155. löggjafarþing 2024–2025.
Þingskjal x — x. mál.
Stjórnarfrumvarp.

Frumvarp til laga

um stafrænan viðnámsþrótt fjármálamarkaðar.

Frá fjármála- og efnahagsráðherra.

1. gr.
Markmið.

Markmið laga þessara er að stuðla að stafrænum rekstrarlegum viðnámsþrótti fjármálastofnana með samræmdum kröfum um áhættustýringu og viðbúnað.

2. gr.
Gildissvið.

Lög þessi gilda um aðila á fjármálamarkaði skv. 2. gr. reglugerðar (ESB) 2022/2554.

Lög þessi gilda einnig um lífeyrissjóði samkvæmt skilgreiningu laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða og teljast þeir til aðila á fjármálamarkaði í skilningi 2. mgr. 2. gr. reglugerðar (ESB) 2022/2554.

3. gr.
Lögfesting.

Ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx, skulu hafa lagagildi hér á landi með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar nr. xxx/2024 frá xx.xxx 2024, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX, bls. X, sbr. einnig bókun 1 um altæka aðlögun við EES-samninginn, sbr. lög um Evrópska efnahagssvæðið, nr. 2/1993, þar sem bókunin er lögfest.

Þegar vísað er til laga þessara í lögunum er jafnframt átt við reglugerð ESB samkvæmt ákvæði þessu.

4. gr.
Skýring hugtaka.

Eftirfarandi hugtök í reglugerð (ESB) 2022/2554 hafa svofellda merkingu:

1. *Aðilar á fjármálamarkaði sem eru tilgreindir sem nauðsynlegar eða mikilvægar rekstrareiningar samkvæmt landslögum sem lögleiða 3. gr. tilskipunar (ESB) 2022/2555:* Rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, sem jafnframt teljast til aðila á fjármálamarkaði samkvæmt lögum þessum.

2. *Aðilar sem um getur í 4.–23. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB:* Aðilar sem um getur í 1. og 3. málsl. 2. mgr. 1. gr. a laga um fjármálafyrirtæki, nr. 161/2002.
3. *Dótturfélag í skilningi 10. liðar 2. gr. og 22. gr. tilskipunar 2013/34/ESB:* Dótturfélag samkvæmt lögum um ársreikninga, nr. 6/2003.
4. *Einstaklingar eða lögaðilar sem njóta undanþágu skv. 2. og 3. gr. tilskipunar 2014/65/ESB:* Einstaklingar eða lögaðilar sem njóta undanþágu skv. 1. mgr. 2. gr. laga um markaði fyrir fjármálagerninga, nr. 115/2021.
5. *Endurtryggingafélag samkvæmt 4. lið 13. gr. tilskipunar 2009/138/EB:* Endurtryggingafélag í skilningi laga um vátryggingastarfsemi, nr. 100/2016.
6. *Endurtryggingamiðlari samkvæmt 5. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97:* Vátryggingamiðlari í skilningi laga um dreifingu vátrygginga, nr. 62/2019.
7. *Greiðslustofnun samkvæmt 4. lið 4. gr. tilskipunar (ESB) nr. 2015/2366:* Greiðslustofnun samkvæmt lögum um greiðsluþjónustu, nr. 114/2021.
8. *Greiðslustofnun sem er undanþegin samkvæmt tilskipun (ESB) 2015/2366*: Greiðslustofnun með takmarkað starfsleyfi samkvæmt 34. gr. laga um greiðsluþjónustu, nr. 114/2021.
9. *Móðurfélag í skilningi 9. liðar 2. gr. og 22. gr. tilskipunar 2013/34/ESB:* Móðurfélag samkvæmt lögum um ársreikninga, nr. 6/2003.
10. *Nauðsynleg eða mikilvæg rekstrareining sem fellur undir tilskipun (ESB) 2022/2555:* Mikilvægir innviðir í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, sem jafnframt teljast til aðila á fjármálamarkaði samkvæmt lögum þessum.
11. *Nauðsynlegir starfsþættir í skilningi 35. liðar 1. mgr. 2. gr. tilskipunar 2014/59/ESB:* Nauðsynleg starfsemi í skilningi laga um skilameðferð lánastofnana og verðbréfafyrirtækja, nr. 70/2020.
12. *Net- og upplýsingakerfi samkvæmt 1. lið 6. gr. tilskipunar (ESB) 2022/2555:* Net- og upplýsingakerfi samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019 .
13. *Póstgíróstofnanir samkvæmt 3. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB:* Póstgíróstofnanir skv. 1. málsl. 2. mgr. 1. gr. a laga um fjármálafyrirtæki, nr. 161/2002.
14. *Rafeyrisfyrirtæki samkvæmt 1. lið 2. gr. tilskipunar Evrópuþingsins og ráðsins 2009/110/EB:* Rafeyrisfyrirtæki samkvæmt lögum um útgáfu og meðferð rafeyris, nr. 17/2013.
15. *Rafeyrisfyrirtæki sem njóta undanþágu samkvæmt tilskipun 2009/110/EB:* Aðilar með takmarkað starfsleyfi skv. 16. gr. laga um útgáfu og meðferð rafeyris, nr. 17/2013.
16. *Reikningsupplýsingaþjónustuveitandi samkvæmt 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366:* Reikningsupplýsingaþjónustuveitandi samkvæmt lögum um greiðsluþjónustu, nr. 114/2021.
17. *Rekstraraðili sérhæfðra sjóða eins og um getur í 2. mgr. 3. gr. tilskipunar 2011/61/ESB:* Rekstraraðilar sérhæfðra sjóða sem falla ekki undir 1. mgr. 6. gr. laga um rekstraraðila sérhæfðra sjóða, nr. 45/2020.
18. *Rekstraraðili samkvæmt b-lið 1. mgr. 4. gr. tilskipunar 2011/61/ ESB:* Rekstraraðili samkvæmt lögum um rekstraraðila sérhæfðra sjóða, nr. 45/2020.
19. *Rekstrarfélag samkvæmt b-lið 1. mgr. 2. gr. tilskipunar 2009/65/EB:* Rekstrarfélag verðbréfasjóða samkvæmt lögum um verðbréfasjóði, nr. 116/2021.
20. *Samstæða í skilningi 11. liðar 2. gr. tilskipunar 2013/34/ESB:* Samstæða samkvæmt lögum um ársreikninga, nr. 6/2003.

21. *Skilavald samkvæmt 3. gr. tilskipunar 2014/59/ESB:* Skilavald samkvæmt 4. gr. laga um skilameðferð lánastofnana og verðbréfafyrirtækja, nr. 70/2020.
22. *Skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni samkvæmt tilskipun (ESB) 2022/2555*: Tilkynningaskylda um alvarleg atvik eða áhættu samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
23. *Stjórn í skilningi 36. liðar 1. mgr. 4. gr. tilskipunar 2014/65/ESB, 7. liðar 1. mgr. 3. gr. tilskipunar 2013/36/ESB og s-liðar 1. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins 2009/65/EB (31):* Stjórn í skilningi laga um hlutafélög.
24. *Stofnun um starfstengdan lífeyri samkvæmt 1. lið 6. gr. tilskipunar (ESB) 2016/2341:* Starfstengdur eftirlaunasjóður samkvæmt lögum um starfstengda eftirlaunasjóði, nr. 78/2007.
25. *Vátrygginga- og endurtryggingafélög eins og um getur í 4. gr. tilskipunar 2009/138/EB:* Vátryggingafélag samkvæmt lögum um vátryggingastarfsemi, nr. 100/2016.
26. *Vátryggingafélag samkvæmt 1. lið 13. gr. tilskipunar 2009/138/EB*: Vátryggingafélag í skilningi laga um vátryggingastarfsemi, nr. 100/2016.
27. *Vátryggingamiðlari í hliðarstarfsemi samkvæmt 4. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97:* Aðili sem dreifir vátryggingu sem aukaafurð í skilningi laga um dreifingu vátrygginga, nr. 62/2019.
28. *Verðbréfafyrirtæki samkvæmt 1. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB:* Verðbréfafyrirtæki samkvæmt lögum um markaði fyrir fjármálagerninga, nr. 115/2021.
29. *Viðbragðsteymi vegna váatvika er varða tölvuöryggi sem er tilnefnt eða komið á fót í samræmi við tilskipun (ESB) 2022/2555:* Netöryggissveit samkvæmt lögum um Fjarskiptastofu, nr. 75/2021.
30. *Viðskiptavettvangur samkvæmt 24. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB:* Viðskiptavettvangur samkvæmt lögum um markaði fyrir fjármálagerninga, nr. 115/2021.
31. *Öryggi net- og upplýsingakerfa samkvæmt 2. lið 6. gr. tilskipunar (ESB) 2022/2555:* Öryggi net- og upplýsingakerfa samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.

5. gr.

Eftirlit og upplýsingagjöf.

Seðlabanki Íslands er lögbært yfirvald hér á landi í skilningi reglugerðar (ESB) 2022/2554 og fer Fjármálaeftirlitið með þau verkefni sem því eru falin.

Fjármálaeftirlitið og Eftirlitsstofnun EFTA annast eftirlit samkvæmt lögum þessum í samræmi við EES-samninginn, sbr. lög um Evrópska efnahagssvæðið og samning milli EFTA-ríkjanna um stofnun eftirlitsstofnunar og dómstóls. Um eftirlitið fer samkvæmt ákvæðum laga þessara, laga um opinbert eftirlit með fjármálastarfsemi og laga um evrópskt eftirlitskerfi á fjármálamarkaði.

Um valdheimildir Eftirlitsstofnunar EFTA er nánar fjallað í 35.–42. gr. reglugerðar (ESB) 2022/2554. Til þeirra rannsóknaraðgerða sem kveðið er á um í 35. og 37.–39. gr. reglugerðar (ESB) nr. 2022/2554 þarf heimild dómara nema samþykki þess aðila sem rannsóknaraðgerðirnar beinast að liggi fyrir. Um beiðni um heimild dómara til rannsóknaraðgerða fer eftir XV. kafla laga um meðferð sakamála eftir því sem við á.

Seðlabanki Íslands ber ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun samkvæmt 9. mgr. 26. gr. reglugerðar (ESB) 2022/2554.

6. gr.

Alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegri netógn.

Tilkynningum aðila á fjármálamarkaði um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir skv. 19. gr. reglugerðar (ESB) 2022/2554 skal í samræmi við ákvæði laga þessara beint til Fjármálaeftirlitsins.

Um miðlun upplýsinga skv. 1. mgr. af hálfu Fjármálaeftirlitsins til Evrópsku bankaeftirlitsstofnunarinnar, Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunarinnar, Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar og Seðlabanka Evrópu fer samkvæmt 6.–7. mgr. 19. gr. reglugerðarinnar.

Við viðtöku tilkynningar skv. 1. mgr. fer um viðbrögð Fjármálaeftirlitsins samkvæmt 22. gr. reglugerðar (ESB) 2022/2554 og ef við á skal Seðlabanki Íslands gera allar ráðstafanir til að vernda öryggi fjármálakerfisins. Hið sama á við þegar Fjármálaeftirlitinu berast upplýsingar um alvarleg atvik eða verulega netógn frá þeim aðilum sem um getur í 2. mgr. Fjármálaeftirlitið skal leggja mat á mikilvægi atviks eða ógnar og tilkynna öðrum innlendum stjórnvöldum tímanlega um það eftir því sem við á.

7. gr.

Heimildir til eftirfylgni og birting ákvarðana aðaleftirlitsaðila.

Um eftirfylgni tilmæla frá aðaleftirlitsaðila af hálfu Fjármálaeftirlitsins fer samkvæmt 42. gr. reglugerðar (ESB) 2022/2554 og er Fjármálaeftirlitinu heimilt að nýta eftirlitsheimildir samkvæmt lögum um opinbert eftirlit með fjármálastarfsemi eftir því sem við á.

Fjármálaeftirlitið skal birta ákvarðanir um ráðstafanir vegna brota á ákvæðum laga þessara í samræmi við 42. gr. og e-lið 4. mgr. 50. gr. reglugerðar (ESB) 2022/2554.

8. gr.

Aðfararhæfi ákvarðana Eftirlitsstofnunar EFTA og dóma EFTA-dómstólsins.

Ákvarðanir Eftirlitsstofnunar EFTA samkvæmt lögum þessum eru aðfararhæfar, sem og dómar og úrskurðir EFTA-dómstólsins.

9. gr.

Úrbætur.

Komi í ljós að ákvæðum laga þessara, eða stjórnvaldsfyrirmæla settra með stoð í þeim, sé ekki fylgt getur Fjármálaeftirlitið krafist þess að úr sé bætt innan hæfilegs frests.

10. gr.

Stjórnvaldssektir.

Fjármálaeftirlitið getur lagt stjórnvaldssektir á hvern þann sem brýtur gegn stjórnvaldsfyrirmælum settum á grundvelli laganna eða eftirtöldum ákvæðum reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554:

a. 5. gr. um stjórnunarhætti og skipulag.
b. 6. gr. um áhættustýringarramma í upplýsinga- og fjarskiptatækni.
c. 7. gr. um upplýsinga- og fjarskiptatæknikerfi, -samskiptareglur og -búnað.
d. 8. gr. um auðkenningu.
e. 9. gr. um verndun og forvarnir.
f. 10. gr. um greiningu.
g. 11. gr. um viðbrögð og endurreisn.

h. 12. gr. um stefnur og verklag við öryggisafritun, verklag og aðferðir við endurheimt og endurreisn.
i. 13. gr. um lærdóm og þróun.
j. 14. gr. um samskipti.
k. 16. gr. um einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni.
l. 17. gr. um atvikastjórnunarferli sem tengist upplýsinga- og fjarskiptatækni.
m. 18. gr. um flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum.
n. 19. gr. um tilkynningar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni.
o. 20. gr. um greiðslutengd rekstrar- eða öryggisatvik sem varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki.
p. 24. gr. um almennar kröfur um framkvæmd prófunar á stafrænum rekstrarlegum viðnámsþrótti.
q. 26. gr. um auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði, kerfum og ferlum sem byggjast á ógnamiðaðri innbrotsprófun.
r. 27. gr. um kröfur fyrir prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun.
s. 28. gr. um almennar meginreglur við stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila.
t. 30. gr. um helstu samningsákvæði við þriðju aðila.

Sektir sem lagðar eru á einstaklinga geta numið frá 100 þús. kr. til 700 millj. kr. Sektir sem lagðar eru á lögaðila geta numið frá 500 þús. kr. til 800 millj. kr., en geta þó verið hærri eða allt að 10% af heildarveltu samkvæmt síðasta samþykkta ársreikningi lögaðilans eða 10% af síðasta samþykkta samstæðureikningi ef lögaðili er hluti af samstæðu.

Þrátt fyrir 2. mgr. er heimilt að ákvarða einstaklingi eða lögaðila sem brýtur gegn lögum þessum eða stjórnvaldsfyrirmælum settum á grundvelli þeirra stjórnvaldssekt sem nemur allt að tvöfaldri þeirri fjárhæð sem fjárhagslegur ávinningur af brotinu nemur.

Ákvarðanir um stjórnvaldssektir eru aðfararhæfar. Sektir renna í ríkissjóð að frádregnum kostnaði við innheimtuna. Séu stjórnvaldssektir ekki greiddar innan mánaðar frá ákvörðun Fjármálaeftirlitsins skal greiða dráttarvexti af fjárhæð sektarinnar. Um ákvörðun og útreikning dráttarvaxta fer eftir lögum um vexti og verðtryggingu, nr. 38/2001.

11. gr.

Saknæmi.

Stjórnsýsluviðurlögum verður beitt óháð því hvort lögbrot eru framin af ásetningi eða gáleysi.

12. gr.

Ákvörðun stjórnsýsluviðurlaga.

Við ákvörðun stjórnsýsluviðurlaga, þar á meðal um fjárhæð stjórnvaldssekta, skal tekið tillit til allra atvika sem máli skipta, þ.m.t. eftirfarandi eftir því sem við á:

a. alvarleika brots og hvað það hefur staðið lengi,
b. ábyrgðar hins brotlega,
c. fjárhagsstöðu hins brotlega, sér í lagi með hliðsjón af ársveltu lögaðila eða árstekjum og eignum einstaklings,
d. þýðingar ávinnings eða taps sem forðað var með broti fyrir hinn brotlega,
e. hvort brot hafi leitt til taps þriðja aðila og, ef við á, hvers konar mögulegra kerfislegra áhrifa brotsins,
f. samstarfsvilja hins brotlega,

g. fyrri brota hins brotlega.

13. gr.

Sátt.

Hafi aðili gerst brotlegur við ákvæði laga þessara eða ákvarðanir Fjármálaeftirlitsins á grundvelli þeirra er Fjármálaeftirlitinu heimilt að ljúka málinu með sátt með samþykki málsaðila, enda sé ekki um að ræða meiri háttar brot sem refsiviðurlög liggja við. Sátt er bindandi fyrir málsaðila þegar hann hefur samþykkt og staðfest efni hennar með undirskrift sinni.

Seðlabanki Íslands setur nánari reglur um framkvæmd 1. mgr.

14. gr.

Réttur grunaðs manns.

Í máli sem beinist að einstaklingi og lokið getur með ákvörðun um stjórnsýsluviðurlög skv. lögum þessum hefur sá sem rökstuddur grunur leikur á að hafi gerst sekur um lögbrot rétt til að neita að svara spurningum eða afhenda gögn eða muni nema hægt sé að útiloka að það geti haft þýðingu fyrir ákvörðun um brot hans. Fjármálaeftirlitið skal leiðbeina hinum grunaða um þennan rétt.

15. gr.

Frestur til að beita stjórnsýsluviðurlögum.

Heimild Fjármálaeftirlitsins til að leggja á stjórnsýsluviðurlög samkvæmt lögum þessum fellur niður þegar sjö ár eru liðin frá því að háttsemi lauk.

Frestur skv. 1. mgr. rofnar þegar Fjármálaeftirlitið tilkynnir aðila um rannsókn á meintu broti. Rof frests hefur réttaráhrif gagnvart öllum sem staðið hafa að broti.

16. gr.

Stjórnvaldsfyrirmæli.

Ráðherra er heimilt að setja reglugerð til að innleiða undirgerðir sem framkvæmdastjórn Evrópusambandsins samþykkir með stoð í reglugerð (ESB) 2022/2554 um þau atriði sem koma fram í eftirfarandi greinum hennar:

1. 6. mgr. 31. gr. um viðmiðanir til grundvallar útnefningu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.
2. 7. mgr. 32. gr. um samstarf og upplýsingaskipti eftirlitsstofnana vegna eftirlitsramma mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.
3. 1. mgr. 41. gr. um samræmingu skilyrða vegna eftirlitsramma mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.
4. 2. mgr. 43. gr. um gjöld sem Eftirlitsstofnun EFTA leggur á mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

Seðlabanka Íslands er heimilt að setja reglur til að innleiða undirgerðir sem framkvæmdastjórn Evrópusambandsins samþykkir með stoð í reglugerð (ESB) 2022/2554 um þau atriði sem koma fram í eftirfarandi greinum hennar:

1. 11. mgr. 11. gr. um mat á samanlögðum árlegum kostnaði og tapi af völdum alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni.
2. 15. gr. um frekari samhæfingu búnaðar, aðferða, ferla og stefna til stýringar á upplýsinga- og fjarskiptatækniáhættu.

3. 3. mgr. 16. gr. um einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni.
4. 3. og 4. mgr. 18. gr. um flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum.
5. 20. gr. um samræmingu á efni og sniðmátum tilkynninga.
6. 11. mgr. 26. gr. um auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði, -kerfum og -ferlum sem byggjast á ógnamiðaðri innbrotsprófun.
7. 9. og 10. mgr. 28. gr. um almennar meginreglur um trausta stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila.
8. 5. mgr. 30. gr. um ákvörðun og mat þegar undirverktaki styður við nauðsynlega eða mikilvæga starfsemi upplýsinga- og fjarskiptatækniþjónustu þriðja aðila.

17. gr.
Innleiðing.

Lög þessi fela í sér innleiðingu á:

1. Tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2556 frá 14. desember 2022 um breytingu á tilskipunum 2009/65/EB, 2009/138/EB, 2011/61/ESB, 2013/36/ESB, 2014/59/ESB, 2014/65/ESB, (ESB) 2015/2366 og (ESB) 2016/2341 að því er varðar stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann sem birt var í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. XX frá XX.XX.XXXX, bls. XX-XX.
2. Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 sem birt var í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. XX frá XX.XX.XXXX, bls. XX-XX.

18. gr.
Gildistaka.

Lög þessi öðlast gildi 1. júlí 2025.

19. gr.
Breyting á öðrum lögum.

Við gildistöku laga þessara verða eftirfarandi breytingar á öðrum lögum:

1. *Lög um verðbréfasjóði, nr. 116/2021*:
   a. Við 2. tölul. 3. mgr. 15. gr. bætist 1. gr. laganna bætist ný málsgrein, svohljóðandi: þ.m.t. að því er varðar net- og upplýsingakerfi sem sett eru upp og stjórnað í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554.
2. *Lög um vátryggingastarfsemi, nr. 100/2016:*
   a. Við 5. mgr. 39. gr. laganna bætist: og skulu setja upp og stjórna net- og upplýsingakerfum í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554.
   b. Eftirfarandi breytingar verða á 44. gr. laganna:
      a. Við 4. mgr. bætist: aðra en þá sem varða stýringu upplýsinga- og fjarskiptatækniáhættu.
      b. Við e-lið 5. mgr. bætist: aðra en þá þætti sem varðar stýringu upplýsinga- og fjarskiptatækniáhættu.
3. *Lög um rekstraraðila sérhæfða sjóða, nr. 45/2020:*

a. Við 2. tölul. 4. mgr. 19. gr. laganna bætist: þ.m.t. er varðar net- og upplýsingakerfi sem sett eru upp og stjórnað í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554.

4. *Lög um fjármálafyrirtæki, nr. 161/2002:*
    a. Á eftir orðunum „þ.m.t. traust stjórnunar- og bókhaldsfyrirkomulag“ í 1. mgr. 50. gr. laganna kemur: net- og upplýsingakerfi, sem sett eru upp og stjórnað í samræmi við reglugerð (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], [og].
    b. 2. mgr. 78. gr. g laganna orðast svo: Fjármálafyrirtæki skal hafa viðbragðsáætlun og áætlun um samfelldan rekstur, þ.m.t. stefnur og áætlanir um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurheimtaráætlanir fyrir þá upplýsinga- og fjarskiptatækni sem notuð er við sendingu upplýsinga, og að þessum áætlunum sé komið á, stjórnað og prófaðar í samræmi við 11. gr. reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], til að tryggja áframhaldandi starfsemi sína og takmörkun á tjóni ef alvarleg röskun verður á starfsemi fyrirtækisins.
    c. C-liður 3. mgr. 80. gr. laganna orðast svo: áhættu sem álagspróf og prófanir á stafrænum rekstrarlegum viðnámsþrótti í samræmi við IV. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], leiða í ljós, með hliðsjón af eðli, umfangi og því hversu margþætt starfsemi fjármálafyrirtækisins er.
    d. Við 6. tölul. 3. mgr. 107. gr. a laganna bætist: s.s. til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og um getur í V. kafla reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].

5. *Lög um skilameðferð lánastofnana og verðbréfafyrirtækja, nr. 70/2020:*
    a. Á eftir orðunum „Starfsemi, þjónusta eða rekstur“ í 28. tölul. 1. mgr. 3. gr. laganna bætist: þ.m.t. net- og upplýsingakerfi eins og um getur í reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].
    b. Á eftir orðunum „áframhald nauðsynlegrar starfsemi“ í 2. mgr. 13. gr. laganna kemur: og stafræns rekstrarlegs viðnámsþróttar.
    c. Á eftir orðunum „frá öðrum starfsþáttum“ í 8. tölul. 3. mgr. 15. gr. laganna kemur: og tryggja stafrænan rekstrarlegan viðnámsþrótt [við].
    d. Eftirfarandi breytingar verða á 62. gr. laganna:
        i. Við 3. mgr. bætist: þ.m.t. að þjónustu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega starfsemi fyrirtækis eða einingu í skilameðferð eins og um getur í reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].
        ii. Við 1. tölul. 4. mgr. bætist: þ.m.t. samningsbundnu fyrirkomulagi um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega starfsemi fyrirtækis eða einingu í skilameðferð að teknu tilliti til niðurstaðna prófana á stafrænum rekstrarlegum viðnámsþrótti samkvæmt reglugerð Evrópuþingsins og ráðsins

(ESB) 2022/20554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].

6. *Lög um markaði fyrir fjármálagerninga, nr. 115/2021:*
   a. Við 1. tölul. 1. mgr. 3. gr. laganna bætist nýr stafliður, svohljóðandi: 62. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx.
   b. Eftirfarandi breytingar verða á 21. gr. laganna:
      i. 3. mgr. orðast svo:
         Verðbréfafyrirtæki skal gera eðlilegar ráðstafanir til að tryggja að fjárfestingarþjónusta og -starfsemi sé samfelld og reglubundin. Með þetta að markmiði skal verðbréfafyrirtækið nota viðeigandi og hæfileg kerfi, þ.m.t. upplýsinga- og fjarskiptatæknikerfi sem sett eru upp og stjórnað í samræmi við 7. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], sem og viðeigandi og hæfileg tilföng og verklag.
      ii. 5. mgr. orðast svo:
         Verðbréfafyrirtæki skal hafa traustar aðferðir fyrir stjórnun og bókhald, innri eftirlitskerfi og skilvirkar verklagsreglur fyrir áhættumat.
      iii. 6. mgr. orðast svo:
         Verðbréfafyrirtæki skal hafa trausta öryggisferla til að tryggja, í samræmi við kröfurnar sem mælt er fyrir um í reglugerð (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], öryggi og sannvottun leiða til að senda upplýsingar, draga eins og kostur er úr hættu á spillingu gagna og óheimiluðum aðgangi og koma í veg fyrir leka upplýsinga, og þar með gæta að leynd gagna á öllum tímum, án þess að slíkt hafi áhrif á heimild Fjármálaeftirlitsins til að krefjast aðgangs að samskiptum í samræmi við lög þessi og reglugerð (ESB) nr. 600/2014.
   c. 1. mgr. 25. gr. laganna orðast svo:
      Verðbréfafyrirtæki sem hefur með höndum algrímsviðskipti skal ráða yfir skilvirkum kerfum og stjórntækjum vegna eftirlits með áhættu sem henta vel til þeirrar starfsemi sem það stundar til að tryggja að viðskiptakerfi þess séu álagsþolin og búi yfir nægilegri getu, í samræmi við kröfurnar sem mælt er fyrir um í II. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], falli undir viðeigandi viðskiptamörk og -takmarkanir og komi í veg fyrir sendingu rangra fyrirmæla eða að kerfin séu að öðru leyti þannig að þau skapi eða stuðli að óróleika á markaði. Slíkt fyrirtæki skal einnig ráða yfir skilvirkum kerfum og sinna áhættuvörnum til að tryggja að ekki sé unnt að nota viðskiptakerfin í tilgangi sem gengur gegn reglugerð (ESB) nr. 596/2014 [sbr. lög um aðgerðir gegn markaðssvikum, nr. 60/2021,] eða reglum þess

viðskiptavettvangs sem það tengist. Verðbréfafyrirtækið skal hafa til staðar skilvirkt fyrirkomulag til að halda samfellu í rekstri við bilun í viðskiptakerfum þess, þ.m.t. stefnu og áætlanir um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlanir fyrir upplýsinga- og fjarskiptatæknikerfi sem komið er á í samræmi við 11. gr. reglugerðar (ESB) 2022/2554, og skal sjá til þess að kerfin séu að fullu prófuð og undir viðeigandi eftirliti til að tryggja að þau uppfylli almennu kröfurnar sem mælt er fyrir um í þessari málsgrein og allar sértækar kröfur sem mælt er fyrir um í II. og IV. kafla reglugerðar (ESB) 2022/2554.

d. 2. tölul. 1. mgr. 78. gr. laganna orðast svo:

Vera nægilega vel í stakk búinn til að stýra áhættum sem að honum snúa, þ.m.t. að stýra upplýsinga- og fjarskiptatækniáhættu í samræmi við II. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], koma á viðeigandi ráðstöfunum og kerfum til að greina allar verulegar áhættur fyrir rekstur hans og koma á skilvirkum ráðstöfunum til að draga úr þeim.

e. 1. mgr. 83. gr. laganna orðast svo:

Skipulegur markaður skal koma á og viðhalda rekstrarlegum viðnámsþrótti sínum í samræmi við kröfurnar sem mælt er fyrir um í II. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar] til að tryggja að viðskiptakerfi hans séu álagsþolin, búi yfir nægilegri getu til að ráða við álagstoppa í magni tilboða og skilaboða, geti tryggt hnökralaus viðskipti þegar mikið álag er á markaði, hafi verið prófuð að fullu til að tryggja að þessi skilyrði séu uppfyllt og falli undir skilvirkt fyrirkomulag til rekstrarsamfellu, þ.m.t. stefnu og áætlanir um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlanir fyrir upplýsinga- og fjarskiptatækni sem komið er á í samræmi við 11. gr. reglugerðar (ESB) 2022/2554, til að tryggja samfellu í þjónustu hans ef bilun verður í viðskiptakerfum hans.

f. 1. mgr. 85. gr. laganna orðast svo:

Skipulegur markaður skal hafa skilvirk kerfi, verkferla og fyrirkomulag sem m.a. skyldar þátttakendur til að framkvæma fullnægjandi prófanir á algrími og bjóði upp á umhverfi til að greiða fyrir slíkri prófun í samræmi við kröfurnar sem mælt er fyrir um í II. og IV. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar] til að tryggja að algrímsviðskiptakerfi geti ekki skapað eða stuðlað að truflunum á aðstæðum til viðskipta og til að bregðast við slíkum truflunum af völdum slíkra algrímskerfa, þ.m.t. kerfi sem getur takmarkað hlutfall óframkvæmdra tilboða sem aðili eða þátttakandi setur inn í kerfið, til að geta hægt á flæði tilboða ef hætta er á því að kerfi þess nálgist getumörk og takmarkað og framfylgt lágmarksverðskrefi sem heimilt er að framkvæma á markaði.

7. *Lög um greiðsluþjónustu, nr. 114/2021:*

a. 10. tölul. 1. mgr. 2. gr. laganna orðast svo:

Þjónustu sem þau tækniþjónustufyrirtæki veita sem annast stoðþjónustu við greiðsluþjónustu, án þess að þau hafi nokkurn tíma eignarhald á þeim fjármunum sem millifæra skal, þ.m.t. úrvinnsla og geymsla gagna,

traustþjónusta og þjónusta við verndun friðhelgi einkalífs, sannvottun gagna og eininga, veitingu upplýsinga- og fjarskiptatækniþjónustu, útvegun og viðhald skjástöðva og búnaðar fyrir greiðsluþjónustu, að undanskilinni greiðsluvirkjun og reikningsupplýsingaþjónustu.

b. Eftirfarandi breytingar verða á 1. mgr. 4. gr. laganna:

i. 11. tölul. orðast svo:

Lýsing á stjórnarformi umsækjanda og innri eftirlitskerfum, þ.m.t. aðferðir við stjórnun, áhættustýringu og reikningsskil, auk fyrirkomulags fyrir notkun upplýsinga- og fjarskiptatækniþjónustu í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], sem sýnir að þeir stjórnarhættir og innra eftirlitskerfi séu í réttu hlutfalli við starfsemina, viðeigandi, traustir og fullnægjandi.

ii. 10. tölul. orðast svo:

Lýsing á málsmeðferðinni sem er fyrir hendi til að hafa eftirlit með, meðhöndla og fylgja eftir rekstrar- eða öryggisfrávikum og kvörtunum viðskiptavina að því er varðar öryggisatriði, þ.m.t. fyrirkomulag skýrslugjafar um atvik sem tekur tillit til tilkynningarskyldu greiðslustofnunarinnar sem mælt er fyrir um í III. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].

iii. 14. tölul. orðast svo:

Lýsing á fyrirkomulagi rekstrarsamfellu sem hefur að geyma skýra tilgreiningu á mikilvægri starfsemi, skilvirkri stefnu og áætlunum um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlunum fyrir upplýsinga- og fjarskiptatækni og ferlinu til að kanna reglulega og endurskoða hversu fullnægjandi og skilvirkar slíkar áætlanir eru í samræmi við reglugerð (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar].

iv. Í stað 2. málsl. 16. tölul. kemur:

Ráðstafanirnar vegna öryggiseftirlits og mildunar sem um getur í 1. málsl. skulu tilgreina hvernig þær tryggja öflugan stafrænan rekstrarlegan viðnámsþrótt í samræmi við II. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], einkum í tengslum við tæknilegt öryggi og persónuvernd, þ.m.t. fyrir hugbúnað og upplýsinga- og fjarskiptatæknikerfi sem umsækjandinn, eða fyrirtækin sem hann útvistar starfsemi sína til að öllu leyti eða að hluta, notar. Þessar ráðstafanir skulu einnig innihalda öryggisráðstafanirnar sem mælt er fyrir um í 1. mgr. 99. gr. og er Seðlabankanum heimilt að setja nánari reglur um þær.

c. 1. málsl. 2. mgr. 18. gr. laganna orðast svo: Útvistun mikilvægra rekstrarþátta, þ.m.t. upplýsinga- og fjarskiptatæknikerfi, skal ekki fara þannig fram að hún rýri verulega gæði innra eftirlits greiðslustofnunar og getu Fjármálaeftirlitsins til að hafa eftirlit með og ganga úr skugga um að

greiðslustofnunin uppfylli allar þær skyldur sem mælt er fyrir um í lögum þessum.

d. Við 99. gr. laganna bætist ný málsgrein, svohljóðandi: Ákvæði 1. mgr. hefur ekki áhrif á framkvæmd II. kafla reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar] gagnvart lánastofnunum, rafeyrisfyrirtækjum, greiðslustofnunum, reikningsupplýsingaþjónustuveitendum, greiðslustofnunum með takmarkað starfsleyfi og aðila með takmarkað starfsleyfi skv. 16. gr. laga um meðferð og útgáfu rafeyris, nr. 17/2013.

e. Nýr málsliður bætist við 1. mgr. 100. gr. laganna, svohljóðandi: Þó gildir ákvæði þetta ekki um þá lánastofnanir, rafeyrisfyrirtæki, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur, greiðslustofnanir með takmarkað starfsleyfi og aðila með takmarkað starfsleyfi skv. 16. gr. laga um meðferð og útgáfu rafeyris, nr. 17/2013, enda gilda um þá ákvæði reglugerðar (ESB) 2022/2554 [sbr. lög um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar], þar með talið um sambærilega tilkynningaskyldu.

8. *Lög um öryggi net- og upplýsingakerfa mikilvægra aðila, nr. 78/2019*:
   a. Við 1. mgr. 8. gr. laganna bætist nýr málsliður, svohljóðandi: Um tilkynningar skv. 1. málsl. fer þó samkvæmt [lögum um stafrænan rekstrarlegan viðnámsþrótt fjármálamarkaðar] í tilviki rekstraraðila nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða.
9. *Lög um lánshæfismatsfyrirtæki, nr. 50/2017:*
   a. Við 1. tölul. 1. mgr. 2. gr. laganna bætist nýr stafliður, svohljóðandi: 59. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx.
10. *Lög um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018:*
   a. Við 1. mgr. 2. gr. laganna bætist nýr stafliður, svohljóðandi: 60. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx.
11. *Lög um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020:*
   a. Á eftir orðunum „bls. 160-192“ í 1. mgr. 3. gr. laganna kemur: og með breytingum samkvæmt 61. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx.
12. *Lög um fjárhagslegar viðmiðanir, nr. 7/2021:*

a. Á undan orðunum „og aðlögunum samkvæmt bókun 1“ í 1. mgr. 1. gr. laganna kemur: og 63. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. X frá XXX 2024, bls. xx-xx.

Greinargerð.

1. Inngangur.

Frumvarp þetta var samið í fjármála- og efnahagsráðuneytinu, í samráði við Seðlabanka Íslands. Tilgangur með framlagningu þess er að innleiða í íslenskan rétt ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (hér eftir DORA-reglugerðin eða DORA).

Með frumvarpinu er einnig lagt til að innleidd verði í landsrétt ákvæði tilheyrandi tilskipunar Evrópuþingsins og ráðsins (ESB) 2022/2556 um breytingu á tilskipunum 2009/65/EB, 2009/138/EB, 2011/61/ESB, 2013/36/ESB, 2014/59/ESB, 2014/65/ESB, (ESB) 2015/2366 og (ESB) 2016/2341 að því er varðar stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann (hér eftir DORA-tilskipunin).

Báðar voru DORA-reglugerðin og -tilskipunin samþykktar 14. desember 2022 og koma til framkvæmda í aðildarríkjum Evrópusambandsins 17. janúar 2025. Þær voru teknar upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. ___ frá ___ 2024, en gert er ráð fyrir að EFTA-ríkin innan Evrópska efnahagssvæðisins fái tiltekinn frest til að lögfesta gerðirnar frá þeim degi að telja.

2. Tilefni og nauðsyn lagasetningar.

2.1. Stafrænn fjármálapakki ESB og stafrænt áfallaþol.

DORA tilheyrir stafrænum fjármálapakka ESB sem fyrst var kynntur árið 2020, líkt og reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 um markaði fyrir sýndareignir og um viðbætur við reglugerðir (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipanir 2013/36/ESB og (ESB) 2019/1937 (MiCA) og reglugerð Evrópuþingsins og ráðsins (ESB) 2022/858 um tilraunaregluverk fyrir innviði markaða sem byggjast á dreifðri færsluskrártækni og um breytingu á reglugerðum (ESB) nr. 600/2014 og (ESB) nr. 909/2014 og tilskipun 2014/65/ESB (DFTR). DFTR var innleidd í landsrétt með lögum um innviði markaða fyrir fjármálagerninga sem byggjast á dreifðri færsluskrártækni, nr. 56/2024. Stafræna fjármálapakkanum er ætlað að stuðla að því að umgjörð fjármálamarkaða mæti nútímaþörfum, efldri samkeppni og nýsköpun, auk þess sem hugað er að fjárfestavernd, net- og upplýsingaöryggi ásamt fjármálastöðugleika. Net- og upplýsingaöryggi er ein tegund rekstraráhættu.

Í DORA er hugtakið stafrænn rekstrarlegur viðnámsþróttur, eða áfallaþol, í forgrunni. Það er skilgreint þannig: Geta aðila á fjármálamarkaði til að byggja upp, viðhalda og endurmeta heilleika og áreiðanleika í rekstri með því að tryggja, hvort heldur beint, eða óbeint með notkun upplýsinga- og fjarskiptatækniþjónustu þriðju aðila, alla þá getu sem tengist upplýsinga- og fjarskiptatækni sem þarf til að tryggja öryggi net- og upplýsingakerfa sem aðili á fjármálamarkaði notar og sem styður samfellda veitingu fjármálaþjónustu og gæði hennar,

þ.m.t. meðan röskun varir. Í stuttu máli kveður reglugerðin á um að aðilar á fjármálamarkaði skuli haga starfsemi sinni þannig að virk og viðeigandi áhættustýring tengd notkun net- og upplýsingatækniþjónustu sé viðhöfð í því skyni að stuðla að öflugum stafrænum viðnámsþrótti og lágmarka rof á mikilvægri þjónustu.

Upptaka DORA í EES-samninginn og innleiðing hennar í landsrétt er skilgreind sem aðgerð í sameiginlegri aðgerðaáætlun stjórnvalda í netöryggismálum, á grundvelli netöryggisstefnu fyrir Ísland 2022-2037.

2.2. Gildissvið og meðalhófsregla.

Gildissvið DORA er víðtækt. Samkvæmt orðanna hljóðan munu eftirtaldar tegundir eftirlitsskyldra aðila falla undir fyrirhuguð lög (sameiginlega nefndir *aðilar á fjármálamarkaði*), auk þjónustuveitenda á sviði net- og upplýsingatækni:

- Lánastofnanir, sbr. lög um fjármálafyrirtæki, nr. 161/2002, þar með talin Byggðastofnun og Lánasjóður sveitarfélaga,
- greiðslustofnanir og reikningsupplýsingaþjónustuveitendur, sbr. lög um greiðsluþjónustu, nr. 114/2021, þó ekki póstgíróstofnanir,
- rafeyrisfyrirtæki, sbr. lög um útgáfu og meðferð rafeyris, nr. 17/2013,
- verðbréfafyrirtæki, viðskiptavettvangar og veitendur gagnaskýrsluþjónustu, sbr. lög um markaði fyrir fjármálagerninga, nr. 115/2021, þó með undantekningum,
- verðbréfamiðstöðvar, sbr. lög um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020,
- miðlægir mótaðilar og afleiðuviðskiptaskrár, sbr. lög um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018,
- rekstraraðilar sérhæfðra sjóða, sbr. lög um rekstraraðila sérhæfðra sjóða, nr. 45/2020, þó með undantekningum,
- rekstrarfélög verðbréfasjóða, sbr. lög um verðbréfasjóði, nr. 116/2021,
- vátrygginga- og endurtryggingafélög, sbr. lög um vátryggingastarfsemi, nr. 100/2016, þó ekki félög sem undanþegin eru gildissviði þeirra skv. 3. gr.,
- vátryggingamiðlarar og aðilar sem dreifa vátryggingu sem aukaafurð, sbr. lög um dreifingu vátrygginga, nr. 62/2019, þó með undantekningum,
- stofnanir sem sjá um starfstengdan lífeyri, sbr. lög um starfstengda lífeyrissjóði, nr. 78/2007, þó með undantekningum,
- lánshæfismatsfyrirtæki, sbr. lög um lánshæfismatsfyrirtæki, nr. 50/2017,
- stjórnendur mikilvægra viðmiðana, sbr. lög um fjárhagslegar viðmiðanir, nr. 7/2021,
- þjónustuveitendur hópfjármögnunar, sbr. [lög um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki],
- verðbréfunarskrár, sbr. [lög um verðbréfun] og
- þjónustuveitendur sýndareigna, sbr. [lög um markaði sýndareigna].

Lagt er til að gildissvið fyrirhugaðra laga verði rýmkað umfram það sem DORA gerir ráð fyrir, þ.e. nái einnig til lífeyrissjóða á grundvelli laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, sbr. nánari umfjöllun um 2. gr. frumvarpsins. Eins og segir í 13.–14. lið inngangsorða DORA ættu aðilar á fjármálamarkaði að fylgja sömu nálgun og meginreglum þegar þeir takast á við upplýsinga- og fjarskiptatækniáhættu, að teknu tilliti til stærðar þeirra og heildaráhættusniðs og eðlis, umfangs og flækjustigs þjónustu þeirra,

starfsemi og reksturs. Samræmi stuðlar að aukinni tiltrú á fjármálakerfið og viðheldur stöðugleika þess. DORA á að stuðla að því að draga úr flækjustigi í framkvæmd, auka samleitni í eftirliti og réttarvissu, takmarka kostnað við að fara að reglum (ekki síst í starfsemi yfir landamæri), svo og draga úr röskun á samkeppni.

Ákvæði 4. gr. DORA kveður á um að aðilar á fjármálamarkaði skuli í starfsemi sinni framfylgja kröfum hennar í samræmi við meðalhófsregluna. Þá gerir DORA vægari kröfur til tiltekinna smærri aðila á fjármálamarkaði, sbr. m.a. 16. gr. og ýmis sérákvæði um örfyrirtæki. Að nokkru marki eru sérkröfur jafnframt tilgreindar í DORA um tiltekna aðila á fjármálamarkaði, svo sem verðbréfamiðstöðvar.

2.3. Mat á nauðsyn og mögulegar leiðir við lagasetningu.

Í inngangsorðum DORA (2. liður) er vísað til þess að upplýsinga- og fjarskiptatækni hefur á síðustu áratugum öðlast lykilhlutverk á sviði fjármálaþjónustu. Dæmigerð dagleg starfsemi aðila á fjármálamarkaði reiðir sig á virka upplýsinga- og fjarskiptatækniþjónustu og -kerfi. Net- og upplýsingatækniáhætta er hratt vaxandi áhættuþáttur á fjármálamarkaði, líkt og í öðrum geirum. Stöðugt þarf að endurmeta og treysta varnir gegn netárásum og styrkja getu til að bregðast við alvarlegum atvikum. Net- og upplýsingatækniöryggi er á meðal helstu stefnumarkandi áherslna og forgangsmála Seðlabanka Íslands í fjármálaeftirliti 2024.

Netógnir eru ekki aðeins í brennidepli frá sjónarhóli fjármálaeftirlits. Þannig hefur Evrópska kerfisáhætturáðið ítrekað varað við hættu á kerfislægum veikleikum og útbreiðslu netatvika óháð landfræðilegum mörkum vegna tenginga aðila og innviða á fjármálamarkaði í skýrslum frá árunum 2020 og 2022-2024. Alvarleg rof í upplýsinga- og fjarskiptatækni sem eiga sér stað í fjármálageiranum hafa ekki einungis áhrif á hvern aðila á fjármálamarkaði fyrir sig, eins og segir í 3. lið inngangsorða DORA. Þau geta einnig haft í för með sér skaðlegar afleiðingar fyrir fjármálastöðugleika, svo sem að skapa möguleg lausafjáráhlaup og almennt tap á trúnaði og trausti á fjármálamörkuðum. Líkt og vikið er að í 4. lið inngangsorða DORA hefur verið unnið að því víðar á alþjóðavettvangi að stuðla að frekari samræmingu bestu starfsvenja, reglusetningar og eftirlits, í því skyni að stuðla að stafrænum viðnámsþrótti á sviði fjármálamarkaða.

Íslandi ber þjóðréttarleg skylda til að taka EES-reglugerðir sem slíkar upp í landsrétt, sbr. a-lið 7. gr. EES-samningsins. DORA-reglugerðin verður því innleidd í landsrétt með tilvísunaraðferð, en ákvæði DORA-tilskipunarinnar með umritun (breytingum á ýmsum lögum).

Um ræðir frumvarp til nýrra laga um stafrænan viðnámsþrótt fjármálamarkaðar. Heildarlög munu leysa af hólmi ákvæði í settum lögum, reglugerðir, viðmiðunarreglur og leiðbeinandi tilmæli, eftir því sem við á. Evrópureglur á sviði fjármálaþjónustu hafa ekki verið samræmd að fullu eða á einsleitan hátt að því er varðar stafrænan rekstrarlegan viðnámsþrótt og öryggi í upplýsinga- og fjarskiptatækni fyrr en nú, með DORA, sbr. 8. lið inngangsorða.

Vikið er að rekstraráhættu í ýmsum gildandi íslenskum lögum um fjármálaþjónustu sem eiga það sameiginlegt að fela í sér innleiðingu á EES-reglum og munu þeir lagabálkar taka breytingum til samræmis við ákvæði DORA-reglugerðarinnar og -tilskipunarinnar. Í gildi eru leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila og nr. 6/2014 um útvistun hjá eftirlitsskyldum aðilum, auk þess sem Seðlabankinn tekur upp, birtir og fylgir eftir ýmsum viðmiðunarreglum evrópsku fjármálaeftirlitsstofnananna sem varða stjórnun áhættu vegna upplýsinga- og fjarskiptatækni. Þá ber þess að geta að fjallað er um rekstraráhættu í reglugerð nr. 590/2017 um eftirlitskerfi

með áhættu lífeyrissjóða, sem starfa á grundvelli laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997.

Fyrirhuguð lög verða sérlög gagnvart almennri netöryggislöggjöf, nú einkum lög um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, er fólu í sér innleiðingu á upphaflegri netöryggistilskipun (ESB) 2016/1148 (NIS1) en þau munu í fyrirsjáanlegri framtíð byggja á endurnýjaðri tilskipun (ESB) 2022/2555 (NIS2). Að því marki sem ný lög (DORA) geyma ríkari kröfur til aðila á fjármálamarkaði ganga þau með öðrum orðum framar, sbr. 16. lið inngangsorða og 2. tölul. 1. gr. DORA. Vísast og til 4. gr. NIS2 í þessu samhengi.

Ýmis ákvæði DORA verða nánar útfærð í afleiddum gerðum (tæknistöðlum), sem að mestu leyti verða innleiddar hér á landi í reglum Seðlabanka Íslands.

3. Meginefni frumvarpsins.

3.1. Samantekt

DORA kveður á um meginreglur og kröfur til umgjarðar áhættustýringar og viðbúnaðar af hálfu aðila á fjármálamarkaði að því er varðar net- og upplýsingaöryggi. Undirliggjandi er því öll fjármálastarfsemi hlutaðeigandi sem byggir á notkun net- og upplýsingakerfa og upplýsinga- og fjarskiptatækniþjónustu.

DORA kveður á um að aðilar á fjármálamarkaði uppfæri reglulega og skjalfesti umgjörð net- og upplýsingaöryggismála og skal hún háð virku eftirliti stjórnar. Framkvæmdastjórn ber að upplýsa stjórn með reglulegum hætti um stöðu upplýsinga- og fjarskiptatækniáhættu. Aðilar á fjármálamarkaði skulu viðhafa skýra yfirsýn yfir starfsemi sína á hverjum tíma, halda skrá yfir mikilvægar og nauðsynlegar upplýsinga- og fjarskiptatæknieignir sem þeir reiða sig á í starfseminni og kortleggja tengsl milli eigin starfsemi og upplýsinga- og fjarskiptatæknieigna þannig að nýtist vel og örugglega, svo sem í viðbrögðum við alvarlegu atviki. Aðili á fjármálamarkaði skal með reglubundnum hætti framkvæma áhættumat sem byggjast skal á greiningu með tilliti til mögulegra áhrifa ólíkra sviðsmynda á rekstur og á áhættusniði hlutaðeigandi starfsemi. Mikilvægum upplýsinga- og fjarskiptatæknieignum skal gefinn sérstakur gaumur í því samhengi, svo og mögulegum netógnum. Þá skulu áætlanir um samfelldan rekstur og viðbúnað skjalfestar, æfðar og uppfærðar reglulega og eftir því sem við á.

Með DORA er lögð á alla aðila á fjármálamarkaði sú skylda að fræða starfslið reglubundið um netöryggi og hættur sem steðjað geta að starfsemi vegna notkunar á upplýsinga- og fjarskiptatækni. Sú skylda nær til stjórnar, stjórnenda og ytri aðila (þjónustuveitenda).

Þá er með DORA kveðið á um samræmda tilkynningaskyldu gagnvart lögbæru yfirvaldi (hér Fjármálaeftirliti Seðlabanka Íslands) að því er varðar alvarleg atvik í eða tengdum net- og upplýsingakerfum og krafa gerð um skráningu og flokkun allra atvika. Valkvætt verður að tilkynna um áhættu eða ógn sem ekki hefur raungerst. Gildandi leiðbeinandi tilmæli gera ráð fyrir miðlun tilkynninga af þessu tagi til Fjármálaeftirlitsins. Vísast og til d-liðar kafla 3.3 í greinargerð þessari um 23. gr. og 5. tölul. 7. gr. DORA-tilskipunarinnar, sem fellir úr gildi skýrslugjöf samkvæmt lögum um greiðsluþjónustu (PSDII) gagnvart greiðsluþjónustuveitendum sem falla innan gildissviðs DORA, í því skyni að einfalda regluverkið. Aðilar á fjármálamarkaði sem útnefndir hafa verið rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi eða innviða fjármálamarkaða á grundvelli laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, eru samkvæmt þeim tilkynningaskyldir beint gagnvart netöryggissveit Fjarskiptastofu (CERT-IS) en með frumvarpi þessu er einnig lagt til að breyting verði á því. Ef við á mun Fjármálaeftirlitið á grundvelli 6. mgr. 19. gr. DORA áframmiðla tímanlega upplýsingum um alvarleg atvik og verulegar netógnir frá aðilum

á fjármálamarkaði til CERT-IS. Sjá jafnframt umfjöllun um 6. gr. frumvarpsins og kafla 3.3 í greinargerð þessari.

DORA gerir ráð fyrir miðlægri söfnun upplýsinga um alvarleg atvik á öllu Evrópska efnahagssvæðinu í því skyni að draga lærdóm af þeim og efla enn frekar þekkingu og viðbragð við mögulegum ógnum.

DORA kveður á um skyldu til almennra prófana á stafrænum rekstrarlegum viðnámsþrótti eða aukinna ógnamiðaðra innbrotsprófana (e. threat-led penetration testing, TLPT), sem stuðla eiga að bættu áfallaþoli innviða aðila á fjármálamarkaði. Ríkar kröfur eru gerðar til fyrirtækja sem gert er að framkvæma prófanir af síðarnefndu tagi. Seðlabanki Íslands hefur innleitt TIBER-EU aðferðafræði áhættumiðaðra innbrotsprófana sem samræmir gæði og verklag slíkra prófana.

Meginreglur eru settar fram í DORA um vöktun áhættu sem steðjað getur að fyrirtæki á fjármálamarkaði frá þriðja aðila (ytri tækniþjónustuveitendum eða *þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu*). Ítarlegar kröfur eru gerðar til samninga um slíka aðkeypta þjónustu, þar á meðal að því er varðar undirbúning/valferli fyrir samningsgerð og um svigrúm til útgöngu úr slíku samningssambandi (e. exit strategy). Áætlanir skulu vera til staðar er miða að því að viðhalda samfelldum rekstri ef til flutnings eða uppsagnar þjónustu ytri tækniþjónustuveitanda kemur.

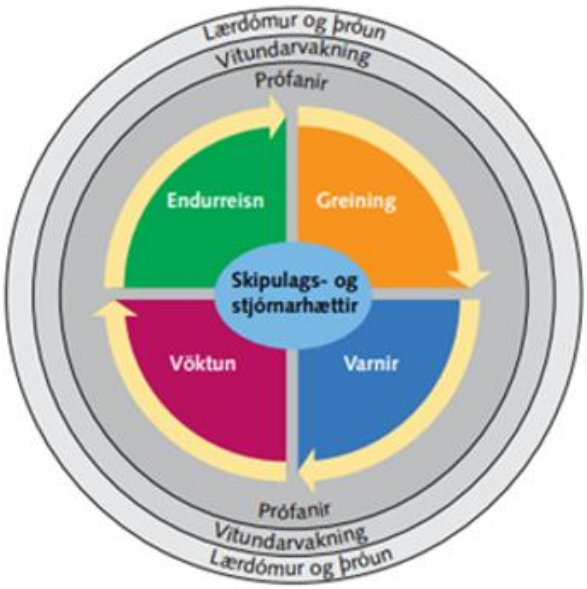
Aðilar á fjármálamarkaði skulu uppfylla framangreindar kröfur í samræmi við meðalhófsreglu, að teknu tilliti til stærðar og áhættusniðs, eðlis, umfangs og flækjustigs starfsemi og kerfislegs mikilvægis.

Með DORA er komið á sameiginlegri umgjörð eftirlits með allra stærstu alþjóðlegu tækniþjónustuveitendum sem sérstaklega verða útnefndir sem mikilvægir á sameiginlegum innri markaði fjármálaþjónustu, svonefndum *eftirlitsramma mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu* (e. Union Oversight Framework). Fyrir hvern slíkan mikilvægan þriðja aðila skulu evrópsku fjármálaeftirlitsstofnanirnar útnefna einhverja úr sínum hópi sem aðaleftirlitsaðila (e. Lead Overseer eða LO), þ.e. ýmist Evrópsku bankaeftirlitsstofnunina (EBA), Evrópsku verðbréfamarkaðseftirlitsstofnunina (ESMA) eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunina (EIOPA). Ef slíkur mikilvægur þriðji aðili frá Íslandi eða öðru EFTA-ríki innan EES væri útnefndur undir eftirlitsrammann yrði Eftirlitsstofnun EFTA falið hlutverk aðaleftirlitsaðila í samræmi við tveggja stoða kerfi EES-samningsins. Á meðal undirliggjandi viðmiða fyrir útnefningu er að hlutaðeigandi veiti upplýsinga- og fjarskiptatækniþjónustu yfir landamæri. Tækniþjónustuveitanda sem fellur undir eftirlitsrammann ber að vinna með hlutaðeigandi aðaleftirlitsaðila í góðri trú og greiða eftirlitsgjald en aðaleftirlitsaðilanum eru í DORA tryggðar heimildir til upplýsingaöflunar, almennra rannsókna, úttekta, útgáfu tilmæla og gerð úrbótatillagna, að viðlögðum viðurlögum sem skulu framfylgjanleg í heimaríki þjónustuveitandans (þ.e. eftirfylgni lögbærra stjórnvalda). Þá gerir DORA ráð fyrir að upplýsa megi opinberlega um bresti á samstarfsvilja eða ef ekki er farið að tilmælum aðaleftirlitsaðila, nema slík upplýsingagjöf teljist ósanngjörn eða geta skaðað fjármálakerfi.

Loks er vert að geta þess að DORA kveður á um heimildir til miðlunar upplýsinga um netógnir sem steðjað geta að stafrænum rekstrarlegum viðnámsþrótti aðila á fjármálamarkaði, enda sé slíkt samstarf formgert og hlíti nánar tilgreindum skilyrðum.

Með frumvarpinu verður tekið mikilvægt skref í að samræma lagakröfur til ólíkra aðila á fjármálamarkaði að því er varðar áhættustýringu og viðbúnað. Áfallaþol net- og upplýsingakerfa þeirra og geta til endurreisnar fjármálaþjónustu ef til rofs kemur eru samfélaginu mikilvæg. Efnisreglur DORA eru í samræmi við alþjóðlega viðurkennd viðmið

um bestu framkvæmd á þessu sviði sem hafa m.a. verið dregin saman með eftirfarandi myndrænum hætti sem tekur til lykilþátta áhættustýringar m.t.t. net- og upplýsingaöryggis (Seðlabanki Íslands, Fjármálainnviðir 2018, bls. 9):



3.2. Áhættustýring og viðbúnaður

Ákvæði II. kafla DORA (5.-16. gr.) fjalla um stýringu upplýsinga- og fjarskiptatækniáhættu. Megininntak hans er eftirfarandi:

a. Stjórnunarhættir og skipulag (5. gr.).

Aðilar á fjármálamarkaði skulu viðhafa innri stjórnun og eftirlit sem tryggir skilvirka og varfærna stýringu upplýsinga- og fjarskiptatækniáhættu til að skapa sem mest stafrænt áfallaþol. DORA gerir ráð fyrir að almennt sé sjálfstæðri eftirlitseiningu falin ábyrgð á þessu í því skyni að forðast hagsmunaárekstur, sbr. 4. mgr. 6. gr. reglugerðarinnar.

Stjórn aðila á fjármálamarkaði skal skilgreina, samþykkja, hafa umsjón með og bera ábyrgð á framkvæmd allra ráðstafana sem tengjast umgjörð áhættustýringar vegna upplýsinga- og fjarskiptatækniáhættu. Henni ber t.d. að koma á stefnu og ferlum sem miða að því að tryggja að strangar kröfur séu gerðar um aðgengi, áreiðanleika (eða ósvikni), heilleika og trúnað gagna. Ennfremur að skilgreina hlutverk og ábyrgð, skipulag og stjórnarhætti, svo sem nánar greinir í ákvæðinu. Á meðal lykilþátta eru stefna um rekstrarsamfellu, viðbragðs- og endurreisnaráætlanir. Stjórn ber að sjá til þess að tilföng séu næg í starfseminni svo uppfylla megi þarfir hlutaðeigandi aðila á fjármálamarkaði fyrir stafrænan rekstrarlegan viðnámsþrótt og tryggja öryggisvitund í starfseminni, þjálfun og færni fyrir allt starfsfólk.

Sérstaklega er vikið að ábyrgð stjórnar með tilliti til notkunar upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita. Stjórn skal upplýst reglulega um tilhögun á hverjum tíma, fyrirhugaðar efnislegar breytingar og hugsanleg áhrif slíkra breytinga. Ennfremur skal stjórn upplýst um að minnsta kosti alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni, áhrif þeirra, ráðstafanir til viðbragða,

endurreisnar og úrbóta. Tilnefna skal fulltrúa í framkvæmdastjórn sem ábyrgan fyrir eftirliti með áhættu tengdri upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita eða koma á hlutverki til að fylgjast með ráðstöfunum sem samið er um við slíka aðila (örfyrirtæki eru þó undanskilin). Loks er kveðið á um að stjórnarmönnum beri að viðhalda uppfærðri þekkingu og færni sem þarf til að skilja og meta upplýsinga- og fjarskiptatækniáhættu og áhrif hennar á starfsemi hlutaðeigandi aðila á fjármálamarkaði.

b. Áhættustýringarrammi í upplýsinga- og fjarskiptatækni (6. gr.).

Traustur, yfirgripsmikill og vel skjalfestur rammi áhættustýringar fyrir upplýsinga- og fjarskiptatækni er forsenda þess að tryggja stafrænt áfallaþol. Í ákvæðinu eru gerðar lágmarkskröfur til slíks ramma. Aðilar á fjármálamarkaði skulu lágmarka áhrif upplýsinga- og fjarskiptatækniáhættu í starfsemi sinni í samræmi við gildandi áhættustýringarramma og standa lögbærum yfirvöldum (hér Fjármálaeftirlitinu) skil á umbeðnum upplýsingum þar að lútandi. Tryggja ber viðeigandi aðgreiningu og sjálfstæði áhættustýringareininga, eftirlitseininga og innri endurskoðunar samkvæmt líkaninu um þrjár varnarlínur eða líkani um innri áhættustýringu og eftirlit.

Áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni skal skjalfestur og endurskoðaður að minnsta kosti einu sinni á ári (eða reglulega ef um er að ræða örfyrirtæki), sem og þegar alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eiga sér stað og í kjölfar tilmæla eftirlitsaðila eða niðurstaðna sem leiða af viðeigandi prófunum eða úttektarferlum. Stöðugt skal unnið að endurbótum á áhættustýringarrammanum á grundvelli fengins lærdóms af framkvæmd og vöktun. Lögbært yfirvald (hér Fjármálaeftirlitið) getur óskað eftir skýrslu um endurskoðun rammans.

Áhættustýringarrammi aðila á fjármálamarkaði (annarra en örfyrirtækja) skal sæta reglulegri innri endurskoðun af hálfu þar til bærra aðila. Komið skal á formlegu eftirfylgni- og úrbótaferli á grundvelli niðurstaðna innri endurskoðunar.

Í stefnuáætlun um stafrænan rekstrarlegan viðnámsþrótt, sem er hluti áhættustýringarramma aðila á fjármálamarkaði, skal tiltaka upplýsingar um hvernig ramminn skal innleiddur. Slík áætlun skal ná yfir nánar tilgreindar aðferðir til að bregðast við upplýsinga- og fjarskiptatækniáhættu og ná sértækum markmiðum í upplýsinga- og fjarskiptatækni, t.d. um ásættanleg áhættuþolmörk, markmið um upplýsingaöryggi, viðmið fyrir tæknihögun, innleiðingu prófana og samskiptaáætlun.

Ef lög mæla ekki fyrir um annað er aðila á fjármálamarkaði heimilt að útvista þeim verkefnum að sannreyna hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu til fyrirtækja innan eða utan samstæðu. Þó svo að slíkum verkefnum sé útvistað er ábyrgð á sannprófun á hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu fjármálastofnunarinnar sjálfrar.

c. Upplýsinga- og fjarskiptatæknikerfi, -samskiptareglur og -búnaður (7. gr.).

Nánar tilgreindar kröfur eru gerðar til upplýsinga- og fjarskiptatæknikerfa, -samskiptareglna (eða aðferðalýsinga) og -búnaðar aðila á fjármálamarkaði sem notaður er til að takast á við og stýra áhættu á þessu sviði. Hann sé einkum viðeigandi fyrir umfang aðgerða sem styðja rekstur á starfsemi þeirra í samræmi við meðalhófsreglu; áreiðanlegur; búi yfir nægri getu til að vinna rétt úr gögnum og tímanlega og með nægilega mikla tæknilega viðnámsgetu til að takast á fullnægjandi hátt á við auknar

þarfir við vinnslu upplýsinga eins og krafist er við erfiðar markaðsaðstæður eða aðrar óhagstæðar aðstæður.

d. Auðkenning (8. gr.).

Aðilar á fjármálamarkaði skulu greina, flokka og skjalfesta á viðunandi hátt alla starfsþætti, hlutverk og ábyrgðarsvið sem upplýsinga- og fjarskiptatækni styður við, upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir, svo og hlutverk og hæði í tengslum við upplýsinga- og fjarskiptatækniáhættu. Endurskoða ber eftir þörfum og a.m.k. árlega hvort flokkunin og hvers kyns viðeigandi gögn séu fullnægjandi. Upplýsingaeignir skulu flokkaðar eftir mikilvægi og tengsl og innbyrðis hæði þeirra vera kortlögð. Öll ferli sem háð eru þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu skulu greind og skjalfest. Skrár yfir framangreint skulu reglulega uppfærðar.

Borin skulu kennsl á allar uppsprettur upplýsinga- og fjarskiptatækniáhættu, einkum áhættu gagnvart og vegna annarra aðila á fjármálamarkaði, og áhættusviðsmyndir reglulega endurmetnar.

Áhættumat skal gert á öllum stórfelldum breytingum á innviðum net- og upplýsingakerfa, í ferlum eða verklagsreglum sem hafa áhrif á upplýsinga- og fjarskiptatæknistudda starfsemi þeirra, upplýsingatæknieignir eða upplýsinga- og fjarskiptatæknieignir (þetta á þó ekki við um örfyrirtæki).

e. Verndun og forvarnir (9. gr.).

Öryggi og virkni upplýsinga- og fjarskiptatæknikerfa og -búnaðar skal vaktað stöðugt og viðeigandi öryggisbúnaður, stefnur og verklag innleidd í því sambandi. Aðilar á fjármálamarkaði skulu nota viðeigandi tæknilausnir og ferli í því skyni að tryggja viðnámsþrótt, samfellu og aðgengileika upplýsinga- og fjarskiptatæknikerfa, einkum þeirra sem styðja við nauðsynlega eða mikilvæga starfsemi. Nánar tilgreindar kröfur ákvæðisins skulu uppfylltar, sem hluti af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni.

f. Greining (10. gr.).

Aðilar á fjármálamarkaði skulu hafa til staðar kerfi til að greina óeðlilegar athafnir án tafar í samræmi við 17. gr. DORA sem tilgreinir nánari kröfur um viðbrögð við atvikum og ógnum, þar með talin vandamál sem varða afköst kerfa. Reglulega skal prófa slík greiningarkerfi og tryggja nægar auðlindir í starfseminni vegna þeirra. Sérstakar kröfur eru tilgreindar í ákvæðinu til veitenda gagnaskýrsluþjónustu.

g. Viðbrögð og endurreisn (11. gr.).

Aðilar á fjármálamarkaði skulu setja fram heildstæða stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og innleiða hana með viðeigandi og skjalfestum ráðstöfunum, ferlum og verklagi. Einkum skal stuðlað að samfellu í nauðsynlegri eða mikilvægri starfsemi hlutaðeigandi og skjótum viðeigandi viðbrögðum við atvikum, þar með talið frummat á áhrifum, skaða og tapi. Settar skulu fram aðgerðir varðandi samskipti og krísustjórnun sem tryggja að uppfærðar upplýsingar séu sendar öllu viðeigandi starfsfólki og ytri hagsmunaaðilum í samræmi við 14. gr. DORA og lögbærum yfirvöldum (hér Fjármálaeftirliti) í samræmi við 19. gr. reglugerðarinnar.

Viðeigandi viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni skulu innleiddar sem hluti af áhættustýringarramma aðila á fjármálamarkaði í samræmi við nánar tilgreindar kröfur, sem meðal annars gera ráð fyrir reglubundinni prófun og endurmati. Sú krafa er gerð til aðila á fjármálamarkaði (þó ekki örfyrirtækja) að starfseining krísustjórnunar setji fram skýrar verklagsreglur til að stjórna krísusamskiptum innan og utan fyrirtækis í samræmi við 14. gr. DORA, ef áætlun um rekstrarsamfellu í upplýsinga- og fjarskiptatækni eða viðbragðs- og endurreisnaráætlanir eru virkjaðar. Aðgerðir fyrir og meðan á röskunaratburði stendur skulu skráðar.

Sérstaklega er kveðið á um að verðbréfamiðstöðvar skuli láta lögbærum yfirvöldum (hér Fjármálaeftirliti) í té afrit af niðurstöðum prófana á rekstrarsamfellu upplýsinga- og fjarskiptatækni eða samsvarandi æfinga.

Æski lögbær yfirvöld upplýsinga um mat á samanlögðum árlegum kostnaði og tapi af völdum alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni skal aðili á fjármálamarkaði (þó ekki örfyrirtæki) standa skil á þeim.

h. Stefnur og verklag við öryggisafritun, verklag og aðferðir við endurheimt og endurreisn (12. gr.).

Aðilar á fjármálamarkaði skulu útfæra og skjalfesta stefnur og verklag um öryggisafritun, svo og verklag og aðferðir við endurheimt og endurreisn. Skylt er að setja upp öryggisafritunarkerfi og prófa reglulega verklag og ferla er þessu tengjast.

Við endurheimt öryggisafritunargagna skulu nánar tilgreindar kröfur uppfylltar og upplýsinga- og fjarskiptatæknikerfin vera tryggilega varin fyrir óheimilum aðgangi eða spillingu og gera kleift að endurreisa þjónustu tímanlega með nýtingu öryggisafrita gagna og kerfa eins og til þarf.

Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu viðhalda varaupplýsinga- og fjarskiptatæknikerfum með tilföngum, getu og starfsþáttum sem eru fullnægjandi til að tryggja viðskiptaþarfir. Örfyrirtæki skulu leggja mat á þörfina á slíku með hliðsjón af áhættusniði sínu.

DORA gerir sérstakar kröfur til veitenda gagnaskýrsluþjónustu og verðbréfamiðstöðva varðandi öryggisafritunar- og endurheimtarkerfi og viðbótarvinnslustað.

Við ákvörðun á markmiðum um endurreisnartíma og endurreisnarpunkt fyrir hvern starfsþátt skulu aðilar á fjármálamarkaði taka tillit til þess hvort hann teljist nauðsynleg eða mikilvæg starfsemi og mögulegra heildaráhrifa á skilvirkni markaðarins. Slík tímamarkmið skulu tryggja að við óvenjulegar aðstæður sé samþykktu þjónustustigi náð.

Við endurreisn eftir atvik sem tengist upplýsinga- og fjarskiptatækni skulu aðilar á fjármálamarkaði framkvæma allar nauðsynlegar athuganir og afstemmingar til að tryggja áfram hæsta stig heilleika gagna. Einnig skal framkvæma þessar athuganir þegar gögn frá ytri hagsmunaaðilum eru endurgerð til að tryggja að öll gögn séu í samræmi milli kerfa.

i. Lærdómur og þróun (13. gr.).

Krafa er gerð til aðila á fjármálamarkaði um að hafa yfir að ráða getu og starfsfólki til að safna upplýsingum um veikleika og netógnir, atvik sem tengjast upplýsinga- og fjarskiptatækni, einkum netárásir, og greina líkleg áhrif þeirra á stafrænan

rekstrarlegan viðnámsþrótt. Atvik og raskanir á kjarnastarfsemi skulu greind, ekki síst orsakir, og kennsl borin á nauðsynlegar úrbætur. Atvikagreining skal meðal annars fela í sér mat á gæðum og hraða viðbragðs og skilvirkni í innri og ytri samskiptum.

Ef þess er óskað skulu aðilar á fjármálamarkaði, aðrir en örfyrirtæki tilkynna lögbærum yfirvöldum (hér Fjármálaeftirliti) um breytingar sem gerðar eru í kjölfar greiningar á atvikum sem tengjast upplýsinga- og fjarskiptatækni.

DORA gerir einnig ráð fyrir að lærdómur sem dreginn er af prófun á stafrænum rekstrarlegum viðnámsþrótti sem framkvæmd er í samræmi við 26. og 27. gr. og af raungerðum atvikum sem tengjast fjarskipta- og upplýsingatækni, einkum netárásum, sé einnig nýttur til úrbóta á ferlum, stefnu og áhættustýringarramma hlutaðeigandi aðila á fjármálamarkaði. Hið sama eigi við í kjölfar til dæmis úttekta eftirlitsaðila. Þá er berum orðum kveðið á um að háttsett starfsfólk á sviði upplýsinga- og fjarskiptatækni skuli a.m.k. árlega gefa stjórn skýrslu um lærdóm og úrbætur og leggja fram ráðleggingar.

Áætlanir um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti skal vera hluti af þjálfunaráætlunum fyrir allt starfsfólk og eftir atvikum ytri þjónustuveitendur. Þá er sérstaklega kveðið á um að aðilar á fjármálamarkaði (þó ekki örfyrirtæki) vakti tækniframfarir, með viðvarandi áfallaþol starfsemi sinnar í huga.

j. Samskipti (14. gr.).

Krísusamskiptaáætlanir, sem gera kleift að upplýsa viðskiptavini, mótaðila og almenning á ábyrgan háttum að minnsta kosti alvarleg atvik eða veikleika sem tengjast upplýsinga- og fjarskiptatækni, skulu vera hluti af áhættustýringarramma sérhvers aðila á fjármálamarkaði. Jafnframt skulu innleiddar samskiptastefnur fyrir starfsfólk og ytri hagsmunaaðila.

k. Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni (16. gr.).

Ákvæði 5.–14. gr. reglugerðarinnar, svo og 15. gr. sem kveður á um nánari útfærslu efnisákvæða DORA í tæknistöðlum, gilda ekki um nánar tilgreinda smærri aðila á fjármálamarkaði, svo sem lítil og ótengd verðbréfafyrirtæki, tilteknar greiðslustofnanir og rafeyrisfyrirtæki. Þeir falla hins vegar undir einfaldaðan áhættustýringarramma, sem skal skjalfestur og endurskoðaður reglulega og ef tilefni er til. Kröfur til aðila sem falla undir einfaldaðan áhættustýringarramma DORA eru útfærðar nánar í tæknistaðli.

3.3. Tilkynningaskylda og meðhöndlun atvika

Ákvæði III. kafla DORA (17.–23. gr.) fjalla um atvikastjórnun, flokkun og skýrslugjöf í tengslum við upplýsinga- og fjarskiptatækni. Leiðbeinandi tilmæli Fjármálaeftirlitsins vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila, nr. 1/2019, gera ráð fyrir slíkri skyldu (5.2.), en sú grundvallarbreyting verður nú á að um beina lagaskyldu verður að ræða og varða brot á henni viðurlögum. Megininntak kaflans er eftirfarandi:

a. Atvikastjórnunarferli (17. gr.).

Aðilum á fjármálamarkaði er skylt að skilgreina, koma á og innleiða ferli til að bera kennsl á, stjórna og tilkynna um atvik í tengslum við upplýsinga- og fjarskiptatækni, svonefnt atvikastjórnunarferli. Það miðar einkum að því að tryggja skilvirk viðbrögð við atvikum svo tryggja megi að þjónusta verði starfhæf og örugg innan ásættanlegs tíma.

Skrá skal haldin yfir öll atvik og verulegar netógnir, vöktun, meðhöndlun og eftirfylgni tryggð með skýrum ferlum og verklagi. Greina skal orsök og afleiðingar, draga lærdóm og gera nauðsynlegar úrbætur svo unnt sé að koma í veg fyrir að sambærileg atvik endurtaki sig. Krafa er meðal annars gerð um uppsetningu snemmbærra viðvörunarvísa, ferla og viðmið um flokkun atvika (sbr. 18. gr. DORA), ábyrgðaraðila við meðhöndlun, skýrslugjöf innan fyrirtækisins og samskiptaáætlanir.

b. Flokkun á atvikum (18. gr.).

Við flokkun og greiningu atvika skal einkum horft til þeirra viðmiða sem greinir í 1. mgr. 18. gr. DORA. Til dæmis fjölda og/eða mikilvægi viðskiptavina eða fjárhagslegra mótaðila sem verða fyrir áhrifum og, eftir atvikum, fjárhæð eða fjölda viðskipta sem atvik sem tengist. Ennfremur, tímalengd atviks, landfræðilegrar dreifingar, gagnataps, eðlis eða mikilvægis þjónustunnar sem atvik hefur áhrif á og efnahagslegra áhrifa af atviki.

c. Tilkynningar um alvarleg atvik og verulegar netógnir (19. gr.).

DORA kveður á um tilkynningaskyldu af hálfu allra sem undir gildissvið hennar heyra um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Tilkynningu skal beint til viðeigandi lögbærs yfirvalds á stöðluðu formi, hér á landi Fjármálaeftirlitsins. Kveðið verður nánar á um staðlað form og efni tilkynninga, tímamörk og fleira í tæknilegum eftirlitsstöðlum á grundvelli 20. gr. DORA.

Skýrslugjöfin er þrískipt samkvæmt ákvæðinu og skal hún uppfyllt innan nánar tilgreindra tímamarka: Upprunaleg tilkynning um atvik (frumtilkynning), áfangaskýrsla með uppfærðum upplýsingum og lokaskýrsla að meðhöndlun og greiningu lokinni.

Frumtilkynningin, svo og áfanga- og lokaskýrslur, skulu innihalda allar nauðsynlegar upplýsingar til þess að lögbært yfirvald geti ákvarðað mikilvægi og möguleg áhrif alvarlegs atviks yfir landamæri. Ef tæknilegur vandi kemur í veg fyrir að frumtilkynning sé lögð fram á tilætluðu stöðluðu formi skal henni komið á framfæri við lögbært yfirvald eftir öðrum leiðum. Þó svo að útvista megi skýrslugjöf samkvæmt ákvæðinu til þriðja aðila ber tilkynningaskyldur aðili á fjármálamarkaði fulla ábyrgð á henni.

Aðilar á fjármálamarkaði geta að eigin frumkvæði tilkynnt lögbæru yfirvaldi um verulegar netógnir þegar þeir telja að ógnin geti skipt fjármálakerfið, notendur þjónustu eða viðskiptavini máli.

Við móttöku frumtilkynningar, svo og áfanga- og lokaskýrslu, verður Fjármálaeftirlitinu einkum skylt að veita eftirtöldum aðilum tímanlega upplýsingar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni, eftir því sem við á hverju sinni: Evrópsku fjármálaeftirlitsstofnunum (EBA, ESMA og EIOPA), Seðlabanka Evrópu (ef í hlut eiga lánastofnanir, greiðslustofnanir eða rafeyrisfyrirtæki), Fjarskiptastofu með vísan til 2. mgr. 13. gr. laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, netöryggissveit Fjarskiptastofu (CERT-IS), skilavaldi Seðlabanka Íslands, Almannavörnum ríkislögreglustjóra og Persónuvernd. Um áframmiðlun af hálfu evrópska eftirlitskerfisins á fjármálamarkaði fer samkvæmt 7. mgr.

Með DORA er miðlæg sýn tryggð á alvarleg atvik, netógnir og veikleika. Stofnanir Evrópusambandsins, í samráði við Netöryggisstofnun ESB (ENISA) og samvinnu við

hlutaðeigandi lögbær yfirvöld, leggja mat á hvort upplýsingar eigi erindi við lögbær yfirvöld í öðrum ríkjum. Tilkynningu er beint til þeirra, ef við á, eins fljótt og auðið er. Ef atvik eða málefni varðar greiðslumiðlun gerir DORA, eins og hún verður tekin upp í EES-samninginn, ráð fyrir tafarlausri miðlun upplýsinga af hálfu Seðlabanka Evrópu til aðila seðlabankakerfis Evrópu og seðlabanka EFTA-ríkjanna innan EES, svo unnt sé að grípa til nauðsynlegra ráðstafana til að vernda fjármálastöðugleika.

Þess má geta að í 21. gr. DORA er kveðið á um að metin verði hagkvæmni frekari miðstýringar á söfnun atvikatilkynninga með því að koma á fót sameiginlegri ESB-miðstöð fyrir tilkynningar aðila á fjármálamarkaði um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Kannaðar verði leiðir til að greiða fyrir flæði tilkynninga, draga úr tengdum kostnaði og renna stoðum undir þemabundnar greiningar með það í huga að auka samleitni eftirlits. Skýrsla liggi fyrir í janúar 2025.

Vikið er að upplýsingaskyldu til haghafa í 19. gr. DORA. Þegar alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni á sér stað og hefur áhrif á fjárhagslega hagsmuni viðskiptavina skulu aðilar á fjármálamarkaði, án ástæðulausrar tafar og um leið og þeir fá vitneskju um það, upplýsa viðskiptavini sína um atvikið og um þær ráðstafanir sem gerðar hafa verið til að draga úr skaðlegum áhrifum af slíku atviki. Ef um er að ræða verulega netógn skulu aðilar á fjármálamarkaði, eftir atvikum, upplýsa þá viðskiptavini sem hugsanlega geta orðið fyrir áhrifum um allar viðeigandi verndarráðstafanir sem þeir gætu íhugað að grípa til.

d. Greiðslutengd rekstrar- eða öryggisatvik (23. gr.).

Kröfur III. kafla DORA skulu samkvæmt 23. gr. gilda um *greiðslutengd rekstrar- eða öryggisatvik* og um *alvarleg greiðslutengd rekstrar- eða öryggisatvik* ef þau varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyris-fyrirtæki. Bæði eru hugtökin skilgreind sérstaklega í 3. gr. DORA (9. og 11. tölul.). Með þessu ákvæði og breytingu á 96. gr. PSDII-tilskipunarinnar (sem innleidd var hér á landi með 100. gr. laga um greiðsluþjónustu), með 5. tölul. 7. gr. DORA-tilskipunarinnar, er krafa um skýrslugjöf samkvæmt PSDII felld úr gildi gagnvart þeim greiðsluþjónustuveitendum sem falla undir gildissvið DORA. Markmiðið er einföldun regluverks og að draga úr hugsanlegri tvöfaldri kvöð um tilkynningaskyldu umræddra aðila.

e. Endurgjöf frá eftirlitsyfirvöldum (22. gr.).

Lögbært yfirvald (hér Fjármálaeftirlitið) skal staðfesta móttöku frumtilkynninga, áfanga- og lokaskýrslna. Ef það er mögulegt, getur það veitt almennar leiðbeiningar eða viðeigandi endurgjöf og er heimilt að ræða úrræði til viðbragða við atviki og aðferðir til að lágmarka og milda neikvæð áhrif þvert á fjármálageirann. Hvað sem slíkri endurgjöf líður bera aðilar á fjármálamarkaði fulla ábyrgð á meðhöndlun og afleiðingum af upplýsinga- og fjarskiptatæknitengdum atvikum sem tilkynnt er um skv. 1. mgr. 19. gr. DORA.

Áréttað er að aðilar sem útnefndir hafa verið rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða tilheyra lögbundnum þjónustuhópi netöryggissveitar Fjarskiptastofu (CERT-IS), sbr. reglugerð nr. 480/2021 og 3. mgr. 15. gr. laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða. Ekki er gert ráð fyrir að breyting verði á því.

DORA kveður á um að evrópsku fjármálaeftirlitsstofnanirnar skuli gefa út viðvaranir og taka saman tölfræðiupplýsingar sem aðilar á fjármálamörkuðum geta stuðst við í mati á ógnum og veikleikum í upplýsinga- og fjarskiptatækni. Árlega munu þær jafnframt gefa út skýrslu með nafnlausum upplýsingum á samanteknu formi um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Gera má ráð fyrir að fjallað verði um fjölda alvarlegra atvika, eðli og áhrif, aðgerðir til úrbóta og tilkostnað.

3.4. Netöryggisprófanir

Ákvæði IV. kafla DORA (24.–27. gr.) fjalla um prófanir á stafrænum rekstrarlegum viðnámsþrótti. Allir aðilar á fjármálamarkaði, önnur en örfyrirtæki, skulu setja sér prófunaráætlun um stafrænan rekstrarlegan viðnámsþrótt í samræmi við ákvæði 24. gr. sem hluta af áhættustýringarramma sínum í upplýsinga- og fjarskiptatækni. Við framkvæmd hennar og val um prófanir hverju sinni skal áhættumiðaðri nálgun fylgt, sbr. 25. gr. reglugerðarinnar. Með prófunum er til dæmis átt við mat og skönnun á veikleikum, greiningu á opnum hugbúnaði, öryggis- og gloppugreining, sviðsmyndatengdar prófanir og innbrotsprófanir. Þó svo að örfyrirtækjum beri ekki skylda til að setja sér prófunaráætlun skulu þau framkvæma lágmarksprófanir í samræmi við tilmæli 3. mgr. 25. gr. DORA. Reglugerðin mælir fyrir um að óháðir aðilar framkvæmi prófanir, hvort heldur innri eða ytri aðilar, á grundvelli nægra tilfanga og að teknu tilliti til mögulegra hagsmunaárekstra.

Prófunum skal fylgt eftir með viðeigandi hætti þannig að ráðin sé full bót á öllum auðkenndum veikleikum og annmörkum hvers konar. Í tilviki upplýsinga- og fjarskiptatæknikerfa og hugbúnaðar sem styðja við nauðsynlega eða mikilvæga starfsemi er lágmarkskrafan að framkvæma prófanir árlega.

Lögbært yfirvald ákveður hvaða aðilar á fjármálamarkaði, aðrir en þeir sem falla undir einfaldaðan áhættustýringarramma skv. 16. gr. og örfyrirtæki, skuli samkvæmt 26. gr. DORA framkvæma aukna prófun með *ógnamiðaðri innbrotsprófun* á að minnsta kosti þriggja ára fresti. Við þá ákvörðun skal byggt á áhættumiðaðri nálgun, svo sem með tilliti til mögulegra áhrifa á fjármálastöðugleika. Lögbært yfirvald getur óskað eftir tíðari eða færri prófunum af hálfu aðila á grundvelli áhættusniðs starfsemi og með tilliti til rekstrarlegra aðstæðna. Ríkar kröfur eru gerðar til slíkra prófana í ákvæðinu, sem náð geta til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og jafnvel vegna þjónustu við fleiri aðila á fjármálamarkaði en einn. Samantekt á niðurstöðum, áætlun um úrbætur og gögn sem sýna að ógnamiðuð innbrotsprófun hafi verið framkvæmd skal afhent lögbæru yfirvaldi. Kröfur fyrir prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun eru útlistaðar í 27. gr. DORA. Ef aðili á fjármálamarkaði notar innri prófunaraðila til að gera ógnamiðaða innbrotsprófun skal ytri prófunaraðili fenginn fyrir þriðju hverju prófun.

Gert er ráð fyrir að Seðlabanki Íslands beri ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun samkvæmt DORA hér á landi. Um nánari viðmið og kröfur fer samkvæmt afleiddum gerðum (tæknistöðlum), sem verða í samræmi við TIBER-EU umgjörð Seðlabanka Evrópu. Seðlabanki Íslands hefur þegar komið á fót umgjörð fyrir netárásarprófanir fyrir stofnanir og fyrirtæki sem eru mikilvæg fyrir íslenskt fjármálakerfi, TIBER-IS, sem byggir á TIBER-EU.

3.5. Áhættustýring vegna þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu

Ákvæði 1. þáttar V. kafla DORA (28.–30. gr.) fjalla um stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, nánar tiltekið helstu meginreglur um trausta stýringu slíkrar áhættu af hálfu aðila á fjármálamarkaði vegna þriðju aðila, en 2. þáttur snýr að

sameiginlegum eftirlitsramma gagnvart stærstu alþjóðlegu tækniþjónustuveitendum, sbr. 3.6 greinargerðar þessarar. Meginreglur þessar eru til viðbótar við sérlög sem gilda um útvistun, sbr. 29. liður inngangsorða DORA.

Samkvæmt 28. gr. skulu aðilar á fjármálamarkaði, aðrir en þeir sem falla undir einfaldaðan áhættustýringarramma skv. 16. gr. og aðrir en örfyrirtæki, samþykkja og endurskoða reglulega stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðja aðila. Stýring upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila er óaðskiljanlegur hluti áhættustýringarramma í upplýsinga- og fjarskiptatækni, sbr. 6. gr. DORA, en skal grundvölluð á meðalhófsreglu. Samningsbundið fyrirkomulag skal skjalfest á viðeigandi hátt og að uppfylltum ítarlegum kröfum 30. gr. DORA. Þá skal uppfærðri upplýsingaskrá viðhaldið í tengslum við allt samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita.

Að minnsta kosti árlega skal lögbærum yfirvöldum gefin skýrsla um fjölda nýrra ráðstafana um notkun upplýsinga- og fjarskiptatækniþjónustu, flokka þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, tegund samningsbundins fyrirkomulags og þá þjónustu og starfsemi upplýsinga- og fjarskiptatækni sem veitt er. Lögbært yfirvald á kröfu um afhendingu hvers kyns upplýsinga sem taldar eru nauðsynlegar til að gera skilvirkt eftirlit með aðilum á fjármálamarkaði mögulegt.

DORA gerir ennfremur ráð fyrir að lögbært yfirvald sé tímanlega upplýst um hvers kyns *fyrirhugað* samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi, sem og þegar starfsemi er orðin nauðsynleg eða mikilvæg. Fyrir samningsgerð við þriðja aðila skal nánar tilgreint mat eiga sér stað af hálfu aðila á fjármálamarkaði, þar á meðal áreiðanleikakönnun og mat á mögulegum hagsmunaárekstrum, og gengið úr skugga um að viðeigandi staðlar um upplýsingaöryggi séu uppfylltir. Nánar tilgreindar kröfur eru gerðar um aðhald af hálfu aðila á fjármálamarkaði gagnvart þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

Sérstaklega er kveðið á um að unnt skuli að segja upp samningsbundnu fyrirkomulagi um notkun á upplýsinga- og fjarskiptatækniþjónustu við tilteknar aðstæður, svo sem við veruleg brot þriðja aðila á gildandi lögum, reglum eða samningsskilmálum, ef í ljós koma veikleikar tengdir aðgangsstýringu, ráðstöfunum til að tryggja áreiðanleika, heilleika og trúnað um gögn eða ef aðstæður hamla framkvæmd skilvirks eftirlits með aðila á fjármálamarkaði.

Að því er varðar þjónustu þriðja aðila sem styður við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði skal gerð útgönguáætlun og viðeigandi viðbúnaðarráðstafanir, í samræmi við nánar tilgreindar kröfur 28. gr. DORA.

Loks er vert að minna á 29. gr. DORA sem gerir kröfur til aðila á fjármálamarkaði um að huga að mati á mögulegri samþjöppunaráhættu sinni í upplýsinga- og fjarskiptatækni.

3.6. Eftirlitsrammi vegna mikilvægra þriðju aðila

Ákvæði 2. þáttar V. kafla DORA (31.–44. gr.) kveða á um sameiginlegan eftirlitsramma gagnvart mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu (e. Union Oversight Framework). Evrópsku fjármálaeftirlitsstofnanirnar og Eftirlitsstofnun EFTA í tilviki EFTA-ríkjanna innan EES skulu útnefna slíka þriðju aðila undir eftirlitsrammann og skipta með sér hlutverki aðaleftirlitsaðila. Þessi hluti DORA lýtur að öðrum en eftirlitsskyldum aðilum í hefðbundnum skilningi laga á sviði fjármálaþjónustu og felur í sér kröfur til starfsemi allra stærstu tækniþjónustuveitenda og er gert ráð fyrir virku eftirliti með framfylgd við þær.

Fyrir hvern slíkan mikilvægan þriðja aðila skulu evrópsku fjármálaeftirlitsstofnanirnar útnefna einhverja úr sínum hópi sem aðaleftirlitsaðila (e. Lead Overseer eða LO), þ.e. ýmist Evrópsku bankaeftirlitsstofnunina (EBA), Evrópsku verðbréfamarkaðseftirlitsstofnunina (ESMA) eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunina (EIOPA). Ef slíkur mikilvægur þriðji aðili frá Íslandi eða öðru EFTA-ríki innan EES væri útnefndur undir eftirlitsrammann yrði Eftirlitsstofnun EFTA falið hlutverk aðaleftirlitsaðila í samræmi við tveggja stoða kerfi EES-samningsins. Undirliggjandi viðmið verða útfærð nánar í framseldri reglugerð framkvæmdastjórnar ESB en þau varða meðal annars kerfislegt mikilvægi og fjölda þjónustukaupa sem reiða sig á tiltekinn tækniþjónustuveitanda. Ekki kemur til útnefningar ef ekki er um veitingu upplýsinga- og fjarskiptatækniþjónustu yfir landamæri að ræða. Tækniþjónustuveitanda sem fellur undir eftirlitsrammann ber að vinna með aðaleftirlitsaðilanum í góðri trú og greiða eftirlitsgjald en aðaleftirlitsaðilanum eru í DORA tryggðar heimildir til upplýsingaöflunar, almennra rannsókna, úttekta, útgáfu tilmæla og gerð úrbótatillagna, að viðlögðum viðurlögum sem skulu framfylgjanleg í heimaríki þjónustuveitandans (þ.e. eftirfylgni lögbærra stjórnvalda). Þá gerir DORA ráð fyrir að upplýsa megi opinberlega um bresti á samstarfsvilja eða ef ekki er farið að tilmælum aðaleftirlitsaðila, nema slík upplýsingagjöf teljist ósanngjörn eða geta skaðað fjármálakerfi. Sérstökum eftirlitsvettvangi (e. Oversight Forum) er komið á fót með 32. gr. DORA sem ætlað er að styðja við aðaleftirlitsaðila, semja drög að sameiginlegri afstöðu og gerðum sameiginlegu nefndarinnar (e. Joint Committee). Unnið er að viðeigandi aðlögun DORA með tilliti til tveggja stoða kerfisins sem EES-samningurinn byggir á.

3.7. Upplýsingamiðlun

Í 45. gr. DORA er fjallað um fyrirkomulag upplýsingaskipta um netógnir. Þannig er aðilum á fjármálamarkaði heimilt að skiptast á upplýsingum og greiningum um netógnir, svo sem vísa sem geta gefið til kynna ógn eða hættu, úrræði, aðferðir, verklag og viðvaranir, að uppfylltum nánar tilgreindum skilyrðum. Í fyrsta lagi miði slík upplýsingaskipti og miðlun vitneskju að því að efla stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði, einkum með vitundarvakningu um netógnir, með því að takmarka eða hindra að netógnir geti breiðst út, styðja við varnargetu og aðferðir til að greina ógnir og verjast áhættu. Í öðru lagi er krafa gerð um að miðlunin eigi sér stað á traustum sameiginlegum vettvangi aðila á fjármálamarkaði. Í þriðja lagi skal við framkvæmdina gætt að því að vernda viðkvæmt eðli upplýsinga, eftir því sem við á, með tilliti til viðskiptaleyndar, persónuverndar og reglna um samkeppnisstefnu. Skilgreina skal skilyrði fyrir þátttöku í slíkum vettvangi og, eftir því sem við á, setja fram upplýsingar um þátttöku opinberra yfirvalda og heimildir þeirra til þess að taka þátt, sem og þátttöku þriðja aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og um rekstrarþætti, svo sem notkun tæknivettvanga. Aðilum á fjármálamarkaði ber að tilkynna lögbærum yfirvöldum um þátttöku sína í slíkum vettvangi, við staðfestingu á aðild, eftir því sem við á, eða þegar þeirri aðild lýkur.

Seðlabankinn heldur úti samstarfsvettvangi um rekstraröryggi fjármálainnviða (SURF) sem ætlað er að móta sameiginlega sýn á aðgerðir til að efla viðnámsþrótt net- og upplýsingakerfa mikilvægra fjármálainnviða og samhæfa aðgerðir komi til rekstrartruflana sem haft geta áhrif á öryggi og skilvirkni fjármálakerfisins á Íslandi. Starfsreglur SURF fjalla meðal annars um málefni sem varða trúnaðarskyldu og samkeppni. Til greina kemur að nýta SURF fyrir upplýsingaskipti skv. 45. gr. DORA enda uppfylli hann áðurnefnd skilyrði.

3.8. Afleiddar gerðir

Lagt er til að afleiddar gerðir DORA verði innleiddar í annars vegar reglugerðum ráðherra og hins vegar reglum Seðlabanka Íslands, sbr. 16. gr. Nú þegar er unnið að undirbúningi upptöku eftirtaldra gerða í EES-samninginn:

(i) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1502 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 sem tilgreinir nánari viðmið til grundvallar útnefningar mikilvægra þriðju aðila sem veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu.

(ii) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1505 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 sem ákvarðar fjárhæð eftirlitsgjalds sem aðaleftirlitsaðili innheimtir af mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og um fyrirkomulag greiðslu þess.

(iii) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1772 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 sem varða tæknistaðla um nánari viðmið til flokkunar á atvikum sem varða upplýsinga- og fjarskiptatækni og verulegar netógnir, tilgreina mikilvægismörk og kröfur til skýrslugjafar um alvarleg atvik.

(iv) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1773 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 sem varða tæknistaðla um efni stefnu varðandi samningsfyrirkomulag við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem styðja við nauðsynlega eða mikilvæga þætti í starfsemi aðila á fjármálamarkaði.

(v) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1774 um viðbætur við reglugerð Evrópuþingsin og ráðsins (ESB) 2022/2554 sem varða tæknistaðla um tól, aðferðir, ferla og stefnu til stýringar á upplýsinga- og fjarskiptatækniáhættu og um einfaldaða áhættustýringarrammann.

4. Samræmi við stjórnarskrá og alþjóðlegar skuldbindingar.

Atvinnufrelsi nýtur verndar 1. mgr. 75. gr. stjórnarskrár lýðveldisins Íslands, nr. 33/1944. Þessu frelsi má þó setja skorður með lögum, enda krefjist almannahagsmunir þess og gætt sé jafnræðis, sbr. 1. mgr. 65. gr. stjórnarskrárinnar. Kröfur frumvarpsins til áhættustýringar og viðbúnaðar aðila á fjármálamarkaði styðjast við lögmæt markmið um neytendavernd og fjármálastöðugleika og taka jafnt til aðila sem eru í sambærilegri stöðu. Því er talið að frumvarpið fullnægi kröfum stjórnarskrárinnar.

Frumvarpið felur í sér upptöku á efnisákvæðum DORA í íslenskan rétt. Eftirlit með framkvæmd þeirra verður í höndum Fjármálaeftirlitsins. Ekki verður talið að frumvarpið feli í sér framsalsheimildir sem séu verulega íþyngjandi eða umfram það sem áður hefur verið talið heimilt vegna EES-samningsins. Innleiðing DORA samræmist skuldbindingum Íslands skv. 7. gr. EES-samningsins og er ekki talin brjóta í bága við þjóðréttarlegar skuldbindingar Íslands.

5. Samráð.

Frumvarpið var samið í fjármála- og efnahagsráðuneytinu í samráði við Seðlabanka Íslands. Á vinnslustigi var ráðuneytið í samskiptum við og átti fundi um netöryggismál með fulltrúum háskóla-, iðnaðar- og nýsköpunarráðuneytis, dómsmálaráðuneytis og forsætisráðuneytis. Áformaskjal var birt í samráðsgátt stjórnvalda á vefnum Ísland.is 29. júní – 4. september 2023 (mál nr. S-120/2023), en engin umsögn barst. Frumvarpsdrög voru birt

til umsagnar í samráðsgátt stjórnvalda XX. júlí 2024 – XX. september 2024 (mál nr. S-___/2024) og bárust __ umsagnir. […].

Ferli skv. 5. gr. reglna um þinglega meðferð EES-mála er lokið. Frumvarpið varðar alla helstu aðila á fjármálamarkaði, viðskiptavini og þjónustuveitendur þeirra, atvinnulíf, stjórnvöld og samfélag almennt. Stafrænn rekstrarlegur viðnámsþróttur fjármálakerfisins, ekki síst kerfislega mikilvægra fjármálastofnana og innviða, varðar almannahagsmuni.

6. Mat á áhrifum.

Markmið frumvarpsins er að stuðla að stafrænum rekstrarlegum viðnámsþrótti fjármálastofnana með samræmdum kröfum um áhættustýringu og viðbúnað, svo lágmarka megi rof á mikilvægri fjármálaþjónustu með tilheyrandi neikvæðum efnahags- og samfélagslegum áhrifum, varðveita fjármálastöðugleika og tryggja öfluga vernd fjárfesta og neytenda. Við undirbúning frumvarpsins var horft til sjónarmiða um meðalhóf og jafnræði.

Tæknileg áhætta hefur engin landamæri. Afar brýnt er að stuðla að mildun neikvæðra áhrifa af atvikum í upplýsinga- og fjarskiptatækni á samfelldan og hagkvæman hátt, eftir því sem unnt er.

6.1. Hagræn áhrif á heildareftirspurn og einstaka markaði – hagstjórnarsjónarmið.

Áhrif frumvarpsins verða jákvæð. Fyrirhuguð lagasetning mun hafa áhrif á flesta aðila á fjármálamarkaði. Ný heildarlög leysa af hólmi og samræma núgildandi regluverk, sem einnig byggist á leiðbeinandi tilmælum Fjármálaeftirlitsins og viðmiðunarreglum evrópsku fjármálaeftirlitsstofnananna. Samræming regluverks er ekki síður hagkvæm fyrir eftirlitsaðila en markaðinn, með tilliti til framfylgni, nánari reglusetningar, þjálfunar, leiðbeininga o.s.frv. Innleiðing DORA mun líklega hafa í för með sér einhvern kostnað fyrir fyrirtækin, en að sama skapi miðar lagasetning að frekari eflingu viðnámsþróttar fyrir áföllum og þannig gæti hún einnig dregið úr eða komið í veg fyrir kostnað vegna áfalla eða áhættu sem tekst að mæta vegna hennar. Fyrirséð þykir að innleiðing DORA, ásamt NIS2-tilskipuninni, mun undirbyggja frekar samvinnu og samhæfingu meðal ólíkra aðila á sviði netöryggismála, einkaaðila ekki síður en stjórnvalda.

6.2. Áhrif á fyrirtækjaeftirlit og reglubyrði.

Efnisreglur DORA eru í samræmi við alþjóðlega viðurkennd viðmið um bestu framkvæmd á sviði net- og upplýsingaöryggis og í innleiðingu hennar er fólgin einföldun regluverks (sama áhætta, sömu reglur). Kostnað af eigin rekstri og uppfyllingu ákvæða fyrirhugaðra laga bera fyrirtækin sjálf.

6.3. Samkeppnisskilyrði.

Ekki eru taldar líkur á því að fyrirhuguð lagasetning hafi áhrif á samkeppni á markaði.

6.4. Áhrif á jafnrétti kynjanna.

Ekki er gert ráð fyrir að samþykkt frumvarpsins hafi sérstök áhrif á stöðu kynjanna.

6.5. Áætluð fjárhagsáhrif fyrir ríkið.

Áformuð lagasetning mun fela í sér aukin verkefni fyrir Seðlabanka Íslands, enda eru kröfur DORA ítarlegar og að einhverju leyti nýmæli í settum lögum. Eftirlit með framkvæmd DORA krefst úttekta, gæðaprófa, gagna- og upplýsingaöflunar frá aðilum á fjármálamarkaði (svo sem vegna utanaðkomandi tækniþjónustuveitenda) og mun vera þörf á uppfærslu

innanhússkerfa Seðlabankans af þeim sökum. Fjármálaeftirlitið fær með fyrirhuguðum lögum heimild til álagningar stjórnvaldssekta vegna brota gegn ákvæðum þeirra. Kröfur DORA um skýrslugjöf aðila á fjármálamarkaði vegna alvarlegra atvika tengdum upplýsinga- og fjarskiptatækni og verulegra netógna krefjast sólarhringsvöktunar af hálfu eftirlitsaðila, enda er meðal annars gert ráð fyrir tímanlegri framsendingu viðeigandi upplýsinga til annarra stjórnvalda innanlands (þar á meðal netöryggissveitar Fjarskiptastofu) og evrópsku fjármálaeftirlitsstofnananna. Greining þarf jafnframt að eiga sér stað við móttöku eftirlitsaðila á upplýsingum um atvik erlendis, tryggja þarf viðeigandi ráðstafanir eða áframmiðlun innanlands og reynt getur á þátttöku Fjármálaeftirlitsins í samevrópsku viðbragðsteymi. Þá er gert ráð fyrir að Seðlabankinn haldi utan um framkvæmd netöryggisprófana, þar með talið ógnamiðaðra innbrotsprófana, og kemur til skoðunar að bankinn haldi úti samstarfsvettvangi aðila á fjármálamarkaði um netógnir samkvæmt 45. gr. DORA. Viðbótarkostnaði vegna aukinna verkefna Seðlabankans með innleiðingu DORA í landsrétt má gera ráð fyrir að verði mætt með hækkun eftirlitsgjalds. Að öðru leyti er ekki talið að áhrifin af innleiðingu DORA í landsrétt hafi bein áhrif á afkomu ríkissjóðs.

Kröfur nútímans, þróun í tækni og viðskiptum og stafrænn fjármálapakki ESB í heild sinni gera stöðuga þekkingaruppbyggingu óhjákvæmilega hjá hinu opinbera. Væntingar eru um ávinning af alþjóðlegu samstarfi í þeim efnum.

Um einstakar greinar frumvarpsins.

Um 1. gr.

Í ákvæðinu, sem byggist á 1. gr. DORA, er markmið frumvarpsins sett fram.

Um 2. gr.

Gildissvið DORA er skilgreint í 2. gr. með víðtækum hætti. Kröfur til áhættustýringar og viðbúnaðar vegna upplýsinga- og fjarskiptatækni eru samræmdar þvert á allan fjármálamarkaðinn. Þannig eru sambærilegar áhættur meðhöndlaðar eins, óháð því hvaða aðili á í hlut (að teknu tilliti til meðalhófsreglu 4. gr. DORA), í því skyni að samræma eftirlit og stuðla að rekstraröryggi og fjármálastöðugleika.

Lagt er til að gildissvið DORA verði útvíkkað þannig að fyrirhuguð lög gildi jafnframt um lífeyrissjóði sem hér á landi starfa á grundvelli laga nr. 129/1997 um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða. Samkvæmt p-lið 1. mgr. 2. gr. DORA falla stofnanir um starfstengdan lífeyri (e. institutions for occupational retirement provision) undir gildissvið hennar. Íslenskir lífeyrissjóðir starfa samkvæmt lögum nr. 129/1997, en ekki tilskipun (ESB) 2016/2341 (IORP II) eða tilskipun 2003/41/EB (IORP I) sem innleidd var hér á landi með lögum um starfstengda lífeyrissjóði, nr. 78/2007. Viðeigandi er talið að beita sömu varúðarsjónarmiðum gagnvart lífeyrissjóðum og öðrum aðilum á fjármálamarkaði, enda er samfélagslegt mikilvægi þeirra óumdeilt. Því er, með vísan til almannahagsmuna, lagt til að íslensku lífeyrissjóðirnir verði felldir undir gildissvið fyrirhugaðra laga, enda tilgangur DORA að samræma reglur um net- og rekstraröryggi á fjármálamarkaði. Með DORA er til dæmis lögð áhersla á aðhald af hálfu þjónustukaupa vegna útvistunar upplýsinga- og fjarskiptatækniþjónustu til þriðja aðila sbr. umfjöllun í kafla 3 í greinargerð með frumvarpinu. Kröfur DORA í þeim efnum munu ná til lífeyrissjóða jafnt sem annarra. Að því marki sem starfsemi lífeyrissjóða rúmast innan skilgreiningar 60. tölul. 3. gr. DORA á örfyrirtæki gilda vægari kröfur reglugerðarinnar um þá. Hins vegar þykir ekki þörf á að yfirfæra stærðarviðmið

á lífeyrissjóði skv. lögum nr. 129/1997 í skilgreiningu DORA á litlum stofnunum um starfstengdan lífeyri (sbr. 53. tölul. 3. gr.), með vísan til 2. mgr. 21. gr. laganna.

Um 3. gr.

Með frumvarpinu er lagt til að ákvæði DORA, eins og hún var aðlöguð og tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. xxx/2024 frá xx.xxx 2024 skuli hafa lagagildi hér á landi. Fyrst og fremst er um aðlaganir að ræða sem taka mið af tveggja stoða kerfi EES-samningsins, ekki síst að því er varðar vísanir til heimilda og hlutverka evrópsku fjármálaeftirlitsstofnananna, sem í tilviki EFTA-ríkjanna innan EES er falið Eftirlitsstofnun EFTA. Með DORA er komið á nýrri umgjörð eftirlits gagnvart mikilvægum tækniþjónustuveitendum með starfsemi út fyrir eigið heimaríki (þ.e. þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu), með vísan til nánari umfjöllunar í kafla 3.6 í greinargerð með frumvarpinu, og er þar um nýmæli að ræða og ný viðfangsefni framangreindra eftirlitsstofnana sem aðaleftirlitsaðila og á sameiginlegum eftirlitsvettvangi.

EFTA-ríkin innan EES hafa öll lagt áherslu á skjóta upptöku DORA í EES-samninginn. Gert er ráð fyrir að þau fái tólf mánuði til að innleiða reglugerðina og koma henni til framkvæmda, frá dagsetningu ákvörðunar um upptöku gerðarinnar í EES-samninginn að telja. Þannig fá stjórnvöld nauðsynlegt svigrúm til að lögfesta og undirbúa framkvæmd fyrirhugaðra laga og innleiða afleiddar gerðir (tæknistaðla) sem útfæra nánar ýmis efnisatriði DORA, auk þess sem markaðsaðilum gefst tími til að undirbúa framfylgd við kröfur hennar.

Í samræmi við hefðbundnar lögskýringarreglur og skýr tilmæli í bæði DORA og NIS2-tilskipuninni verður um sérlög um aðila á fjármálamarkaði að ræða sem ganga framar almennari ákvæðum settra laga um öryggi net- og upplýsingakerfa mikilvægra innviða. Kröfur DORA til áhættustýringar og viðbúnaðar af hálfu aðila á fjármálamarkaði vegna stafræns rekstrarlegs viðnámsþróttar eru útfærðar nánar í tæknistöðlum og ákvæði um tilkynningaskyldu um atvik gera ráð fyrir tímanlegri áframmiðlun upplýsinga til viðeigandi aðila, svo sem netöryggissveitar Fjarskiptastofu innanlands.

Um 4. gr.

Í DORA er nokkuð um vísanir til hugtaka í skilningi annarra Evrópugerða sem teknar hafa verið upp í íslenskan rétt. Með ákvæðinu eru lagðar til skýringar með vísunum til þess hvar viðkomandi hugtök úr tilskipunum hafa verið innleidd í landsrétt.

Hér á eftir er útskýrt hvar þær reglugerðir Evrópusambandsins, sem eru EES-tækar og helst er vísað til í DORA, hafa verið innleiddar:

1. Reglugerð (ESB) nr. 909/2014 um bætt verðbréfauppgjör í Evrópusambandinu og um verðbréfamiðstöðvar og um breytingu á tilskipunum 98/26/EB og 2014/65/ESB og reglugerð (ESB) nr. 236/2012 (CSDR) er innleidd með lögum um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020.
2. Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/1011 um vísitölur sem notaðar eru sem viðmiðanir í fjármálagerningum og fjárhagslegum samningum eða til að mæla árangur fjárfestingarsjóða og um breytingu á tilskipunum 2008/48/EB og 2014/17/ESB og reglugerð (ESB) nr. 596/2014 er innleidd með lögum um fjárhagslegar viðmiðanir, nr. 7/2021.
3. Reglugerð (ESB) nr. 575/2013 um varfærniskröfur að því er varðar lánastofnanir og verðbréfafyrirtæki og um breytingu á reglugerð (ESB) nr. 648/2012 (CRR) er innleidd með lögum um fjármálafyrirtæki, nr. 161/2002.

4. Reglugerð (EB) nr. 648/2012 um OTC-afleiður, miðlæga mótaðila og afleiðuviðskiptaskrár er innleidd með lögum um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018.
5. Reglugerð (ESB) nr. 600/2014 um markaði fyrir fjármálagerninga og um breytingu á reglugerð (ESB) nr. 648/2012 (MiFIR) er innleidd með lögum um markaði fyrir fjármálagerninga, nr. 115/2021.
6. Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1060/2009 um lánshæfismatsfyrirtæki er innleidd með lögum um lánshæfismatsfyrirtæki, nr. 50/2017.
7. Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska bankaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og niðurfellingu ákvörðunar framkvæmdastjórnarinnar 2009/78/EB er innleidd með lögum um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017.
8. Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/79/EB er innleidd með lögum um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017.
9. Reglugerð (ESB) nr. 1095/2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska verðbréfamarkaðseftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/77/EB er innleidd með lögum um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017.
10. Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (GDPR) er innleidd með lögum um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018.

Á yfirstandandi löggjafarþingi áformar fjármála- og efnahagsráðherra að leggja fram á Alþingi frumvörp til innleiðingar á eftirtöldum reglugerðum, sem eru EES-tækar og vísað er til í DORA:

- Reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 um markaði fyrir sýndareignir og um viðbætur við reglugerðir (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipanir 2013/36/ESB og (ESB) 2019/1937 (MiCA).
- Reglugerð (ESB) 2019/2033 um varfærniskröfur til verðbréfafyrirtækja (IFR).
- Reglugerð Evrópuþingsins og ráðsins (ESB) 2020/1503 um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki og um breytingu á reglugerð (ESB) 2017/1129 og tilskipun (ESB) 2019/1937 (ECSP).
- Reglugerð Evrópuþingsins og ráðsins (ESB) 2017/2402 um almennan ramma fyrir verðbréfun og gerð sértæks ramma fyrir einfalda, gagnsæja og staðlaða verðbréfun, og um breytingu á tilskipunum 2009/65/EB, 2009/138/EB og 2011/61/EB og reglugerðum (EB) nr. 1060/2009 og (ESB) nr. 648/2012 (STS).

Þess ber að geta að netöryggistilskipun Evrópusambandsins, 2016/1148 (NIS1), var innleidd hér á landi með lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. Ný netöryggistilskipun, 2022/2555 (NIS2), leysti þá fyrrnefndu af hólmi samhliða samþykkt DORA. Í háskóla-, iðnaðar- og nýsköpunarráðuneytinu er unnið að undirbúningi upptöku NIS2 í EES-samninginn og innleiðingu hér á landi og því fyrirséðar breytingar á lögum nr. 78/2019. Þrátt fyrir að nokkuð sé um vísanir til NIS2 í DORA þykir ekkert því til fyrirstöðu að innleiða DORA hér á landi meðan innleiðingar NIS2 er beðið. Háskóla-, iðnaðar- og nýsköpunarráðuneytið áformar einnig innleiðingu reglugerðar Evrópuþingsins og

ráðsins (ESB) 2019/881 um Netöryggisstofnun Evrópu (ENISA) og netöryggisvottunarkerfi upplýsinga- og samskiptatækja og um niðurfellingu reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 526/2013 á grundvelli reglugerðarheimildar í f-lið 1. mgr. 30. gr. laga um Fjarskiptastofu, nr. 75/2021.

Um 5. gr.

Lagt er til að Seðlabanki Íslands teljist lögbært yfirvald hér á landi í skilningi DORA og að Fjármálaeftirlitinu verði falið eftirlit með framkvæmd fyrirhugaðra laga, skv. VII. kafla DORA. Um eftirlitið og upplýsingagjöf innlendra aðila gilda ákvæði frumvarps þessa, þar á meðal ákvæði DORA, ákvæði laga um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017, og lög um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998. Um kostnað við eftirlitið fer samkvæmt lögum um greiðslu kostnaðar við opinbert eftirlit með fjármálastarfsemi og skilavald, nr. 99/1999.

Um hlutverk Eftirlitsstofnunar EFTA fer samkvæmt ákvæðum laga um Evrópska efnahagssvæðið, nr. 2/1993, og samningi EFTA-ríkjanna um stofnun eftirlitsstofnunar og dómstóls. Fjallað er um hlutverk og valdheimildir Eftirlitsstofnunar EFTA á sviði fjármálaeftirlits í 25. gr. a í þeim samningi og bókun 8 við hann, sbr. auglýsing nr. 64/2021 í C-deild Stjórnartíðinda. Með eftirlitsramma DORA vegna mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sbr. umfjöllun í kafla 3.6 í greinargerð með frumvarpinu, verður Eftirlitsstofnun EFTA falið nýtt beint aðhaldshlutverk gagnvart tækniþjónustuveitendum. Lögbærum yfirvöldum er ætluð aðkoma að framfylgni gagnvart slíkum aðilum ef á reynir. Nánar er kveðið á um valdheimildir í þessu samhengi í 35.–42. gr. DORA.

Samkvæmt 9. mgr. 26. gr. DORA geta aðildarríki tilnefnt eitt opinbert yfirvald í fjármálageiranum til að bera ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun á þessu sviði á landsvísu. Lagt er til að Seðlabanka Íslands verði falið þetta hlutverk, sbr. nánari umfjöllun í köflum 3.1 og 3.4 í greinargerð með frumvarpinu.

Um 6. gr.

Með DORA er komið á tilkynningaskyldu af hálfu allra sem undir gildissvið hennar falla um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulega netógn. Leiðbeinandi tilmæli Fjármálaeftirlitsins vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila, nr. 1/2019, kveða á um slíka skyldu (sbr. lið 5.2), en ekki er um viðurlagaheimildir að ræða ef aðilar láta hjá líða að tilkynna um atvik.

Löggjafinn hefur þegar tekið af skarið um skyldu til að tilkynna netöryggissveit Fjarskiptastofu um alvarleg atvik eða áhættu tengda net- og upplýsingakerfum mikilvægra innviða í skilningi laga nr. 78/2019 og NIS1-tilskipunarinnar. NIS1 var endurnýjuð samhliða samþykkt DORA og bíður NIS2-tilskipunin nú upptöku í EES-samninginn og innleiðingar í landsrétt. Eins og vikið er að í umfjöllun um 3. gr. frumvarpsins verður um sérlög að ræða um aðila á fjármálamarkaði. Kröfur DORA ganga með öðrum orðum framar almennum netöryggislögum (NIS1/NIS2) og á það einnig við að því er varðar skýrslugjöf um atvik. Því er með frumvarpi þessu lögð til sú breyting á 1. mgr. 8. gr. laga nr. 78/2019 (sbr. 8. tölul. 19. gr. frumvarpsins) að atvikatilkynningum frá aðilum á fjármálamarkaði sem þó falla undir gildissvið þeirra laga skuli framvegis beint til Fjármálaeftirlitsins. DORA kveður enda á um skyldu eftirlitsaðilans til tímanlegrar áframmiðlunar upplýsinga um atvik eða verulega netógn til innlendra stjórnvalda, þar á meðal netöryggissveitar Fjarskiptastofu, og evrópsku fjármálaeftirlitsstofnananna. Annað þykir stangast á við kröfur nútímans um einföldun

regluverks en með breytingunni má ljóst vera að þörf er á sólarhringsvöktun tilkynningagáttar Fjármálaeftirlitsins. Gengið er út frá að rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða í skilningi laga nr. 78/2019 tilheyri framvegis sem hingað til þjónustuhópi netöryggissveitar, með vísan til reglugerðar um netöryggissveit Fjarskiptastofu (CERT-IS), nr. 480/2021.

Við útfærslu ákvæðisins var meðal annars horft til 100. gr. laga um greiðsluþjónustu, nr. 114/2021, sem kveður á um sambærilega tilkynningaskyldu til Fjármálaeftirlitsins. Undirliggjandi tilgangur er að miðla áfram, eins skjótt og unnt er, upplýsingum sem kunna að nýtast öðrum aðilum á fjármálamarkaði (og jafnvel öðrum mikilvægum innviðum) til að verjast ógnum við net- og upplýsinga- eða rekstraröryggi. Berist Fjármálaeftirlitinu upplýsingar um alvarleg atvik eða verulega netógn geta ferlar tengdir öðrum ábyrgðarsviðum Seðlabankans virkjast, svo sem fjármálastöðugleika og rekstri millibankakerfisins.

Um 7. gr.

Eins og nánar er vikið að í kafla 3.6 í greinargerð með frumvarpinu er lögbæru yfirvaldi í heimaríki tækniþjónustuveitanda sem fellur undir nýjan eftirlitsramma vegna mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ætlað að framfylgja ákvörðunum og tilmælum hlutaðeigandi aðaleftirlitsaðila, sem í tilviki EFTA-ríkjanna innan EES verður Eftirlitsstofnun EFTA. Ekki þykir líklegt að íslenskur tækniþjónustuveitandi falli undir viðmið DORA í þeim efnum í næstu framtíð, en um ræðir útvíkkun á beinu andlagi löggjafar á sviði fjármálamarkaðar (aðrir en eftirlitsskyldir aðilar). Með ákvæðinu er áréttuð skylda Fjármálaeftirlitsins samkvæmt 42. gr. og 50. gr. DORA.

Um 8. gr.

Lagt er til að kveðið verði á um aðfararhæfi ákvarðana Eftirlitsstofnunar EFTA og dóma og úrskurða EFTA-dómstólsins og þannig tryggt að úrlausnir á grundvelli DORA verði fullnustaðar með atbeina íslenskra stjórnvalda. Í 11. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989, kemur fram að úrlausnir eða ákvarðanir erlendra dómstóla eða yfirvalda eða sættir gerðar fyrir þeim séu aðfararhæfar ef íslenska ríkið hefur skuldbundið sig að þjóðarétti og með lögum til að viðurkenna slíkar aðfararheimildir, enda verði fullnusta kröfu talin samrýmanleg íslensku réttarskipulagi. Að öðru leyti gilda lög um aðför um fullnustu ákvarðana Eftirlitsstofnunar EFTA og dóma og úrskurða EFTA-dómstólsins.

Um 9. gr.

Ákvæðið er árétting á heimildum sem telja verður að eftirlitsaðilar hafi almennt í krafti eftirlitsskyldu sinnar gagnvart eftirlitsskyldum aðilum á fjármálamarkaði og er sambærilegt 1. mgr. 10. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998.

Um heimildir Fjármálaeftirlitsins til álagningar févítis og dagsekta fer skv. 11. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998. Á heimild til álagningar dagsekta getur reynt ef aðili veitir ekki umbeðnar upplýsingar eða sinnir ekki kröfum um úrbætur innan hæfilegs frests. Dagsektir greiðast þar til farið hefur verið að kröfum Fjármálaeftirlitsins og geta þær numið frá 10.000 kr. til 1 millj. kr. á dag og er heimilt að ákveða þær sem hlutfall af tilteknum stærðum í rekstri eftirlitsskylds aðila. Fjármálaeftirlitið getur lagt févíti á aðila sem brýtur gegn ákvörðun sem eftirlitið hefur tekið, þar á meðal kröfur um úrbætur. Févíti getur samkvæmt lögunum numið frá 10.000 kr. til 2 millj. kr.

Um 10. gr.

Í samræmi við 50.–52. gr. DORA er í ákvæðinu kveðið á um rétt eftirlitsaðila til að beita stjórnsýsluviðurlögum vegna brota á tilgreindum ákvæðum reglugerðarinnar til að tryggja skilvirka framkvæmd þeirra. Er þar um að ræða kröfur sem gerðar eru til aðila á fjármálamarkaði eins og mælt er fyrir um í II. –IV. kafla reglugerðarinnar, nánar tiltekið um stýringu upplýsinga- og fjarskiptatækniáhættu, atvikastjórnun, flokkun og skýrslugjöf í tengslum við upplýsinga- og fjarskiptatækni og prófanir á stafrænum rekstrarlegum viðnámsþrótti aðila á fjármálamarkaði.

Í samræmi við lög um fjármálafyrirtæki er lagt til að fjárhæð sekta vegna brota gegn frumvarpinu sem lagðar eru á einstaklinga geti numið frá 100 þús. kr. til 700 millj. kr. og sekt sem lögð er á lögaðila geti numið á bilinu 500 þús. kr. til 800 millj. kr. eða hærri allt að 10% af heildarveltu samkvæmt síðasta samþykkta ársreikningi lögaðila eða 10% af síðasta samþykkta samstæðureikningi ef lögaðili er hluti af samstæðu. Hver þessara fjárhæða sem hæst reynist mun þannig ákvarða hámarksfjárhæð sekta hverju sinni. Þannig gæti til dæmis sekt sem er lögð á lögaðila orðið hærri en 800 millj. kr. ef 10% af veltu hans samkvæmt síðasta samþykkta ársreikningi væru meiri en 800 millj. kr. Jafnframt gildir 800 millj. kr. hámarkið þótt 10% af veltu lögaðilans séu minni en 800 millj. kr.

Um 11. gr.

Gert er ráð fyrir að bæði ásetnings- og gáleysisbrot varði stjórnvaldssektum og öðrum viðurlögum samkvæmt frumvarpinu til að styrkja varnaðaráhrif þeirra og til samræmis við það sem almennt gildir um stjórnsýsluviðurlög á sviði fjármálamarkaðar, sbr. 3. og 7. mgr. 110. laga um fjármálafyrirtæki. Saknæmisstig getur þó haft áhrif á það hversu alvarlegt brot er talið og þar með ákvörðun stjórnvaldssektar og annarra viðurlaga.

Um 12. gr.

Ákvæðið, sem byggist á 51. gr. DORA og er í samræmi við gildandi löggjöf á sviði fjármálaþjónustu, kveður á um að Fjármálaeftirlitið skuli taka tillit til allra atvika sem máli skipta þegar það ákveður tegund og umfang stjórnsýsluviðurlaga samkvæmt frumvarpinu. Talin eru upp nokkur atriði sem skal líta til eftir því sem við á hverju sinni. Meginatriðið er að viðurlög hafi tilhlýðileg varnaðaráhrif. Þau þurfa því meðal annars að vinna gegn því að brotlegir aðilar hagnist á brotum eða komi sér undan tapi.

Um 13. gr.

Í samræmi við aðra gildandi löggjöf á sviði fjármálaþjónustu er með ákvæðinu lagt til að Fjármálaeftirlitinu verði veitt heimild til að ljúka málum með sátt. Til að unnt sé að ljúka máli með sátt verður samþykki málsaðila að liggja fyrir. Sættir eru því ekki einhliða ákvarðanir stjórnvalds heldur koma málsaðilar einnig að þeim. Því er lagt til að kveðið verði skýrt á um að sátt sé bindandi fyrir aðila þegar hann hefur samþykkt hana og staðfest efni hennar með undirskrift sinni. Fjármálaeftirlitið hefur á grundvelli annarra laga á sviði fjármálamarkaða sett reglur um heimild Fjármálaeftirlitsins til að ljúka máli með sátt, nr. 326/2019.

Um 14. gr.

Mannréttindadómstóll Evrópu hefur talið að það sé þáttur í réttlátri málsmeðferð skv. 6. gr. mannréttindasáttmála Evrópu að þeim sem sakaður er um refsiverða háttsemi í skilningi þess ákvæðis sé ekki skylt að tjá sig eða láta í té upplýsingar sem leitt geta til sakfellingar hans. Dómstóllinn hefur komist að þeirri niðurstöðu að ákvæðið geti við ákveðnar aðstæður verndað rétt manns til að fella ekki á sig sök í tengslum við meðferð stjórnsýslumála og

ákvörðun stjórnsýsluviðurlaga, einkum stjórnvaldssekta. Ekki hefur þó enn verið sett almenn regla í íslensk lög um rétt einstaklinga til þess að fella ekki á sig sök við meðferð stjórnsýslumála sem geta leitt til ákvörðunar stjórnsýsluviðurlaga. Því er lagt til að rétturinn verði tilgreindur í 14. gr. frumvarpsins. Ákvæðið byggist á lögum um breytingar á lagaákvæðum um viðurlög við brotum á fjármálamarkaði, nr. 55/2007, sem aftur byggðust á skýrslu nefndar um viðurlög við efnahagsbrotum frá 12. október 2006.

Ákvæðið tekur aðeins til einstaklinga en ekki til lögaðila. Ákvæðinu er ekki ætlað að taka til réttinda annarra einstaklinga en þeirra sem eru aðilar að stjórnsýslumáli. Því hefur maður ekki rétt til að neita að svara spurningum eða afhenda gögn með vísan til þess að uppi sé rökstuddur grunur um lögbrot þriðja manns og upplýsingar eða gögn kunni að fella sök á hann.

Vernd ákvæðisins verður virk þegar rökstuddur grunur vaknar um að einstaklingur hafi gerst sekur um lögbrot. Þannig verða að vera til staðar aðstæður eða sönnunargögn sem benda til sektar hans og rannsókn að beinast að honum sérstaklega en ekki stærri hópi manna.

Ef til staðar er rökstuddur grunur um að viðkomandi hafi framið lögbrot sem varðað getur stjórnsýsluviðurlögum er honum aðeins skylt að veita upplýsingar eða gögn ef unnt er að útiloka að þær geti haft þýðingu fyrir ákvörðun um sekt hans. Væri honum því t.d. skylt að veita upplýsingar um nafn sitt og heimilisfang. Einstaklingur getur aftur á móti ákveðið að nýta sér ekki þagnarrétt sinn og bæði tjáð sig og afhent gögn í stjórnsýslumáli sem kann að ljúka með stjórnsýsluviðurlögum. Við þær aðstæður telst ekki brotið gegn þagnarrétti hans.

Áréttað skal að rétturinn er víðtækari en að neita að gefa munnlegar upplýsingar. Hann tekur einnig til þess að þurfa ekki að afhenda gögn eða ljá atbeina sinn að öðru leyti við rannsókn máls sem getur fellt sök á mann. Það breytir þó ekki heimildum sem lög veita til þess að afla gagna með þvingunaraðgerðum þar sem ekki er þörf á atbeina hins grunaða eins og á t.d. við um húsleit og haldlagningu gagna sem finnast við slíka leit. Þá er ákvæðinu ekki ætlað að leysa einstakling undan lögmæltri skyldu til að veita stjórnvaldi aðgang að húsnæði eða hirslum í fyrirtækjum. Það sem mestu skiptir og ákvæðið stefnir að er að einstaklingi verður ekki gert skylt að ljá rannsókn atbeina sinn á virkan hátt þegar rökstuddur grunur leikur á að hann hafi gerst sekur um lögbrot.

Um 15. gr.

Lagt er til að heimild Fjármálaeftirlitsins til að beita stjórnvaldssektum og öðrum stjórnsýsluviðurlögum samkvæmt fyrirhuguðum lögum falli niður þegar sjö ár eru liðin frá því að háttsemi lauk til að knýja á um úrlausn mála. Sams konar ákvæði er til að mynda að finna í 9. gr. laga um skortsölu og skuldatryggingar, nr. 55/2017, 11. gr. laga um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018, 130. gr. laga um markaði fyrir fjármálagerninga, nr. 115/2021, og 15. gr. laga um fjármögnunarviðskipti með verðbréf, nr. 41/2023. Rétt er að taka mið af meginreglum refsiréttar og fjármálamarkaðsréttar um það hvenær háttsemi telst lokið. Af því leiðir meðal annars að ef um samfellda brotastarfsemi eða ástandsbrot er að ræða telst broti ekki lokið fyrr en hinu ólögmæta ástandi linnir og upphaf frestsins telst þá einnig frá þeim tíma.

Af 2. mgr. leiðir meðal annars að þótt rannsókn beinist í upphafi að einum aðila hindrar 1. mgr. ekki að aðrir aðilar sem síðar kemur í ljós að stóðu einnig að broti verði beittir stjórnvaldssektum eða öðrum stjórnsýsluviðurlögum. Reglan á sér að nokkru leyti hliðstæðu í 4. mgr. 82. gr. almennra hegningarlaga, nr. 19/1940.

Um 16. gr.

Framkvæmdastjórn Evrópusambandsins er í nokkrum ákvæðum reglugerðarinnar veitt vald til að samþykkja undirgerðir (tæknistaðla) til að útfæra nánar ákveðin efnisatriði DORA. Lagt er til að ráðherra verði heimilað að innleiða þær gerðir sem varða nýjan eftirlitsramma vegna mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu með reglugerð en að Seðlabanka Íslands verði heimilað að innleiða aðrar gerðir með reglum. Tíðkast hefur að Seðlabankinn innleiði tæknistaðla frá evrópsku fjármálaeftirlitsstofnununum þar sem hann hefur áheyrnaraðild að stofnununum og tekur þátt í starfi vinnuhópa á þeirra vegum sem fást við mótun tæknistaðla.

Um 17. gr.

Breytingatilskipun (ESB) 2022/2556 fylgir DORA-reglugerðinni. Um ræðir hefðbundið innleiðingarákvæði.

Um 18. gr.

Stafrænn rekstrarlegur viðnámsþróttur eða áfallaþol fjármálamarkaða eru hvarvetna í brennidepli. Öll hafa EFTA-ríkin innan EES lagt áherslu á skjóta upptöku DORA í EES-samninginn og innleiðingu í landsrétt. Upptaka er áformuð hausið 2024 og ætlunin er að tryggja EFTA-ríkjunum 12 mánaða svigrúm til innleiðingar í landsrétt. Lagt er til að gildistaka miðist við 1. júlí 2025 hér landi.

Um 19. gr.

Með ákvæðinu eru lagðar til breytingar á öðrum lögum, til samræmis við efni DORA-reglugerðarinnar og DORA-tilskipunarinnar um breytingar á ýmsum EES-gerðum.

Ennfremur er í 8. tölul. lagt til að tekið verði af skarið um lagaskil að því er varðar tilkynningaskyldu um atvik og verulega netógn af hálfu rekstraraðila nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. Aðilar á fjármálamarkaði beini slíkum tilkynningum til Fjármálaeftirlitsins, sem hins vegar verður skylt að áframmiðla þeim tímanlega til netöryggissveitar Fjarskiptastofu ef við á. Vísast til fyrri umfjöllunar um þetta, m.a. um 6. gr.