156. löggjafarþing 2025.
Þingskjal 293 — 261. mál.
Stjórnarfrumvarp.

Frumvarp til laga

um stafrænan viðnámsþrótt fjármálamarkaðar.

Frá fjármála- og efnahagsráðherra.

1. gr.
Lögfesting.

Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (ESB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011, sem er birt á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025, hefur lagagildi hér á landi með þeim aðlögunum sem leiðir af bókun 1 um altæka aðlögun við samninginn um Evrópska efnahagssvæðið og ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 frá 20. febrúar 2025, sem er birt í auglýsingu nr. 8/2025 í C-deild Stjórnartíðinda.

2. gr.
Vísanir til tilskipana.

Eftirfarandi vísanir til tilskipana í reglugerð (ESB) 2022/2554 skulu skiljast svo:

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 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.
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 skv. 4. lið 13. gr. tilskipunar 2009/138/EB*: Endurtryggingafélag samkvæmt lögum um vátryggingastarfsemi.
6. *Endurtryggingamiðlari skv. 5. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97*: Vátryggingamiðlari í skilningi laga um dreifingu vátrygginga.
7. *Greiðslustofnun skv. 4. lið 4. gr. tilskipunar (ESB) nr. 2015/2366*: Greiðslustofnun samkvæmt lögum um greiðsluþjónustu.
8. *Greiðslustofnun sem er undanþegin samkvæmt tilskipun (ESB) 2015/2366*: Greiðslustofnun með takmarkað starfsleyfi skv. 34. gr. laga um greiðsluþjónustu, nr. 114/2021.

9. *Móðurfyrirtæki í skilningi 9. liðar 2. gr. og 22. gr. tilskipunar 2013/34/ESB*: Móðurfélag samkvæmt lögum um ársreikninga.
10. *Nauðsynleg eða mikilvæg rekstrareining sem fellur undir tilskipun (ESB) 2022/2555*: Mikilvægir innviðir í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða 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 samkvæmt lögum um skilameðferð lánastofnana og verðbréfafyrirtækja.
12. *Net- og upplýsingakerfi skv. 1. lið 6. gr. tilskipunar (ESB) 2022/2555*: Net- og upplýsingakerfi samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða.
13. *Rafeyrisfyrirtæki skv. 1. lið 2. gr. tilskipunar Evrópuþingsins og ráðsins 2009/110/EB*: Rafeyrisfyrirtæki samkvæmt lögum um útgáfu og meðferð rafeyris.
14. *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.
15. *Reikningsupplýsingaþjónustuveitandi skv. 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366*: Reikningsupplýsingaþjónustuveitandi samkvæmt lögum um greiðsluþjónustu.
16. *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.
17. *Rekstraraðili skv. b-lið 1. mgr. 4. gr. tilskipunar 2011/61/ ESB*: Rekstraraðili samkvæmt lögum um rekstraraðila sérhæfðra sjóða.
18. *Rekstrarfélag skv. b-lið 1. mgr. 2. gr. tilskipunar 2009/65/EB*: Rekstrarfélag verðbréfasjóða samkvæmt lögum um verðbréfasjóði.
19. *Samstæða í skilningi 11. liðar 2. gr. tilskipunar 2013/34/ESB*: Samstæða samkvæmt lögum um ársreikninga.
20. *Skilastjórnvald skv. 3. gr. tilskipunar 2014/59/ESB*: Skilastjórnvald samkvæmt lögum um skilameðferð lánastofnana og verðbréfafyrirtækja.
21. *Stjórn og/eða framkvæmdastjórn 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*: Stjórn og/eða framkvæmdastjórn.
22. *Stofnun um starfstengdan lífeyri skv. 1. lið 6. gr. tilskipunar (ESB) 2016/2341*: Starfstengdur eftirlaunasjóður samkvæmt lögum um starfstengda eftirlaunasjóði.
23. *Vátrygginga- og endurtryggingafélög eins og um getur í 4. gr. tilskipunar 2009/138/EB*: Vátryggingafélag sem eru undanþegin gildissviði vegna stærðar skv. 3. mgr. 3. gr. laga um vátryggingastarfsemi, nr. 100/2016.
24. *Vátryggingafélag skv. 1. lið 13. gr. tilskipunar 2009/138/EB*: Vátryggingafélag samkvæmt lögum um vátryggingastarfsemi.
25. *Vátryggingamiðlari í hliðarstarfsemi skv. 4. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97*: Aðili sem dreifir vátryggingu sem aukaafurð samkvæmt lögum um dreifingu vátrygginga.
26. *Verðbréfafyrirtæki skv. 1. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB*: Verðbréfafyrirtæki samkvæmt lögum um markaði fyrir fjármálagerninga.
27. *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.
28. *Viðskiptavettvangur skv. 24. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB*: Viðskiptavettvangur samkvæmt lögum um markaði fyrir fjármálagerninga.

29. *Öryggi net- og upplýsingakerfa skv. 2. lið 6. gr. tilskipunar (ESB) 2022/2555*: Öryggi net- og upplýsingakerfa samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða.

3. gr.

Lögbært yfirvald og eftirlit.

Seðlabanki Íslands er lögbært yfirvald hér á landi í skilningi laga þessara og ber ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun samkvæmt reglugerð (ESB) 2022/2554.

Fjármálaeftirlitið hefur eftirlit með því að farið sé að lögum þessum og fer með önnur þau verkefni sem reglugerð (ESB) 2022/2554 felur lögbæru yfirvaldi. Um eftirlitið fer samkvæmt ákvæðum laga þessara, laga um opinbert eftirlit með fjármálastarfsemi og laga um evrópskt eftirlitskerfi á fjármálamarkaði.

4. gr.

Úrbætur.

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

5. gr.

Stjórnvaldssektir.

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

1. 5.–14. gr. um kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu,
2. 16. gr. um kröfur um einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni,
3. 17. gr. um kröfur um atvikastjórnunarferli sem tengist upplýsinga- og fjarskiptatækni, eftir atvikum sbr. 23. gr.,
4. 1. og 2. mgr. 18. gr. um skyldu til að flokka atvik sem tengjast upplýsinga- og fjarskiptatækni og netógnum, eftir atvikum sbr. 23. gr.,
5. 1., 3. og 4. mgr. 19. gr. um skyldu til að tilkynna alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni, eftir atvikum sbr. 23. gr.,
6. 24. gr. um almennar kröfur um framkvæmd prófunar á stafrænum viðnámsþrótti,
7. 25. gr. um prófun á upplýsinga- og fjarskiptatæknibúnaði og -kerfum,
8. 26. gr. um kröfur um auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði, tilheyrandi kerfum og ferlum sem byggjast á ógnamiðaðri innbrotsprófun,
9. 27. gr. um kröfur fyrir prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun,
10. 28. gr. og 29. gr. um kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu,
11. 1.–3. mgr. 30. gr. um kröfur varðandi samninga við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu,
12. 12. mgr. 31. gr. um kröfur sem gerðar eru varðandi nýtingu þjónustu mikilvægs þriðja aðila með staðfestu í þriðja ríki,
13. 3. og 6. mgr. 42. gr. um skyldu aðila á fjármálamarkaði til að taka tillit til áhættu sem tilgreind er í tilmælum aðaleftirlitsaðila til mikilvægra þriðja aðila sem veita upplýsinga- og fjarskiptaþjónustu og, ef við á, um skyldu til að hlíta ákvörðun Fjármálaeftirlitsins um notkun eða nýtingu þjónustu slíkra aðila.

Sektir sem lagðar eru á einstaklinga geta numið frá 100 þús. kr. til 65 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 af sér með þeim hætti sem í 1. mgr. greinir stjórnvaldssekt sem nemur allt að tvöfaldri þeirri fjárhæð sem fjárhagslegur ávinningur af brotinu nemur.

Ákvarðanir Fjármálaeftirlitsins 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.

6. gr.

Saknæmi.

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

7. gr.

Ákvörðun stjórnsýsluviðurlaga.

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

1. alvarleika brots og hvað það hefur staðið lengi,
2. ábyrgðar hins brotlega einstaklings eða lögaðila,
3. fjárhagsstöðu hins brotlega, sér í lagi með hliðsjón af ársveltu lögaðila eða árstekjum og eignum einstaklings,
4. þýðingar ávinnings eða taps sem forðað var með broti fyrir hinn brotlega,
5. hvort brot hafi leitt til tjóns þriðja aðila,
6. samstarfsvilja hins brotlega,
7. fyrri brota hins brotlega og hvort um ítrekað brot er að ræða.

8. 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.

9. gr.

Réttur grunaðs manns.

Í máli sem beinist að einstaklingi og lokið getur með ákvörðun um stjórnsýsluviðurlög samkvæmt 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.

10. gr.

Frestur til að beita stjórnsýsluviðurlögum.

Heimild Fjármálaeftirlitsins til að leggja á stjórnsýsluviðurlög samkvæmt lögum þessum fellur niður þegar fimm 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.

11. gr.

Stjórnvaldsfyrirmæli.

Ráðherra setur reglugerð um nánari framkvæmd reglugerðar (ESB) 2022/2554 um þau atriði sem koma fram í:

1. 6. mgr. 31. gr. um viðmiðanir til grundvallar útnefningu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.
2. 2. mgr. 43. gr. um gjöld sem Eftirlitsstofnun EFTA leggur á mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

Seðlabanki Íslands setur reglur um nánari framkvæmd reglugerðar (ESB) 2022/2554 um þau atriði sem koma fram í:

1. 15. gr. um frekari samhæfingu búnaðar, aðferða, ferla og stefna til stýringar á upplýsinga- og fjarskiptatækniáhættu.
2. 3. mgr. 16. gr. um einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni.
3. 3. og 4. mgr. 18. gr. um flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum.
4. 20. gr. um samræmingu á efni og sniðmátum tilkynninga.
5. 11. mgr. 26. gr. um auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði og samsvarandi kerfum og ferlum sem byggjast á ógnamiðaðri innbrotsprófun.
6. 9. og 10. mgr. 28. gr. um almennar meginreglur um trausta stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila.
7. 5. mgr. 30. gr. um helstu samningsákvæði.
8. 2. mgr. 41. gr. um samræmingu skilyrða vegna eftirlitsramma mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

12. gr.

Undanþegnir aðilar.

Lög þessi gilda ekki um Byggðastofnun, Lánasjóð sveitarfélaga ohf. og Náttúruhamfaratryggingu Íslands.

13. gr.

Gildistaka.

Lög þessi öðlast gildi 1. nóvember 2025.

14. gr.

Breyting á öðrum lögum.

Við gildistöku laga þessara verða eftirfarandi breytingar á öðrum lögum:

1. *Lög um verðbréfasjóði, nr. 116/2021:* Við 2. tölul. 3. mgr. 15. gr. laganna bætist: þ.m.t. að því er varðar net- og upplýsingakerfi sem sett eru upp og stjórnað í samræmi við reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar.

2. *Lög um vátryggingastarfsemi, nr. 100/2016:*
   a. Við 5. mgr. 39. gr. laganna bætist: og skal setja upp og stjórna net- og upplýsingakerfum í samræmi við reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar.
   b. Eftirfarandi breytingar verða á 44. gr. laganna:
      1. Við 4. mgr. bætist: aðra en þá sem varða stýringu upplýsinga- og fjarskiptatækniáhættu.
      2. Við e-lið 5. mgr. bætist: aðra en þá sem varða stýringu upplýsinga- og fjarskiptatækniáhættu.
3. *Lög um rekstraraðila sérhæfðra sjóða, nr. 45/2020:* 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 (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar.
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 viðnámsþrótt fjármálamarkaðar.
   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 tækni sem notuð er við upplýsingamiðlun, og tryggja að þessum áætlunum sé komið á, stjórnað og þær prófaðar í samræmi við 11. gr. reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, til að tryggja áframhaldandi starfsemi sína og takmörkun á tjóni ef alvarleg röskun verður á starfsemi fyrirtækisins.
   c. Við 3. mgr. 80. gr. laganna bætist nýr stafliður, svohljóðandi: áhættu sem prófanir á stafrænum viðnámsþrótti leiða í ljós í samræmi við IV. kafla reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar.
5. *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 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 á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025.
   b. Eftirfarandi breytingar verða á 21. gr. laganna:
      1. 3. mgr. orðast svo:
         Verðbréfafyrirtæki skal gera eðlilegar ráðstafanir til að tryggja að fjárfestingarþjónusta og fjárfestingarstarfsemi 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 viðnámsþrótt fjármálamarkaðar, sem og viðeigandi og hæfileg tilföng og verklag.
      2. 5. mgr. orðast svo:
         Verðbréfafyrirtæki skal hafa traustar aðferðir fyrir stjórnun og bókhald, innra eftirlitskerfi og skilvirkar verklagsreglur fyrir áhættumat.
      3. 6. mgr. orðast svo:

Verðbréfafyrirtæki skal hafa trausta öryggisferla, í samræmi við kröfurnar sem mælt er fyrir um í reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, til að:

1. tryggja öryggi og sannvottun aðferða til að senda upplýsingar,
2. draga eins og kostur er úr hættu á spillingu gagna og óheimiluðum aðgangi og
3. 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 upplýsingum.

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 viðnámsþrótt fjármálamarkaðar, falli undir viðeigandi viðskiptamörk og viðskiptatakmarkanir og komi í veg fyrir sendingu rangra fyrirmæla eða að kerfin séu að öðru leyti þannig að þau geti skapað eða stuðlað 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, 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. Eftirfarandi breytingar verða á 1. mgr. 78. gr. laganna:

1. 2. tölul. orðast svo: Vera nægilega vel í stakk búinn til að stýra áhættu sem að honum snýr, þ.m.t. að stýra upplýsinga- og fjarskiptatækniáhættu í samræmi við II. kafla reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, koma á viðeigandi ráðstöfunum og kerfum til að greina alla verulega áhættuþætti fyrir rekstur hans og koma á skilvirkum ráðstöfunum til að draga úr þeim.
2. 3. tölul. fellur brott.

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

Skipulegur markaður skal koma á og viðhalda stafrænum viðnámsþrótti sínum í samræmi við kröfurnar sem mælt er fyrir um í II. kafla reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan 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 rækilega prófuð til að tryggja að þessi skilyrði séu uppfyllt og falli undir skilvirkt fyrirkomulag til að tryggja 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. Í stað orðsins „prófunarumhverfi“ í 1. málsl. 1. mgr. 85. gr. laganna kemur: 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 viðnámsþrótt fjármálamarkaðar.

6. *Lög um greiðsluþjónustu, nr. 114/2021:*
   a. Í stað orðanna „þjónustu við verndun trúnaðarupplýsinga og friðhelgi einkalífs, sannvottun gagna og eininga, þjónustuveitu upplýsingatækni- og samskiptanets“ í 10. tölul. 1. mgr. 2. gr. laganna kemur: traustþjónustu og þjónustu við verndun friðhelgi einkalífs, sannvottun gagna og eininga, veitingu upplýsinga- og fjarskiptatækniþjónustu.
   b. Eftirfarandi breytingar verða á 1. mgr. 4. gr. laganna:
      1. 10. tölul. orðast svo: Lýsing á verkferli sem fylgja skal 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 viðnámsþrótt fjármálamarkaðar.
      2. 11. tölul. orðast svo: Lýsing á fyrirkomulagi stjórnarhátta umsækjanda og innri eftirlitskerfum hans, þ.m.t. aðferðum við stjórnun, áhættustýringu og reikningsskil, auk fyrirkomulags fyrir notkun upplýsinga- og fjarskiptatækniþjónustu í samræmi við reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, sem sýnir að stjórnarhættir og innra eftirlitskerfi séu í réttu hlutfalli við starfsemina, viðeigandi, traust og fullnægjandi.
      3. 14. tölul. orðast svo: Lýsing á fyrirkomulagi rekstrarsamfellu þar sem mikilvæg starfsemi er skýrt tilgreind, 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 viðnámsþrótt fjármálamarkaðar.
      4. 16. tölul. orðast svo: Öryggisstefna og lýsing á öryggiskerfi umsækjanda, sem skal innihalda ítarlegt áhættumat í tengslum við greiðsluþjónustu, lýsingu á ráðstöfunum vegna öryggiseftirlits og mildunarráðstafana sem gripið er til í því skyni að vernda notendur greiðsluþjónustu með fullnægjandi hætti fyrir tilgreindri áhættu, svo sem svikum og ólöglegri notkun viðkvæmra gagna og persónuupplýsinga. Lýsing skal fylgja á ráðstöfunum til að tryggja öflugan stafrænan viðnámsþrótt í samræmi við II. kafla reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan 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 þáttum í starfsemi sinni til, notar. Ráðstafanir skv. 1. málsl. skulu einnig taka til ráðstafana skv. 99. gr. um eftirlitskerfi rekstrar- og öryggisáhættu.
   c. 1. málsl. 2. mgr. 18. gr. laganna orðast svo: Útvistun mikilvægra rekstrarþátta, þar á meðal upplýsinga- og fjarskiptatæknikerfa, 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. Á eftir 1. mgr. 99. gr. laganna kemur ný málsgrein, svohljóðandi:

Ákvæði 1. mgr. hefur ekki áhrif á framkvæmd II. kafla reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, gagnvart lánastofnunum, rafeyrisfyrirtækjum, greiðslustofnunum, reikningsupplýsingaþjónustuveitendum, greiðslustofnunum með takmarkað starfsleyfi og rafeyrisfyrirtækjum með takmarkað starfsleyfi skv. 16. gr. laga um meðferð og útgáfu rafeyris, nr. 17/2013.

e. Eftirfarandi breytingar verða á 1. mgr. 100. gr. laganna:
   1. Við bætist: í samræmi við grein þessa.
   2. Við bætist nýr málsliður, svohljóðandi: Þrátt fyrir 1. málsl. gildir grein þessi ekki um 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, sem falla undir gildissvið reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar.

f. Í stað tilvísunarinnar „2. mgr. 99. gr.“ í 3. mgr. 101. gr. og 58. tölul. 1. mgr. 106. gr. laganna kemur: 3. mgr. 99. gr.

7. *Lög um öryggi net- og upplýsingakerfa mikilvægra aðila, nr. 78/2019:* Við 1. mgr. 8. gr. laganna bætist nýr málsliður, svohljóðandi: Um tilkynningar skv. 1. málsl. fer þó samkvæmt reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, í tilviki rekstraraðila nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða.
8. *Lög um lánshæfismatsfyrirtæki, nr. 50/2017:* 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 á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025.
9. *Lög um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018:* Við 2. gr. laganna bætist nýr töluliður, 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 á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025.
10. *Lög um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020:*

a. Eftirfarandi breytingar verða á 3. gr. laganna:
   1. 1. mgr. orðast svo:

      Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 909/2014 frá 23. júlí 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, sem er birt á bls. 255–326 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 25 frá 28. mars 2019, hefur lagagildi með þeim aðlögunum sem leiðir af bókun 1 um altæka aðlögun við samninginn um Evrópska efnahagssvæðið og ákvörðun sameiginlegu EES-nefndarinnar nr. 18 frá 8. febrúar 2019, sem er birt á bls. 8–10 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 17 frá 28. febrúar 2019, og með breytingum samkvæmt:

1. 17. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/858 frá 30. maí 2022 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, sem er birt á bls. 160–192 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 92 frá 20. desember 2023.
2. 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 á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025.

2. 2. mgr. orðast svo: Í lögum þessum er vísað til reglugerðar (ESB) nr. 909/2014 með aðlögunum og breytingum skv. 1. mgr. sem reglugerðar (ESB) nr. 909/2014.

11. *Lög um fjárhagslegar viðmiðanir, nr. 7/2021:*

a. Eftirfarandi breytingar verða á 1. gr. laganna:

1. 1. mgr. orðast svo:

Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/1011 frá 8. júní 2016 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, sem er birt á bls. 72–136 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 16 frá 12. mars 2020, hefur lagagildi með þeim aðlögunum sem leiðir af bókun 1 um altæka aðlögun við samninginn um Evrópska efnahagssvæðið og ákvörðun sameiginlegu EES-nefndarinnar nr. 190/2019 frá 10. júlí 2019, sem er birt á bls. 5–6 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 73 frá 12. september 2019, og með breytingum samkvæmt:

1. 1. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/2089 frá 27. nóvember 2019 um breytingu á reglugerð (ESB) 2016/1011 að því er varðar viðmiðanir ESB vegna loftslagstengdra umbreytinga, viðmiðanir ESB sem eru lagaðar að Parísarsamningnum og upplýsingagjöf um sjálfbærni fyrir viðmiðanir, sem er birt á bls. 658–668 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 26 frá 23. apríl 2020.
2. 1. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2021/168 frá 10. febrúar 2021 um breytingu á reglugerð (ESB) 2016/1011 að því er varðar undanþágu fyrir tilteknar viðmiðanir fyrir stundargengi gjaldmiðla þriðju landa og tilnefningu viðmiðana í stað viðmiðana sem verður hætt með og um breytingu á reglugerð (ESB) nr. 648/2012, sem er birt á bls. 47–58 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 4 frá 17. janúar 2022.
3. 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 á bls. 1–79 í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 15 frá 13. mars 2025.

2. 2. mgr. orðast svo:

Í lögum þessum er vísað til reglugerðar (ESB) 2016/1011 með aðlögunum og breytingum skv. 1. mgr. sem reglugerðar (ESB) 2016/1011.

12. *Lög um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997:* Á eftir 36. gr. f laganna kemur ný grein, 36. gr. g, ásamt fyrirsögn, svohljóðandi:

Rekstraráhætta.

Lífeyrissjóður skal hafa stefnu og ferla til að meta og stýra rekstraráhættu, þ.m.t. vegna útvistunar og fátíðra atburða sem geta haft alvarlegar afleiðingar.

Lífeyrissjóður skal stýra upplýsinga- og fjarskiptatækniáhættu í samræmi við ákvæði 5.–14. gr., 17. gr., 1. og 2. mgr. 18. gr., 1. mgr. 22. gr. og 24.–30. gr. reglugerðar (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar. Ráðstafanir til að stuðla að stafrænum viðnámsþrótti lífeyrissjóðs skulu vera í réttu hlutfalli við stærð og heildaráhættusnið lífeyrissjóðs og eðli, umfang og flækjustig þjónustu hans, starfsemi og reksturs.

Um lífeyrissjóði með færri sjóðfélaga en 100 fer skv. 16. gr. í stað 5.–14. gr. reglugerðar (ESB) 2022/2554 um einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni.

Lífeyrissjóður skal tilkynna Fjármálaeftirlitinu um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir skv. 1. og 2. mgr. 19. gr. reglugerðar (ESB) 2022/2554. Um slíkar tilkynningar fer skv. 3.–5. mgr. 19. gr. reglugerðarinnar. Fjármálaeftirlitið skal leggja mat á mikilvægi atviks eða ógnar og tilkynna öðrum innlendum stjórnvöldum tímanlega um það eftir því sem við á.

Lífeyrissjóður getur átt aðild að fyrirkomulagi upplýsingaskipta hér á landi vegna upplýsinga og greiningargagna um netógnir skv. 45. gr. reglugerðar (ESB) 2022/2554.

Seðlabanka Íslands er heimilt að setja nánari reglur um rekstraráhættu lífeyrissjóða og útfæra nánar skyldur lífeyrissjóða samkvæmt þessari grein.

G r e i n a r g e r ð .

Efnisskipan.

1. Inngangur.
2. Tilefni og nauðsyn lagasetningar.
   - 2.1. Stafrænn fjármálapakki ESB og stafrænt áfallaþol.
   - 2.2. Gildissvið og meðalhófsregla.
   - 2.3. Mat á nauðsyn og mögulegar leiðir við lagasetningu.
3. Meginefni frumvarpsins.
   - 3.1. Samantekt.
   - 3.2. Áhættustýring og viðbúnaður.
     a. Stjórnunarhættir og skipulag (5. gr.).
     b. Áhættustýringarrammi í upplýsinga- og fjarskiptatækni (6. gr.).
     c. Upplýsinga- og fjarskiptatæknikerfi, - samskiptareglur og -búnaður (7. gr.).
     d. Auðkenning (8. gr.).
     e. Verndun og forvarnir (9. gr.).
     f. Greining (10. gr.).
     g. Viðbrögð og endurreisn (11.gr.).
     h. Stefnur og verklag við öryggisafritun, verklag og aðferðir við endurheimt og endurreisn (12. gr.).
     i. Lærdómur og þróun (13. gr.).
     j. Samskipti (14. gr.).
     k. Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni (16. gr.).

1. Inngangur.

Frumvarp þetta til nýrra heildarlaga um stafrænan viðnámsþrótt fjármálamarkaðar var samið í fjármála- og efnahagsráðuneytinu. Tilgangur með framlagningu þess er að innleiða í íslenskan rétt 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 (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 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 (hér eftir DORA-tilskipunin).

Báðar voru DORA-reglugerðin og DORA-tilskipunin samþykktar 14. desember 2022 og komu til framkvæmda í aðildarríkjum Evrópusambandsins 17. janúar 2025. Þær voru teknar upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 frá 20. febrúar 2025, að undangengnu samráði við utanríkismálanefnd Alþingis með vísan til reglna um þinglega meðferð EES-mála.

2. Tilefni og nauðsyn lagasetningar.

2.1. Stafrænn fjármálapakki ESB og stafrænt áfallaþol.

DORA tilheyrir stafrænum fjármálapakka Evrópusambandsins (ESB) sem fyrst var kynntur árið 2020, líkt og reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 frá 31. maí 2023 um markaði fyrir sýndareignir og um breytingu á reglugerðum (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipunum 2013/36/ESB og (ESB) 2019/1937 (MiCA) og reglugerð Evrópuþingsins og ráðsins (ESB) 2022/858 frá 30. maí 2022 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 hér á landi með lögum um innviði markaða fyrir fjármálagerninga sem byggjast á dreifðri færsluskrártækni, nr. 56/2024. Stafræna fjármálapakkanum er ætlað að stuðla að efldri samkeppni og nýsköpun og að umgjörð fjármálamarkaða mæti nútímaþörfum, auk þess sem hugað er að fjárfestavernd, net- og upplýsingaöryggi og fjármálastöðugleika. Ógnir við net- og upplýsingaöryggi eru ein tegund rekstraráhættu.

Í DORA er hugtakið stafrænn rekstrarlegur viðnámsþróttur í forgrunni eða, til einföldunar, stafrænn viðnámsþróttur. Það er skilgreint sem 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 fjármálaþjónustu og gæði hennar, þ.m.t. á 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 upplýsinga- og fjarskiptatækniþjónustu sé viðhöfð í því skyni að stuðla að öflugum stafrænum viðnámsþrótti og lágmarka rof á mikilvægri þjónustu.

Upptaka DORA í EES-samninginn og innleiðing í landsrétt er skilgreind sem aðgerð í sameiginlegri aðgerðaáætlun stjórnvalda í netöryggismálum, á grundvelli Netöryggisstefnu Íslands 2022–2037. Stafrænn fjármálapakki ESB var jafnframt á forgangslista ríkisstjórnarinnar um hagsmunagæslu Íslands gagnvart Evrópusambandinu fyrir árin 2022–2023.

2.2. Gildissvið og meðalhófsregla.

Gildissvið DORA er víðtækt, en reglugerðin miðar að því að efla stafrænt öryggi og rekstrarþol á fjármálamarkaði með skýrum og samræmdum kröfum um áhættustýringu og viðbúnað. Reglugerðin nær yfir breiðan hóp aðila á fjármálamarkaði. Efniskröfur DORA ná jafnframt til fyrirtækja sem veita aðilum á fjármálamarkaði þjónustu á sviði upplýsinga- og fjarskiptatækni, en kröfunum skal framfylgt gagnvart hinum eftirlitsskylda aðila sem kaupir þá þjónustu. Þó er með DORA komið á sértækum eftirlitsramma með allra stærstu alþjóðlegu þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, sem sérstaklega eru tilnefndir sem mikilvægir í samræmi við II. þátt V. kafla DORA. Ef þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í EFTA-ríki innan Evrópska efnahagssvæðisins (EES) verður tilnefndur sem mikilvægur gildir eftirlitsramminn um hann og Eftirlitsstofnun EFTA er þá falið hlutverk aðaleftirlitsaðila gagnvart honum, sem felur í sér beint eftirlit með starfseminni, sbr. nánari umfjöllun í kafla 3.6.

Stafrænar lausnir liggja til grundvallar fjármálastarfsemi nútímans. Markmið DORA er að stuðla að stafrænum viðnámsþrótti á fjármálamarkaði með samræmdum kröfum um áhættustýringu og viðbúnað til eftirlitsskyldra aðila. Þannig skulu sambærilegir áhættuþættir í grunninn meðhöndlaðir eins óháð því hvaða aðili á í hlut í því skyni að samræma eftirlit og stuðla að rekstraröryggi og fjármálastöðugleika, að teknu tilliti til 4. og 16. gr. DORA um meðalhófsreglu og einfaldaðan áhættustýringarramma. Kröfur DORA skulu aðlagaðar að stærð og eðli rekstrar þannig að vægari kröfur eru gerðar til minni fyrirtækja og tilteknir aðilar eru jafnframt undanskildir gildissviði reglugerðarinnar samkvæmt orðanna hljóðan. Að nokkru marki eru sérkröfur jafnframt tilgreindar í DORA um tiltekna aðila á fjármálamarkaði, svo sem veitendur gagnaskýrsluþjónustu og verðbréfamiðstöðvar.

Eftirtaldir aðilar munu skv. 2. gr. DORA falla undir gildissvið fyrirhugaðra laga hér á landi (sameiginlega nefndir *aðilar á fjármálamarkaði*), auk þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu:

- Lánastofnanir (viðskiptabankar, sparisjóðir og lánafyrirtæki), sbr. lög um fjármálafyrirtæki, nr. 161/2002, þó ekki Byggðastofnun og Lánasjóður sveitarfélaga ohf., sbr. 12. gr. frumvarpsins,
- greiðslustofnanir og reikningsupplýsingaþjónustuveitendur, sbr. lög um greiðsluþjónustu, nr. 114/2021,
- 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,
- 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 Náttúruhamfaratrygging Íslands og félög sem eru undanþegin vegna smæðar,
- vátryggingamiðlarar og aðilar sem dreifa vátryggingu sem aukaafurð, sbr. lög um dreifingu vátrygginga, nr. 62/2019, þó með undantekningum,
- starfstengdir eftirlaunasjóðir, 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. reglugerð Evrópuþingsins og ráðsins (ESB) 2020/1503 frá 7. október 2020 um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki og um breytingu á reglugerð (ESB) 2017/1129 og tilskipun (ESB) 2019/1937 sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 30/2024 frá 2. febrúar 2024 og áformað er að innleiða hér á landi síðari hluta árs 2025,
- verðbréfunarskrár, sbr. reglugerð Evrópuþingsins og ráðsins (ESB) 2017/2402 frá 12. desember 2017 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/ESB og reglugerðum (EB) nr. 1060/2009 og (ESB) nr. 648/2012, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 145/2024 frá 12. júní 2024 og áformað er að innleiða hér á landi á fyrri hluta árs 2025,
- þjónustuveitendur sýndareigna, sbr. reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 frá 31. maí 2023 um markaði fyrir sýndareignir og um breytingu á við reglugerðum (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipunum 2013/36/ESB og (ESB) 2019/1937, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 41/2025 frá 20. febrúar 2025 og áformað er að innleiða hér á landi á fyrri hluta árs 2025.

Samkvæmt 3. mgr. 2. gr. DORA eru eftirtaldir aðilar undanþegnir gildissviði fyrirhugaðra laga, sjá og orðskýringar í 3. gr. DORA:

- Rekstraraðilar sérhæfðra sjóða sem ekki falla undir 1. mgr. 6. gr. laga um rekstraraðila sérhæfðra sjóða, nr. 45/2020,

- vátryggingafélög sem eru undanþegin gildissviði vegna stærðar skv. 3. mgr. 3. gr. laga um vátryggingastarfsemi, nr. 100/2016,
- starfstengdir eftirlaunasjóðir samkvæmt lögum um starfstengda lífeyrissjóði, nr. 78/2007, sem starfrækja lífeyriskerfi þar sem sjóðfélagar eru samtals ekki fleiri en 15,
- einstaklingar eða lögaðilar sem njóta undanþágu skv. 1. mgr. 2. gr. laga um markaði fyrir fjármálagerninga, nr. 115/2021,
- vátryggingamiðlarar, endurtryggingamiðlarar og vátryggingamiðlarar í hliðarstarfsemi sem eru örfyrirtæki eða lítil eða meðalstór fyrirtæki í merkingu 60., 63. og 64. tölul. 3. gr. DORA,
- póstgíróstofnanir.

Undanþága vegna póstgíróstofnana á ekki við hér á landi enda er ekki minnst á slíkar stofnanir í lögum um póstþjónustu, nr. 98/2019, og engin slík er starfandi hér á landi. Engir starfstengdir eftirlaunasjóðir eru starfræktir á Íslandi. Áætlað er að ríflega helmingur starfandi rekstraraðila sérhæfðra sjóða hér á landi falli utan gildissviðs fyrirhugaðra laga. Sama eigi við um öll vátryggingamiðlunarfyrirtæki og tvö af átta vátryggingafélögum á skrá Fjármálaeftirlitsins yfir eftirlitsskylda aðila samkvæmt lögum um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, þar á meðal Náttúruhamfaratryggingu Íslands.

Með 12. gr. frumvarpsins er lagt til að tekin verði öll tvímæli af um að Byggðastofnun, Lánasjóður sveitarfélaga ohf. og Náttúruhamfaratrygging Íslands skuli undanþegin ákvæðum fyrirhugaðra laga, sbr. skýringar við 12. gr.

Með frumvarpinu er lagt til að kveðið verði á um það í lögum um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, að helstu ákvæði DORA nái einnig til lífeyrissjóða, sbr. 12. tölul. 14. gr. frumvarpsins. Nauðsynlegt er að endurmeta kröfur gildandi laga í þessum efnum til lífeyrissjóða, eins og annarra aðila á fjármálamarkaði. Íslenskir lífeyrissjóðir falla ekki undir evrópskt regluverk um starfstengda lífeyrissjóði (IORP) og þar með ekki undir gildissvið DORA eins og það er skilgreint í reglugerðinni. Með því að sambærilegar kröfur gildi um helstu aðila á fjármálamarkaði, þ.m.t. lífeyrissjóði, þannig að sambærilegir áhættuþættir séu meðhöndlaðir eins er stuðlað að aukinni tiltrú á fjármálakerfið og stöðugleika þess. Það er í samræmi við markmið DORA sem m.a. á að stuðla að því að draga úr flækjustigi í framkvæmd, auka samræmi í eftirliti og réttarvissu. Vísast til umfjöllunar í skýringum við 12. tölul. 14. gr.

Um þá aðila á íslenskum fjármálamarkaði sem ekki falla undir DORA fer, eftir því sem við á, samkvæmt gildandi lögum.

2.3. Mat á nauðsyn og mögulegar leiðir við lagasetningu.

Dæmigerð dagleg starfsemi aðila á fjármálamarkaði reiðir sig á virka upplýsinga- og fjarskiptatækniþjónustu. 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. Áhætta sem varðar net- og upplýsingaöryggi var á meðal helstu stefnumarkandi áherslna og forgangsmála Seðlabanka Íslands í fjármálaeftirliti 2024.

Um er að ræða frumvarp til nýrra heildarlaga um stafrænan viðnámsþrótt fjármálamarkaðar. Til þessa hafa kröfur um stafrænan viðnámsþrótt og öryggi í upplýsinga- og fjarskiptatækni á sviði fjármálaþjónustu hvorki verið ítarlega útfærðar né samræmdar, þvert á ólíka starfsemi, með þeim hætti sem DORA gerir ráð fyrir. DORA felur í sér réttarbót að því er varðar skýrleika um kröfur er varða áhættustýringu og eftirlitskerfi vegna nýtingar net- og upplýsingakerfa í fjármálaþjónustu, fyrir bæði markaðsaðila og eftirlitsaðila. Með lögfestingu

þeirra og tilheyrandi viðurlagaheimildum til álagningar stjórnvaldssekta, er eftirfylgni jafnframt gert hærra undir höfði en til þessa. Frá sjónarhóli neytenda og fjárfesta er einföldun í formi miðlægs regluverks, með tilheyrandi gagnsæi á samræmdar kröfur, jafnframt réttarbót. Ýmis ákvæði DORA verða nánar útfærð í afleiddum gerðum, sem að mestu leyti verða innleiddar hér á landi í reglum Seðlabanka Íslands.

Því ber að halda til haga að í gildandi lögum er að finna ýmis ákvæði sem gera kröfur til aðila á fjármálamarkaði er varða stýringu áhættu vegna upplýsinga- og fjarskiptatækni, en ný heildarlög munu að mestu leysa af hólmi og samræma löggjöfina á öllum fjármálamarkaðinum.

Í 78. gr. g laga um fjármálafyrirtæki, nr. 161/2002, er kveðið á um að fjármálafyrirtæki skuli hafa stefnu og ferla til að meta og stýra rekstraráhættu, þ.m.t. vegna líkana, útvistunar og fátíðra atburða sem geta haft alvarlegar afleiðingar. Fjármálafyrirtæki skal í þessum tilgangi tilgreina hvað telst til rekstraráhættu, hafa viðbragðsáætlun og áætlun um samfelldan rekstur til að tryggja áframhaldandi starfsemi og takmörkun á tjóni ef til alvarlegrar röskunar á starfsemi fyrirtækisins kemur. Um eftirlit með áhættustýringu fjármálafyrirtækja í þessum efnum fer skv. 79. gr. laga nr. 161/2002, sbr. og 80.–82. gr. um könnunar- og matsferli, álagspróf o.fl.

Fjármálafyrirtæki, rafeyrisfyrirtæki, greiðslustofnanir og aðrir þeir sem teljast greiðsluþjónustuveitendur í skilningi laga um greiðsluþjónustu, nr. 114/2021, skulu uppfylla kröfur þeirra um stýringu áhættu, sbr. og lög um útgáfu og meðferð rafeyris, þar á meðal rekstraráhættu. Öllum greiðsluþjónustuveitendum er skylt að tilkynninga til Fjármálaeftirlitsins um alvarleg rekstrar- eða öryggisfrávik skv. 100. gr. laganna, án ástæðulausrar tafar.

Vikið er að rekstraráhættu í ýmsum öðrum gildandi lögum á sviði fjármálaþjónustu sem flest 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, sbr. 14. gr. frumvarpsins. Stýringu rekstraráhættu er til dæmis gert hátt undir höfði í lögum um vátryggingastarfsemi, nr. 100/2016, og hið sama er uppi á teningnum í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 909/2014 frá 23. júlí 2014 um bætt verðbréfauppgjör í Evrópusambandinu og um verðbréfamiðstöðvar o.fl., sbr. lög um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020.

Um alla eftirlitsskylda aðila gilda leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila og leiðbeinandi tilmæli nr. 6/2014 um útvistun hjá eftirlitsskyldum aðilum, sem samkvæmt orðanna hljóðan beinast að öllum eftirlitsskyldum aðilum skv. 2. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998. Með upptöku viðmiðunarreglna Evrópsku bankaeftirlitsstofnunarinnar (EBA) um stjórnun upplýsinga- og fjarskiptatækniáhættu og um útvistun hafa fjármálafyrirtæki þó að mestu verið felld undan gildissviði þessara tilmæla. Áhersla er lögð á ábyrgð stjórnar eftirlitsskylds aðila á að leiðbeinandi tilmælum sé fylgt í framkvæmd, kveðið á um að til staðar séu stefnur og verkferlar um áhættugreiningu og áhættumat, áætlanir um viðbúnað og samfelldan rekstur, kröfur eru gerðar um breytingastjórnun, vöktun frávika og tilkynningarskyldu til Fjármálaeftirlitsins um öll frávik svo fljótt sem verða má og eigi síðar en 4 klukkustundum eftir að atvik uppgötvast, krafa gerð um aðhald og samninga við útvistunaraðila o.fl. Í leiðbeinandi tilmælum nr. 1/2019 segir að komist Fjármálaeftirlitið að þeirri niðurstöðu að um brot á lögum eða reglum sé að ræða geri það kröfu um úrbætur, sbr. 1. mgr. 10. gr. laga nr. 87/1998, og leggur mat á hvort tilefni sé til að beita öðrum úrræðum til að bregðast við broti.

Seðlabankinn tekur auk þess upp, birtir og fylgir eftir viðmiðunarreglum evrópsku fjármálaeftirlitsstofnananna sem varða stjórnun áhættu vegna upplýsinga- og fjarskiptatækni, eftir

því sem við á. Þannig beindi Fjármálaeftirlitið til dæmis viðmiðunarreglum EBA (EBA/GL/2019/021) um fyrirkomulag útvistunar til fjármálafyrirtækja, greiðslustofnana og rafeyrisfyrirtækja, með dreifibréfi nr. 67/2019 í árslok 2019. Þær komu í stað leiðbeinandi tilmæla Fjármálaeftirlitsins nr. 6/2014 um útvistun, að því er varðar þá eftirlitsskyldu aðila sem viðmiðunarreglurnar taka til. Með dreifibréfi nr. 26/2018 beindi Fjármálaeftirlitið því til fjármálafyrirtækja að kynna sér og taka mið af tilmælum EBA (EBA/REC/2017/03) varðandi útvistun til þjónustuveitenda vegna skýjalausna. Þá beindi Fjármálaeftirlitið viðmiðunarreglum EBA varðandi stjórnun áhættu vegna upplýsinga- og samskiptatækni og öryggisáhættu (EBA/GL/2019/04) til fjármálafyrirtækja með dreifibréfi nr. 21/2021 sem koma að mestu í stað leiðbeinandi tilmæla 1/2019 að því er varðar þá eftirlitsskyldu aðila sem viðmiðunarreglurnar taka til.

Fyrirhuguð lög um stafrænan viðnámsþrótt fjármálamarkaðar verða sérlög gagnvart almennri netöryggislöggjöf, nú einkum lög um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, er fólu í sér innleiðingu á tilskipun Evrópuþingsins og ráðsins (ESB) 2016/1148 frá 6. júlí 2016 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu (NIS1). Almenn netöryggislöggjöf mun í fyrirsjáanlegri framtíð byggjast á tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2555 frá 14. desember 2022 um ráðstafanir til að ná háu sameiginlegu stigi á sviði netöryggis í öllu Sambandinu, um breytingu á reglugerð (ESB) nr. 910/2014 og tilskipun (ESB) 2018/1972 og um niðurfellingu á tilskipun (ESB) 2016/1148 (NIS2), sem var samþykkt samhliða DORA. Að því marki sem DORA geymir ríkari kröfur til aðila á fjármálamarkaði ganga fyrirhuguð lög um stafrænan viðnámsþrótt fjármálamarkaðar framar ákvæðum laga nr. 78/2019, sbr. 16. lið inngangsorða og 2. mgr. 1. gr. DORA. Vísast og til 4. gr. NIS2 í þessu samhengi.

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 valdið útbreiðslu staðbundinna veikleika og 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 frekari samræmingu bestu starfsvenja, reglusetningar og eftirlits víða á alþjóðavettvangi, í því skyni að stuðla að stafrænum viðnámsþrótti á sviði fjármálamarkaða. Innleiðing DORA, með tilheyrandi eftirfylgni og þróun frekari samræmdra mælikvarða og tölfræði mun einnig stuðla að fjármálastöðugleika hér á landi í almannaþágu, sporna við uppsöfnun kerfisáhættu og stuðla að samhæfðum viðbrögðum við sérstakar aðstæður.

Íslandi ber þjóðréttarleg skylda til að taka EES-reglugerðir sem slíkar upp í landsrétt, sbr. a-lið 7. gr. EES-samningsins, en hefur val um form og aðferð við innleiðingu EES-tilskipana, sbr. b-lið sömu greinar. DORA-reglugerðin verður því innleidd í landsrétt með tilvísunaraðferð, en ákvæði DORA-tilskipunarinnar með umritun, þ.e. breytingum á ýmsum lögum.

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 byggist á notkun net- og upplýsingakerfa í skilningi

2. tölul. 3. gr. DORA og upplýsinga- og fjarskiptatækniþjónustu í skilningi 21. tölul. sama ákvæðis.

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 reglulega 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 reglubundið 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.

Sérstök áhersla er lögð á það lykilhlutverk og endanlega ábyrgð stjórnar og/eða framkvæmdastjórnar aðila á fjármálamarkaði að tryggja framfylgni við kröfur DORA. Stýringu upplýsinga- og fjarskiptatækniáhættu er þannig gert hærra undir höfði en áður og er ekki verkefni sem einvörðungu verður lagt á herðar og ábyrgð öryggisstjóra. Þetta krefst þess einnig að stjórnarmenn og framkvæmdastjóri hafi þekkingu á upplýsinga- og fjarskiptatækniáhættu og að málefnin komi reglulega við sögu á stjórnarfundum. Þannig er upplýsinga- og fjarskiptatækniáhættu gert jafn hátt undir höfði og öðrum áhættuþáttum.

Með DORA er lögð á alla helstu aðila á fjármálamarkaði sú skylda að fræða starfslið sitt 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, þ.e. þjónustuveitenda.

Þá er með DORA kveðið á um samræmda tilkynningarskyldu gagnvart lögbæru yfirvaldi, hér Fjármálaeftirlitinu, 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. DORA og 5. tölul. 7. gr. DORA-tilskipunarinnar, sem fellir úr gildi skýrslugjöf samkvæmt lögum um greiðsluþjónustu (PSD II) 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 tilkynningarskyldir beint gagnvart netöryggissveit Fjarskiptastofu (CERT-ÍS) 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 miðla upplýsingum tímanlega áfram um alvarleg atvik og verulegar netógnir frá aðilum á fjármálamarkaði til CERT-ÍS. Sjá jafnframt umfjöllun um 3. 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 viðnámsþrótti eða aukinna ógnamiðaðra innbrotsprófana, sem stuðla eiga að bættu áfallaþoli innviða aðila á fjármála-

markaði. 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 sem veitir upplýsinga- og fjarskiptatækniþjónustu, sem til einföldunar má vísa til sem ytri tækniþjónustuveitanda. 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. Áætlanir skulu vera til staðar er miða að því að viðhalda samfelldum rekstri ef kemur til flutnings eða uppsagnar þjónustu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

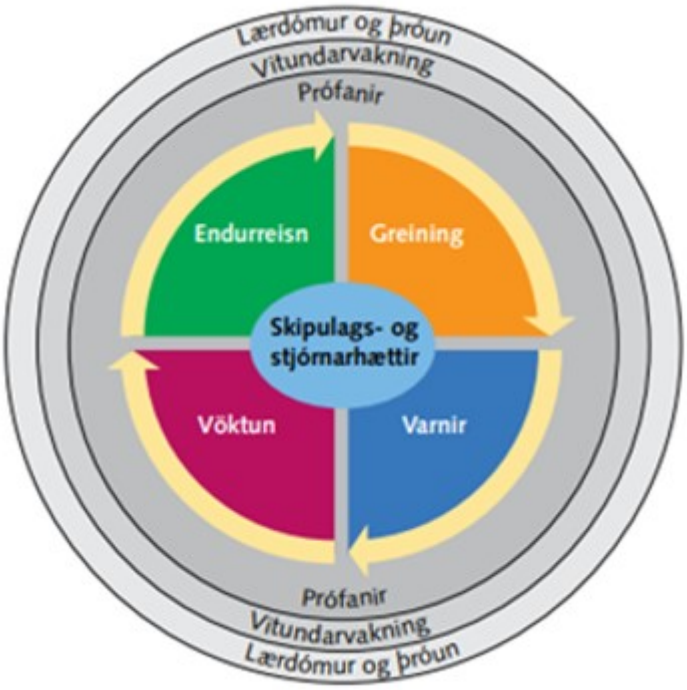
Aðilar á fjármálamarkaði skulu uppfylla framangreindar kröfur í samræmi við meðalhófsreglu, að teknu tilliti til stærðar og áhættusniðs, eðlis, umfangs og flækjustigs starfsemi og kerfislegs mikilvægis.

Með DORA er komið á sameiginlegri umgjörð eftirlits með allra stærstu alþjóðlegu tækniþjónustuveitendum sem sérstaklega verða útnefndir sem mikilvægir á sameiginlegum innri markaði fjármálaþjónustu, þ.e. 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, 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 eru staðgönguhæfni og möguleg kerfislæg áhrif á stöðugleika, samfellu eða gæði fjármálaþjónustu, ef hlutaðeigandi stæði frammi fyrir umfangsmiklu þjónusturofi, að teknu tilliti til fjölda aðila á fjármálamarkaði sem reiðir sig á þjónustu hans og annarra undirliggjandi hagsmuna. Slíkum þriðja aðila 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 gerðar úrbótatillagna, að viðlögðum viðurlögum sem skal vera unnt að framfylgja í heimaríki þjónustuveitandans. DORA gerir ráð fyrir að upplýsa megi opinberlega um bresti á samstarfsvilja eða ef ekki er farið að tilmælum aðaleftirlitsaðila, nema slík upplýsingagjöf teljist ósanngjörn eða geti skaðað aðila á fjármálamarkaði.

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

Með fyrirhugaðri lagasetningu verður tekið mikilvægt skref í að samræma lögbundnar kröfur 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 myndrænt með hliðsjón af lykilþáttum áhættustýringar með tilliti til net- og upplýsingaöryggis (Seðlabanki Íslands, Fjármálainnviðir 2018, bls. 9). Myndin sýnir að áhersla er lögð á skipulags- og stjórnarhætti aðila sem grunnstoð fyrir allar aðgerðir og til að styðja við alla þætti áhættustýringar. Sífellt þarf að viðhafa greiningu á mögulegum áhættum og veikleikum í kerfum og ferlum, innleiðingu varna gegn þeim ógnum sem greindar eru og vöktun til stöðugrar eftir-

fylgni með rekstrarumgjörðinni í því skyni að greina og bregðast við öryggisógnum eða atvikum. Loks kemur að endurreisn sem snýst um viðbúnað og aðgerðir til að endurheimta starfsemi eftir áföll. Nauðsynlegt er að prófa kerfi og ferla reglulega til að tryggja virkni og áreiðanleika. Mikilvægt er að tryggja vitund starfsmanna um öryggismál og ógnir og loks að reynsla og niðurstöður í atvikagreiningu séu nýttar til að bæta ferla og þróa lausnir. Hringlaga skipulag myndarinnar sýnir hvernig áhættustýring er stöðugt, endurtekið ferli og leggur áherslu á heildræna nálgun til að tryggja áreiðanleika og stafrænt áfallaþol.



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.

Samkvæmt DORA skal stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði skilgreina, samþykkja, hafa umsjón með og bera ábyrgð á framkvæmd allra ráðstafana sem tengjast umgjörð áhættustýringar vegna upplýsinga- og fjarskiptatækniáhættu. Um ábyrgð stjórnar og/eða framkvæmdastjóra samkvæmt einstökum ákvæðum DORA fer samkvæmt landslögum, þ.e. lögum um hlutafélög, nr. 2/1995, hér á landi og eftir atvikum öðrum lögum, og veltur á eðli verkefna sem um ræðir. Hugtakið stjórn og/eða framkvæmdastjóri er skilgreint í 30. tölul. 3. gr. DORA.

Sérstaklega er vikið að kröfum til stjórnar og/eða framkvæmdastjórnar í 2. og 4. mgr. 5. gr. (stjórnunarhættir og skipulag), 2. mgr. 28. gr. (almennar meginreglur um trausta stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila) og í 5. mgr. 50. gr. (stjórnsýsluviðurlög og ráðstafanir til úrbóta) DORA.

Hér á landi er það í samræmi við löggjöf á sviði félagaréttar, t.d. 68. gr. laga um hlutafélög, nr. 2/1995, að félagsstjórn fari með málefni félagsins og hafi eftirlit með því að skipulag og starfsemi þess séu í réttu og góðu horfi. Í því felst að stjórn ber endanlega ábyrgð á að skilgreina, samþykkja og hafa yfirumsjón með áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Framkvæmdastjórn annast daglegan rekstur félagsins og skal í þeim efnum fara eftir stefnu og fyrirmælum stjórnar, en hinn daglegi rekstur tekur ekki til ráðstafana sem eru óvenjulegar eða mikils háttar nema samkvæmt sérstakri heimild stjórnar.

Það er sameiginlegt hlutverk stjórnar og framkvæmdastjóra að koma á stefnu og ferlum sem miða að því að tryggja að strangar kröfur séu gerðar um að gögn séu tiltæk, ósvikin, áreiðanleg og að viðeigandi trúnaðar sé gætt um þau. Það að skilgreina hlutverk og ábyrgð, skipulag og stjórnarhætti kemur hins vegar í hlut stjórnar, enda ber hún ábyrgð á að nægilegt eftirlit sé haft með bókhaldi og meðferð fjármuna félagsins. Á meðal lykilþátta í því samhengi er ákvörðun áhættuþolmarka upplýsinga- og fjarskiptatækniáhættu, stefna um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir.

Að því er varðar tilföng og færni er það í samræmi við 68. gr. laga um hlutafélög, nr. 2/1995, að stjórn beri að sjá til þess að skipulag og starfsemi félagsins séu í réttu og góðu horfi. Því ber henni að sjá til þess að tilföng séu næg í starfseminni svo unnt sé að uppfylla þarfir hlutaðeigandi aðila á fjármálamarkaði fyrir stafrænan viðnámsþrótt, ásamt því að tryggja öryggisvitund í starfseminni, þjálfun og færni fyrir allt starfsfólk.

Sérstaklega er vikið að ábyrgð stjórnar og/eða framkvæmdastjórnar 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. Enn fremur skal stjórn upplýst um a.m.k. 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. Örfyrirtæki eru þó undanskilin.

Loks ber að hafa í huga að DORA kveður á um að meðlimum stjórnar og framkvæmdastjórnar 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 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 ber aðilinn ávallt sjálfur ábyrgð á hlítni við kröfur laga um stýringu upplýsinga- og fjarskiptatækniáhættu.

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

Nánar tilgreindar kröfur eru gerðar til upplýsinga- og fjarskiptatæknikerfa, tilheyrandi 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, sé 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 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 frávik 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, sem m.a. feli í sér að leggja frummat á áhrif. 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 Fjármálaeftirlitinu, 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 m.a. gera ráð fyrir reglubundinni prófun og endurmati. Sú krafa er gerð til aðila á fjármálamarkaði, þó ekki örfyrirtækja, að krísustjórnunarteymi 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 atviki stendur skulu skráðar.

Sérstaklega er kveðið á um að verðbréfamiðstöðvar skuli láta lögbærum yfirvöldum, hér Fjármálaeftirlitinu, 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 því 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 viðnámsþrótt. Atvik og raskanir á kjarnastarfsemi skulu greind, ekki síst orsakir, og kennsl borin á nauðsynlegar úrbætur. Atvikagreining skal m.a. 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 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, stefnum 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 veita ráðleggingar.

Áætlanir um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun sem tengist stafrænum 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 hátt um 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. Tilkynningarskylda 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), auk leiðbeininga Fjármálaeftirlitsins um tilkynningu frávika, en sú grundvallarbreyting verður nú á að um beina lagaskyldu verður að ræða og varða brot á henni viðurlögum.

Löggjafinn hefur þegar tekið af skarið um skyldu rekstraraðila nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða til að tilkynna netöryggissveit Fjarskiptastofu (CERT-ÍS) um alvarleg atvik eða áhættu sem tengist net- og upplýsingakerfum, þ.e. í lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, en með þeim var NIS1-tilskipunin innleidd hér á landi. Til þeirra teljast nú kerfislega mikilvægu bankarnir þrír og kauphöll, sbr. auglýsingu um skrá yfir rekstraraðila nauðsynlegrar þjónustu, nr. 1331/2023. NIS1 var endurnýjuð samhliða samþykkt DORA og bíður NIS2 nú upptöku í EES-samninginn og innleiðingar í landsrétt. Eins og vikið er að í umfjöllun um 2. gr. og kafla 2.3 verður um sérlög að ræða um aðila á fjármálamarkaði. Kröfur DORA ganga með öðrum orðum framar almennum netöryggisgerðum ESB (NIS1/NIS2) að því er varðar aðila á fjármálamarkaði 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. 7. tölul. 14. gr. frumvarpsins, að atvikatilkynningum frá aðilum á fjármálamarkaði sem jafnframt falla undir gildissvið þeirra laga skuli framvegis beint til Fjármálaeftirlitsins. DORA kveður enda á um skyldu lögbærs yfirvalds til tímanlegrar áframmiðlunar upplýsinga um atvik eða verulega netógn til innlendra stjórnvalda, þar á meðal CERT-ÍS, og evrópsku fjármálaeftirlitsstofnananna. Annað þykir stangast á við kröfur nútímans um einföldun regluverks en með breytingunni má ljóst vera að þörf er á skilvirkum og áreiðanlegum boðleiðum gagnvart CERT-ÍS. 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 CERT-ÍS, með vísan til reglugerðar um netöryggissveit Fjarskiptastofu (CERT-ÍS), nr. 480/2021. Ekki þykir tilefni til að nýta valkvæðar heimildir 1. og 2. mgr. 19. gr. DORA um að tilkynningum skuli einnig beint til netöryggissveitar, sbr. kafla 3.8.

Megininntak III. kafla DORA 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 orsakir og afleiðingar, draga lærdóm og gera nauðsynlegar úrbætur svo unnt sé að koma í veg fyrir að sambærileg atvik endurtaki sig. Krafa er m.a. 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. Þar ber að líta til þátta á borð við fjölda og/eða mikilvægi viðskiptavina eða fjárhagslegra mótaðila sem verða fyrir áhrifum. Einnig skal meta fjárhæð eða fjölda viðskipta sem tengjast atvikinu, tímalengd þess, landfræðilega dreifingu, umfang gagnataps, eðli eða mikilvægi þjónustu sem atvikið hefur áhrif á og efnahagsleg áhrif þess.

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

DORA kveður á um tilkynningarskyldu af hálfu allra aðila á fjármálamarkaði sem undir gildissvið hennar heyra um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Tilkynningu skal beint til viðeigandi lögbærs yfirvalds á stöðluðu formi, sem hér á landi er Fjármálaeftirlitið. 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 tilkynningarskyldur aðili á fjármálamarkaði óskoraða ábyrgð á að henni sé sinnt í samræmi við ákvæði DORA.

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 fjármálaeftirlitsstofnununum (EBA, ESMA og EIOPA), Seðlabanka Evrópu ef í hlut eiga lánastofnanir, greiðslustofnanir eða rafeyrisfyrirtæki, Fjarskiptastofu með vísan til 2. mgr. 13. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, netöryggissveit Fjarskiptastofu (CERT-ÍS), skilavaldi Seðlabanka Íslands, embætti ríkislögreglustjóra og Persónuvernd. Um áframmiðlun af hálfu evrópska eftirlitskerfisins á fjármálamarkaði fer skv. 7. mgr.

Í síðustu undirgreinum 1. og 2. mgr. 19. gr. DORA eru valkvæðar heimildir aðildarríkja til að kveða á um miðlun atvikatilkynninga til lögbærra yfirvalda eða netöryggissveita sem eru tilnefndar eða komið á fót í samræmi við NIS2-tilskipunina, hér Fjarskiptastofu eða CERT-ÍS. Með frumvarpinu er sú heimild ekki nýtt, heldur lagt til að öllum tilkynningum um atvik eða ógnir tengdar net- og upplýsingakerfum aðila á fjármálamarkaði verði beint til Fjármálaeftirlitsins í samræmi við sjónarmið um einföldun regluverks. DORA kveður enda á um skyldu eftirlitsaðilans til tímanlegrar áframmiðlunar upplýsinga um atvik eða verulega netógn til innlendra stjórnvalda, þar á meðal til framangreindra aðila. Þannig segir í 52. tölul. inngangsorða DORA að fjármálaeftirlitsaðilar ættu síðan að miðla upplýsingum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni til opinberra aðila sem ekki tengjast fjármálageiranum, svo sem lögbærra yfirvalda samkvæmt NIS2-tilskipuninni. Í þessu felst skylda Fjármálaeftirlitsins til að vísa öllum atvikatilkynningum áfram til Fjarskiptastofu eða CERT-ÍS án tafar og

sérstaks mats á alvarleika þeirra til að fyrirbyggja og draga úr áhættu, ógnum og atvikum í íslensku netumdæmi.

Með DORA er miðlæg sýn tryggð á alvarleg atvik, netógnir og veikleika. Stofnanir Evrópusambandsins, í samráði við Netöryggisstofnun ESB (ENISA) og í 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 var 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 samræmi eftirlits. Skýrsla evrópsku eftirlitsstofnananna átti að liggja fyrir í janúar 2025 og var afhent Evrópuþinginu, Ráðinu og framkvæmdastjórn Evrópusambandsins 17. 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 skv. 23. gr. gilda um greiðslutengd rekstrar- eða öryggisatvik og um alvarleg greiðslutengd rekstrar- eða öryggisatvik ef þau varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki. Bæði hugtök eru skilgreind í 3. gr. DORA (9. og 11. tölul.). Með þessu ákvæði og breytingu á 96. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2015/2366 frá 25. nóvember 2015 um greiðsluþjónustu á innri markaðnum, um breytingu á tilskipunum 2002/65/EB, 2009/110/EB og 2013/36/ESB og á reglugerð (ESB) nr. 1093/2010 og niðurfellingu á tilskipun 2007/64/EB (PSD II-tilskipunarinnar), sem innleidd var hér á landi með 100. gr. laga um greiðsluþjónustu, nr. 114/2021, með 5. tölul. 7. gr. DORA-tilskipunarinnar er krafa um skýrslugjöf samkvæmt PSD II felld úr gildi gagnvart þeim greiðsluþjónustuveitendum sem falla undir gildissvið DORA. Markmiðið er einföldun regluverks og að draga úr hugsanlegri tvöfaldri kvöð um tilkynningarskyldu 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 fjármálamarkaðinn. 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-ÍS), sbr. reglugerð nr. 480/2021, sem notið getur forgangsaðstoðar CERT-ÍS ef við á skv. 3. mgr. 15. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. 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 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 viðnámsþrótti. Allir aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu setja sér prófunaráætlun um stafrænan 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 gloppugreiningu, 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.

Seðlabankinn sem lögbært yfirvald ákveður hvaða aðilar á fjármálamarkaði, aðrir en þeir sem falla undir einfaldaðan áhættustýringarramma skv. 16. gr. og örfyrirtæki, skuli skv. 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 fjarskiptatæknibjónustu 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 skulu 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 hverja prófun.

Gert er ráð fyrir að Seðlabanki Íslands beri ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun samkvæmt DORA hér á landi, sbr. 1. mgr. 3. gr. frumvarpsins. Um nánari viðmið og kröfur fer samkvæmt afleiddum gerðum (tæknistöðlum). Horft er til TIBER-EU-umgjarðar Seðlabanka Evrópu sem fyrirmyndar. Helstu áherslur í TIBER-EU eru að efla viðnámsþrótt fjármálamarkaðar gegn netógnum, staðla og samræma netárásarpróf innan Evrópusambandsins og að veita stuðning fyrir prófanir vegna stofnana sem starfa í fleiri en einu landi.

Seðlabanki Íslands hefur þegar komið á fót umgjörð fyrir netárásarprófanir fyrir stofnanir og fyrirtæki sem eru mikilvæg fyrir íslenskt fjármálakerfi, TIBER-IS, sem byggist á TIBER-EU.

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

Ákvæði I. þáttar V. kafla DORA (28.–30. gr.) fjalla um stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, t.d. aðila sem sjá um afritunartöku og varðveislu gagna, nánar tiltekið helstu meginreglur um trausta stýringu slíkrar áhættu af hálfu aðila á fjármálamarkaði vegna þriðju aðila, en II. þáttur snýr að sameiginlegum eftirlitsramma gagnvart mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, sbr. kafla 3.6 í greinargerð þessari. Meginreglur þessar eru til viðbótar við sérlög sem gilda um útvistun, sbr. 29. lið 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 þriðju 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 enn fremur 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. Þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu í skilningi DORA kunna er fram líða stundir að falla undir gildissvið NIS2-tilskipunarinnar, sem unnið er að upptöku á í EES-samninginn.

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 aðilum 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 mikilvægustu tækniþjónustuveitenda.

Ákvæði II. þáttar V. kafla DORA (31.–44. gr.) kveða á um sameiginlegan eftirlitsramma gagnvart mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og eru sérstaklega útnefndir sem slíkir á grundvelli reglugerðarinnar. Evrópsku fjármálaeftirlitsstofnanirnar og Eftirlitsstofnun EFTA, í tilviki EFTA-ríkjanna innan EES, útnefna aðila sem falla undir eftirlitsrammann á grundvelli skilgreindra viðmiða, sbr. 31. gr. DORA. Vísast og til framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2024/1502 frá 22. febrúar 2024 um viðbætur við DORA sem tilgreinir nánari viðmið til grundvallar útnefningu mikilvægra þriðju aðila sem veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu.

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 þriðju aðila sem veita fjármálastofnunum upplýsinga- og fjarskiptaþjónustu þvert á landamæri og er gert ráð fyrir virku eftirliti með framfylgd þeirra. Ávinningur af upptöku og innleiðingu DORA er m.a. fólginn í þessu nýja miðlæga aðhaldi, sem Fjármálaeftirlitið líkt og aðrar fjármálaeftirlitsstofnanir á EES mun byggja á og geta vísað til.

Fyrir hvern mikilvægan þriðja aðila í aðildarríki ESB skulu evrópsku fjármálaeftirlitsstofnanirnar útnefna einhverja úr sínum hópi sem aðaleftirlitsaðila, þ.e. ýmist Evrópsku bankaeftirlitsstofnunina (EBA), Evrópsku verðbréfamarkaðseftirlitsstofnunina (ESMA) eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunina (EIOPA). Ef til útnefningar mikilvægs þriðja aðila kemur sem veitir upplýsinga- og fjarskiptatækniþjónustu frá Íslandi eða öðru EFTA-ríki innan EES verður Eftirlitsstofnun EFTA falið hlutverk aðaleftirlitsaðila, í samræmi við tveggja stoða kerfi EES-samningsins. Ekki er þó talið líklegt að á þetta reyni í næstu framtíð. Hið sama ætti við um þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu frá þriðja ríki með dótturfélag í EFTA-ríki innan EES.

Viðmiðin sem liggja eiga til grundvallar útnefningu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu varða m.a. kerfislegt mikilvægi og fjölda aðila á fjármálamarkaði sem reiða sig á hlutaðeigandi í starfsemi sinni. Ekki kemur til útnefningar ef aðili veitir eingöngu upplýsinga- og fjarskiptatækniþjónustu í einu aðildarríki til aðila á fjármálamarkaði sem starfa eingöngu í því ríki. Fjármálastofnun sem veitir öðrum aðilum á fjármálamarkaði slíka þjónustu er einnig undanþegin útnefningu og sama máli gegnir ef aðeins er um veitingu þjónustu að ræða innan sömu samstæðu. Þá eru þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu og þegar eru háðir yfirsýn seðlabanka á grundvelli hlutverks þeirra að stuðla að fjármálastöðugleika, virku og öruggu fjármálakerfi, þ.m.t. greiðslumiðlun í landinu og við útlönd, undanþegnir útnefningu undir sameiginlega eftirlitsrammann. Síðastnefnd undanþága nær til dæmis til aðila sem veita upplýsinga- og fjarskiptatækniþjónustu vegna rekstrar millibankakerfis Seðlabanka Íslands.

3.7. Upplýsingamiðlun.

Í 45. gr. DORA er fjallað um fyrirkomulag upplýsingaskipta um netógnir. Aðilum á fjármálamarkaði er heimilt að skiptast á upplýsingum og greiningum um netógnir, svo sem vísum sem geta gefið til kynna ógn eða hættu, úrræðum, aðferðum, verklagi og viðvörunum, að uppfylltum nánar tilgreindum skilyrðum. Í fyrsta lagi miði slík upplýsingaskipti og miðlun vitneskju að því að efla stafrænan viðnámsþrótt aðila á fjármálamarkaði, einkum með vitundarvakningu um netógnir, með því að takmarka eða hindra að netógnir geti breiðst út, og 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, og þegar þeirri aðild lýkur.

Seðlabankinn heldur úti samstarfsvettvangi um rekstraröryggi fjármálainnviða (SURF) en aðkomu að honum eiga Seðlabankinn, Reiknistofa bankanna, fjármála- og efnahagsráðuneytið, CERT-ÍS, Samtök fyrirtækja í fjármálaþjónustu, viðskiptabankar, Kauphöllin og Nasdaq verðbréfamiðstöð. Vettvanginum er ætlað 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 m.a. um málefni sem varða trúnaðarskyldu og samkeppni.

3.8. Svigrúm við innleiðingu.

Með frumvarpinu er lagt til að DORA, með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 um upptöku hennar í EES-samninginn og bókun 1 um altæka aðlögun við samninginn, skuli hafa lagagildi hér á landi. DORA verði þannig, í samræmi við a-lið 1. mgr. 7. gr. EES-samningsins, tekin í heild upp í landsrétt. DORA gerir ríkar kröfur til helstu aðila á fjármálamarkaði um áhættustýringu, viðbúnað og tilkynningarskyldu um atvik. Ekki er svigrúm til að víkja frá efnisákvæðum reglugerðarinnar.

Valkvæðar heimildir er að finna í síðustu undirgreinum 1. og 2. mgr. 19. gr. DORA. Þannig er aðildarríkjum heimilt að kveða einnig á um miðlun atvikatilkynninga til lögbærra yfirvalda eða netöryggissveita sem eru tilnefndar eða komið á fót í samræmi við netöryggistilskipanir ESB (hér Fjarskiptastofu eða CERT-ÍS, þ.e. samhliða miðlun tilkynninga til Fjármálaeftirlitsins hér á landi). Með frumvarpinu er ekki lagt til að sú heimild verði nýtt, heldur gengið út frá að öllum tilkynningum um atvik eða ógnir tengdar net- og upplýsingakerfum aðila á fjármálamarkaði verði beint til Fjármálaeftirlitsins, enda ber því að miðla slíkum upplýsingum áfram til innlendra stjórnvalda svo fyrirbyggja megi og draga úr áhættu, ógnum og atvikum í íslensku netumdæmi. Tillagan er í samræmi við sjónarmið um einföldun regluverks og væntingar um skilvirka samvinnu og útfærslu boðleiða í þessum efnum milli þeirra stofnana sem í hlut eiga. Vísast til nánari umfjöllunar í skýringum við 3. mgr. 2. gr. frumvarpsins og kafla 3.3 í greinargerð þessari.

DORA kveður ekki á um fjárhæðarviðmið stjórnvaldssekta, sem stundum á við í Evrópugerðum. Því er um landsbundna útfærslu ákvæða um stjórnsýsluviðurlög að ræða með frumvarpinu. Lagt er til að hámarksfjárhæðarviðmið stjórnvaldssekta vegna brota gegn ákvæðum DORA verði skilgreind í samræmi við nærtækar fyrirmyndir á málefnasviðinu, þ.e. 65 millj. kr. í tilviki einstaklinga og 800 millj. kr. í tilviki lögaðila, sbr. 5. gr. frumvarpsins.

Með frumvarpinu er lagt til að Byggðastofnun, Lánasjóður sveitarfélaga ohf. og Náttúruhamfaratrygging Íslands verði skýrt undanþegin gildissviði fyrirhugaðra laga. Í tilviki Byggðastofnunar og Lánasjóðs sveitarfélaga ohf. er sú tillaga í samræmi við aðlögun í ákvörðun sameiginlegu EES-nefndarinnar nr. 79/2019 um upptöku CRD IV í EES-samninginn, sjá og 4. mgr. 2. gr. DORA, og í tilviki Náttúruhamfaratryggingar Íslands í samræmi við aðlögun í ákvörðun sameiginlegu EES-nefndarinnar nr. 78/2011 um upptöku Gjaldþolsáætlunar II (Solvency II) í EES-samninginn. Vísast til 12. gr. frumvarpsins og umfjöllunar um hana, auk kafla 2.2 í greinargerð þessari.

Með frumvarpinu er lagt til að kveðið verði á um sambærilegar kröfur til innlendra lífeyrissjóða, sem starfa á grundvelli laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, og annarra helstu aðila á fjármálamarkaði um stafrænan viðnámsþrótt. Sú tillaga er gerð með hagsmuni sjóðfélaga í huga. Í ljósi þess að um landsbundna tilhögun ræðir þykir betur fara á að koma ákvæðinu fyrir í lögum um lífeyrissjóði heldur en í lögum sem innleiða DORA. Vísast til umfjöllunar um 12. tölul. 14. gr. frumvarpsins.

3.9. Breytingar á öðrum lögum.

Með frumvarpinu eru lagðar til breytingar á ýmsum lögum á sviði fjármálaþjónustu sem varða kröfur til aðila á fjármálamarkaði um stafrænan viðnámsþrótt, til samræmis við kröfur DORA og breytingar á gildandi tilskipunum og reglugerðum. Vísast til umfjöllunar um 14. gr. frumvarpsins.

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. Uppfylli innlendir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skilyrði tilnefningar sem mikilvægir og falla þar með undir eftirlitsramma II. þáttar V. kafla DORA, verður Eftirlitsstofnun EFTA falið hlutverk aðaleftirlitsaðila gagnvart þeim. 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, með vísan til tveggja stoða kerfisins. 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 og samráð viðhaft við fulltrúa Seðlabanka Íslands við undirbúning þess. Á vinnslustigi var ráðuneytið m.a. í samskiptum við og átti fundi um netöryggismál með fulltrúum háskóla-, iðnaðar- og nýsköpunarráðuneytis, Fjarskiptastofu, þar á meðal netöryggissveitar (CERT-ÍS), dómsmálaráðuneytis og forsætisráðuneytis, auk Reiknistofu bankanna. Enn fremur fundaði ráðuneytið með Samtökum fyrirtækja í fjármálaþjónustu og Landssamtökum lífeyrissjóða um DORA.

Áformaskjal var birt til umsagnar 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 11. júlí – 10. september 2024 (mál nr. S-146/2024) og barst ein umsögn, frá Samtökum fyrirtækja í fjármálaþjónustu (SFF). Í umsögninni kom fram að samtökin fögnuðu innleiðingu DORA í íslensk lög og styðja markmið hennar. Þau bentu þó á að innleiðingin verði áskorun vegna umfangs og ítarleika regluverksins. SFF lögðu áherslu á í umsögninni að tryggja þurfi skýrleika og stuðning frá eftirlitsstofnununum, m.a. með leiðbeiningum og upplýsingagjöf, og vöruðu við því að áætlanir um gildistöku og viðurlög kunni að vera óraunhæfar með tilliti til smærri markaðsaðila. Þau lögðu því til að frekari útskýringar og leiðbeiningar verði veittar til að draga úr

óvissu og áhættu. Þá áréttuðu samtökin að innleiðingin gæti haft kostnaðar- og samkeppnisáhrif, sér í lagi fyrir smærri aðila á fjármálamarkaði, og mótmæltu á sama tíma að innleiðingin leiði til hækkunar eftirlitsgjalds. Mikilvægt væri að huga að hagræðingu og nýrri forgangsröðun verkefna í eftirliti til að koma í veg fyrir eða lágmarka þörf á hækkun eftirlitsgjalds. Ráðuneytið hefur tekið framangreind sjónarmið SFF til skoðunar og horfði til athugasemda í umsögninni við frágang frumvarpsins. Með frumvarpinu er lagt til að gildistaka miðist við 1. nóvember 2025, m.a. í ljósi orðinna tafa á upptöku DORA í EES-samninginn og framlagningu frumvarpsins af þeim sökum. Efniskröfur DORA byggjast á alþjóðlega viðurkenndum viðmiðum um bestu framkvæmd, en málefnalegt má telja að gefa aðilum á fjármálamarkaði sem fyrirhuguð lög munu gilda um viðeigandi svigrúm til að undirbúa uppfyllingu ákvæða reglugerðarinnar, t.d. að því er varðar stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem getur t.d. kallað á endurskoðun samninga. Stjórnvaldssektarákvæði hefur tekið breytingum frá því sem gert var ráð fyrir í drögunum sem birt voru í samráðsgátt, þar á meðal hámarksfjárhæðarviðmið sekta á einstaklinga, sem nú er lagt til að verði 65 millj. kr., en horft er til fyrirmynda í öðrum lögum, sbr. skýringar við 5. gr. frumvarpsins.

Undir lok árs 2024 bárust ráðuneytinu ábendingar frá Fjarskiptastofu og háskóla-, iðnaðar- og nýsköpunarráðuneyti, Byggðastofnun og Lánastofnun sveitarfélaga ohf. sem nýttust við undirbúning frumvarpsins. Fjarskiptastofa og háskóla-, iðnaðar- og nýsköpunarráðuneytið studdu frumvarp til innleiðingar DORA og lögðu áherslu á mikilvægi samræmdrar framkvæmdar fyrirhugaðra laga um stafrænan viðnámsþrótt fjármálamarkaðar, NIS2 og innlendra netöryggislaga. Skýrar og skilvirkar boðleiðir milli Fjármálaeftirlits Seðlabankans og Fjarskiptastofu/CERT-IS, í tilefni tilkynninga um atvik eða verulegar netógnir, eru áherslumál af þeirra hálfu. Fjarskiptastofa hefur haldið til haga mikilvægi þess að allir aðilar á fjármálamarkaði hafi aðgang að sambærilegri viðbragðsþjónustu, svo tryggja megi öryggi og samræmi í netöryggismálum. Með frumvarpinu er ekki lagt til að formlegur þjónustuhópur netöryggissveitar, samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, verði útvíkkaður frá því sem nú er, en aðeins kerfislega mikilvægu bankarnir þrír og kauphöll teljast til rekstraraðila nauðsynlegrar þjónustu samkvæmt þeim. Það álitaefni kann hins vegar að koma til skoðunar á ný við innleiðingu NIS2 hér á landi. Við vinnslu frumvarpsins var leitað til Byggðastofnunar og Lánastofnunar sveitarfélaga ohf. um afstöðu þeirra til gildissviðs DORA. Fulltrúar beggja aðila andmæltu áformum um að gildissvið reglugerðarinnar nái til þeirra með vísan til sérstöðu og smæðar. Innviðaráðuneytið, sem fer með málefni Byggðastofnunar og Lánasjóðs sveitarfélaga ohf., er á sama máli og því er lagt til að báðir aðilar verði undanþegnir gildissviði fyrirhugaðra laga. Samráð var jafnframt haft við Landssamtök lífeyrissjóða og Náttúruhamfaratryggingu Íslands. Fram hefur komið að lífeyrissjóðum er verulega umhugað um upplýsinga- og netöryggi og styðja samkvæmt því markmið fyrirhugaðra laga og gera ekki athugasemdir við að kröfur DORA verði innleiddar í lög um lífeyrissjóði.

6. Mat á áhrifum.

Markmið frumvarpsins er að stuðla að stafrænum viðnámsþrótti aðila á fjármálamarkaði 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.

Talið er að heildaráhrif frumvarpsins verði jákvæð. Fyrirhuguð lagasetning mun hafa áhrif á flesta aðila á fjármálamarkaði. Ný heildarlög leysa af hólmi og samræma gildandi 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 kostnað fyrir fyrirtækin í aðdraganda og við gildistöku fyrirhugaðra laga, ekki síst að því er varðar endurmat og eftirfylgni samninga um þjónustu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Ekki liggur fyrir tölulegt kostnaðarmat, en líkur eru til að undirbúningur gildistöku fyrirhugaðra laga geti mælst í ársverkum hjá a.m.k. stærstu fyrirtækjum á fjármálamarkaði. Vinna við rýni og uppfærslu ferla og samninga verður mest í upphafi við gildistöku DORA hér á landi. Lagasetningin miðar 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, muni 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. Regluverkið er þó umfangsmikið og í eðli sínu matskennt, sem getur skapað áskoranir við innleiðingu, sér í lagi fyrir minni aðila á fjármálamarkaði. Framkvæmd þess krefst vandaðrar skjalfestingar og markvissrar áhættustýringar. Fyrirtækin bera sjálf kostnað við að hlíta ákvæðum fyrirhugaðra laga og af eigin rekstri. Óhjákvæmilegt er að hver aðili á fjármálamarkaði móti sjálfur stefnu í upplýsinga- og fjarskiptatæknimálum, vandi val á þjónustuveitendum og takist á herðar þá ábyrgð að veita birgðakeðju sinni viðeigandi aðhald.

Fjármálaeftirlitsstofnunum í EFTA-ríkjunum innan EES er með DORA tryggður aðgangur að mikilvægum vettvöngum, þar sem framkvæmd DORA verður fyrirsjáanlega til umfjöllunar og framþróunar á næstu árum, til jafns við systurstofnanir í ESB-ríkjum.

Ekki er talið líklegt að komi til útnefningar hérlendra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu undir sameiginlegan eftirlitsramma II. þáttar V. kafla DORA í næstu framtíð, en komi til þess verður Eftirlitsstofnun EFTA útnefnd aðaleftirlitsaðili gagnvart hlutaðeigandi.

6.3. Samkeppnisskilyrði.

Ekki eru taldar líkur á því að fyrirhuguð lagasetning hafi áhrif á samkeppni á markaði. Með meðalhófi í kröfum til smærri aðila í DORA er stuðlað að jafnvægi á sameiginlegum innri markaði.

6.4. Áætluð fjárhagsáhrif fyrir ríkið.

Áformuð lagasetning mun fela í sér aukin verkefni fyrir Fjármálaeftirlit Seðlabanka Íslands, enda eru kröfur DORA ítarlegar og að ýmsu leyti um nýmæli ræða í settum lögum. Eftirlit með framkvæmd DORA krefst úttekta, gæðaprófa, gagna- og upplýsingaöflunar frá aðilum á fjármálamarkaði, svo sem vegna þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Framangreint mun krefjast uppfærslu innanhússkerfa Seðlabankans. Kröfur

DORA um skýrslugjöf aðila á fjármálamarkaði vegna alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni og verulegra netógna krefjast vöktunar af hálfu eftirlitsaðila, enda er m.a. gert ráð fyrir tímanlegri framsendingu viðeigandi upplýsinga til annarra stjórnvalda innan lands, ekki síst netöryggissveitar Fjarskiptastofu (CERT-ÍS), 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 beri ábyrgð á netöryggisprófunum, þ.m.t. ógnamiðuðum innbrotsprófunum en samkvæmt DORA eiga aðildarríki að tilnefna yfirvald sem ábyrgðaraðila í öllum málum sem tengjast slíkum ógnamiðuðum prófunum. Loks þarf Seðlabankinn að innleiða ráðstafanir vegna söfnunar, greiningar og áframsendingar atvikatilkynninga sem og vegna söfnunar, greiningar og áframsendingar lista yfir þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

Mögulegum viðbótarkostnaði vegna aukinna verkefna Seðlabankans með innleiðingu DORA í landsrétt má gera ráð fyrir að verði mætt með hækkun eftirlitsgjalds samkvæmt lögum um greiðslu kostnaðar við opinbert eftirlit með fjármálastarfsemi og skilavald, nr. 99/1999, að hluta eða öllu leyti. Samræmingin sem felst í DORA frá því sem nú er, sbr. kafla 2.3 í greinargerðinni, er jafnframt að einhverju leyti hagkvæm fyrir eftirlitsaðilann. Ekki liggur fyrir tölulegt mat Seðlabankans á viðbótarkostnaði vegna DORA og/eða hvort fjölga þurfi stöðugildum og þá hve mikið.

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.

Gerðir sem eru teknar upp í EES-samninginn og samsvara reglugerðum ESB skulu teknar sem slíkar upp í landsrétt, sbr. a-lið 7. gr. EES-samningsins. Í þessu felst sú skylda að leiða ESB-reglugerðir, eins og þær hafa verið aðlagaðar við upptöku í EES-samninginn, óbreyttar í landsrétt. Því er lagt til að DORA, eins og hún var aðlöguð við upptöku í EES-samninginn, verði lögfest í heild sinni.

Reglugerðin sætti bæði svonefndum altækum aðlögunum á grundvelli bókunar 1 við EES-samninginn og sértækum aðlögunum samkvæmt ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025. Altækar aðlaganir eru aðlaganir sem eiga við um allar gerðir sem eru teknar upp í EES-samninginn og er ætlað að tryggja að efni gerða taki mið af eðli samningsins. Þær fela í sér atriði á borð við að vísanir til yfirráðasvæða og ríkisborgara aðildarríkja Evrópusambandsins eigi við um yfirráðasvæði og ríkisborgara aðildarríkja EES-samningsins.

Aðlaganir í ákvörðun sameiginlegu EES-nefndarinnar taka fyrst og fremst mið af tveggja stoða kerfinu, ekki síst að því er varðar vísanir til hlutverks evrópsku fjármálaeftirlitsstofnananna sem aðaleftirlitsaðila og tilheyrandi valdheimilda, sem í tilviki mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu í EFTA-ríkjunum innan EES er falið Eftirlitsstofnun EFTA. Aðaleftirlitsaðilar skulu eiga með sér samstarf, enda markmið DORA að stuðla að samræmi í aðhaldi með þeim þriðju aðilum sem tilnefndir eru sem mikilvægir á öllu Evrópska efnahagssvæðinu. Með aðlögunum er viðeigandi aðkoma Eftirlitsstofnunar EFTA tryggð, en þess má geta að rétt þótti að gera ráð fyrir valkvæðri þátttöku af hennar hálfu í sameiginlegum skoðunarhópum þegar eftirlit beinist ekki að mikilvægum þriðja aðila í EFTA-

ríki, sbr. aðlögun vegna 40. gr. DORA. Ef kemur til tilnefningar þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með starfsemi í EFTA-ríki ákveður fastanefnd EFTA hvert fjárhæðir févítis sem Eftirlitsstofnun EFTA sem aðaleftirlitsaðili leggur á slíkan aðila skulu renna, sbr. aðlögun vegna 35. gr. DORA. Í aðlögun vegna sama ákvæðis er andmælaréttur mikilvægs þriðja aðila áréttaður, gagnvart evrópsku fjármálaeftirlitsstofnununum vegna aðkomu þeirra að undirbúningi ákvörðunar Eftirlitsstofnunar EFTA um slíka viðurlagabeitingu. Ef hún hyggst krefjast upplýsinga frá þriðja aðila á grundvelli 37. gr. DORA ber samkvæmt aðlögun að halda til haga rétti þriðja aðilans til að áfrýja ákvörðun um févíti vegna ófullnægjandi upplýsinga eða höfnun slíkrar kröfugerðar til EFTA-dómstólsins, með vísan til samnings EFTA-ríkjanna um stofnun eftirlitsstofnunar og dómstóls. Þá má geta aðlögunar vegna 7. mgr. 19. gr., þar sem kveðið er á um að Seðlabanki Evrópu skuli tilkynna seðlabönkum í EFTA-ríkjunum, líkt og aðilum seðlabankakerfis Evrópu, um málefni sem varða greiðslukerfið, en á grundvelli slíkrar tilkynningar ber lögbærum yfirvöldum eftir því sem við á að gera allar nauðsynlegar ráðstafanir til að vernda tafarlaust stöðugleika fjármálakerfisins. Loks er gert ráð fyrir svigrúmi EFTA-ríkjanna til að innleiða DORA í landsrétt, í aðlögun við 64. gr.

Lagt er til að vísað verði til birtingar gerðarinnar í EES-viðbæti við Stjórnartíðindi Evrópusambandsins, til samræmis við heimild 1. málsl. 2. mgr. 2. gr. laga um Stjórnartíðindi og Lögbirtingablað, nr. 15/2005, sbr. 2. málsl. 1. mgr. 4. gr. sömu laga. Bókun 1 við EES-samninginn er birt í fylgiskjali í lögum um Evrópska efnahagssvæðið, nr. 2/1993. Ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 um upptöku DORA í EES-samninginn er birt í auglýsingu nr. 8/2025 í C-deild Stjórnartíðinda.

Verði frumvarp þetta að lögum verður reglugerð (ESB) 2022/2554, með þeim aðlögunum sem greint er frá í 1. mgr., hluti laganna. Þegar vísað er til laga þessara í ákvæðum frumvarpsins er jafnframt átt við DORA, sbr. 1. gr.

Um 2. gr.

Í DORA er nokkuð um vísanir til hugtaka sem koma fram í tilskipunum sem hafa verið teknar upp í EES-samninginn og innleiddar hér á landi. Tilgangur ákvæðisins er að greina frá því hvar viðkomandi hugtök hafa verið tekin upp í íslenskan rétt.

Rétt þykir að vekja sérstaka athygli á að skýringu 21. tölul. ákvæðisins er ætlað að varpa ljósi á fyrri hluta skilgreiningar 30. tölul. 3. gr. DORA-reglugerðarinnar, þ.e. þeim hluta setningarinnar sem vísar til tilskipana. Um ábyrgð stjórnar og/eða framkvæmdastjóra samkvæmt einstökum ákvæðum DORA fer samkvæmt landslögum, þ.e. hún veltur á eðli verkefna sem um ræðir. Nánar er fjallað um þetta í a-lið kafla 3.2.

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 Evrópuþingsins og ráðsins (ESB) nr. 909/2014 frá 23. júlí 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 frá 8. júní 2016 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 Evrópuþingsins og ráðsins (ESB) nr. 575/2013 frá 26. júní 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 Evrópuþingsins og ráðsins (ESB) nr. 648/2012 frá 4. júlí 2012 um OTC-afleiður, miðlæga mótaðila og afleiðuviðskiptaskrár er innleidd með lögum um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018.
5. Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 600/2014 frá 15. maí 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 frá 16. september 2009 um lánshæfismatsfyrirtæki er innleidd með lögum um lánshæfismatsfyrirtæki, nr. 50/2017.
7. Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 frá 24. nóvember 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 frá 24. nóvember 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 Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 frá 24. nóvember 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 frá 27. apríl 2016 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.

Hér á landi er áformuð upptaka og/eða innleiðing eftirtaldra reglugerða, sem eru EES-tækar og vísað er til í DORA:

- Reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 frá 23. maí 2023 um markaði fyrir sýndareignir og um breytingu á reglugerðum (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipunum 2013/36/ESB og (ESB) 2019/1937 (MiCA). Hún var tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 41/2025 frá 20. febrúar 2025 og er innleiðing í landsrétt áformuð á yfirstandandi þingi, með nýjum heildarlögum um markaði fyrir sýndareignir.
- Reglugerð Evrópuþingsins og ráðsins (ESB) 2019/2033 frá 27. nóvember 2019 um varfærniskröfur fyrir verðbréfafyrirtæki og breytingu á reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 575/2013, (ESB) nr. 600/2014 og (ESB) nr. 806/2014. Unnið er að upptöku hennar í EES-samninginn og innleiðing í landsrétt áformuð, með nýjum lögum um varfærniskröfur til verðbréfafyrirtækja.
- Reglugerð Evrópuþingsins og ráðsins (ESB) 2020/1503 frá 7. október 2020 um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki og um breytingu á reglugerð (ESB)

2017/1129 og tilskipun (ESB) 2019/1937. Hún var tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 30/2024 frá 2. febrúar 2024 og er innleiðing í landsrétt áformuð, með nýjum heildarlögum um hópfjármögnun fyrir fyrirtæki.

- Reglugerð Evrópuþingsins og ráðsins (ESB) 2017/2402 frá 12. desember 2017 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. Hún var tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 145/2024 frá 12. júní 2024 og er innleiðing í landsrétt áformuð á yfirstandandi þingi, með nýjum heildarlögum um verðbréfun.

Hafa ber í huga að netöryggistilskipun ESB (NIS1) var innleidd hér á landi með lögum um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. Endurnýjuð netöryggistilskipun ESB (NIS2) var samþykkt samhliða DORA. Í ráðuneyti fjarskipta- og netöryggismála (nú innviðaráðuneyti) 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, enda verður um sérlög að ræða gagnvart almennri netöryggislöggjöf, sbr. kafla 2.3. Sama ráðuneyti áformar einnig innleiðingu reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881 frá 17. apríl 2019 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 3. gr.

Aðildarríki skulu skv. 46. gr. DORA tilnefna lögbært yfirvald sem hefur eftirlit með því að farið sé eftir ákvæðum hennar. Lagt er til að Seðlabanki Íslands verði lögbært yfirvald hér á landi. Meðal verkefna Seðlabankans er að stuðla að virku og öruggu fjármálakerfi og hann annast almennt eftirlit með því að starfsemi eftirlitsskyldra aðila sé í samræmi við lög og stjórnvaldsfyrirmæli og að hún sé að öðru leyti í samræmi við heilbrigða og eðlilega viðskiptahætti, sbr. 1. og 4. mgr. laga um Seðlabanka Íslands, nr. 92/2019. Verkefni lögbærs yfirvalds samkvæmt DORA falla vel að því.

Enn fremur er í 1. mgr. lagt til að Seðlabankanum verði falin ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun hér á landi skv. 9. mgr. 26. gr. DORA, sem nánar er fjallað um í kafla 3.4. Seðlabankinn hefur þegar innleitt svonefnda TIBER-EU aðferðafræði að fyrirmynd Seðlabanka Evrópu og evrópskra seðlabanka. Um ræðir umgjörð um netárásarprófanir fyrir stofnanir og fyrirtæki sem eru mikilvæg fyrir íslenskt fjármálakerfi (TIBER-IS). DORA gerir kröfur til slíkra prófana, þar á meðal til prófunaraðila, sbr. 27. gr. Hér á landi mun Seðlabankinn veita aðilum á fjármálamarkaði staðfestingu á að prófun hafi verið gerð í samræmi við kröfur DORA til að heimila gagnkvæma viðurkenningu á ógnamiðuðum innbrotsprófunum á milli lögbærra yfirvalda á EES-svæðinu, sbr. 7. mgr. 26. gr. reglugerðarinnar.

Lagt er til að tilgreint verði að Fjármálaeftirlitið fari með eftirlit með lögunum og fari með önnur verkefni lögbærs yfirvalds samkvæmt DORA. Þannig skuli tilkynningum aðila á fjármálamarkaði um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir skv. 19. gr. DORA t.d. beint til Fjármálaeftirlitsins. Leiðbeinandi tilmæli Fjármálaeftirlitsins vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila, nr. 1/2019, kveða á um slíka skyldu (liður 5.2). Skv. 4. mgr. 19. gr. DORA verður um þríþætta skýrslugjöf að ræða:

Frumtilkynningu, áfangaskýrslu og lokaskýrslu. Um áframmiðlun upplýsinga um atvik og verulega netógn af hálfu Fjármálaeftirlitsins til Evrópsku bankaeftirlitsstofnunarinnar, Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunarinnar, Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar, Seðlabanka Evrópu, ríkislögreglustjóra, Fjarskiptastofu, netöryggissveitar Fjarskiptastofu (CERT-ÍS) og eftir atvikum annarra fer skv. 6.–7. mgr. 19. gr. DORA. Upplýsingarnar kunna að nýtast öðrum til að verjast ógnum við net- og upplýsinga- eða rekstraröryggi. Af þeim sökum er mikilvægt að viðeigandi upplýsingar berist CERT-ÍS sem allra fyrst, eftir móttöku tilkynninga. Markmið með starfrækslu CERT-ÍS er ekki síst að fyrirbyggja og draga úr hættu á netárásum og öðrum atvikum á Íslandi og takmarka útbreiðslu þeirra og tjón eins og kostur er, sbr. 9. gr. laga um Fjarskiptastofu, nr. 75/2021. Berist Fjármálaeftirlitinu upplýsingar um alvarleg atvik eða verulega netógn geta ferlar tengdir öðrum ábyrgðarsviðum Seðlabankans virkjast, svo sem fjármálastöðugleika og rekstri millibankakerfisins. Um endurgjöf Fjármálaeftirlitsins við tilkynningum fer skv. 22. gr. DORA. Vísast til nánari umfjöllunar um tilkynningarskyldu og meðhöndlun atvika í kafla 3.3.

Fjármálaeftirlitið er hluti af Seðlabankanum, sbr. 1. málsl. 4. mgr. 2. gr. laga um Seðlabanka Íslands. Fjármálaeftirlitsnefnd bankans kemur að ákvörðunum sem faldar eru Fjármálaeftirlitinu í lögum eftir því sem nánar greinir í 3. málsl. 2. mgr. 3. gr. og 15. gr. laganna. Starfsemi Fjármálaeftirlitsins er fjármögnuð með eftirlitsgjaldi sem eftirlitsskyldir aðilar og aðrir gjaldskyldir aðilar greiða samkvæmt lögum um greiðslu kostnaðar við opinbert eftirlit með fjármálastarfsemi og skilavald, nr. 99/1999.

Um eftirlit Fjármálaeftirlitsins gilda lög um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, sbr. 1.–3. mgr. 2. gr. og 3. mgr. 8. gr. þeirra laga. Lögin fela Fjármálaeftirlitinu m.a. víðtækar heimildir til að afla upplýsinga og gagna, þar á meðal með vettvangskönnunum og með því að kalla einstaklinga til skýrslugjafar, og til að krefjast úrbóta að viðlögðum dagsektum ef eftirlitsskyldir aðilar fylgja ekki lögum og reglum. Um eftirlitið gilda einnig stjórnsýslulög, nr. 37/1993, og aðrar almennar reglur stjórnsýsluréttar, svo sem reglur um jafnræði, meðalhóf og andmælarétt.

Seðlabankinn er sjálfstæð stofnun, sbr. 1. mgr. 1. gr. laga um Seðlabanka Íslands, og ákvarðanir Fjármálaeftirlitsins verða ekki kærðar til annars stjórnvalds. Þær sæta aftur á móti endurskoðun dómstóla eftir almennum reglum, sbr. m.a. 60. gr. og 1. mgr. 70. gr. stjórnarskrár lýðveldisins Íslands, nr. 33/1944. Sá sem telur sig hafa verið beittan rangsleitni af hálfu Fjármálaeftirlitsins getur einnig kvartað til umboðsmanns Alþingis samkvæmt lögum um umboðsmann Alþingis, nr. 85/1997. Umboðsmaður getur látið í ljós álit sitt á því hvort athöfn Fjármálaeftirlitsins hafi brotið í bága við lög eða hvort annars hafi verið brotið gegn vönduðum stjórnsýsluháttum og beint til þess tilmælum um úrbætur. Álit umboðsmanns er þó ekki lagalega bindandi.

Samkvæmt ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 um upptöku DORA í EES-samninginn er Eftirlitsstofnun EFTA falið að framfylgja ákvæðum reglugerðarinnar gagnvart mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu í EFTA-ríkjunum. Að því er varðar valdheimildir Eftirlitsstofnunar EFTA gagnvart þeim vísast til umfjöllunar í kafla 3.6 og samnings EFTA-ríkjanna um stofnun eftirlitsstofnunar og dómstóls. Um hlutverk og valdheimildir Eftirlitsstofnunar EFTA á sviði fjármálaeftirlits er fjallað í 25. gr. a í þeim samningi og bókun 8 við hann, sbr. auglýsingu nr. 64/2021 í C-deild Stjórnartíðinda. Fjallað er um samstarf Fjármálaeftirlitsins við Eftirlitsstofnun EFTA og hinar evrópsku eftirlitsstofnanir á fjármálamarkaði í lögum um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017. Um samstarf lögbærra yfirvalda (innanlands og milli landa), við aðaleftirlitsaðila, CERT-ÍS, evrópskar stofnanir og vettvanga fer skv. 47.–49. gr. DORA.

Um 4. gr.

Í ákvæðinu er lagt til að áréttuð verði skylda eftirlitsaðilans til að krefjast úrbóta, komi í ljós að ákvæðum laganna, verði frumvarpið óbreytt að lögum, eða stjórnvaldsfyrirmælum settum með stoð í þeim sé ekki fylgt, sbr. 10. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998.

Ákvæði 4. mgr. 50. gr. DORA kveður á um lágmarksstjórnsýsluviðurlög eða ráðstafanir til úrbóta vegna brota á reglugerðinni sem veita á lögbærum yfirvöldum vald til að beita. Í a- og b-lið ákvæðisins segir að tryggja skuli lögbæru yfirvaldi heimild til að gefa út fyrirmæli um að einstaklingur eða lögaðili láti af háttsemi sem felur í sér brot á lögum þessum og endurtaki hana ekki, og til að óska eftir að bundinn verði endi á hvers konar framkvæmd eða framferði, tímabundið eða varanlega, sem það telur brjóta í bága við ákvæði laga þessara og komið sé í veg fyrir að slík framkvæmd eða framferði endurtaki sig. Skv. 3. mgr. 8. gr. laga nr. 87/1998 er Fjármálaeftirlitinu heimilt að beita eftirlitsúrræðum þeirra við eftirlit og önnur verkefni gagnvart einstaklingum og lögaðilum sem því er falið að framkvæma á grundvelli sérlaga og annarra reglna.

Ef aðili sinnir ekki kröfum um úrbætur innan hæfilegs frests getur Fjármálaeftirlitið lagt dagsektir á hann skv. 1. mgr. 11. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998. 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 enn fremur skv. 4. mgr. sömu greinar 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.

Að því marki sem það er heimilt samkvæmt landslögum er í d-lið 4. mgr. 50. gr. DORA gert ráð fyrir að aðildarríki veiti lögbæru yfirvaldi vald til að krefjast gagnaumferðarskráa sem liggja hjá fjarskiptafyrirtæki, ef rökstuddur grunur er um brot á reglugerðinni og ef slíkar skrár geta skipt máli fyrir rannsókn á brotum. Hér á landi er í 3. mgr. 89. gr. laga um fjarskipti, nr. 70/2022, kveðið á um að fjarskiptafyrirtæki skuli í þágu rannsókna sakamála og almanna-öryggis varðveita lágmarksskráningu ganga um fjarskiptaumferð notenda í sex mánuði. Um aðgengi að fjarskiptaumferðarupplýsingum fer skv. 89. og 92. gr. sömu laga og er krafa gerð um dómsúrskurð eða lagaheimild. Fjarskiptafyrirtæki er skv. 2. mgr. 92. gr. rétt og skylt að veita lögreglu, í þágu rannsóknar sakamáls, upplýsingar um hver sé skráður notandi ákveðins símanúmers og/eða notandi vistfangs (IP-tölu), svo og hvaða símanúmer tiltekinn viðskiptavinur var með á tilteknu tímabili. Með frumvarpinu er ekki lagt til að Fjármálaeftirlitið fái beinan aðgang að fjarskiptaumferðarupplýsingum í tengslum við eftirlit með framkvæmd DORA hér á landi. Leiki grunur á refsiverðri háttsemi er gengið út frá að brotaþoli tilkynni um atvik til lögreglu, svo sem á grundvelli 229. gr. (heimildarlaus aðgangur að gögnum eða forritum annarra sem geymd eru á tölvutæku formi), 249. gr. a (ólögmæt breyting, viðbót eða eyðilegging tölvuvélbúnaðar, gagna eða forrita sem geymd eru á tölvutæku formi eða ráðstafanir með öðrum hætti sem eru til þess fallnar að hafa áhrif á niðurstöðu tölvuvinnslu), 257. gr. (heimildarlaus sending, breyting, viðbót, útþurrkun eða eyðilegging gagna eða forrita sem geymd eru á tölvutæku formi og ætluð eru til tölvuvinnslu) almennra hegningarlaga, nr. 19/1940.

Um 5. gr.

Í samræmi við 3. mgr. og c-lið 4. mgr. 50. gr., sbr. 51. gr., DORA er í 1. mgr. lagt til að Fjármálaeftirlitinu verði heimilt að beita stjórnvaldssektum vegna brota gegn nánar tilgreindum ákvæðum reglugerðarinnar, eftir atvikum eins og þau eru nánar útfærð í stjórnvaldsfyrirmælum, til að tryggja skilvirka framkvæmd laganna, verði frumvarpið óbreytt að lögum. Er þar um að ræða kröfur sem gerðar eru til aðila á fjármálamarkaði skv. 2. gr. DORA og mælt er fyrir um í II.–V. kafla reglugerðarinnar. Þær lúta að áhættustýringu, þar á meðal vegna þriðju aðila, svo og prófunum, stjórnun, flokkun og skýrslugjöf um atvik. Í 12. tölul. og 13. tölul. er gert ráð fyrir sektarheimildum sem varða skyldur aðila á fjármálamarkaði hér á landi sem nýta þjónustu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem útnefndir hafa verið sem slíkir og falla undir eftirlitsramma II. þáttar V. kafla DORA. Í 12. mgr. 31. gr. DORA, að teknu tilliti til bókunar 1 um altæka aðlögun við EES-samninginn, er kveðið á um að aðilar á fjármálamarkaði skuli aðeins nýta sér þjónustu mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi ef sá þriðji aðili hefur stofnað dótturfélag á Evrópska efnahagssvæðinu innan 12 mánaða frá útnefningu undir eftirlitsrammann. Þá ber Fjármálaeftirlitinu skv. 42. gr. DORA, ef við á, að fylgja eftir tilmælum aðaleftirlitsaðila til mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu gagnvart innlendum aðilum á fjármálamarkaði. Þeir skulu skv. 3. mgr. upplýstir um áhættu sem tilgreind er í slíkum tilmælum, enda skal áhættustýring af þeirra hálfu taka mið af henni, ef við á. Fjármálaeftirlitið getur skv. 6. mgr. krafist þess að notkun eða nýtingu þjónustu slíks aðila sé frestað tímabundið, að hluta eða öllu leyti, þar til brugðist hefur verið við þeirri áhættu sem tilgreind er í tilmælunum sem beint er til þriðja aðilans og ef nauðsyn krefur krafist þess að samningi sé slitið. Heimilt verði að leggja stjórnvaldssektir á hvern þann sem brýtur gegn tilgreindum ákvæðum DORA, bæði einstaklinga og lögaðila.

Lagt er til að sektir sem lagðar verði á einstaklinga vegna brota gegn ákvæðum DORA geti numið frá 100 þús. kr. til 65 millj. kr. Það er sama hámarksviðmið og gildir um einstaklinga í tilviki brota gegn lögum um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018 (4. mgr. 7. gr.) og lögum um greiðsluþjónustu, nr. 114/2021 (2. mgr. 106. gr.). Í samræmi við ýmis önnur lög á fjármálamarkaði er í 2. mgr. lagt til að fjárhæð sekta vegna brota gegn ákvæðum DORA sem lagðar verða 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 ræðir sama hámarksviðmið og gildir um lögaðila í tilviki brota gegn áðurnefndum lögum, nr. 15/2018 og 114/2021. Meginmarkmið viðurlagaákvæða er að hafa tilhlýðileg varnaðaráhrif.

Í 3. mgr. er, þrátt fyrir 2. mgr., gert ráð fyrir að heimilt verði að sekta aðila um fjárhæð sem nemur allt að tvöfaldri fjárhæð ávinnings af broti, enda sé unnt að ákvarða hann. Ávinningur af broti getur hvort heldur falist í því að hagnast eða komast hjá tapi. Eðli máls samkvæmt verður aðeins miðað við ávinning af broti ef unnt er að meta fjárhæð hans. Velta lögaðila eða samstæðu miðast við síðustu reikningsskil sem stjórn lögaðilans eða endanlegs móðurfélags samstæðunnar hefur samþykkt. Í tilviki samstæðu skal miðað við samstæðureikning.

Í 4. mgr. er lagt til að gera megi aðför til fullnustu ákvörðunum Fjármálaeftirlitsins um stjórnvaldssektir, sbr. 6. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989, til að stuðla að því að þær hafi tilskilin áhrif. Réttur aðila til að bera ákvörðun Fjármálaeftirlitsins undir dómstóla er

talinn tryggja réttaröryggi nægjanlega. Um framkvæmd fullnustunnar fer samkvæmt lögum um aðför. Lagt er til að dráttarvextir leggist á stjórnvaldssekt sem er ekki greidd innan mánaðar frá ákvörðun Fjármálaeftirlitsins til að knýja á um greiðslu. Fjallað er nánar um dráttarvexti í III. kafla laga um vexti og verðtryggingu, nr. 38/2001.

Fjármálaeftirlitið skal skv. 54. gr. DORA, sbr. einnig e-lið 4. mgr. 50. gr. reglugerðarinnar, birta ákvarðanir um stjórnvaldssektir vegna brota gegn lögunum, þar með talið opinberar yfirlýsingar sem tilgreina auðkenni einstaklings eða lögaðila sem brotið hefur gegn ákvæðum laganna og hvers eðlis brotið er. Þær skulu birtar á vef Fjármálaeftirlitsins.

Tilteknar undantekningar eru gerðar á skyldu til birtingar auðkenna lögaðila eða auðkenna og persónuupplýsinga þegar einstaklingur á í hlut skv. 3. mgr. 54. gr. DORA. Það á við þegar birting myndi vera í ósamræmi við brot, m.a. með tilliti til áhættu í tengslum við vernd persónuupplýsinga, tefla stöðugleika fjármálamarkaða eða yfirstandandi rannsókn sakamáls í tvísýnu eða valda hlutaðeigandi óhóflegum skaða. Vísast og til 9. gr. a í lögum um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, og gagnsæisstefnu Fjármálaeftirlitsins.

Um 6. gr.

Gert er ráð fyrir að bæði ásetnings- og gáleysisbrot varði stjórnvaldssektum samkvæmt frumvarpinu til að styrkja varnaðaráhrif þeirra og til samræmis við það sem almennt gildir um stjórnsýsluviðurlög á sviði fjármálamarkaðar, sbr. einnig 2. mgr. 51. gr. DORA. Saknæmisstig getur þó haft áhrif á það hversu alvarlegt brot er talið og þar með ákvörðun stjórnvaldssektar.

Um 7. gr.

Ákvæðið, sem byggist á 2. mgr. 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 m.a. að vinna gegn því að brotlegir aðilar hagnist á brotum eða komi sér undan tapi.

Um 8. gr.

Oft er unnt að greiða fyrir úrlausn mála og spara bæði Fjármálaeftirlitinu og málsaðila tíma og fé með því að ljúka máli með sátt fremur en með einhliða ákvörðun eftirlitsins um beitingu stjórnsýsluviðurlaga. Af þeim sökum er í ýmsum lögum á sviði fjármálamarkaðar mælt fyrir um heimild Fjármálaeftirlitsins til að ljúka málum með sátt við málsaðila. Seðlabankinn hefur á grundvelli þeirra sett reglur um heimild fjármálaeftirlits Seðlabanka Íslands til að ljúka máli með sátt, nr. 1234/2024.

Í sátt felst yfirleitt að málsaðili gengst við broti og upplýsir að fullu um það auk þess að greiða sekt, sem er þó lægri en ef Fjármálaeftirlitið hefði einhliða lagt á stjórnvaldssekt. Sátt getur einnig falið í sér annars konar úrræði, svo sem um viðeigandi úrbætur. Brjóti málsaðili gegn sátt getur Fjármálaeftirlitið fellt hana úr gildi og tekið mál til meðferðar á ný og þá eftir atvikum gert honum stjórnvaldssekt eða beitt öðrum ráðstöfunum.

Um 9. 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 9. gr. frumvarpsins. Ákvæðið byggist á lögum nr. 55/2007 um breytingar á lagaákvæðum um viðurlög við brotum á fjármálamarkaði sem aftur byggðust á skýrslu nefndar um viðurlög við efnahagsbrotum frá 12. október 2006.

Ákvæðið tekur aðeins til einstaklinga en ekki til lögaðila. Því 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 þau 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 lagalegri skyldu til að veita stjórnvaldi aðgang að húsnæði eða hirslum í fyrirtækjum. Mestu skiptir markmiðið með ákvæðinu um 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 10. gr.

Lagt er til að heimild Fjármálaeftirlitsins til að beita stjórnvaldssektum samkvæmt lögunum, verði frumvarpið óbreytt að lögum, falli niður þegar fimm ár eru liðin frá því að háttsemi lauk til að knýja á um úrlausn mála. Sams konar ákvæði er að finna í ýmsum lögum á sviði fjármálaþjónustu og er uppruna þess að rekja til laga nr. 55/2007, um breytingar á lagaákvæðum um viðurlög við brotum á fjármálamarkaði.

Rétt er að taka mið af meginreglum refsiréttar og fjármálamarkaðsréttar um það hvenær háttsemi telst lokið. Af því leiðir m.a. 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. Þótt rannsókn beinist í upphafi að einum aðila hindrar 1. málsl. 2. mgr. ekki að aðrir aðilar, sem síðar kemur í ljós að stóðu einnig að broti, verði beittir stjórnvaldssektum. Reglan á sér að nokkru leyti hliðstæðu í 4. mgr. 82. gr. almennra hegningarlaga, nr. 19/1940.

Um 11. gr.

Framkvæmdastjórn Evrópusambandsins er í ýmsum ákvæðum DORA veitt vald til að samþykkja undirgerðir til að útfæra nánar viss atriði reglugerðarinnar. 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. Annars vegar verður um framselda gerð að ræða sem tilgreinir nánar viðmiðanir sem liggja munu til grundvallar útnefningu aðila undir eftirlitsrammann og hins vegar framselda gerð um gjöld sem Eftirlitsstofnun EFTA leggur á slíka aðila.

Lagt er til að Seðlabanka Íslands verði heimilað að innleiða aðrar undirgerðir með útgáfu reglna. 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. Innleiðing þeirra stendur honum því nær og eru þessi viðmið lögð til grundvallar í mörgum lagabálkum á sviði fjármálamarkaðar.

Um 12. gr.

Lagt er til að tekin verði öll tvímæli af um að Byggðastofnun, Lánasjóður sveitarfélaga ohf. og Náttúruhamfaratrygging Íslands skuli undanþegin ákvæðum fyrirhugaðra laga. Með frumvarpinu er lagt til að DORA verði tekin í heild upp í landsrétt, í samræmi við a-lið 1. mgr. 7. gr. EES-samningsins. Undanþágan er í samræmi við gildandi EES-rétt um fjármálafyrirtæki og vátryggingastarfsemi. Vísast til a- og n-liða 1. mgr. 2. gr., b-liðar 3. mgr. 2. gr., 4. mgr. 2. gr. og 31., 47 og 48. tölul. 3. gr. DORA.

Samkvæmt e-lið 1. mgr. 1. gr. í ákvörðun sameiginlegu EES-nefndarinnar nr. 79/2019 frá 29. mars 2019 um upptöku tilskipunar 2013/36/ESB um aðgang að starfsemi lánastofnana og varfærnieftirliti með lánastofnunum og verðbréfafyrirtækjum (CRD IV) í EES-samninginn, eru Byggðastofnun og Lánasjóður sveitarfélaga ohf. undanþegin gildissviði hennar. Engu að síður gilda um báða aðila, sem hafa starfsleyfi sem lánafyrirtæki, ýmis ákvæði laga um fjármálafyrirtæki, nr. 161/2002. Til dæmis má nefna ákvæði laganna um stjórnun og meðhöndlun áhættuþátta í starfsemi fjármálafyrirtækja, m.a. rekstraráhættu, og ber þeim í dag að starfa samkvæmt viðmiðunarreglum EBA um stjórnun upplýsinga- og fjarskiptatækniáhættu og um útvistun. Byggðastofnun er stofnun í eigu íslenska ríkisins og heyrir undir yfirstjórn ráðherra, samkvæmt lögum um Byggðastofnun, nr. 106/1999. Stofnunin gegnir víðtækara hlutverki á sviði byggðaþróunar en útlánastarfsemi og er m.a. falið eftirlit með framkvæmd laga um póstþjónustu, sbr. 2. gr. laga nr. 106/1999. Lánasjóður sveitarfélaga ohf. er opinbert hlutafélag í eigu sveitarfélaga á Íslandi og nýtur ekki opinberrar ábyrgðar í rekstri né ábyrgðar eigenda á skuldbindingum sínum umfram hlutafé. Íslensk sveitarfélög hafa þó heimild til að veita sjóðnum veð í tekjustraumum sínum. Lánasjóðurinn starfar samkvæmt lögum um stofnun opinbers hlutafélags um Lánasjóð sveitarfélaga, nr. 150/2006. Útlánastarfsemi sjóðsins takmarkast við afmarkaðan hóp opinberra aðila. Ákvæðið er í samræmi við afstöðu innviðaráðuneytisins sem fer með málefni Byggðastofnunar og Lánasjóðs sveitarfélaga ohf.

Samkvæmt a-lið 3. mgr. 1. gr. í ákvörðun sameiginlegu EES-nefndarinnar nr. 78/2011 frá 1. júlí 2011 um upptöku tilskipunar 2009/138/EB um stofnun og rekstur fyrirtækja á sviði vátrygginga og endurtrygginga (Gjaldþolsáætlun II) í EES-samninginn, er Náttúruhamfaratrygging Íslands (áður Viðlagatrygging Íslands) undanþegin gildissviði hennar. Um hana gilda lög um Náttúruhamfaratryggingu Íslands, nr. 55/1992, og ýmis ákvæði laga um vátryggingastarfsemi, nr. 100/2016, þó ekki t.d. 39. og 44. gr. um almennar kröfur til stjórnkerfis og áhættustýringu, skv. 3. mgr. 3. gr. laganna. Skv. 19. gr. a í lögum nr. 55/1992 skal Náttúruhamfaratrygging hafa skilvirkt kerfi áhættustýringar.

Því skal til haga haldið að um ríkisaðila í A-hluta ríkissjóðs (þar á meðal Byggðastofnun og Náttúruhamfaratryggingu Íslands) gildir 65. gr. laga um opinber fjármál, nr. 123/2015, um

innra eftirlit og innri endurskoðun, sem m.a. felur í sér kerfisbundið, óháð og hlutlægt mat á virkni áhættustýringar, eftirlits og stjórnarhátta hlutaðeigandi aðila.

Um 13. gr.

Stafrænn viðnámsþróttur eða áfallaþol fjármálamarkaða eru víða í brennidepli. Upplýsinga- og samskiptatækni gegnir lykilhlutverki á fjármálamarkaði nútímans. Breytt öryggisumhverfi kallar á aukna öryggisvitund og þekkingu sem krefst samráðs og samhæfingar bæði innan ríkja og á alþjóðavettvangi.

Öll EFTA-ríkin innan EES hafa lagt áherslu á skjóta upptöku DORA í EES-samninginn og innleiðingu í landsrétt. Í ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025, frá 20. febrúar 2025, er gert ráð fyrir 12 mánaða svigrúmi til innleiðingar DORA í landsrétt EFTA-ríkjanna.

Í ljósi orðinna tafa á upptöku DORA í EES-samninginn og tilheyrandi tafa á framlagningu og þinglegri meðferð frumvarpsins, frá því sem upphafleg áform ráðuneytisins gerðu ráð fyrir, er lagt til að gildistaka miðist við 1. nóvember 2025. Með því fá bæði aðilar á fjármálamarkaði og Seðlabankinn hæfilegt rými til undirbúnings gildistöku.

Um 14. gr.

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

Um 1. tölul. Lögð er til breyting á lögum um verðbréfasjóði, nr. 116/2021, til að innleiða breytingar á a-lið 2. undirgr. 1. mgr. 12. gr. tilskipunar Evrópuþingsins og ráðsins 2009/65/ESB frá 13. júlí 2009 um samræmingu á lögum og stjórnsýslufyrirmælum að því er varðar verðbréfasjóði (UCITS), sem var innleidd hér á landi í 3. og 4. mgr. 15. gr. laga nr. 116/2021. Rekstrarfélag skal skv. 3. mgr. 15. gr. laganna hafa viðeigandi mannauð og nauðsynlega tækni til að geta rekið verðbréfasjóði á fullnægjandi hátt með hliðsjón af eðli þeirra, m.a. er varðar eftirlit og öryggisráðstafanir vegna rafrænnar gagnavinnslu. Í frumvarpsákvæðinu er lagt til að tekið verði fram að eftirlitið og öryggisráðstafanirnar skuli ná til net- og upplýsingakerfa sem sett eru upp og stjórnað í samræmi við DORA.

Um 2. tölul. Um er að ræða innleiðingu á breytingum á 4. mgr. 41. gr. tilskipunar Evrópuþingsins og ráðsins 2009/138/EB frá 25. nóvember 2009 um stofnun og rekstur fyrirtækja á sviði vátrygginga og endurtrygginga sem var innleidd með lögum um vátryggingastarfsemi, nr. 100/2016. Í a-lið er lagt til að við 5. mgr. 39. gr. laganna bætist viðbótartexti um skyldu vátryggingafélags til að setja upp og stjórna net- og upplýsingakerfum í samræmi við DORA sem lið í ráðstöfunum þeirra til að tryggja samfellu og reglufestu í starfseminni. Í þessu felst að nota viðeigandi og hæfileg kerfi, tilföng og málsmeðferðir. Þá er í b-lið gert ráð fyrir breytingum á 4. og 5. mgr. 44. gr. laganna þar sem fjallað er um áhættustýringu vátryggingafélags og þættir sem varða stýringu upplýsinga- og fjarskiptatækniáhættu undanskildir en um þá þætti á reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að gilda, sbr. a-liður.

Um 3. tölul. Um er að ræða innleiðingu á breytingu á 18. gr. tilskipunar Evrópuþingsins og ráðsins 2011/61/ESB frá 8. júní 2011 um rekstraraðila sérhæfða sjóða og um breytingu á tilskipunum 2003/41/EB og 2009/65/EB og reglugerðum (EB) nr. 1060/2009 og (ESB) nr. 1095/2010 en tilskipunin var innleidd hér á landi með lögum um rekstraraðila sérhæfða sjóða, nr. 45/2020. Lagt er til að tilgreint verði að eftirlit og öryggisráðstafanir með rafrænni gagnavinnslu skuli ná til net- og upplýsingakerfa sem sett eru upp og skal stjórnað í samræmi við DORA.

Um 4. tölul. Í töluliðnum eru breytingar á tilskipun 2013/36/ESB um aðgang að starfsemi lánastofnana og varfærniseftirlit með lánastofnunum og verðbréfafyrirtækjum, sem er oft

nefnd CRD IV, færðar inn í lög um fjármálafyrirtæki, nr. 161/2002. Byggðastofnun og Lánasjóður sveitarfélaga ohf. eru ekki undanþegin gildissviði 50. og 78. gr. g og ber, eins og hingað til, að stýra rekstraráhættu sinni í samræmi við efni þeirra að teknu tilliti til undanþágu frá gildissviði DORA, sbr. 12. gr. frumvarpsins.

Í a-lið er lagt til að 1. mgr. 50. gr. laganna taki breytingum til samræmis við breytingar á 1. mgr. 74. gr. CRD IV eins og ákvæðinu er breytt með 2. tölul. 4. gr. DORA-tilskipunarinnar. Kveðið verði á um að fjármálafyrirtæki skuli hafa traust fyrirkomulag stjórnarhátta og innra eftirlitskerfi hvað viðkemur net- og upplýsingakerfum, sem sett eru upp og stjórnað er í samræmi við DORA, líkt og öðrum þáttum sem þegar er kveðið er á um í ákvæðinu. Eins og ákvæði DORA fela í sér skal áhersla ekki síst lögð á skýrt stjórnskipulag með vel skilgreindri, gagnsærri og samræmdri skiptingu ábyrgðar, skilvirku ferli til að sannreyna, stjórna, fylgjast með og tilkynna um áhættu sem fjármálafyrirtæki eru eða kunna að vera óvarðar fyrir.

Í b-lið er lögð til breyting á 2. mgr. 78. gr. g í samræmi við breytingar sem gerðar eru á 2. mgr. 85. gr. CRD IV með 3. tölul. 4. gr. DORA-tilskipunarinnar. Ítarlegri kröfur eru gerðar um viðbragðsáætlanir og áætlun um rekstrarsamfellu, sér í lagi viðbragðs- og endurheimtaráætlanir fyrir þá upplýsinga- og fjarskiptatækni sem notuð er í starfsemi fjármálafyrirtækis, í samræmi við DORA. Markmiðið er að lágmarka röskun á starfsemi og tap sem verður vegna slíkrar röskunar.

Í c-lið er lögð til breyting á 3. mgr. 80. gr. laganna í samræmi við 4. tölul. 4. gr. DORA-tilskipunarinnar sem breytir 1. mgr. 97. gr. CRD IV. Þannig skal Fjármálaeftirlitið við könnun og mat skv. 2. mgr. 80. gr. laga nr. 161/2002 m.a. leggja áherslu á þá áhættu sem prófanir á stafrænum viðnámsþrótti í samræmi við IV. kafla DORA leiða í ljós.

Að því er varðar breytingu á vi. lið a-liðar 3. mgr. 65. gr. CRD IV með DORA-tilskipuninni vísast til 9. gr. laga nr. 87/1998, um opinbert eftirlit með fjármálastarfsemi. Skv. 3. mgr. 9. gr. er einstaklingum og lögaðilum skylt að láta Fjármálaeftirlitinu í té allar upplýsingar og gögn sem það telur nauðsynleg í tengslum við eftirlit og athuganir mála samkvæmt ákvæðum sérlaga og getur Fjármálaeftirlitið kallað einstaklinga til skýrslugjafar í því skyni. Skiptir ekki máli í því sambandi hvort upplýsingarnar varða þann aðila sem beiðninni er beint til eða þau skipti annarra aðila við hann er hann getur veitt upplýsingar um og varða athuganir og eftirlit Fjármálaeftirlitsins. Ákvæði 9. gr. laga nr. 87/1998 gildir m.a. um þriðju aðila sem veita lánastofnunum upplýsinga- og fjarskiptatækniþjónustu, með vísan til V. kafla DORA.

Um 5. tölul. Með ákvæðinu eru lagðar til breytingar á lögum um markaði fyrir fjármálagerninga, nr. 115/2021, vegna breytinga á tilskipun Evrópuþingsins og ráðsins 2014/65/ESB frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á tilskipun 2002/92/EB og tilskipun 2011/61/ESB (MiFID II) og reglugerð Evrópuþingsins og ráðsins (ESB) nr. 600/2014 frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á reglugerð (ESB) nr. 648/2012 (MiFIR) samkvæmt DORA-tilskipuninni og -reglugerðinni.

Í a-lið er lagt til að breytingum á MiFIR með 62. gr. DORA verði veitt lagagildi.

Í b-lið eru lagðar til breytingar á 21. gr. laganna í þremur liðum í samræmi við 1. tölul. 6. gr. DORA-tilskipunarinnar, en með ákvæðinu voru innleiddar hér á landi 4. og 5. mgr. 16. gr. MiFID II. Þannig er í fyrsta lagi lögð til breyting á orðalagi 3. mgr. ákvæðisins sem felur í sér að verðbréfafyrirtæki noti viðeigandi kerfi til að tryggja að fjárfestingarþjónusta og fjárfestingarstarfsemi sé samfelld og reglubundin, þ.m.t. með upplýsinga- og fjarskiptatæknikerfi sem sett eru upp og stjórnað í samræmi við 7. gr. DORA, og hafi til þess viðeigandi og hæfileg tilföng og verklag. Í öðru og þriðja lagi er lagt til að breytt orðalag 5. og 6. mgr. ákvæðisins taki breytingum í samræmi við auknar kröfur um stafrænan viðnámsþrótt með DORA þegar kemur að verkferlum um áhættumat og öryggisferla til að tryggja öryggi og

sannvottun aðferða til að senda upplýsingar, draga úr hættu á spillingu gagna og óheimiluðum aðgangi og koma í veg fyrir leka upplýsinga og tryggja leynd gagna.

Í c-lið er lagt til breytt orðalag 1. mgr. 25. gr. laganna í samræmi við a-lið 2. tölul. 6. gr. DORA-tilskipunarinnar, sem breytir 1. mgr. 17. gr. MiFID II. Þannig skal verðbréfafyrirtæki sem stundar algrímsviðskipti tryggja að viðskiptakerfi þess séu álagsþolin og búi yfir nægilegri getu í samræmi við kröfur DORA um stafrænan viðnámsþrótt. Þá skuli verðbréfafyrirtækið hafa til staðar stefnu og áætlanir um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlanir fyrir upplýsinga- og fjarskiptatæknikerfi sem komið er á í samræmi við DORA. Jafnframt skal verðbréfafyrirtækið tryggja að kerfin séu prófuð að fullu í samræmi við II. og IV. kafla DORA. Ekki er þörf á lagabreytingu vegna b-liðar 2. tölul. 6. gr. DORA-tilskipunarinnar, sem varðar gerð tæknistaðla.

Í d-lið eru lagðar til tvær breytingar á 1. mgr. 78. gr. laganna, sem kveður á um kröfur til skipulegs markaðar um stýringu upplýsinga- og fjarskiptatækniáhættu, í samræmi við a- og b-lið 3. tölul. 6. gr. DORA-tilskipunarinnar um breytingar á 1. mgr. 47. gr. MiFID II.

Í e-lið er lagt til að breyting verði á 1. mgr. 83. gr. laganna, um kröfur til skipulegs markaðar um að koma á og viðhalda stafrænum viðnámsþrótti sínum, til samræmis við orðalag a-liðar 4. tölul. 6. gr. DORA-tilskipunarinnar um breytingu á 1. mgr. 48. gr. MiFID II.

Loks er í f-lið lögð til breyting á 1. málsl. 1. mgr. 85. gr. laganna til að innleiða b-lið 4. tölul. DORA-tilskipunarinnar, sem breytir 6. mgr. 48. gr. MiFID II. Þannig þurfi prófunarumhverfi á algrími sem skipulegur markaður skal bjóða upp á að taka mið af kröfunum sem mælt er fyrir um í II. og IV. kafla DORA. Ekki er þörf á lagabreytingu vegna c-liðar 4. tölul. 6. gr. DORA-tilskipunarinnar, sem varðar gerð tæknistaðla.

Um 6. tölul. Í töluliðnum er lagt til að breytingar á tilskipun (ESB) 2015/2366, oft nefnd PSD II, verði færðar inn í lög um greiðsluþjónustu, nr. 114/2021.

Í a-lið eru lagðar til tvær orðalagsbreytingar á 10. tölul. 1. mgr. 2. gr. laganna sem undanþiggur tiltekna þjónustu gildissviði þeirra, í samræmi við 1. tölul. 7. gr. DORA-tilskipunarinnar, sem breytir j-lið 3. gr. PSD II. Annars vegar er tilvísun bætt við til traustþjónustu og hins vegar er hugtakanotkun samræmd DORA, þ.e. vísað til upplýsinga- og fjarskiptatækniþjónustu.

Í b-lið eru lagðar til breytingar í fjórum liðum á 1. mgr. 4. gr. laganna í samræmi við 2. tölul. 7. gr. DORA-tilskipunarinnar sem varða umsóknir til að öðlast starfsleyfi sem greiðslustofnun hér á landi, sbr. 5. gr. PSD II. Breytingarnar miða að því að samþætta kröfur til umsækjenda um starfsleyfi sem greiðslustofnun efni DORA, enda falla slíkir aðilar á fjármálamarkaði undir gildissvið DORA.

Í 1. tölul. b-liðar er lagt til að innleidd verði breyting á f-lið 1. mgr. 5. gr. PSD II, sbr. ii-lið 2. tölul. 7. gr. DORA-tilskipunarinnar. Á meðal þess sem koma skal fram í umsókn um starfsleyfi til Fjármálaeftirlitsins samkvæmt tillögu að breyttum 10. tölul. 1. mgr. 4. gr. laga nr. 114/2021 er lýsing á fyrirkomulagi skýrslugjafar um atvik sem tekur tillit til tilkynningarskyldu greiðslustofnunar skv. III. kafla DORA.

Í 2. tölul. b-liðar er lagt til að innleidd verði breyting á e-lið 1. mgr. 5. gr. PSD II, sbr. i-lið 2. tölul. 7. gr. DORA-tilskipunarinnar. Í umsókn um starfsleyfi sem greiðslustofnun skal fyrirkomulagi stjórnarhátta og innri eftirlitskerfum umsækjanda lýst, þar á meðal aðferðum við áhættustýringu og fyrirkomulagi um notkun upplýsinga- og fjarskiptatækniþjónustu í samræmi við DORA, sbr. tillaga að breyttum 11. tölul. 1. mgr. 4. gr. laga nr. 114/2021.

Í 3. tölul. b-liðar er lagt til að innleidd verði breyting á h-lið 1. mgr. 5. gr. PSD II, sbr. iii-lið 2. tölul. 7. gr. DORA-tilskipunarinnar. Í umsókn um starfsleyfi sem greiðslustofnun skal

umsækjandi lýsa fyrirkomulagi rekstrarsamfellu, ekki síst að því er varðar upplýsinga- og fjarskiptatækni í samræmi við kröfur DORA, sbr. tillaga að breyttum 14. tölul. 1. mgr. 4. gr. laga nr. 114/2021.

Í 4. tölul. b-liðar er lagt til að innleidd verði breyting á þriðju undirgrein 1. mgr. 5. gr. PSD II, sem innleidd var hér á landi í 16. tölul. 1. mgr. 4. gr. laga nr. 114/2021. Umsækjandi um starfsleyfi skal þannig m.a. sýna fram á að öryggisráðstafanir í fyrirhugaðri starfsemi séu í samræmi við kröfur DORA.

Í c-lið er lagt til breytt orðalag 1. málsl. 2. mgr. 18. gr. laga nr. 114/2021, sem fjallar um útvistun mikilvægra rekstrarþátta í samræmi við DORA og tekur mið af 3. tölul. 7. gr. DORA-tilskipunarinnar, sem breytir annarri undirgrein 6. mgr. 19. gr. PSD II.

Í d-lið er lagt til að við 99. gr. laga nr. 114/2021 bætist ný málsgrein, sem verður 2. mgr., í samræmi við 4. tölul. 7. gr. DORA-tilskipunarinnar sem kveður á um að ákvæði 1. mgr. 95. gr. PSD II, sem innleidd var hér á landi í 1. mgr. 99. gr. laganna, hafi ekki áhrif á framkvæmd II. kafla DORA. Með breytingunni er áréttað að ákvæði DORA gildi um lánastofnanir, rafeyrisfyrirtæki, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur, greiðslustofnanir með takmarkað starfsleyfi og rafeyrisfyrirtæki með takmarkað starfsleyfi.

Þá er í e-lið er lagt til að nýjum málslið verði bætt við 1. mgr. 100. gr. laga nr. 114/2021 í samræmi við 5. tölul. 7. gr. DORA-tilskipunarinnar, sem breytir 96. gr. PSD II. Ákvæðið, sem innleitt var með 100. gr. laganna, kveður á um tilkynningarskyldu um rekstrar- eða öryggisfrávik. Ákvæði DORA sem varða sambærilega tilkynningarskyldu skulu þannig ganga framar 100. gr. laga nr. 114/2021 að því er varðar þá flokka greiðsluþjónustuveitanda sem taldir eru upp í nýjum 2. málsl. 1. mgr. 100. gr., enda gildi DORA um þá, sbr. fyrirhuguð lög um stafrænan viðnámsþrótt fjármálamarkaða. Til skýringar eru lokaorð 1. málsl. aðlöguð að nýmæli 2. málsl.

Loks er í f-lið um breytingar á tilvísunum til 99. gr. í tveimur ákvæðum laga nr. 114/2021 að ræða, vegna breytingarinnar sem lögð er til í d-lið.

Um 7. tölul. Lagt er til að tekið verði af skarið um lagaskil að því er varðar tilkynningarskyldu 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 samkvæmt DORA-reglugerðinni, sbr. fyrirhuguð lög um stafrænan viðnámsþrótt fjármálamarkaðar, sem hins vegar verður skylt að áframmiðla þeim tímanlega til netöryggissveitar Fjarskiptastofu ef við á. Vísast til fyrri umfjöllunar um þetta, m.a. kafla 3.3 og um 3. gr. frumvarpsins.

Um 8.–11. tölul. Í töluliðunum er lagt til að færðar verði í lög breytingar á reglugerðum sem leiðir af DORA-reglugerðinni, sbr. 59.–61. og 63. gr. hennar. Þetta leiðir til breytinga á lögum um lánshæfismatsfyrirtæki, nr. 50/2017, lögum um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár, nr. 15/2018, lögum um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga, nr. 7/2020, og lögum um fjárhagslegar viðmiðanir, nr. 7/2021.

Um 12. tölul. Lagt er til að nýmæli verði fundinn staður í lögum um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, um rekstraráhættu. Sem kunnugt er falla innlendir lífeyrissjóðir ekki undir evrópskt regluverk um starfstengda eftirlaunasjóði og þar með ekki undir gildissvið DORA eins og það er skilgreint í reglugerðinni. Í tillögunni felst að þau ákvæði DORA sem við eiga nái einnig til lífeyrissjóða á grundvelli nýmælis í lögum nr. 129/1997.

Tímabært þykir að endurmeta kröfur gildandi laga í þessum efnum til lífeyrissjóða, eins og annarra aðila á fjármálamarkaði. Með því að sambærilegar kröfur gildi um helstu aðila á fjármálamarkaði, þ.m.t. lífeyrissjóði, þannig að sambærilegir áhættuþættir séu meðhöndlaðir eins, er stuðlað að aukinni tiltrú á fjármálakerfið og stöðugleika þess. Það er í samræmi við markmið DORA sem m.a. á að stuðla að því að draga úr flækjustigi í framkvæmd, auka samræmi í eftirliti og réttarvissu. Lífeyrissjóðir eru mikilvægir þátttakendur á öllum mörkuðum hér á landi. Tillagan er gerð með hagsmuni sjóðfélaga í huga.

Ekki er fjallað sérstaklega um rekstraráhættu í efnisákvæðum laga nr. 129/1997, þó svo að skýrt orðalag 36. gr. e laganna um áhættustýringu nái ljóslega til þeirrar tegundar áhættu, enda er fjallað um rekstraráhættu í reglugerð um eftirlitskerfi með áhættu lífeyrissjóða, nr. 590/2017. Ógnir við net- og upplýsingaöryggi eru ein tegund rekstraráhættu. Skökku þykir skjóta við að fella inn í lögin sérákvæði um slíkar ógnir, án þess að tæpa á rekstraráhættu almennt. Við útfærslu almenns málsliðar um rekstraráhættu er lagt til að horft verði til nærtækrar fyrirmyndar í 78. gr. g laga um fjármálafyrirtæki, nr. 161/2002, og þykir ekki um íþyngjandi eða auknar kröfur að ræða með vísan í framanritað. Lagt er til að í 1. mgr. nýrrar 36. gr. g verði kveðið á um að lífeyrissjóður skuli hafa stefnu og ferla til að meta og stýra rekstraráhættu, þ.m.t. vegna útvistunar og fátíðra atburða sem geta haft alvarlegar afleiðingar. Skv. 8. og 9. tölul. 3. mgr. 29. gr. laga nr. 129/1997 annast stjórn lífeyrissjóðs m.a. þau verkefni að móta innra eftirlit lífeyrissjóðsins og skjalfesta eftirlitsferla, svo og að setja áhættustefnu og móta eftirlitskerfi með áhættu sjóðsins, sbr. 36. gr. e. Eðli máls samkvæmt rúmast áhættustýring vegna rekstraráhættu, þ.m.t. stafræns viðnámsþróttar, innan þeirra.

Í 2. mgr. nýrrar greinar í lögum nr. 129/1997, um rekstraráhættu, er lagt til að öll helstu ákvæði DORA um stýringu upplýsinga- og fjarskiptatækniáhættu skuli gilda gagnvart lífeyrissjóðum. Nánar tiltekið er um að ræða 5.–14. gr. um áhættustýringu, 17. gr. og 1. og 2. mgr. 18. gr. um stjórnun og flokkun atvika og 24.–30. gr. um prófanir og stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila. Þá er í 2. mgr. nýrrar 36. gr. g gert ráð fyrir að 1. mgr. 22. gr. DORA gildi um endurgjöf frá Fjármálaeftirlitinu við móttöku tilkynninga gagnvart lífeyrissjóðum. Ráðstafanir lífeyrissjóða til að stuðla að stafrænum viðnámsþrótti sínum skulu taka mið af stærð og heildaráhættusniði lífeyrissjóðsins og þar með meðalhófsreglu DORA, sbr. 4. gr. reglugerðarinnar.

Í 3. mgr. er gert ráð fyrir að um lífeyrissjóði með færri sjóðfélaga en 100 fari skv. 16. gr. DORA, um einfaldaðan áhættustýringarramma, í stað 5.–14. gr. DORA. Þetta er sama undanþága og við á um starfstengda eftirlaunasjóði samkvæmt umræddu ákvæði DORA. Tveir íslenskir lífeyrissjóðir myndu falla undir þessa málsgrein miðað við núverandi stöðu.

Í 4. mgr. er lagt til að kveðið verði á um skyldu lífeyrissjóða til að tilkynna Fjármálaeftirlitinu um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir, sbr. 1. og 2. mgr. 19. gr. DORA. Um slíkar tilkynningar fer skv. 3.–5. mgr. 19. gr. DORA, sem kveða á um upplýsingaskyldu gagnvart viðskiptavinum (sjóðfélögum í tilviki lífeyrissjóða) í tilviki alvarlegra atvika og þrískipta skýrslugjöf og ábyrgð á uppfyllingu tilkynningarskyldu um atvik hvað sem líður mögulegri útvistun, sbr. kafla 3.2.c í greinargerð. Í lokamálslið 4. mgr. er gert ráð fyrir að kveðið verði á um skyldu Fjármálaeftirlitsins til að áframmiðla upplýsingum um alvarleg atvik eða ógnar til annarra innlendra stjórnvalda, ekki síst netöryggissveitar CERT-ÍS, ef við á, í því skyni að stuðla sem best að því að fyrirbyggja og draga úr áhættu, ógnum og atvikum í íslensku netumdæmi.

Í 5. mgr. er lagt til að sett lög geri ráð fyrir mögulegri aðild lífeyrissjóða að fyrirkomulagi upplýsingaskipta vegna upplýsinga og greiningargagna um netógnir skv. 45. gr. DORA. Lífeyrissjóðir hafa ekki síður hagsmuni af aðgangi að slíkum upplýsingum en aðrir aðilar á fjármálamarkaði.

Loks er í 6. mgr. gert ráð fyrir reglusetningarheimild til handa Seðlabankanum, sem gerir honum m.a. kleift að kveða á um gildi tæknistaðla sem settir hafa verið og/eða verða settir á grundvelli DORA gagnvart lífeyrissjóðum, eftir því sem við á, svo sem um stýringu á upplýsinga- og fjarskiptatækniáhættu, flokkun og tilkynningar um atvik, prófanir og stýringu upplýsinga og fjarskiptatækniáhættu vegna þriðju aðila. Viðeigandi er að þess verði gætt við framkvæmd nýrrar 36. gr. g að hugsanlegar breytingar á stöðluðum formum/sniðmátum eftirlitsaðila vegna upplýsingamiðlunar af hálfu lífeyrissjóða frá því sem nú tíðkast, í tengslum við eftirlit með rekstraráhættu þeirra, leiði ekki til mikils kostnaðarauka. Kostnaði við breytingar vegna skýrsluskila verði að minnsta kosti haldið í lágmarki. Gert er ráð fyrir að viðmiðunarreglur, sem útfæra nánar ákvæði DORA sem lífeyrissjóðir falla undir, muni jafnframt ná til þeirra. Fjármálaeftirlitið hefur jafnframt heimild til útgáfu leiðbeinandi tilmæla á grundvelli 2. mgr. 8. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998.

Af framangreindu leiðir að ekki er gert ráð fyrir að ákvæði DORA um miðlun upplýsinga sem veittar eru lögbæru yfirvaldi til evrópskra eftirlitsstofnana gildi um lífeyrissjóði. Þá er undanskilinn II. þáttur V. kafla DORA, en með honum er komið á sameiginlegum eftirlitsramma með sérstaklega tilnefndum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, enda falla innlendir lífeyrissjóðir ekki undir gildissvið reglugerðarinnar eins og hún var samþykkt og gildir á Evrópska efnahagssvæðinu og svigrúm er ekki til staðar til að bæta við efni hennar. Loks er ekki gert ráð fyrir að viðurlagaheimildir samkvæmt fyrirhuguðum lögum um stafrænan viðnámsþrótt fjármálamarkaðar gildi gagnvart lífeyrissjóðum, heldur gildandi ákvæði laga nr. 129/1997.

Tillagan byggist á sjónarmiðum um að kröfur DORA sem stuðla eiga að stafrænum viðnámsþrótti eigi ekki síður við þá en aðra aðila á fjármálamarkaði, enda byggist hún í meginatriðum á alþjóðlega almennt viðurkenndum viðmiðum um bestu framkvæmd.

Með frumvarpi þessu er lagt til að DORA-reglugerðin verði innleidd með tilvísunaraðferð, þar sem taka ber EES-reglugerðir upp í landsrétt sem slíkar skv. a-lið 7. gr. EES-samningsins. Því þykir rétt að kveða á um þetta í hlutaðeigandi sérlögum, auk þess sem talið er aðgengilegra fyrir lífeyrissjóði að þessa sé getið í meginlöggjöfinni um starfsemi þeirra. Ekki er gert ráð fyrir frekari breytingum á lögum nr. 129/1997 með frumvarpinu.