 ska kommissionen, efter samråd med de europeiska tillsynsmyndigheterna och kommittén för europeiska tillsynsorgan för revisorer, genomföra en översyn och överlämna en rapport till Europaparlamentet och rådet, vid behov åtföljd av ett lagstiftningsförslag, om huruvida det är lämpligt att stärka kraven för lagstadgade revisorer och revisionsföretag när det gäller digital operativ motståndskraft genom att inkludera lagstadgade revisorer och revisionsföretag i tillämpningsområdet för denna förordning eller genom att ändra Europaparlamentets och rådets direktiv 2006/43/EG ([39]).

Avsnitt II

Ändringar

Artikel 59

Ändringar av förordning (EG) nr 1060/2009

Förordning (EG) nr 1060/2009 ska ändras på följande sätt:

1. I bilaga I avsnitt A punkt 4 ska första stycket ersättas med följande:

"Ett kreditvärderingsinstitut ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder samt effektiva kontroll- och skyddssystem för förvaltningen av sina IKT-system i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) 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 (EUT L 333, 27.12.2022, s. 1)."

2. I bilaga III ska punkt 12 ersättas med följande:

"12. Ett kreditvärderingsinstitut bryter mot artikel 6.2, jämförd med bilaga I avsnitt A punkt 4, om det inte tillämpar sunda förfaranden för förvaltning eller redovisning eller inte har mekanismer för internkontroll eller effektiva riskbedömningsmetoder samt effektiva kontroll- eller skyddssystem för förvaltningen av sina IKT-system i enlighet med förordning (EU) 2022/2554, eller om det inte tillämpar eller upprätthåller beslutsförfaranden och organisationsstrukturer enligt vad som krävs i den punkten."

Artikel 60

Ändringar av förordning (EU) nr 648/2012

Förordning (EU) nr 648/2012 ska ändras på följande sätt:

1. Artikel 26 ska ändras på följande sätt:

a) Punkt 3 ska ersättas med följande:

"3. En central motpart ska upprätthålla en organisationsstruktur som säkerställer en kontinuerlig och väl fungerande verksamhet och tillhandahållande av tjänster. Den ska använda lämpliga och proportionella system, resurser och förfaranden, inbegripet IKT-system som förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) 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 (EUT L 333, 27.12.2022. s. 1)."

([39]) Europaparlamentets och rådets direktiv 2006/43/EG av den 17 maj 2006 om lagstadgad revision av årsbokslut och sammanställd redovisning och om ändring av rådets direktiv 78/660/EEG och 83/349/EEG samt om upphävande av rådets direktiv 84/253/EEG (EUT L 157, 9.6.2006, s. 87).

b) Punkt 6 ska utgå.

2. Artikel 34 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. En central motpart ska etablera, genomföra och upprätthålla lämpliga riktlinjer för kontinuerlig verksamhet och en lämplig katastrofplan, vilket ska innefatta IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har upprättats och genomförts i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt återuppta den och fullgöra den centrala motpartens skyldigheter.”

b) I punkt 3 ska första stycket ersättas med följande:

”3. För att säkerställa en konsekvent tillämpning av denna artikel ska Esma, efter samråd med ECBS-medlemmarna, utarbeta förslag till tekniska standarder för tillsyn med närmare uppgifter om minimiinnehåll och krav avseende riktlinjerna för kontinuerlig verksamhet och katastrofplanen, exklusive IKT-kontinuitetspolicy och IKT-katastrofplanerna.”

3. I artikel 56.3 ska första stycket ersättas med följande:

”3. För att säkerställa en konsekvent tillämpning av denna artikel ska Esma utarbeta förslag till tekniska standarder för tillsyn med närmare uppgifter om den ansökan om registrering som avses i punkt 1, utom för krav som rör IKT-riskhantering.”

4. I artikel 79 ska punkterna 1 och 2 ersättas med följande:

”1. Ett transaktionsregister ska kartlägga operativa riskkällor och minimera dem genom att utveckla lämpliga system, kontroller och förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2022/2554.

2. Ett transaktionsregister ska utforma, tillämpa och upprätthålla tillräckliga riktlinjer för kontinuerlig verksamhet och en katastrofplan, inbegripet IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra transaktionsregistrets skyldigheter.”

5. I artikel 80 ska punkt 1 utgå.

6. I bilaga I ska avsnitt II ändras på följande sätt:

a) Leden a och b ska ersättas med följande:

”a) Ett transaktionsregister bryter mot artikel 79.1 om det inte identifierar operativa riskkällor eller inte minimerar dessa risker genom att utveckla lämpliga system, kontroller och förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2022/2554.

b) Ett transaktionsregister bryter mot artikel 79.2 om det inte utformar, tillämpar eller upprätthåller en lämplig strategiplan för kontinuerlig verksamhet och en katastrofplan som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra transaktionsregistrets skyldigheter.”

b) Led c ska utgå.

7. Bilaga III ska ändras på följande sätt:

a) Avsnitt II ska ändras på följande sätt:

i) Led c ska ersättas med följande:

”c) En central motpart i kategori 2 överträder artikel 26.3 om den inte upprätthåller en organisationsstruktur som säkerställer en kontinuerlig och väl fungerande verksamhet och tillhandahållande av tjänster, eller om den inte använder lämpliga och proportionella system, resurser eller förfaranden, inbegripet IKT-system som förvaltas i enlighet med förordning (EU) 2022/2554.”

ii) Led f ska utgå.

b) I avsnitt III ska led a ersättas med följande:

”a) En central motpart i kategori 2 överträder artikel 34.1 om den inte utformar, genomför eller upprätthåller lämpliga riktlinjer för kontinuerlig verksamhet och en åtgärds- och återställningsplan som har upprättats i enlighet med förordning (EU) 2022/2554, för att säkerställa verksamheten, snabbt kunna återuppta den och fullgöra den centrala motpartens skyldigheter, vilket åtminstone ger möjlighet att återställa alla transaktioner till vad de var vid tidpunkten för störningen, så att den centrala motpartens verksamhet är fortsatt säker och den kan fullfölja avvecklingen vid fastställt datum.”

Artikel 61

Ändringar av förordning (EU) nr 909/2014

Artikel 45 i förordning (EU) nr 909/2014 ska ändras på följande sätt:

1. Punkt 1 ska ersättas med följande:

”1. En värdepapperscentral ska identifiera källor till operativ risk, såväl interna som externa, och minimera deras effekt genom att använda lämpliga IKT-verktyg, IKT-processer och IKT-strategier som har inrättats och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), samt andra relevanta lämpliga verktyg, kontroller och förfaranden för andra typer av operativa risker, inbegripet för samtliga avvecklingssystem för värdepapper som den driver.

_____

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

2. Punkt 2 ska utgå.

3. Punkterna 3 och 4 ska ersättas med följande:

”3. En värdepapperscentral ska för tjänster som den tillhandahåller samt för varje avvecklingssystem för värdepapper som den driver upprätta, genomföra och upprätthålla ändamålsenliga riktlinjer för driftskontinuitet och en plan för katastrofberedskap, inbegripet IKT-kontinuitetspolicy och åtgärds- och återställningsplaner avseende IKT som har inrättats i enlighet med förordning (EU) 2022/2554, för att se till att dess tjänster kan upprätthållas, driften snabbt kan återupptas och värdepapperscentralens skyldigheter kan fullgöras vid händelser som medför en betydande risk för avbrott i verksamheten.

4. Den plan som avses i punkt 3 ska göra det möjligt att återupprätta alla transaktioner och deltagares positioner vid tidpunkten för avbrottet, så att värdepapperscentralens deltagare kan fortsätta sin verksamhet på ett säkert sätt och avvecklingen kan fullföljas på fastställd dag, inbegripet genom att säkerställa att driften av avgörande it-system kan återupptas från och med tidpunkten för avbrottet i enlighet med vad som föreskrivs i artikel 12.5 och 12.7 i förordning (EU) 2022/2554.”

4. Punkt 6 ska ersättas med följande:

”6. En värdepapperscentral ska identifiera, övervaka och hantera de risker för verksamheten som de viktigaste deltagarna i det avvecklingssystem för värdepapper som den driver samt tjänsteleverantörer, andra värdepapperscentraler eller andra marknadsinfrastrukturer kan utgöra för dess verksamhet. Den ska på begäran tillhandahålla behöriga och relevanta myndigheter information om varje sådan risk som har identifierats. Den ska även utan dröjsmål informera den behöriga myndigheten och de relevanta myndigheterna om alla operativa incidenter till följd av sådana risker, med undantag för IKT-risk.”

5. I punkt 7 ska första stycket ersättas med följande:

”7. Esma ska i nära samarbete med medlemmarna i ECBS utarbeta förslag till tekniska standarder för tillsyn i syfte att fastställa de operativa risker som avses i punkterna 1 och 6, med undantag för IKT-risker, och de metoder för att testa, hantera och minimera de riskerna, inbegripet de riktlinjer för driftskontinuitet och planer för katastrofberedskap som avses i punkterna 3 och 4 samt metoderna för att bedöma dessa.”

Artikel 62

Ändringar av förordning (EU) nr 600/2014

Förordning (EU) nr 600/2014 ska ändras på följande sätt:

1. Artikel 27g ska ändras på följande sätt:

   a) Punkt 4 ska ersättas med följande:

   ”4. APA ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

   (*) 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 (EUT L 333, 27.12.2022, s. 1).”

   b) Punkt 8 c ska ersättas med följande:

   ”c) De konkreta organisatoriska krav som avses i punkterna 3 och 5.”

2. Artikel 27h ska ändras på följande sätt:

   a) Punkt 5 ska ersättas med följande:

   ”5. CTP ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i förordning (EU) 2022/2554.”

   b) Punkt 8 e ska ersättas med följande:

   ”e) De konkreta organisatoriska krav som avses i punkt 4.”

3. Artikel 27i ska ändras på följande sätt:

   a) Punkt 3 ska ersättas med följande:

   ”3. ARM ska uppfylla de krav avseende säkerhet i nätverks- och informationssystem som fastställs i förordning (EU) 2022/2554.”

   b) Punkt 5 b ska ersättas med följande:

   ”b) De konkreta organisatoriska krav som avses i punkterna 2 och 4.”

Artikel 63

Ändringar av förordning (EU) 2016/1011

I artikel 6 i förordning (EU) 2016/1011 ska följande punkt läggas till:

”6. För kritiska referensvärden ska administratören tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder samt effektiva kontroll- och skyddssystem för förvaltningen av IKT-system i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

Artikel 64

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 17 januari 2025.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

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

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 53.1 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Unionen måste på ett lämpligt och heltäckande sätt ta itu med de digitala risker som uppstår för alla finansiella entiteter till följd av en ökad användning av informations- och kommunikationsteknik (IKT) vid tillhandahållande och konsumtion av finansiella tjänster, och därmed bidra till att förverkliga den digitala finanssektorns potential när det gäller att stimulera innovation och främja konkurrens i en säker digital miljö.

(2) Finansiella entiteter är mycket beroende av digital teknik i sin dagliga verksamhet. Det är därför ytterst viktigt att säkerställa att deras digitala transaktioner har en operativ motståndskraft mot IKT-risk. Detta behov har blivit allt större på grund av den ökade marknaden för banbrytande teknik, särskilt teknik som möjliggör att digitala representationer av värde eller rättigheter kan överföras och lagras elektroniskt, med hjälp av teknik för distribuerade liggare eller liknande teknik (kryptotillgångar) och för tjänster relaterade till sådana tillgångar.

([1]) EUT C 343, 26.8.2021, s. 1.
([2]) EUT C 155, 30.4.2021, s. 38.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.

(3) De krav som rör hantering av IKT-risk för finanssektorn på unionsnivå fastställs för närvarande i Europaparlamentets och rådets direktiv 2009/65/EG ([4]), 2009/138/EG ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) och (EU) 2016/2341 ([11]).

Dessa krav skiljer sig åt och är ibland ofullständiga. IKT-risk har i vissa fall endast behandlats indirekt som en del av den operativa risken, medan den i andra fall inte har behandlats över huvud taget. Dessa problem åtgärdas genom antagandet av Europaparlamentets och rådets förordning (EU) 2022/2554 ([12]). Dessa direktiv bör därför ändras för att säkerställa konsekvens med den förordningen. I detta direktiv antas en rad ändringar som är nödvändiga för att bringa rättslig klarhet och enhetlighet i fråga om hur de finansiella entiteter som auktoriseras och övervakas i enlighet med dessa direktiv ska tillämpa olika krav på digital operativ motståndskraft som är nödvändiga för att de ska kunna bedriva sin verksamhet och tillhandahålla tjänster och därigenom garantera en smidigt fungerande inre marknad. Det är nödvändigt att se till att dessa krav är förenliga med marknadsutvecklingen, samtidigt som proportionalitet uppmuntras, särskilt med avseende på de finansiella entiteternas storlek och de särskilda ordningar som är tillämpliga på dem, i syfte att minska efterlevnadskostnaderna.

(4) Inom området för banktjänster innehåller direktiv 2013/36/EU i dagsläget endast allmänna regler om intern styrning och operativ risk med krav på beredskaps- och kontinuitetsplaner vilka underförstått används som en grund för att hantera IKT-risk. För att uttryckligen och tydligt hantera IKT-risk bör dock kraven på beredskaps- och kontinuitetsplaner ändras så att de även innefattar kontinuitets- och åtgärds- och återställningsplaner även för IKT-risk, i enlighet med kraven i förordning (EU) 2022/2554. Dessutom ingår IKT-risk endast indirekt, som en del av den operativa risken, i den översyns- och utvärderingsprocess (ÖUP) som utförs av behöriga myndigheter, och kriterierna för deras bedömning fastställs för närvarande i riktlinjerna om IKT-riskbedömning inom ramen för översyns- och utvärderingsprocessen (ÖUP), utfärdade av den europeiska tillsynsmyndigheten (Europeiska bankmyndigheten, EBA), inrättad genom Europaparlamentets och rådets förordning (EU) nr 1093/2010 ([13]). För att skapa rättslig klarhet och säkerställa att banktillsynsmyndigheterna effektivt identifierar IKT-risk och övervakar finansiella entiteters hantering därav, i linje med den nya ramen för digital operativ motståndskraft, bör ÖUP:s

([4]) Europaparlamentets och rådets direktiv 2009/65/EG av den 13 juli 2009 om samordning av lagar och andra författningar som avser företag för kollektiva investeringar i överlåtbara värdepapper (fondföretag) (EUT L 302, 17.11.2009, s. 32).

([5]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

([6]) Europaparlamentets och rådets direktiv 2011/61/EU av den 8 juni 2011 om förvaltare av alternativa investeringsfonder samt om ändring av direktiv 2003/41/EG och 2009/65/EG och förordningarna (EG) nr 1060/2009 och (EU) nr 1095/2010 (EUT L 174, 1.7.2011, s. 1).

([7]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([8]) Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190).

([9]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

([10]) Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (EUT L 337, 23.12.2015, s. 35).

([11]) Europaparlamentets och rådets direktiv (EU) 2016/2341 av den 14 december 2016 om verksamhet i och tillsyn över tjänstepensionsinstitut (EUT L 354, 23.12.2016, s. 37).

([12]) 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 (se sidan 1 i detta nummer av EUT).

([13]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12).

tillämpningsområde även ändras så att det uttryckligen hänvisar till de krav som fastställs i förordning (EU) 2022/2554 och i synnerhet omfattar de risker som påvisats i rapporter om allvarliga IKT-relaterade incidenter och resultaten av den testning av digital operativ motståndskraft som finansiella entiteter utfört i enlighet med den förordningen.

(5) Digital operativ motståndskraft är nödvändigt för att upprätthålla en finansiell entitets kritiska funktioner och kärnaffärsområden i händelse av dess resolution och för att undvika störningar i realekonomin och det finansiella systemet. Allvarliga operativa incidenter kan hämma en finansiell entitets förmåga att fortsätta att driva sin verksamhet och kan äventyra resolutionsmålen. Vissa kontraktsmässiga arrangemang som rör användningen av IKT-tjänster är väsentliga för att säkerställa driftskontinuitet och tillhandahålla nödvändiga uppgifter i händelse av resolution. För att vara anpassat till målen för unionens ram för operativ motståndskraft bör direktiv 2014/59/EU ändras i enlighet med detta så att det säkerställs att information relaterad till operativ motståndskraft beaktas i samband med resolutionsplanering och bedömning av finansiella entiteters möjligheter till resolution.

(6) I direktiv 2014/65/EU fastställs hårdare IKT-riskregler för värdepappersföretag och handelsplatser när dessa bedriver algoritmisk handel. Mindre utförliga krav tillämpas på datarapporteringstjänster och transaktionsregister. Dessutom hänvisas det i direktiv 2014/65/EU endast i begränsad mån till kontroll- och skyddssystem för informationsbehandlingssystem och användning av lämpliga system, resurser och förfaranden för att sörja för kontinuitet och regelbundenhet i affärstjänster. Det direktivet bör dessutom harmoniseras med förordning (EU) 2022/2554 i fråga om kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och utförandet av investeringsverksamhet, operativ motståndskraft, handelssystemens kapacitet och effektiva arrangemang för kontinuitet och riskhantering.

(7) I direktiv (EU) 2015/2366 fastställs särskilda regler om IKT-relaterade säkerhetskontroll- och begränsningsaspekter för erhållande av en auktorisation att utföra betaltjänster. Dessa auktorisationsregler bör ändras för att anpassas till förordning (EU) 2022/2554. För att minska den administrativa bördan och undvika komplexitet och överlappande rapporteringskrav bör dessutom reglerna om incidentrapportering i det direktivet upphöra att tillämpas för betaltjänstleverantörer som regleras enligt det direktivet och som omfattas av förordning (EU) 2022/2554, vilket gör det möjligt för dessa betaltjänstleverantörer att dra nytta av en gemensam, fullständigt harmoniserad incidentrapporteringsmekanism med avseende på alla operativa incidenter eller säkerhetsincidenter, oavsett om sådana incidenter är IKT-relaterade.

(8) Direktiven 2009/138/EG och (EU) 2016/2341 fångar delvis upp IKT-risk i sina allmänna bestämmelser om styrning och riskhantering, vilket innebär att vissa krav ska specificeras genom delegerade akter med eller utan särskilda hänvisningar till IKT-risk. På samma sätt tillämpas endast mycket allmänna regler på förvaltare av alternativa investeringsfonder som omfattas av direktiv 2011/61/EU och förvaltningsbolag som omfattas av direktiv 2009/65/EG. Dessa direktiv bör därför anpassas till kraven i förordning (EU) 2022/2554 när det gäller förvaltningen av IKT-system och IKT-verktyg.

(9) Ytterligare IKT-krav har i många fall redan fastställts i delegerade akter och genomförandeakter, antagna utifrån förslag till tekniska tillsynsstandarder och tekniska standarder för genomförande vilka utarbetats av den behöriga europeiska tillsynsmyndigheten. Eftersom bestämmelserna i förordning (EU) 2022/2554 hädanefter utgör den rättsliga ramen för IKT-risk för finanssektorn bör vissa befogenheter att anta delegerade akter och genomförandeakter i direktiven 2009/65/EG, 2009/138/EG, 2011/61/EU och 2014/65/EU ändras för att stryka IKT-riskbestämmelserna från tillämpningsområdet för dessa befogenheter.

(10) För att säkerställa ett enhetligt genomförande av den nya ramen för digital operativ motståndskraft för finanssektorn bör medlemsstaterna tillämpa de bestämmelser i nationell rätt som införlivar detta direktiv från och med tillämpningsdagen för förordning (EU) 2022/2554.

(11) 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 har antagits på grundval av artikel 53.1 eller artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) eller båda. Ändringarna genom detta direktiv har tagits med i en och samma lagstiftningsakt på grund av det inbördes förhållandet mellan sakfrågan och ändringarnas syften. Följaktligen bör detta direktiv antas på grundval av såväl artikel 53.1 som artikel 114 i EUF-fördraget.

(12) Eftersom målen för detta direktiv inte i tillräcklig utsträckning kan uppnås av medlemsstaterna, eftersom de innebär en harmonisering av redan befintliga krav i direktiven, utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(13) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument ([14]), har medlemsstaterna åtagit sig att, när det är motiverat, låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i direktivet och motsvarande delar i de nationella instrumenten för införlivande. Lagstiftaren anser att det är motiverat att sådana dokument översänds avseende detta direktiv.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av direktiv 2009/65/EG

Artikel 12 i direktiv 2009/65/EG ska ändras på följande sätt:

1. I punkt 1 andra stycket ska led a ersättas med följande:

”a) har sunda administrativa förfaranden och redovisningsrutiner, kontroll- och säkerhetsarrangemang för elektronisk databehandling, inbegripet när det gäller nätverks- och informationssystem som inrättas och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), samt lämpliga interna kontrollmekanismer, särskilt regler för de anställdas personliga transaktioner eller för innehav eller förvaltning av investeringar i finansiella instrument i syfte att placera på egna konton, och att det minst säkerställs att varje transaktion i vilken fondföretaget medverkar är möjlig att rekonstruera med avseende på dess ursprung, de deltagande parterna, dess art samt tiden och platsen då den ägde rum och att fondföretagets tillgångar som förvaltas av förvaltningsbolaget placeras i enlighet med fondbestämmelserna eller bolagsordningen samt gällande lagstiftning, och

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

2. Punkt 3 ska ersättas med följande:

”3. Utan att det påverkar tillämpningen av artikel 116 ska kommissionen, genom delegerade akter i enlighet med artikel 112a, anta åtgärder som specificerar

a) de förfaranden och arrangemang som avses i punkt 1 andra stycket a, andra än de förfaranden och arrangemang som gäller nätverks- och informationssystem,

b) de strukturer och organisatoriska krav för att minimera intressekonflikter som avses i punkt 1 andra stycket b.”

([14]) EUT C 369, 17.12.2011, s. 14.

Artikel 2

Ändringar av direktiv 2009/138/EG

Direktiv 2009/138/EG ska ändras på följande sätt:

1. Artikel 41.4 ska ersättas med följande:

”4. Försäkrings- och återförsäkringsföretag ska vidta rimliga åtgärder för att säkerställa att deras verksamhet bedrivs med kontinuitet och på ett korrekt sätt, inklusive utvecklingen av beredskapsplaner. Företaget ska i detta syfte använda lämpliga och proportionella system, resurser och förfaranden och ska i synnerhet inrätta och förvalta nätverks- och informationssystem i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

2. I artikel 50.1 ska leden a och b ersättas med följande:

”a) Delarna i de system som avses i artiklarna 41, 44, särskilt de områden som förtecknas i artikel 44.2, och artiklarna 46 och 47, andra än de delar som avser hantering av informations- och kommunikationsteknisk risk.

b) De funktioner som avses i artiklarna 44, 46, 47 och 48, andra än de funktioner som avser hantering av informations- och kommunikationsteknisk risk.”

Artikel 3

Ändring av direktiv 2011/61/EU

Artikel 18 i direktiv 2011/61/EU ska ersättas med följande:

”*Artikel 18*

Allmänna principer

1. Medlemsstaterna ska kräva att AIF-förvaltare alltid ska använda tillfredsställande och lämpliga personella och tekniska resurser som krävs för att de ska kunna förvalta AIF-fonderna på ett korrekt sätt.

De behöriga myndigheterna i AIF-förvaltarens hemmedlemsstat ska, även med beaktande av arten av de AIF-fonder som AIF-förvaltaren förvaltar, särskilt kräva att AIF-förvaltaren har sunda administrativa förfaranden och redovisningsrutiner, kontroll- och säkerhetsarrangemang för elektronisk databehandling, inbegripet när det gäller nätverks- och informationssystem som upprättas och förvaltas i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*) och tillfredsställande interna kontrollmekanismer, särskilt regler för de anställdas personliga transaktioner eller för innehav eller förvaltning av investeringar i syfte att investera för egen räkning, och att det åtminstone säkerställs att varje transaktion i vilken AIF-förvaltaren medverkar avseende AIF-fonderna är möjlig att rekonstruera med avseende på dess ursprung, de deltagande parterna, dess art samt tiden och platsen då den ägde rum, och att tillgångarna i de AIF-fonder som förvaltas av AIF-förvaltaren investeras i enlighet med fondbestämmelserna eller bolagsordningen samt gällande lagstiftning.

2. Kommissionen ska, genom delegerade akter i enlighet med artikel 56, och med förbehåll för villkoren i artiklarna 57 och 58, anta åtgärder för att närmare ange de förfaranden och arrangemang som avses i punkt 1 i den här artikeln, andra än de förfaranden och arrangemang som gäller nätverks- och informationssystem.

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

Artikel 4

Ändringar av direktiv 2013/36/EU

Direktiv 2013/36/EU ska ändras på följande sätt:

1. I artikel 65.3 ska led a vi ersättas med följande:

   ”vi) Tredje parter till vilka enheterna i leden i–iv har gett i uppdrag att utföra uppgifter eller verksamhet, inbegripet de tredjepartsleverantörer av IKT-tjänster som avses i kapitel V i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

   _____

   (*) 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 (EUT L333, 27.12.2022, s. 1).”

2. I artikel 74.1 ska första stycket ersättas med följande:

   ”Instituten ska ha en robust företagsstyrning, i vilket ingår en tydlig organisationsstruktur med väldefinierade, genomlysta och konsekventa ansvarskedjor, effektiva processer för att identifiera, hantera, övervaka och rapportera risker som instituten är eller kan bli exponerade för, tillfredsställande metoder för intern kontroll, inklusive sunda administrations- och redovisningsrutiner och nätverks- och informationssystem som inrättas och förvaltas i enlighet med förordning (EU) 2022/2554, samt ersättningspolicy och ersättningspraxis som är förenliga med och främjar sund och effektiv riskhantering.”

3. Artikel 85.2 ska ersättas med följande:

   ”2. De behöriga myndigheterna ska se till att instituten har lämpliga beredskaps- och kontinuitetspolicyer och -planer, inbegripet IKT-kontinuitetspolicyer och -planer samt IKT-relaterade åtgärds- och återställningsplaner för den teknik som de använder för meddelande av information, och att de planerna inrättas, förvaltas och testas i enlighet med artikel 11 i förordning (EU) 2022/2554, så att instituten kan fortsätta att bedriva sin verksamhet vid en allvarlig störning i verksamheten och begränsa de förluster som orsakas till följd av sådan störning.”

4. I artikel 97.1 ska följande led läggas till:

   ”d) risker som påvisats vid testning av digital operativ motståndskraft i enlighet med kapitel IV i förordning (EU) 2022/2554.”

Artikel 5

Ändringar av direktiv 2014/59/EU

Direktiv 2014/59/EU ska ändras på följande sätt:

1. Artikel 10 ska ändras på följande sätt:

   a) I punkt 7 ska led c ersättas med följande:

      ”c) En beskrivning av hur kritiska funktioner och kärnaffärsområden, i den utsträckning som krävs, skulle kunna avskiljas juridiskt och ekonomiskt från övriga funktioner för att säkerställa fortsatt verksamhet och digital operativ motståndskraft efter institutets fallissemang.”

   b) I punkt 7 ska led q ersättas med följande:

      ”q) En beskrivning av grundläggande operationer och system för kontinuerlig drift av institutets operativa processer, inbegripet nätverks- och informationssystem som avses i Europaparlamentets och rådets förordning (EU) 2022/2554 (*).

      _____

      (*) 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 (EUT L 333, 27.12.2022, s. 1).”

c) I punkt 9 ska följande stycke läggas till:

”I enlighet med artikel 10 i förordning (EU) nr 1093/2010 ska EBA se över och vid behov uppdatera de tekniska standarderna för tillsyn i syfte att bland annat ta hänsyn till bestämmelserna i kapitel II i förordning (EU) 2022/2554.”

2. Bilagan ska ändras på följande sätt:

a) I avsnitt A ska punkt 16 ersättas med följande:

”16. Arrangemang och åtgärder som är nödvändiga för att fortlöpande upprätthålla institutets operativa verksamhet, inbegripet nätverks- och informationssystem som inrättas och förvaltas i enlighet med förordning (EU) 2022/2554.”

b) Avsnitt B ska ändras på följande sätt:

i) Punkt 14 ska ersättas med följande:

”14. Uppgifter om ägarna till de system som avses i led 13, tillhörande servicenivåavtal och alla datorprogram, system eller verksamhetstillstånd, inklusive per juridiska enheter, kritisk verksamhet och centrala affärsområden samt uppgifter om kritiska tredjepartsleverantörer av IKT-tjänster enligt definitionen i artikel 3.23 i förordning (EU) 2022/2554.”

ii) Följande punkt ska införas:

”14a. Resultaten av institutionernas testning av digital operativ motståndskraft enligt förordning (EU) 2022/2554.”

c) Avsnitt C ska ändras på följande sätt:

i) Punkt 4 ska ersättas med följande:

”4. I vilken mån serviceavtal, inbegripet kontraktsmässiga arrangemang som rör användningen av IKT-tjänster, som institutet ingått är solida och kan hävdas om institutet avvecklas.”

ii) Följande punkt ska införas:

”4a. Den digitala operativa motståndskraften hos de nätverks- och informationssystem som stöder institutets kritiska funktioner och kärnaffärsområden, med beaktande av rapporter om allvarliga IKT-relaterade incidenter och resultaten av testning av digital operativ motståndskraft enligt förordning (EU) 2022/2554.”

Artikel 6

Ändringar av direktiv 2014/65/EU

Direktiv 2014/65/EU ska ändras på följande sätt:

1. Artikel 16 ska ändras på följande sätt:

a) Punkt 4 ska ersättas med följande:

”4. Varje värdepappersföretag ska vidta rimliga åtgärder för att sörja för kontinuitet och regelbundenhet i tillhandahållandet av investeringstjänster och utförandet av investeringsverksamhet. Värdepappersföretaget ska i det syftet använda lämpliga och proportionella system, inbegripet informations- och kommunikationstekniska system (IKT-system) som inrättas och förvaltas i enlighet med artikel 7 i Europaparlamentets och rådets förordning (EU) 2022/2554 (*) samt lämpliga och proportionella resurser och förfaranden.

(*) 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 (EUT L333, 27.12.2022, s. 1).”

b) I punkt 5 ska andra och tredje styckena ersättas med följande:

”Varje värdepappersföretag ska tillämpa sunda förfaranden för förvaltning och redovisning samt ha mekanismer för internkontroll och effektiva riskbedömningsmetoder.

Utan att det påverkar behöriga myndigheters möjlighet att kräva tillgång till kommunikation i enlighet med detta direktiv och förordning (EU) nr 600/2014, ska ett värdepappersföretag ha inrättat sunda skyddsmekanismer för att, i enlighet med kraven i förordning (EU) 2022/2554, säkerställa skyddet och autentiseringen vid informationsöverföring, för att minimera risken för dataförvanskning och för obehörig åtkomst och för att förhindra informationsläckor så att uppgifterna därmed alltid behandlas konfidentiellt.”

2. Artikel 17 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Ett värdepappersföretag som bedriver algoritmisk handel ska ha inrättat effektiva system och riskkontroller som är anpassade för den verksamhet som bedrivs, så att det säkerställs att dess handelssystem är motståndskraftiga och har tillräcklig kapacitet i enlighet med kraven i kapitel II i förordning (EU) 2022/2554, att de omfattas av lämpliga handelströsklar och handelslimiter och att de förhindrar att felaktiga order skickas eller att systemet på annat sätt fungerar så att det kan skapa eller bidra till en oordnad marknad.

Ett sådant företag ska också ha inrättat effektiva system och riskkontrollåtgärder för att säkerställa att handelssystemen inte kan användas för något ändamål som strider mot förordning (EU) nr 596/2014 eller mot reglerna för en handelsplats till vilken det är anslutet.

Värdepappersföretaget ska ha inrättat effektiva arrangemang för kontinuitet för att hantera alla avbrott i driften i sina handelssystem, inbegripet en IKT-kontinuitetspolicy och -planer samt IKT-relaterade åtgärds- och återställningsplaner för informations- och kommunikationsteknik som inrättas i enlighet med artikel 11 i förordning (EU) 2022/2554, och ska säkerställa att systemen är fullständigt testade och vederbörligen övervakade för att säkerställa att de uppfyller de allmänna krav som föreskrivs i denna punkt och eventuella särskilda krav i kapitlen II och IV i förordning (EU) 2022/2554.”

b) I punkt 7 ska led a ersättas med följande:

”a) Detaljerna i de organisatoriska krav som fastställs i punkterna 1–6, andra än de krav som rör IKT-riskhantering, och som ska föreskrivas för värdepappersföretag som tillhandahåller olika slags investeringstjänster, investeringsverksamheter, sidotjänster eller kombinationer därav, varigenom specifikationerna av de organisatoriska krav som fastställs i punkt 5 ska innehålla specifika krav för direkt marknadstillträde och för sponsrat tillträde så att det säkerställs att de kontroller som tillämpas på sponsrat tillträde åtminstone motsvarar dem som tillämpas på direkt marknadstillträde.”

3. Artikel 47.1 ska ändras på följande sätt:

a) Led b ska ersättas med följande:

”b) har tillräckliga förutsättningar för att kunna hantera de risker den är exponerad för, inbegripet att hantera IKT-risk i enlighet med kapitel II i förordning (EU) 2022/2554, vidtar lämpliga åtgärder och inför system för att identifiera betydande risker för dess verksamhet och vidtar effektiva åtgärder för att reducera sådana risker,”

b) Led c ska utgå.

4. Artikel 48 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Medlemsstaterna ska kräva att en reglerad marknad inrättar och upprätthåller en operativ motståndskraft i enlighet med kraven i kapitel II i förordning (EU) 2022/2554 för att säkerställa att dess handelssystem är motståndskraftiga, har tillräcklig kapacitet för att kunna hantera toppbelastning i fråga om order- och meddelandevolymer, kan säkerställa ordnad handel under svåra förhållanden på marknaden, är till fullo testade för att säkerställa att sådana villkor är uppfyllda och omfattas av effektiva arrangemang för kontinuitet, inbegripet en IKT-kontinuitetspolicy och -planer samt IKT-relaterade åtgärds- och återställningsplaner som inrättas i enlighet med artikel 11 i förordning (EU) 2022/2554, för att säkerställa kontinuitet i sin verksamhet vid eventuella driftsavbrott i sina handelssystem.”

b) Punkt 6 ska ersättas med följande:

”6. Medlemsstaterna ska kräva att en reglerad marknad har inrättat effektiva system, förfaranden och arrangemang, bland annat krav på medlemmar eller deltagare att utföra lämpliga tester av algoritmer och att tillhandahålla miljöer för att underlätta sådana tester, i enlighet med kraven i kapitlen II och IV i förordning (EU) 2022/2554, för att säkerställa att algoritmiska handelssystem inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden och att hantera eventuella otillbörliga marknadsförhållanden som kan uppstå till följd av sådana algoritmiska handelssystem, inbegripet system för att begränsa andelen ej utförda order i förhållande till transaktionerna som kan läggas in i systemet av en medlem eller en deltagare, för att det ska vara möjligt att bromsa orderflödet om det finns en risk för att systemkapaciteten ska uppnås och för att begränsa och genomdriva den minsta tick-size som får tillämpas på marknaden.”

c) Punkt 12 ska ändras på följande sätt:

i) Led a ska ersättas med följande:

”a) kraven för att säkerställa att handelssystem på reglerade marknader är motståndskraftiga och har tillräcklig kapacitet, förutom kraven rörande digital operativ motståndskraft,”.

ii) Led g ska ersättas med följande:

”g) kraven för att säkerställa lämplig testning av algoritmer, annat än testning av digital operativ motståndskraft, så att det kan säkerställas att algoritmiska handelssystem inbegripet system för algoritmisk högfrekvenshandel inte kan skapa eller bidra till otillbörliga marknadsförhållanden på marknaden.”

Artikel 7

Ändring av direktiv (EU) 2015/2366

Direktiv (EU) 2015/2366 ska ändras på följande sätt:

1. I artikel 3 ska led j ersättas med följande:

”j) Tjänster som tillhandahålls av leverantörer av tekniska tjänster som stöder tillhandahållandet av betaltjänster, utan att de vid någon tidpunkt kommer i besittning av de medel som ska överföras, inklusive behandling och lagring av uppgifter, förtroendeskapande tjänster och integritetsskydd, autentisering av uppgifter och enheter, tillhandahållande av nät för informations- och kommunikationsteknik (IKT) och kommunikationsnät samt tillhandahållande och underhåll av terminaler och utrustning för betaltjänster, med undantag för tjänster för betalningsinitiering och kontoinformationstjänster.”

2. Artikel 5.1 ska ändras på följande sätt:

a) Första stycket ska ändras på följande sätt:

i) Led e ska ersättas med följande:

”e) En beskrivning av den sökandes styrsystem och interna kontrollmekanismer, inklusive förvaltnings-, riskhanterings- och redovisningsförfaranden samt arrangemang för användning av IKT-tjänster i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), vilken ska visa att dessa styrsystem och interna kontrollmekanismer är proportionella, lämpliga, sunda och tillräckliga.

(*) 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 ((EUT L333, 27.12.2022, s. 1).”

ii) Led f ska ersättas med följande:

”f) En beskrivning av de förfaranden som finns för att övervaka, hantera och följa upp säkerhetsincidenter och säkerhetsrelaterade kundklagomål, inklusive en rapporteringsmekanism för incidenter som beaktar betalningsinstitutets informationsskyldigheter enligt kapitel III i förordning (EU) 2022/2554.”

iii) Led h ska ersättas med följande:

”h) En beskrivning av arrangemang för verksamhetens kontinuitet, inklusive en tydlig angivelse av kritiska verksamheter, en effektiv IKT-kontinuitetspolicy och -planer samt effektiva IKT-relaterade åtgärds- och återställningsplaner och ett förfarande för att regelbundet kontrollera och se över dessa planers lämplighet och effektivitet i enlighet med förordning (EU) 2022/2554.”

b) Tredje stycket ska ersättas med följande:

”I samband med de säkerhetskontroll- och begränsningsåtgärder som avses i första stycket j ska det anges på vilket sätt de säkrar en hög nivå av digital operativ motståndskraft i enlighet med kapitel II i förordning (EU) 2022/2554, särskilt när det gäller teknisk säkerhet och dataskydd, däribland för de programvaru- och IKT-system som används av sökanden eller de företag till vilka denne utkontrakterar hela eller delar av sin verksamhet. Dessa åtgärder ska också omfatta de säkerhetsåtgärder som fastställs i artikel 95.1 i detta direktiv. I samband med dessa åtgärder ska hänsyn tas till EBA:s riktlinjer för säkerhetsåtgärder som avses i artikel 95.3 i detta direktiv när dessa har införts.”

3. I artikel 19.6 ska andra stycket ersättas med följande:

”Utkontraktering av viktiga operativa funktioner, inbegripet IKT-system, får inte ske på så sätt att det väsentligt försämrar kvaliteten på betalningsinstitutets interna kontroll och de behöriga myndigheternas möjligheter att övervaka och följa upp att betalningsinstitutet fullgör alla skyldigheter enligt detta direktiv.”

4. I artikel 95.1 ska följande stycke läggas till:

”Första stycket påverkar inte tillämpningen av kapitel II i förordning (EU) 2022/2554 på

a) betaltjänstleverantörer som avses i artikel 1.1 a, b och d i detta direktiv,

b) leverantörer av kontoinformationstjänster som avses i artikel 33.1 i detta direktiv,

c) betalningsinstitut som är undantagna enligt artikel 32.1 i detta direktiv, och

d) institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.”

5. I artikel 96 ska följande punkt läggas till:

”7. Medlemsstaterna ska säkerställa att punkterna 1–5 i denna artikel inte tillämpas på

a) betaltjänstleverantörer som avses i artikel 1.1 a, b och d i detta direktiv,

b) leverantörer av kontoinformationstjänster som avses i artikel 33.1 i detta direktiv,

c) betalningsinstitut som är undantagna enligt artikel 32.1 i detta direktiv, och

d) institut för elektroniska pengar som omfattas av ett undantag enligt artikel 9.1 i direktiv 2009/110/EG.”

6. Artikel 98.5 ska ersättas med följande:

”5. I enlighet med artikel 10 i förordning (EU) nr 1093/2010 ska EBA se över och vid behov regelbundet uppdatera de tekniska standarderna för tillsyn i syfte att bland annat ta hänsyn till innovation och teknisk utveckling, samt till bestämmelserna i kapitel II i förordning (EU) 2022/2554.”

Artikel 8

Ändring av direktiv (EU) 2016/2341

Artikel 21.5 i direktiv (EU) 2016/2341 ska ersättas med följande:

”5. Medlemsstaterna ska säkerställa att tjänstepensionsinstituten vidtar rimliga åtgärder för att säkerställa att deras verksamhet bedrivs med kontinuitet och på ett korrekt sätt, inklusive utarbetandet av beredskapsplaner. Tjänstepen-

sionsinstitutet ska i detta syfte använda lämpliga och proportionella system, resurser och förfaranden, och ska i synnerhet inrätta och förvalta nätverks- och informationssystem i enlighet med Europaparlamentets och rådets förordning (EU) 2022/2554 (*), i tillämpliga fall.

(*) 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 (EUT L 333, 27.12.2022, s. 1).”

Artikel 9

Införlivande

1. Medlemsstaterna ska senast den 17 januari 2025 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 17 januari 2025.

När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska underrätta kommissionen om texten till de centrala bestämmelser i nationell rätt som de antar inom det område som omfattas av detta direktiv.

Artikel 10

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 11

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

Regeringskansliet

Remiss

2024-01-15
Fi2024/00073

Finansdepartementet
Finansmarknadsavdelningen, Enheten för
försäkring, pension och myndighetsstyrning

Promemorian Digital operativ motståndskraft för finanssektorn

Remissinstanser

1. Bolagsverket
2. Ekonomistyrningsverket
3. Euroclear Sweden AB
4. Finansbolagens Förening
5. Finansförbundet
6. Finansinspektionen
7. Fondbolagens förening
8. Företagarna
9. Försvarets materielverk
10. Försvarets radioanstalt
11. Försvarsmakten
12. Förvaltningsrätten i Stockholm
13. Getswish AB
14. Integritetsskyddsmyndigheten
15. Justitiekanslern
16. Kammarrätten i Stockholm
17. Kommerskollegium
18. Kommunförsäkringsföreningen
19. Konkurrensverket
20. Konsumentverket

Telefonväxel: 08-405 10 00

Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 24
E-post: fi.registrator@regeringskansliet.se

21. Kronofogdemyndigheten
22. Kungl. Tekniska Högskolan, Cybercampus Sverige
23. Myndigheten för digital förvaltning (Digg)
24. Myndigheten för samhällsskydd och beredskap
25. Nasdaq Clearing AB
26. Nasdaq Stockholm AB
27. Nordic Growth Market NGM AB
28. Pensionsmyndigheten
29. Polismyndigheten
30. Post- och telestyrelsen
31. Regelrådet
32. Revisorsinspektionen
33. RISE Research Institute of Sweden
34. Riksdagens ombudsmän (JO)
35. Riksgäldskontoret
36. Småföretagarnas Riksförbund
37. Sparbankernas Riksförbund
38. Stockholms universitet, Juridiska fakulteten
39. Svensk försäkring
40. Svensk Värdepappersmarknad
41. Svenska Bankföreningen
42. Svenska försäkringsförmedlares förening
43. Svenska journalistförbundet
44. Svenska Kreditföreningen
45. Svenska Pensionsstiftelsers Förening
46. Svenska skeppshypotekskassan
47. Svenskt Näringsliv
48. Sveriges Advokatsamfund
49. Sveriges konsumenter
50. Sveriges riksbank

51. Swedish FinTech Association
52. Swedish House of Finance
53. Swedish Private Equity & Venture Capital Association (SVCA)
54. Säkerhetspolisen
55. Tech Sverige
56. Totalförsvarets forskningsinstitut
57. Trafikförsäkringsföreningen
58. TU – medier i Sverige
59. Vetenskapsrådet
60. Verket för innovationssystem (Vinnova)

Remissvaren ska ha kommit in till Finansdepartementet **senast den 15 april 2024**. Svaren bör lämnas per e-post till fi.remissvar@regeringskansliet.se och med kopia till anna.stenberg@regeringskansliet.se. Ange diarienummer Fi2024/00073 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i promemorian. Om remissen är begränsad till en viss del av promemorian, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Promemorian kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Lotta Hardvik Cederstierna
Rättschef