Samtök fyrirtækja í fjármálaþjónustu

Samráðsgátt
Fjármála- og efnahagsráðuneytið
Mál nr. S-146/2024

Reykjavík, 5. september 2024

Efni: Umsögn um drög að frumvarpi til laga um stafrænan viðnámsþrótt fjármálamarkaðar (innleiðing DORA)

Samtök fyrirtækja í fjármálaþjónustu (SFF) vísa til draga að frumvarpi til laga um stafrænan viðnámsþrótt fjármálamarkaðar. SFF vilja koma eftirfarandi athugasemdum og ábendingum á framfæri:

Markmið DORA regluverksins er að stuðla að stafrænum rekstrarlegum viðnámsþrótti fjármálastofnana. Þetta markmið styður við ríka almannahagsmuni. SFF fagna innleiðingu DORA regluverksins í íslensk lög. Innleiðing regluverksins í starfsemi þeirra aðila hér á landi sem falla munu undir gildissvið þess verður hins vegar áskorun, enda er regluverkið ítarlegt, flókið og matskennt. Mikilvægt er að vel takist til við þá innleiðingu. Því er brýnt að þær stofnanir sem munu annast eftirlit með framkvæmd regluverksins styðji við þá vinnu með því að veita leiðbeiningar þar að lútandi og upplýsa fyrir fram um skilning þeirra á regluverkinu og helstu áherslum í eftirliti.

Athugasemdir við einstakar greinar frumvarpsins

Í 3. gr. frumvarpsins er lagt til að ákvæði DORA reglugerðarinnar skuli hafa lagagildi hér á landi. Í athugasemd með ákvæðinu kemur m.a. fram að 12 mánaða innleiðingarfrestur eigi að vera nægur tími fyrir markaðsaðila til að undirbúa framfylgd við kröfur hennar. Ekki koma fram í frumvarpinu upplýsingar um það á hverju þessi fullyrðing er byggð. Full aðlögun markaðsaðila hér á landi að kröfum DORA verður án efa flókið og vandasamt verk. Draga má í efa að umræddur 12 mánaða frestur verði nægilegur öllum markaðsaðilum í því skyni.

Í 2. mgr. 5. gr. frumvarpsins er lagt til að Fjármálaeftirlitið og Eftirlitsstofnun EFTA annist eftirlit samkvæmt lögunum í samræmi við EES-samninginn. Hvað varðar Eftirlitsstofnun EFTA mun þetta væntanlega þýða að hún annist eftirlit á grundvelli ákvæða DORA reglugerðarinnar sem veitt verður lagagildi hér á landi, fremur en að stofnunin annist eftirlit samkvæmt þeim íslensku lögum sem sett verða til að innleiða reglugerðina. Í 3. mgr. 5. gr. frumvarpsins er fjallað um valdheimildir Eftirlitsstofnunar EFTA. Mikilvægt er að tryggja að þær séraðstæður sem íslenskir aðilar munu búa við vegna tveggja stoða kerfis EES-samningsins muni virka og verði ekki til þess að koma niður á samkeppnishæfni þeirra gagnvart keppinautum frá ESB-ríkjum.

sff@sff.is
www.sff.is

Í 7. gr. frumvarpsins er kveðið á um heimildir til eftirfylgni og birtingar ákvarðana svokallaðs aðaleftirlitsaðila. Í kafla 3.6. í frumvarpinu er að finna umfjöllun um þetta, þ.e. um ákvæði 2. þáttar V. kafla DORA sem fjalla um sameiginlegan eftirlitsramma gagnvart mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu (e. Union Oversight Framework). Fram kemur að fyrir hvern slíkan mikilvægan þriðja aðila skuli evrópsku fjármálaeftirlitsstofnanirnar útnefna einhverja úr sínum hópi sem aðaleftirlitsaðila, þ.e. ýmist EBA, ESMA eða EIOPA. Jafnframt kemur fram að 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. Í umfjöllun í greinargerð með 7. gr. frumvarpsins kemur fram að ekki þyki líklegt að íslenskur tækniþjónustuveitandi falli undir viðmið DORA í þessum efnum í næstu framtíð. Æskilegt væri að fram kæmi í frumvarpinu nánari umfjöllun um þetta og þá einkum hvaða forsendur eða aðstæður gætu leitt til þess að slíkur mikilvægur þriðji aðili hér á landi yrði útnefndur undir sameiginlega eftirlitsrammann.

Í 8. gr. frumvarpsins er fjallað um aðfararhæfi ákvarðana Eftirlitsstofnunar EFTA og dóma EFTA-dómstólsins. Í umfjöllun um þetta ákvæði í greinargerð er vísað til þess að um sé að ræða ákvarðanir Eftirlitsstofnunar EFTA og dóma og úrskurði EFTA-dómstólsins á grundvelli DORA. Ekki kemur fram í frumvarpinu nánari útskýringar á því hvaða ákvarðanir þetta gætu verið eða hvert eðli þeirra gæti verið. Þeir aðilar sem munu falla undir löggjöfina hafa hagsmuni af því að fá nánari upplýsingar um þetta.

Í 1. mgr. 10. gr. frumvarpsins er lagt til að Fjármálaeftirlitið geti lagt stjórnvaldssektir á hvern þann sem brýtur gegn stjórnvaldsfyrirmælum settum á grundvelli laganna eða nánar tilteknum ákvæðum DORA reglugerðarinnar. Í 2. mgr. 10. gr. frumvarpsins er lagt til að sektir sem lagðar eru á einstaklinga geti numið frá 100 þús. kr. til 700 millj. kr. og að sektir sem lagðar eru á lögaðila geti numið frá 500 þús. kr. til 800 millj. kr., en geti þó verið hærri eða allt að 10% af heildarveltu. Tillagan felur þannig í sér að mjög alvarleg viðurlög geti legið við brotum á ákvæðum gerðanna. Skoða þarf viðurlagarammann sem þarna er lagður til í ljósi þess að í DORA reglugerðinni er víða að finna fremur óljósa lýsingu þeirri háttsemi (verknaðarlýsingu) sem legið getur til grundvallar brotum sem geta varðað svo alvarlegum viðurlögum. Í reglugerðinni er þannig víða að finna lýsingu á háleitum markmiðum um stafrænt áfallaþol og fyrirmyndareinkennum stjórnarhátta og áhættustýringar. Dæmi um þetta eru ákvæði 1. tölul. 5. gr. (*„…innri stjórnunar- og eftirlitsramma sem tryggir skilvirka og varfærna stýringu upplýsinga- og fjarskiptatækniáhættu […] til að skapa sem mestan stafrænan rekstrarlegan viðnámsþrótt“)* og 1. tölul. 6. gr. (*„traustan, yfirgripsmikinn og vel skjalfestan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni […] sem gerir þeim kleift að bregðast við upplýsinga- og fjarskiptatækniáhættu á skjótan, skilvirkan og heildstæðan hátt og tryggja hátt stig stafræns rekstrarlegs viðnámsþróttar“*). DORA reglugerðin kveður aftur á móti að takmörkuðu leyti á um það hvaða aðgerðum og aðferðum skuli nákvæmlega beita til að ná þessum markmiðum. Því standa þeir aðilar sem falla undir gildissvið reglugerðarinnar frammi fyrir þeim vanda að ákveða og innleiða slíkar aðgerðir og aðferðir, án þess að geta að öllu leyti sótt nákvæm fyrirmæli þar að lútandi til DORA reglugerðarinnar eða undirgerða hennar. Innleiðing DORA löggjafarinnar í starfsemi þeirra sem falla undir hana verður því mikil áskorun, einkum fyrir aðila hér á landi sem verða að teljast smáir í samanburði við aðila sem starfa í öðrum EES-ríkjum. Áhættan fyrir innlenda aðila af rangri

eða ófullnægjandi innleiðingu í starfsemi sína verður því að teljast töluverð. Mikil óvissa mun t.d. ríkja um það hvort eftirlitsaðilar muni eftir á telja að innleiðing í starfsemi hafi verið fullnægjandi eða hvort viðbrögð við atvikum hafi verið eins og best var á kosið. Í ljósi þessa verður að telja óvarlegt að kveða á um svo alvarleg viðurlög sem frumvarpið gerir ráð fyrir. Þetta á ekki síst við um viðurlög gagnvart einstaklingum.

Í 18. gr. frumvarpsins er lagt til að lögin öðlist gildi 1. júlí 2025. Þetta verður að teljast stuttur frestur í ljósi umfangs og flækjustigs löggjafarinnar. Hafa verður í huga allan þann fjölda Evrópugerða sem verða hluti löggjafarinnar til viðbótar við sjálfa DORA reglugerðina.

Athugasemdir við almenna umfjöllun í greinargerð frumvarpsins

Í greinargerð frumvarpsins er orðið „meðalhófsregla“ notað fyrir enska hugtakið „proportionality principle“. Tekið er undir réttmæti þessarar orðnotkunar. Fjármálaeftirlitið hefur stundum notað orðið „hlutfallsregla“ sem er óheppilegt þar sem það orð hefur aðra og óskylda lagalega merkingu í íslenskum rétti.

Í kafla 2.3. í greinargerðinni segir að heildarlög muni leysa af hólmi ákvæði í settum lögum, reglugerðir, viðmiðunarreglur og leiðbeinandi tilmæli, eftir því sem við á. Æskilegt væri að taka skýrt fram í frumvarpinu hvort og þá að hvaða leyti samþykkt laganna muni fela í sér brottfall núgildandi reglna og tilmæla, þ.m.t. leiðbeinandi tilmæla Fjármálaeftirlitsins vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila, nr. 1/2019.

Í kafla 3.1 í greinargerðinni segir að DORA kveður á um að aðilar á fjármálamarkaði uppfæri reglulega og skjalfesti umgjörð net- og upplýsingaöryggismála og skal hún háð virku eftirliti stjórnar. Æskilegt væri að taka skýrar fram í frumvarpinu hvað teljist sem reglulegt einnig þar sem þetta kemur oftar fyrir í lögunum. Ítarlegri skilgreining væri til þess fallin að skýra kröfur sem gerðar eru og stuðla að samræmi í framkvæmd.

Í köflum 3.1. og 3.2.a. í greinargerðinni er orðið „stjórn“ notað fyrir enska hugtakið „management body“ og orðið „framkvæmdastjórn“ notað fyrir hugtakið „senior management“. Sama orðnotkun er notuð í drögum að íslenskri þýðingu á DORA reglugerðinni, sem er fylgiskjal í samráðsgátt. Draga verður í efa réttmæti þessarar orðnotkunar. Hugtakið „management body“ getur haft víðtækari merkingu en orðið stjórn og hugtakið „senior management“ getur haft víðtækari merkingu en orðið framkvæmdastjórn. Í eftirlitsframkvæmd hefur Fjármálaeftirlitið talið að hugtakið „management body“ nái til stjórnar, framkvæmdastjóra (forstjóra/bankastjóra) og framkvæmdastjórnar. Mikilvægt er að þýðing á enskum hugtökum í DORA og innleiðing þeirra í íslensk lög verði ekki til þess að setja aðilum hér á landi þrengri skorður en felast í DORA reglugerðinni hvað varðar tilhögun ábyrgðar og fyrirkomulag stjórnarhátta.

Enn fremur segir í kafla 3.2.a. að „…koma skuli á stefnu og ferlum sem miða að því að tryggja að strangar kröfur séu gerðar…“. Í enskri útgáfu DORA reglugerðarinnar er einungis notast við hugtakið „policies“. Í greinargerðinni er þannig gengið lengra en í texta DORA reglugerðarinnar,

með viðbót hugtaksins „ferlum“.

Í kafla 3.2.b. í greinargerðinni segir að þegar alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eiga sér stað eða í kjölfar tilmæla eftirlitsaðila eða niðurstaðna sem leiða af viðeigandi prófunum eða úttektarferlum skuli *áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni* endurskoðaður á grundvelli fengins lærdóms af framkvæmd og vöktun. Ætla verður að nægjanlegt sé að endurskoðun skuli fara fram á þeim hlutum *áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni* sem tengjast atvikinu, en ekki rammann í heild sinni.

Í kafla 3.2.f. í greinargerðinni er hugtakið „óeðlilegar athafnir“ notað fyrir enska hugtakið „anomalous activities”. Sama orðnotkun er notuð í drögum að íslenskri þýðingu á DORA reglugerðinni, sem er fylgiskjal í samráðsgátt. Draga verður í efa réttmæti þessarar orðnotkunar, og lagt til að notast verði við orð á borð við frávik, í samræmi við ætlaðan markmið enska textans.

Í kafla 3.2.g. í greinargerðinni er hugtakið „starfseining krísustjórnunar“ notað fyrir enska hugtakið „crisis management function“. Sama orðnotkun er notuð í drögum að íslenskri þýðingu á DORA reglugerðinni, sem er fylgiskjal í samráðsgátt. Draga má í efa réttmæti þessarar orðnotkunar, enda getur hugtakið „crisis management function“ haft víðtækari merkingu en orðið „starfseining“.

Í kafla 3.2.h. í greinargerðinni segir að tryggja skuli *hæsta stig* heilleika gagna. Hugtakið er bein þýðing á enska hugtakinu „highest level of data integrity“ en getur ekki talist skýrt. Til þess að tryggja áhrifaríka innleiðingu DORA myndi fara vel á því að greinargerðin innihéldi nánari tilgreiningu á hugtakinu „hæsta stig“. Ítarlegri skilgreining væri til þess fallin að skýra kröfur sem gerðar eru og stuðla að samræmi í framkvæmd.

Í kafla 3.2.j. í greinargerðinni er orðið „samskiptastefnur“ notað fyrir enska hugtakið „communication strategy“. Sama orðnotkun er notuð í drögum að íslenskri þýðingu á DORA reglugerðinni, sem er fylgiskjal í samráðsgátt. SFF velta fyrir sér þýðingu hugtaksins „strategy“ en orðið „policy“ hefur yfirleitt verið þýtt sem stefna. Mikilvægt er að þýðing á enskum hugtökum í DORA og innleiðing þeirra í íslensk lög verði ekki til þess að setja aðilum hér á landi þrengri skorður en felast í DORA reglugerðinni hvað varðar tilhögun ábyrgðar og fyrirkomulag stjórnarhátta og því mikilvægt að skoðað sé hvort átt sé við eitthvað annað en stefnu í þessu tilviki.

Í kafla 3.4. í greinargerðinni segir að fyrir samningsgerð við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu skuli ganga úr skugga um að viðeigandi staðlar um upplýsingaöryggi séu uppfylltir. Þannig er orðið „staðlar“ notað fyrir enska hugtakið „standards“. Orðalagið „viðeigandi staðlar um upplýsingaöryggi“ hefur þannig í för með sér að fyrirtæki sem fjármálastofnanir kaupa þjónustu af þurfi að hafa vissa staðla sem enn fremur eru ekki listaðir nákvæmlega. Enska útgáfan, „appropriate information security standards“ virðist frekar vísa til verklags eða hæfni tengdu upplýsingaöryggi en formlegra staðla.

Í kafla 3.5. í greinargerðinni er fjallað um ákvæði 1. þáttar V. kafla DORA um stýringu upplýsinga-

og fjarskiptatækniáhættu vegna þriðju aðila (ICT third-party service provider). Æskilegt væri að fjallað væri um það í frumvarpinu, t.d. með notkun dæma, hvaða þriðju aðilar þetta eru eða gætu verið hér á landi, að teknu tilliti til þeirra aðstæðna sem hér ríkja. Aðilar á fjármálamarkaði eiga í samstarfi við ýmsa þriðju aðila á sviði upplýsinga- og fjarskiptatækni, og er slíkt samstarf með ýmsu móti, allt frá því að vera tilfallandi þjónustukaup til þess að vera umfangsmikil, samningsbundin útvistun. Þá eru slíkir þriðju aðilar hér á landi almennt mun smærri en í öðrum EES-ríkjum. Æskilegt væri að veita hérlendum aðilum leiðbeiningar um það hvernig afmarka eigi þriðju aðila í skilningi DORA til þess að greiða fyrir innleiðingu regluverksins í starfsemi þeirra.

Í kafla 6.1. í greinargerðinni segir að innleiðing DORA muni líklega hafa í för með sér einhvern kostnað fyrir þau fyrirtæki sem munu falla undir gildissvið löggjafarinnar. Ekki er að sjá að endanlegt mat á áhrifum fylgi frumvarpinu eins og gert er ráð fyrir í ferli við vinnslu stjórnarfrumvarpa heldur er eingöngu um að ræða smávægilega umfjöllun í greinargerð frumvarpsdraganna. [1] Ekki er vitað til þess að óskað hafi verið eftir upplýsingum um mat á kostnaði frá fyrirtækjunum en telja má að hann verði verulegur í ljósi umfangs og flækjustigs DORA reglugerðarinnar og undirgerða hennar. Í 2. mgr. samþykktar ríkisstjórnarinnar um undirbúning og frágang stjórnarfrumvarpa og þingsályktunartillagna, sbr. 10. gr. reglna um starfshætti ríkisstjórnar, nr. 791/2018 segir að umfang mats á áhrifum ráðist m.a. að því hve mikil fyrirsjáanleg áhrif af lagasetningu eru. Að mati SFF eru fyrirsjáanleg áhrif mikil á fyrirtækin sem löggjöfin beinist að.

Í kafla 6.2. í greinargerðinni kemur fram að efnisreglur DORA feli í sér einföldun regluverks. Deila má um þessa fullyrðingu. DORA regluverkið er hvorki einfalt né skýrt og mun fela í sér áskorun og lagaáhættu fyrir þau fyrirtæki hér á landi sem munu falla undir gildissvið þess.

Í kafla 6.3 segir að ekki séu taldar líkur á því að fyrirhuguð lagasetning hafi áhrif á samkeppni á markaði. Ástæða er til að staldra við þessa fullyrðingu, enda aukast kröfur verulega með tilkomu DORA, og tilfallandi kostnaður einnig. Ætla má að áhrif þeirra krafna sem gerðar eru, ekki síst til þriðju aðila, kunni að hafa meiri áhrif á minni fyrirtæki en stærri og valda samþjöppun innan þeirra geira sem falla undir reglugerðina. Framangreint á ekki síst við ef krafa verður gerð um að fyrir samningsgerð við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu skuli ganga úr skugga um að viðeigandi staðlar um upplýsingaöryggi séu uppfylltir, líkt og bent hefur verið á með athugasemdum við kafla 3.4.

Í kafla 6.5. í greinargerðinni segir að gera megi ráð fyrir að viðbótarkostnaði vegna aukinna

---

[1]

F. Til útfyllingar vegna endanlegs mats – breytingar frá frummati
1. Voru áform um lagasetninguna ásamt frummati á áhrifum kynnt fyrir FJR? 2. Eru helstu efnisatriði frumvarpsins óbreytt/lítið breytt frá þeim tíma? 3. Ef gerðar hafa verið breytingar umfram það, sbr. það frummat á áhrifum frumvarpsins sem áður var kynnt, hverjar eru þær og hver eru fjárhagsáhrifin?

verkefna Seðlabankans með innleiðingu DORA í landsrétt verði mætt með hækkun eftirlitsgjalds. Ástæða er til að staldra við þessa fullyrðingu. Ný eftirlitsverkefni þurfa ekki og eiga ekki endilega að kalla sjálfkrafa á hækkun eftirlitsgjalds en eftirlit á Íslandi virðist vera hlutfallslega mjög mikið sbr. nýlega skýrslu Viðskiptaráðs Íslands[2]. Þá hefur eftirlitsgjaldið einnig hækkað töluvert síðustu ár[3]. Mikilvægt er að hugað verði að hagræðingu og nýrri forgangsröðun eftirlitsverkefna Seðlabankans til þess að koma í veg fyrir eða lágmarka þörf fyrir hækkun eftirlitsgjalds vegna innleiðingar DORA.

Í ljósi þess að frumvarpsdrögin voru til umsagnar yfir sumarleyfistíma telja SFF mögulegt að samtökin komi með frekari athugasemdir síðar til ráðuneytisins.

Með vinsemd og virðingu
f. h. Samtaka fyrirtækja í fjármálaþjónustu,

Margrét Arnheiður Jónsdóttir, lögfræðingur

[2] https://www.vi.is/skodanir/rettum-kursinn
[3] https://vb.is/frettir/eftirlitsgjaldid-haekkar-um-435-milljonir/