ÁFORM UM LAGASETNINGU

– sbr. samþykkt ríkisstjórnar frá 10. mars 2017, 1.-4. gr.

Málsheiti og nr.	Frumvarp til laga um stafrænan viðnámsþrótt fjármálamarkaðar / FJR23030021
Ráðuneyti /verkefnisstjóri	Fjármála- og efnahagsráðuneyti / Sigríður Rafnar Pétursdóttir
Innleiðing EES-gerðar?	☒ Já ☐ Nei
Dags.	28. júní 2023

A. Úrlausnarefni

1. Forsaga máls og tilefni

Frumvarpið mun fela í sér innleiðingu í íslenskan rétt á reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 um stafrænan viðnámsþrótt fjármálamarkaðar (e. regulation on **d**igital **o**perational **r**esilience for the financial sector eða DOR-Act, hér eftir **DORA**) og um breytingar á ýmsum gildandi reglugerðum.[1] Ennfremur verða innleidd hér á landi með frumvarpinu ákvæði tilskipunar Evrópuþingsins og ráðsins (ESB) 2022/2556 um breytingar á ýmsum gildandi tilskipunum að því er varðar stafrænan viðnámsþrótt (eða áfallaþol) fjármálamarkaðar.[2]

DORA var samþykkt í árslok 2022 en kemur ekki til framkvæmda í aðildarríkjum ESB fyrr en í ársbyrjun 2025. Hún tilheyrir svonefndum *stafrænum fjármálapakka ESB* sem fyrst var kynntur árið 2020, líkt og reglugerð ESB um skipulag til reynslu fyrir innviði markaða sem byggjast á dreifðri færsluskrártækni (DLT)[3] og nýsamþykkt reglugerð um markaði sýndareigna[4] (MiCA). Stafræna fjármálapakkanum er ætlað að stuðla að því að umgjörð fjármálamarkaða mæti nútímaþörfum, samkeppni og nýsköpun verði efld frekar, auk þess sem hugað er að neytendavernd, net- og upplýsingaöryggi, svo og fjármálastöðugleika.

Í DORA er hugtakið ‘stafrænn viðnámsþróttur’ (e. *digital operational resilience*) í forgrunni. Aðilar á fjármálamarkaði skulu haga starfsemi sinni þannig að virk og viðeigandi áhættustýring tengd notkun net- og upplýsingatækniþjónustu sé viðhöfð í því skyni að stuðla að öflugum stafrænum viðnámsþrótti. Hugtakið er skilgreint þannig:

„Geta aðila á fjármálamarkaði til að byggja upp, viðhalda og endurmeta rekstrarlegan heilleika og áreiðanleika sinn með því að tryggja, hvort heldur beint eða óbeint með notkun þjónustu á vegum utanaðkomandi tækniþjónustuveitanda, alla þá getu sem byggir á net- og upplýsingatækni og þörf er til að tryggja öryggi net- og upplýsingakerfa og styðja við samfellda veitingu og gæði fjármálaþjónustu, þar á meðal til að takast á við þjónusturof“. [5]

[1] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (*DORA-reglugerðin* eða *DORA*).
[2] Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (*DORA-tilskipunin*).
[3] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) 909/2014 and Directive 2014/65/EU.
[4] Regulation (EU) 2023/1114 of the European Parliament and of the of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
[5] E. The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions (1. tölul. 3. gr.).

Í stuttu máli eru helstu efnisatriði DORA eftirtalin:

- Samræmdar meginreglur og kröfur til umgjarðar áhættustýringar aðila á fjármálamarkaði að því er varðar net- og upplýsingaöryggi (öll starfsemi sem byggir á notkun net- og upplýsingatækni).
- Tilkynningaskylda er samræmd að því er varðar alvarleg atvik (og áhættu) í/tengd net- og upplýsingakerfum og krafa gerð um skráningu og flokkun allra atvika. Áætlanir um samfelldan rekstur og viðbúnað skulu skjalfestar og hugað skal að viðeigandi forvörnum. Þá er í DORA gert ráð fyrir miðlægri söfnun upplýsinga um alvarleg atvik á öllu Evrópska efnahagssvæðinu og miðlun upplýsinga þar um svo draga megi lærdóm af atvikum og efla enn frekar þekkingu og viðbragð við mögulegum ógnum.
- Skylda til einfaldra eða ógnamiðaðra netöryggisprófana (e. threat-led penetration testing, TLPT) sem stuðla eiga að bættu áfallaþoli innviða ólíkra aðila á fjármálamarkaði. Ríkar kröfur eru gerðar til fyrirtækja sem framkvæma slíkar netöryggisprófanir.
- Meginreglur eru settar fram í reglugerðinni um vöktun áhættu sem steðjað getur að fyrirtæki á fjármálamarkaði frá þriðja aðila (ytri tækniþjónustuveitendum).[6] Ítarlegar kröfur eru þannig gerðar til samninga um slíka aðkeypta þjónustu, þar á meðal að því er varðar undirbúning/valferli fyrir samningsgerð um kaup á þjónustu af ytri tækniþjónustuveitendum og svigrúm til útgöngu úr slíku samningssambandi (e. exit strategy). Áætlanir skulu vera til staðar er miða að því að viðhalda samfelldum rekstri ef til flutnings eða uppsagnar þjónustu ytri tækniþjónustuveitanda kemur.
- Aðilar á fjármálamarkaði skulu uppfylla framangreindar kröfur í samræmi við meðalhófsreglu, að teknu tilliti til stærðar og áhættusniðs, eðlis, umfangs og flækjustigs þjónustu/starfsemi/rekstrar hlutaðeigandi og kerfislegs mikilvægis.
- Með DORA er komið á sameiginlegri umgjörð yfirsýnar með allra stærstu tækniþjónustuveitendum sem sérstaklega verða útnefndir sem mikilvægir á sameiginlegum innri markaði fjármálaþjónustu (e. Union Oversight Framework). Fyrir hvern mikilvægan tækniþjónustuveitanda skulu evrópsku fjármálaeftirlitsstofnanirnar útnefna einhverja úr sínum hópi sem aðal-yfirsýnaraðila (e. Lead Overseer eða LO), þ.e. ýmist EBA, ESMA eða EIOPA.[7] Tækniþjónustuveitanda sem fellur undir yfirsýn skv. DORA ber að vinna með LO í góðri trú og greiða eftirlitsgjald, en LO eru í DORA tryggðar heimildir til upplýsingaöflunar, almennra rannsókna, úttekta, útgáfu tilmæla og gerð úrbótatillagna, að viðlögðum viðurlögum sem skulu framfylgjanleg í heimaríki þjónustuveitandans (eftirfylgni lögbærra stjórnvalda). Þá er gert ráð fyrir að upplýsa megi opinberlega um bresti á samstarfsvilja eða ef ekki er farið að tilmælum LO, nema slík upplýsingagjöf teljist ósanngjörn eða geta skaðað fjármálakerfi.
- Síðast en ekki síst kveður DORA á um heimildir til miðlunar upplýsinga um ógnir og áhættu sem steðjað getur að starfsemi á fjármálamarkaði, enda sé slíkt samstarf formgert og hlíti nánar tilgreindum skilyrðum.

Gildissvið DORA-reglugerðarinnar er víðtækt. Lagt er til að eftirtaldir aðilar verði felldir undir gildissvið fyrirhugaðra laga í samræmi við 2. gr. DORA (hér eftir sameiginlega nefndir *aðilar á fjármálamarkaði*):[8]

- *lánastofnanir*, sbr. lög nr. 161/2002 um fjármálafyrirtæki,

[6] Í DORA eru hugtökin tækniþjónustuveitandi og net-/upplýsingatækniþjónusta skilgreind rúmt.

[7] Yfirsýnarfyrirkomulagið er í anda þess sem komið hefur verið á fót með SWIFT (Society for Worldwide Interbank Financial Telecommunication), þ.e. stöðluðu samskiptakerfi sem miðlun greiðslna yfir landamæri fer í gegnum víðast hvar í heiminum og hefur sérstöðu vegna mikillar útbreiðslu. Félagið er almennt skilgreint sem mikilvægur tækniþjónustuveitandi á fjármálamörkuðum, enda getur rof á tengingu við SWIFT hugsanlega valdið alvarlegri röskun í fjármálakerfum. Vegna einstakrar stöðu og víðtækrar notkunar SWIFT hafa seðlabankar tiltekinna ríkja (G10 og G20) samvinnu um yfirsýn með starfsemi SWIFT, á grundvelli alþjóðlega viðurkenndra viðmiða um bestu framkvæmd (ekki síst PFMI). Höfuðstöðvar félagsins eru í Belgíu og hefur belgíski seðlabankinn alla tíð haft forystu um sameiginlega yfirsýn með fyrirtækinu. Sjá m.a. Fjármálainnviði SÍ, 2015, bls. 29 og Fjármálainnviði SÍ, 2016, bls. 32. DORA breytir þessu fyrirkomulagi ekki.

[8] Nokkuð er um sérákvæði í DORA, sem aðeins eiga við um tilteknar tegundir aðila á fjármálamarkaði. Þá eru smærri aðilar undanþegnir vissum skyldum.

- *greiðslustofnanir* og *reikningsupplýsingaþjónustuveitendur*, sbr. lög nr. 114/2021 um greiðsluþjónustu, þó ekki póstgíróstofnanir,
- *rafeyrisfyrirtæki*, sbr. lög nr. 17/2013 um útgáfu og meðferð rafeyris,
- *verðbréfafyrirtæki*, *viðskiptavettvangar* og *veitendur gagnaskýrsluþjónustu*, sbr. lög nr. 115/2021 um markaði fyrir fjármálagerninga, þó með undantekningum,
- *verðbréfamiðstöðvar*, sbr. lög nr. 7/2020 um verðbréfamiðstöðvar, uppgjör og rafræna eignarskráningu fjármálagerninga,
- *miðlægir mótaðilar* og *afleiðuviðskiptaskrár*, sbr. lög nr. 15/2018 um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár,
- *rekstraraðilar sérhæfðra sjóða*, sbr. lög nr. 45/2020 um rekstraraðila sérhæfðra sjóða, þó með undantekningum,
- *rekstrarfélög verðbréfasjóða*, sbr. lög nr. 116/2021 um verðbréfasjóði,
- *vátrygginga-* og *endurtryggingafélög*, sbr. lög nr. 100/2016 um vátryggingastarfsemi, þó ekki félög sem undanþegin eru gildissviði laga nr. 100/2016 skv. 3. gr. þeirra,
- *vátryggingamiðlarar* og *aðilar sem dreifa vátryggingu sem aukaafurð*, sbr. lög nr. 62/2019 um dreifingu vátrygginga, þó með undantekningum,
- *stofnanir sem sjá um starfstengdan lífeyri*, sbr. lög nr. 78/2007 um starfstengda lífeyrissjóði, þó með undantekningum,
- *lánshæfismatsfyrirtæki*, sbr. lög nr. 50/2017 um lánshæfismatsfyrirtæki,
- *stjórnendur mikilvægra viðmiðana*, sbr. lög nr. 7/2021 um fjárhagslegar viðmiðanir,
- *þjónustuveitendur á sviði net- og upplýsingatækni* (skv. skilgreiningu DORA).

Ennfremur verður lagt til að eftirtaldir aðilar verði felldir undir gildissvið fyrirhugaðra laga, enda nái frumvörp sem lögð verða fram samhliða á 154. löggjafarþingi fram að ganga:

- *þjónustuveitendur hópfjármögnunar*, í merkingu reglugerðar (ESB) 2020/1503 um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki, og
- *verðbréfunarskrár*, í merkingu reglugerðar (ESB) 2017/2402 um almennan ramma fyrir verðbréfun og gerð sértæks ramma fyrir einfalda, gagnsæja og staðlaða verðbréfun.

DORA-reglugerðin gerir ráð fyrir að *þjónustuveitendur sýndareigna* falli undir gildissvið hennar, en stofnanir ESB hafa nú samþykkt reglugerð (ESB) 2023/1114 um markaði sýndareigna, MiCA.[9]

Áformað er að í frumvarpi til nýrra laga um stafrænan viðnámsþrótt fjármálamarkaðar verði gerðar sambærilegar kröfur og DORA kveður á um til innlendra *lífeyrissjóða* sem starfa á grundvelli laga nr. 129/1997 um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða. Í gildi er reglugerð um eftirlitskerfi með áhættu lífeyrissjóða, nr. 590/2017.

Unnið er að undirbúningi upptöku DORA-reglugerðarinnar (ESB) 2022/2554 í EES-samninginn. Bæði DORA-reglugerðin og tilskipun (ESB) 2022/2556 (DORA-tilskipunin) breyta ýmsum þegar gildandi reglugerðum og tilskipunum á fjármálamarkaði. Vikið er að rekstraráhættu (þ.m.t. net- og upplýsingaöryggi) í ýmsum gildandi lögum,[10] sem eiga það sameiginlegt að fela í sér innleiðingu á EES-reglum og munu þeir lagabálkar taka breytingum til samræmis við ákvæði DORA-reglugerðarinnar og -tilskipunarinnar.

Hugtakið rekstraráhætta (e. operational risk) felur ekki aðeins í sér mögulegan tæknilegan vanda sem getur átt rætur að rekja til árásar á net- og upplýsingakerfi eða veikleika í kerfunum, heldur getur slíkur vandi líka stafað af hugsanlegum mannlegum mistökum, svikum, skorti á starfsfólki eða þekkingu, eða náttúruhamförum. Í gildi eru leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila og nr. 6/2014 um útvistun hjá eftirlitsskyldum aðilum, auk þess sem Seðlabankinn tekur upp, birtir og fylgir eftir ýmsum

[9] Sbr. nmgr. 4.
[10] Til dæmis er vikið að rekstraráhættu í lögum nr. 161/2002 um fjármálafyrirtæki, lögum nr. 100/2016 um vátryggingastarfsemi og lögum nr. 114/2021 um greiðsluþjónustu.

viðmiðunarreglum evrópsku fjármálaeftirlitsstofnananna sem snertiflöt hafa við rekstraráhættu aðila á fjármálamarkaði, s.s. viðmiðunarreglur evrópsku eftirlitsstofnananna varðandi stjórnun áhættu vegna upplýsinga- og samskiptatækni og öryggisáhættu.

Með lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða var innleidd hér á landi fyrsta netöryggistilskipun (ESB) 2016/1148 eða NIS1. Þau kveða á um samræmdar lágmarkskröfur þvert á mikilvæga geira samfélagsins að því er varðar áhættustýringu og viðbúnað. Að því marki sem sérlög geyma ítarlegri reglur ganga þau þó framar lágmarkskröfum laga nr. 78/2019 og reglugerða settum á grundvelli þeirra. Lög nr. 78/2019 kveða einnig á um tilkynningaskyldu um atvik/áhættu til netöryggissveitar Fjarskiptastofu (CERT-ÍS). CERT-ÍS er sem landsbundnu öryggis- og viðbragðsteymi ætlað að takmarka útbreiðslu/smitáhrif og tjón af völdum atvika eins og kostur er, fyrirbyggja og draga úr hættu á netárásum í netumdæmi Íslands. Kerfislega mikilvægu bankarnir þrír og kauphöllin falla undir gildissvið laga nr. 78/2019 sem rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða samkvæmt útnefningu Fjármálaeftirlitsins á grundvelli gildandi viðmiða í reglugerð,[11] sbr. auglýsingu í B-deild Stjórnartíðinda.[12] Framangreindir aðilar, ásamt öðrum mikilvægum innviðum í skilningi þeirra laga, fjarskiptafyrirtækjum og Stjórnarráði Íslands, njóta þjónustu CERT-ÍS á grundvelli laga nr. 78/2019, en allir geta leitað til hennar um aðstoð. Ef þörf krefur er CERT-ÍS heimilt að forgangsraða í starfsemi sinni þannig að brugðist sé við tilkynningum um atvik eða áhættu frá lögbundnum þjónustuhópum sveitarinnar áður en brugðist er við upplýsingum eða tilkynningum frá öðrum.[13]

Samhliða samþykkt DORA var NIS1 tilskipunin endurnýjuð í heild sinni með NIS2[14] og er gildissvið hennar mun víðtækara en þeirrar fyrri. Í 2. mgr. 1. gr. DORA er skilmerkilega tekið af skarið um að efnisákvæði hennar teljist sérlög (e. sector-specific Union legal act) og ganga þar með framar efnisreglum NIS2 að því er varðar aðila á fjármálamarkaði sem skilgreindir verða að landslögum á grundvelli NIS2 sem ómissandi eða mikilvægir (e. essential or important entities).

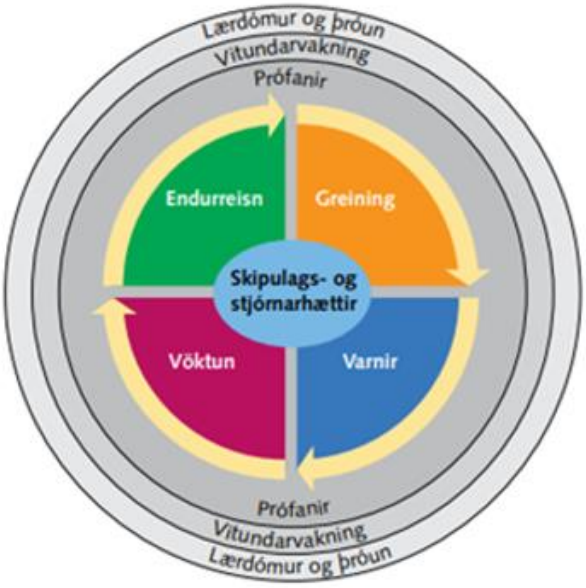
Samkvæmt 19. gr. DORA skulu *alvarleg atvik* tengd net- og upplýsingakerfum aðila á fjármálamarkaði tilkynnt lögbæru stjórnvaldi (hér Fjármálaeftirliti Seðlabanka Íslands, sjá og 46. gr. DORA), en valkvætt er að tilkynna um *áhættu*. DORA rúmar áframmiðlun tilkynninga til annarra viðeigandi stjórnvalda (t.d. Fjarskiptastofu/CERT-ÍS).

Samkvæmt 22. gr. DORA skulu lögbær stjórnvöld (hér Fjármálaeftirlit Seðlabanka Íslands) staðfesta móttöku tilkynninga. Lögbæru stjórnvaldi er ennfremur heimilt að bregðast með viðeigandi hætti við tilkynningu, s.s. með almennum leiðbeiningum um mögulegar ráðstafanir, gera aðgengilegar upplýsingar um/tengdar tilteknum tegundum ógna/atvika eða ræða mótvægisaðgerðir og aðferðir til að lágmarka tjón þvert á fjármálakerfið. Sérhver aðili er þó ávallt ábyrgur fyrir þeim aðgerðum sem gripið er til.

Með fyrirhuguðu frumvarpi til innleiðingar á DORA verður tekið mikilvægt skref í að samræma lagakröfur til ólíkra aðila á fjármálamarkaði að því er áhættustýringu og viðbúnað varðar. Áfallaþol net- og upplýsingakerfa þeirra og geta til endurreisnar fjármálaþjónustu ef til rofs kemur eru samfélaginu mikilvæg. Ör þróun í tækni og viðskiptum krefst stöðugs endurmats viðbúnaðar og öryggisráðstafana af hálfu markaðsaðila, svo og stjórnvalda. Löggjöf á sviði fjármálamarkaðar byggir á samevrópsku regluverki og markmiðum um að skapa og viðhalda virku samkeppnisumhverfi, sem þó mega ekki vera á kostnað öryggissjónarmiða í tilviki

[11] Reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu.
[12] Auglýsing nr. 67/2022 um skrá yfir rekstraraðila nauðsynlegrar þjónustu.
[13] Um þjónustu og samstarf við netöryggissveit (CERT-ÍS) vísast m.a. til IV. kafla laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, 9. gr. laga nr. 75/2021 um Fjarskiptastofu og reglugerðar nr. 480/2021 um netöryggissveit Póst- og fjarskiptastofnunar (nú Fjarskiptastofa), CERT-ÍS.
[14] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

mikilvægustu innviða. Efnisreglur DORA eru í samræmi við alþjóðlega viðurkennd viðmið um bestu framkvæmd á þessu sviði sem hafa m.a. verið dregin saman með eftirfarandi myndrænum hætti, þ.e. lykilþættir áhættustýringar m.t.t. net- og upplýsingaöryggis: [15]



2. Hvert er úrlausnarefnið?

EES-gerðir ber að taka upp í landsrétt samningsaðila, sbr. a-lið 7. gr. EES-samningsins. Úrlausnarefnið er innleiðing reglugerðar (ESB) 2022/2554 og tilskipunar (ESB) 2022/2556, er varða stafrænan viðnámsþrótt fjármálamarkaðar og eru hluti af *stafrænum fjármálapakka ESB*.

Innleiðing DORA á Íslandi er skilgreind sem aðgerð á ábyrgð fjármála- og efnahagsráðuneytis í aðgerðaráætlun stjórnvalda í netöryggismálum, á grundvelli *netöryggisstefnu Íslands 2022-2037*.[16]

3. Að hvaða marki duga gildandi lög og reglur ekki til?

Með fyrirhuguðum lögum verður regluverk um áhættustýringu og viðnámsþrótt net- og upplýsingakerfa aðila á fjármálamarkaði samræmt og heildstætt. Aðeins fáir eftirlitsskyldir aðilar á fjármálamarkaði falla undir gildissvið laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019 (er fólu í sér innleiðingu á NIS1). Net- og upplýsingatækniáhætta er hratt vaxandi áhættuþáttur á fjármálamarkaði, stöðugt þarf að endurmeta og treysta varnir gegn netárásum og styrkja getu til að bregðast við alvarlegum atvikum.[17] Með frumvarpinu verða lagðar til ýmsar breytingar á gildandi lögum á fjármálamarkaði, sem þegar víkja að einhverju marki að viðnámsþrótti ólíkra aðila.

Fyrirhuguð lög munu leiða til heildstæðari og samræmdari framkvæmdar áhættustýringar í starfsemi ólíkra aðila á fjármálamarkaði, þar á meðal gagnvart ytri tækniþjónustuveitendum,[18] ásamt því að leiða til bættrar yfirsýnar og skilvirkara viðeigandi aðhalds og þar með aukinni neytendavernd og fjármálastöðugleika. Skylt verður að tilkynna Fjármálaeftirliti Seðlabanka Íslands um öll alvarleg atvik tengd net- og upplýsingakerfum í starfsemi aðila á fjármálamarkaði sem falla munu undir gildissvið fyrirhugaðra laga.

[15] Skýringarmynd byggð á leiðbeiningum CPMI/IOSCO um viðnámsþrótt fjármálainnviða gegn netárásum frá 2016 (e. Guidance on cyber resilience for financial market infrastructures). Um þær var fjallað í riti Seðlabanka Íslands, *Fjármálainnviðum*, 2018, sjá mynd I-2 (bls. 9). CPMI stendur fyrir nefnd um greiðslu- og markaðsinnviði á vegum Alþjóðagreiðslubankans (BIS) og IOSCO fyrir Alþjóðasamtök eftirlitsaðila á verðbréfamarkaði.

[16] Netöryggisstefna Íslands 2022-2037 (útgefin af háskóla-, iðnaðar- og nýsköpunarráðuneyti í febrúar 2022) og upplýsingar um aðgerðaráætlun stjórnvalda í netöryggi 2022-2027, á grundvelli stefnunnar, aðgengilegar á vef HVIN.

[17] Sbr. Stefnumarkandi áherslur við eftirlit á fjármálamarkaði 2022-2024, Seðlabanki Íslands (2022).

[18] Rétt er að vekja athygli á að ýmsar tegundir tækniþjónustuveitenda, sem aðilar á fjármálamarkaði reiða sig á, munu í framtíðinni falla undir almennar kröfur netöryggislaga, með vísan til útvíkkaðs gildissviðs NIS2. Til dæmis aðilar sem veita skýjavinnsluþjónustu og traustþjónustu, gagnaver og fjarskiptafyrirtæki.

Fyrirhuguð lög til innleiðingar DORA hér á landi munu stuðla að frekari samhæfingu innan stjórnkerfisins, öflugri öryggismenningu og vitund um áhættu og þar með viðnámsþrótti/áfallaþoli fjármálamarkaðar. Samhliða undirbúningi frumvarpsins er æskilegt að huga að snertiflötum DORA við NIS2. Hafa þarf í huga að undirbúningur upptöku NIS2 í EES-samninginn og innleiðingar í landsrétt er einnig skilgreind aðgerð í aðgerðaráætlun stjórnvalda í netöryggismálum (á ábyrgð háskóla-, iðnaðar- og nýsköpunarráðuneytisins), sem kann að krefjast endurmats á skipulagi netöryggismála eða ferlum þeim tengdum.

B. Markmið

1. Stefna hins opinbera á viðkomandi málefnasviði/málaflokki

Í stjórnarsáttmála kemur fram að ríkisstjórnin leggi áherslu á framkvæmd og þróun EES-samningsins þannig að hagsmunir og fullveldi Íslands í samstarfi og viðskiptum við önnur ríki sé tryggt. Í honum er bæði vikið að tækifærum en einnig nýjum áskorunum sem fylgja tækniþróun og stafrænni umbreytingu. Unnið verði markvisst að því að efla net- og fjarskiptaöryggi, auka traust almennings á upplýsingatækni og frekari skoðun á þeim fjölþættu ógnum sem samfélög standa frammi fyrir vegna örra tæknibreytinga o.fl. Ríkisstjórnin leggur áherslu á að öryggismál þjóðarinnar séu í traustum skorðum í samræmi við markmið þjóðaröryggisstefnu fyrir Ísland sem samþykkt er af Alþingi.[19] Hún leggur áherslu á vernd og órofa virkni þýðingarmikilla innviða og að stuðla að skilvirkum og samhæfðum aðgerðum sem miða að því að tryggja víðtæka öryggishagsmuni þjóðarinnar.

Fyrirhugað frumvarp fellur undir málefnasvið 16 um markaðseftirlit, neytendamál og stjórnsýslu atvinnumála og nýsköpunar í fjármálaáætlun, nánar tiltekið málaflokkana markaðseftirlit og neytendamál. Meginmarkmið málefnasviðsins er að auka alþjóðlega samkeppnishæfni atvinnulífs sem byggist á efnahagslegu, umhverfislegu og samfélagslegu jafnvægi. Innleiðing gerðanna sem hér um ræðir og stuðla eiga að stafrænum viðnámsþrótti fjármálakerfisins samræmist því meginmarkmiði málefnasviðsins.

2. Markmið sem að er stefnt með lagasetningu í ljósi úrlausnarefnis og stefnu stjórnvalda

Með fyrirhuguðu frumvarpi og innleiðingu DORA verður stuðlað að því að umgjörð fjármálamarkaðar mæti nútímaþörfum og net- og upplýsingaöryggi verði tryggt sem best, þar með forsendur fyrir efldri samkeppni og nýsköpun, svo og neytendavernd og fjármálastöðugleika. Virk stýring áhættu er tengist notkun net- og upplýsingatækniþjónustu í starfsemi á fjármálamarkaði og viðeigandi eftirfylgni af hálfu lögbærra stjórnvalda mun stuðla að öflugum stafrænum viðnámsþrótti (áfallaþoli) innviða og fjármálakerfisins í heild.

C. Leiðir

1. Ekkert aðhafst - hvaða afleiðingar hefði það?

Rekstraráhættu, þar á meðal net- og upplýsingaöryggi, er brýnt að gera hátt undir höfði og tryggja viðunandi auðlindir/bolmagn stjórnvalda til eftirfylgni með lagakröfum er miða að því að lágmarka hana. Verði ekkert aðhafst mun það geta haft áhrif á almenning og atvinnulíf, stöðu Íslands og íslenskra fyrirtækja á alþjóðlegum fjármálamörkuðum, auk þess sem það mun brjóta gegn skuldbindingum Íslands á grundvelli EES-samningsins.
Áhættustýring felur í sér ráðstafanir til að bera kennsl á hættu á atvikum í rekstri/starfsemi og koma í veg fyrir, greina, takast á við og lágmarka áhrif þeirra. Það á meðal annars við aðgengi að þjónustu, uppruna, réttleika og/eða trúnað um vistuð, send eða unnin gögn eða tengda þjónustu sem boðin er eða er aðgengileg um hlutaðeigandi net- og upplýsingakerfi.

2. Mögulegar leiðir við lagasetningu

Íslandi ber þjóðréttarleg skylda til að taka EES-reglugerðir sem slíkar upp í landsrétt , sbr. a-lið 7. gr. EES-samningsins. Með frumvarpinu er fyrirhugað að innleiða ákvæði DORA-

[19] Þjóðaröryggisstefnu fyrir Ísland, sem samþykkt var á Alþingi 13. apríl 2016 (þingsályktun nr. 26/145, þskj. 1166 – 327. mál á 145. lögþ.) var breytt 28. febrúar sl. (þingsályktun nr. 7/153, þskj. 1213 – 487. mál á 153. lögþ.). Heildarskjal m.áo.br. er aðgengilegt á vef Stjórnarráðsins.

reglugerðarinnar í landsrétt með tilvísunaraðferð og ákvæði tilskipunar 2022/2556 með umritun (breytingum á ýmsum lögum).

D. Hvaða leið er áformuð og hvers vegna?

1. Stutt lýsing á þeirri leið sem áformuð er og rökstuðningur fyrir henni

Lagt er til að DORA-reglugerðin verði tekin upp í íslenskan rétt með tilvísunaraðferð og þá að fullu innleidd samkvæmt orðanna hljóðan í samræmi við a-lið 7. gr. EES-samningsins, sbr. lög um Evrópska efnahagssvæðið, nr. 2/1993. DORA-tilskipunin verður innleidd með breytingum á ákvæðum ýmissa þegar gildandi laga á sviði fjármálamarkaðar.
Áformað er að fela Fjármálaeftirliti Seðlabanka Íslands eftirlit með framkvæmd fyrirhugaðra laga enda fer það almennt með eftirlit með fjármálastarfsemi, sbr. lög um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998. Gert er ráð fyrir að unnt verði að leggja á stjórnvaldssektir fyrir brot gegn ákvæðum fyrirhugaðra laga (DORA) og, eftir atvikum, beitingu annarra stjórnsýsluviðurlaga.

2. Helstu fyrirhuguðu breytingar á gildandi lögum og reglum, hvort heldur bætt er við eða fellt brott

Um ræðir frumvarp til nýrra heildarlaga um stafrænan viðnámsþrótt á fjármálamarkaði, auk þess sem gert er ráð fyrir breytingum á ýmsum lögum, sem innleiða aðrar EES-gerðir og aðlagaðar hafa verið að breyttri lagaumgjörð með DORA-reglugerðinni og -tilskipun.

E. Samræmi við stjórnarskrá og þjóðarétt – aðrar grundvallarspurningar

1. Koma áformin inn á svið stjórnarskrár og þjóðréttarskuldbindinga?

Já, um er að ræða innleiðingu í íslenskan rétt á EES-gerðum. Eftirlit með framkvæmd fyrirhugaðra laga verður aðallega í höndum Fjármálaeftirlits Seðlabanka Íslands, en DORA-reglugerðin inniheldur tilvísanir til heimilda og hlutverka evrópsku fjármálaeftirlitsstofnananna (EBA, ESMA og EIOPA), sem í tilviki EES-ríkja innan EFTA er falið Eftirlitsstofnun EFTA. Um framsal valdheimilda á fjármálamarkaði er nánar fjallað í þingsályktunartillögu um upptöku hins evrópska eftirlitskerfis á fjármálamarkaði, sem setur ramma um starfsemi þeirra, sjá og lög um evrópskt eftirlitskerfi á fjármálamarkaði, nr. 24/2017. Þá er t.d. gert ráð fyrir tilkynningaskyldu til Seðlabanka Evrópu, í tilviki atvika í rekstri lánastofnana, greiðslustofnana og rafeyrisfyrirtækja, sem kann að kalla á aðlögun við upptöku gerðarinnar. Komi til útnefningar mikilvægra tækniþjónustuveitenda á grundvelli DORA með snertiflöt við Ísland eða innlenda aðila á fjármálamarkaði getur ennfremur reynt á samevrópskt yfirsýnarfyrirkomulag (e. Union Oversight Framework, sbr. bls. 2), sem m.a. gerir ráð fyrir innheimtu eftirlitsgjalds. Ekki er talið að efni DORA gefi að öðru leyti tilefni til sérstakrar skoðunar á samræmi við stjórnarskrá.
Það athugast að í 1. gr. DORA er hefðbundinn fyrirvari varðandi eigin öryggishagsmuni aðildarríkja, enda ein af frumskyldum stjórnvalda hvers ríkis að tryggja öryggi og varnir lands og þjóðar. Þjóðaröryggisstefna fyrir Ísland er samþykkt af Alþingi. Markmið hennar er að tryggja sjálfstæði, fullveldi og friðhelgi landamæra Íslands, öryggi borgaranna og vernd stjórnkerfis og grunnvirkja samfélagsins.

2. Varða áformin ákvæði EES-samningsins um ríkisaðstoð, tæknilegar reglur um vöru og fjarþjónustu eða frelsi til að veita þjónustu?

Já. Áformin varða fjármálaþjónustu sem fellur undir 3. kafla III. hluta EES-samningsins, sbr. einnig IX. viðauka samningsins.

3. Er önnur grundvallarlöggjöf sem taka þarf tillit til?

Nei.

F. Samráð

1. Hverjir eru helstu hagsmunaaðilar?

Aðilar á fjármálamarkaði, viðskiptavinir og þjónustuveitendur þeirra, atvinnulíf og samfélag almennt.

2. Er skörun við stjórnarmálefni annarra ráðuneyta?

Fyrirhuguð lög, sem innleiða munu DORA-reglugerðina hér á landi, verða sérlög gagnvart almennri netöryggislöggjöf (sem í dag byggir á NIS1-tilskipuninni en í fyrirsjáanlegri framtíð á NIS2), þ.e. lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða. Að því marki sem þau geyma ríkari kröfur til aðila á fjármálamarkaði ganga þau framar.

DORA var samþykkt samhliða endurnýjaðri netöryggistilskipun ESB (NIS2), sem háskóla-, iðnaðar- og nýsköpunarráðuneyti undirbýr upptöku og innleiðingu á hér á landi. Stefnt er að því að upptaka og innleiðing DORA og NIS2 haldist í hendur, ef þess er kostur, í ljósi efnislegra snertiflata gerðanna og millivísana.

Tilkynningaskylda um atvik (og áhættu) skv. fyrirhuguðum DORA-lögum verður til Fjármálaeftirlits Seðlabanka Íslands. Rekstraraðilar nauðsynlegrar þjónustu á sviði bankastarfsemi og innviða fjármálamarkaða, sem útnefndir eru á grundvelli 3. gr. og 2. mgr. 11. gr. laga nr. 78/2019, verða að óbreyttum þeim lögum skyldir til að miðla tilkynningum um alvarleg atvik til bæði Fjármálaeftirlitsins og CERT-ÍS. Sömu aðilum verður ennfremur, að óbreyttum lögum nr. 78/2019, tryggð forgangsþjónusta CERT-ÍS, ef á þarf að halda (teljast til þjónustuhópa netöryggissveitar í skilningi reglugerðar nr. 480/2021).[20]

3. Samráð sem þegar hefur farið fram

Vinna við undirbúning frumvarpsins er hafin í samráði við Seðlabanka Íslands.

4. Fyrirhugað samráð

Áform um lagasetningu og drög að frumvarpi verða birt í samráðsgátt Stjórnarráðsins. Gert er ráð fyrir að fjármála- og efnahagsráðuneytið og Seðlabanki Íslands hafi samráð við innleiðingu afleiddra gerða eftir þörfum.

G. Mat á áhrifum þeirrar leiðar sem áformuð er

1. Niðurstaða frummats á áhrifum, sbr. fylgiskjal

Áhrif frumvarpsins á fjármálamarkaðinn verða jákvæð. Um ræðir frumvarp til nýrra laga um stafrænan viðnámsþrótt fjármálamarkaðar, með innleiðingu EES-gerða (DORA-reglugerð og -tilskipun), sem verða nýmæli hér á landi. Heildarlög leysa af hólmi og samræma brotakennda og ósamhæfða lagaumgjörð.

Rekstraráhættu, þar á meðal net- og upplýsingaöryggi, er brýnt að gera hátt undir höfði og tryggja viðunandi auðlindir og bolmagn stjórnvalda til eftirfylgni með lagakröfum er miða að því að lágmarka hana. Verði ekkert aðhafst mun það geta haft áhrif á almenning og atvinnulíf, stöðu Íslands og íslenskra fyrirtækja á alþjóðlegum fjármálamörkuðum (þar á meðal orðsporsáhættu/trúverðugleika), auk þess sem að það myndi brjóta í bága við skuldbindingar Íslands á grundvelli EES-samningsins.

Fyrirhuguð lagasetning mun hafa áhrif á flesta aðila á fjármálamarkaði. Áhrifin munu líklega hafa í för með sér einhvern kostnað fyrir fyrirtækin en að sama skapi ætti hún líka að efla viðnámsþrótt þeirra 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. Ekki er gert ráð fyrir fjárhagsáhrifum á ríkissjóð. Hugsanlega verður þó þörf á hækkun eftirlitsgjaldsins sem stendur undir rekstri Fjármálaeftirlitsins.

Um ræðir frumvarp til nýrra heildarlaga, ásamt breytingum á gildandi lögum, sem stuðla mun að því að umgjörð fjármálamarkaðar mæti nútímaþörfum og net- og upplýsingaöryggi verði tryggt sem best, þar með að forsendur verði fyrir efldri samkeppni og nýsköpun, svo og neytendavernd og fjármálastöðugleika. Virk stýring áhættu er tengist notkun net- og upplýsingatækniþjónustu í starfsemi á fjármálamarkaði og viðeigandi eftirfylgni af hálfu lögbærra stjórnvalda mun stuðla að öflugum stafrænum viðnámsþrótti (áfallaþoli) innviða og fjármálakerfisins í heild. Fyrirhuguð lög og undirliggjandi EES-gerð byggja á reyndum alþjóðlegum viðurkenndum viðmiðum um bestu framkvæmd. Það að tryggja framkvæmd þeirra, þvert á víðtækt gildissvið, kann að verða áskorun og því er mikilvægt að huga tímanlega að

[20] Sbr. nmgr. 13.

undirbúningi bæði gagnvart markaðsaðilum og Seðlabanka Íslands sem eftirlitsaðila/lögbæru stjórnvaldi.

H. Næstu skref, innleiðing

1. **Hefur verið gerð verkefnisáætlun fyrir frumvarpssmíðina?**

   Unnið er að frumvarpsdrögum sem ráðgert er að birta í samráðsgátt stjórnvalda fyrir lok árs 2023. Núverandi áætlanir gera ráð fyrir að framlagning frumvarps fyrir Alþingi verði möguleg á vorþingi 2024 (ella á haustþingi 2024), en tímasetning upptöku gerðanna í EES-samninginn er ekki ljós þegar þetta er ritað.

2. **Hvernig verður staðið að innleiðingu löggjafar? Hvað má gera ráð fyrir að þeir sem verða fyrir áhrifum, opinberar stofnanir/hagsmunaaðilar/almenningur, þurfi langan tíma til undirbúnings/aðlögunar?**

   Núverandi áætlanir gera ráð fyrir tillögugerð um gildistöku fyrirhugaðra laga í ársbyrjun 2025, sem er í samræmi við gildistöku DORA-gerðanna í aðildarríkjum ESB. Framvinda upptökuferlis í EES-samninginn mun þó hafa áhrif á endanlega tillögu um gildistöku þegar þar að kemur. Eftirlits- og hagsmunaaðilum á því að gefast rúmur tími til undirbúnings og aðlögunar að breyttu og ítarlegra regluverki.

3. **Hvaða forsendur þurfa að vera fyrir hendi til að lagasetning beri árangur?**

   Undirbúningstími til aðlögunar að ítarlegri lagakröfum fyrir ólíka markaðsaðila en fyrirhuguð lög munu gilda um alla aðila á fjármálamarkaði, nema þá sem falla undir undanþágu 3. mgr. 2. gr. DORA-reglugerðarinnar. Gert er ráð fyrir að Fjármálaeftirlit Seðlabanka Íslands fái tilteknar valdheimildir til framfylgdar ákvæðum laganna. Þá verður gert ráð fyrir nánari reglusetningarheimildum til handa ráðherra og Seðlabanka Íslands í frumvarpinu.

I. Annað

J. Fylgiskjöl

1. **Mat á áhrifum lagasetningar – Frummat, sbr. eyðublað.** Viðfest.
2. **Önnur fylgiskjöl eftir atvikum.** Á ekki við.