

**Fylgiskjal 1.****FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1772**

frá 13. mars 2024

**um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmið fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik**

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálagæirann 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 <sup>(1)</sup>, einkum þriðju undirgrein 4. mgr. 18. gr.,

*og að teknu tilliti til eftirfarandi:*

- 1) Reglugerð (ESB) 2022/2554 miðar að því að samræma og einfalda kröfur um skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik sem varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki („atvik“). Í ljósi þess að skýrslugjafarkröfurnar ná yfir 20 mismunandi tegundir aðila á fjármálamarkaði ætti að skilgreina flokkunarviðmið og mikilvægismörk til að ákvarða alvarleg atvik og verulegar netógnir á einfaldan, samræmdan og samkvæman hátt sem tekur tillit til sérstöðu þjónustunnar og starfsemi allra viðkomandi aðila á fjármálamarkaði.
- 2) Til að tryggja meðalhóf ættu flokkunarviðmið og mikilvægismörk að endurspegla stærð og heildaráhættusnið og eðli, umfang og flækjustig þjónustu allra aðila á fjármálamarkaði. Auk þess ættu viðmiðin og mikilvægismörkin að vera hönnuð þannig að þau eigi við alla aðila á fjármálamarkaði með samræmdum hætti, óháð stærð þeirra og áhættusniði, og valdi minni aðilum á fjármálamarkaði ekki óhóflegri skýrslugjafarbyrði. Til að taka á aðstæðum þar sem verulegur fjöldi viðskiptavina verður fyrir áhrifum af atviki sem fer sem slíkt ekki yfir gildandi viðmiðunarmörk ætti þó að setja algild viðmiðunarmörk sem beinast aðallega að stærri aðilum á fjármálamarkaði.
- 3) Í tengslum við ramma utan um skýrslugjöf vegna atvika, sem voru til áður en reglugerð (ESB) 2022/2554 tók gildi, ætti að tryggja samfellu fyrir aðila á fjármálamarkaði. Því ættu flokkunarviðmið og mikilvægismörk að vera aðlöguð að og innblásin af viðmiðunarreglum Evrópsku bankaftirlitsstofnunarinnar um skýrslugjöf um alvarleg atvik samkvæmt tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 <sup>(2)</sup>, leiðbeiningum um reglubundnar upplýsingar og tilkynningar um verulegar breytingar sem viðskiptaskrár verða að senda til Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar, ramma Seðlabanka Evrópu/samræmdrar eftirlitsráðstöfunar um skýrslugjöf vegna netatvika (e. *ECB/SSM Cyber Incident Reporting Framework*) og öðrum viðeigandi leiðbeiningum. Flokkunarviðmið og viðmiðunarmörk ættu einnig að henta fyrir þá aðila á fjármálamarkaði sem hafa ekki áður fallið undir kröfur um skýrslugjöf vegna atvika fyrr en nú, undir reglugerð (ESB) 2022/2554.
- 4) Að því er varðar flokkunarviðmiðið „fjárhæð og fjöldi viðskipta sem verða fyrir áhrifum“ er hugtakið viðskipti viðtækt og nær yfir ólíka starfsemi og þjónustu í geirabundnum gerðum sem gilda um aðila á fjármálamarkaði. Að því er þetta flokkunarviðmið varðar ætti það að ná yfir greiðslur og allar gerðir viðskipta með fjármálagæringa, sýndareignir, hrávörur eða hvers kyns aðrar eignir, einnig í formi tryggingarfjár, veðs eða trygginga, bæði gegn reiðufé og öðrum eignum. Taka ætti tillit til allra viðskipta sem varða eignir sem hægt er að gefa upp sem fjárhæð í flokkunartilgangi.

<sup>(1)</sup> Stjtið. ESB L 333, 27.12.2022, bls. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

<sup>(2)</sup> Tilskipun 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, 2013/36/ESB og á reglugerð (ESB) nr. 1093/2010 og niðurfellingu á tilskipun 2007/64/EB (Stjtið. ESB L 337, 23.12.2015, bls. 35, ELI: <http://data.europa.eu/eli/dir/2015/2366/oj>).

- 5) Með flokkunarviðmiðunum ætti að tryggja að allar viðeigandi tegundir alvarlegra atvika séu fangaðar. Ekki eru endilega mörg flokkunarviðmið sem ná utan um netárásir sem tengjast innbrotum í net- eða upplýsingakerfi. Þær eru hins vegar mikilvægar þar sem hvers kyns innbrot í net- og upplýsingakerfi geta skaðað aðila á fjármálamarkaði. Til samræmis við það ætti að skilgreina flokkunarviðmiðin „mikilvæg þjónusta sem verður fyrir áhrifum“ og „gagnatap“ þannig að þau nái yfir þessar tegundir alvarlegra atvika, einkum innrás óviðkomandi aðila sem getur haft alvarlegar afleiðingar, jafnvel þótt áhrifin liggi ekki strax fyrir, einkum gagnabrot og gagnaleka.
- 6) Þar sem lánastofnanir falla bæði undir ramma utan um flokkun á atvikum skv. 18. gr. reglugerðar (ESB) 2022/2554 og ramma um rekstraráhættu samkvæmt framseldri reglugerð framkvæmdastjórnarinnar (ESB) 2018/959 <sup>(3)</sup> ætti nálgun við mat á efnahagslegum áhrifum atviks, byggt á útreikningi á kostnaði og tapi að vera eins samræmt og mögulegt er milli beggja ramma til að forðast að ósamrýmanlegar eða misvísandi kröfur.
- 7) Viðmið í tengslum við landfræðilega útbreiðslu atviks eins og sett er fram í c-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554 ætti að leggja áherslu á áhrif atviksins yfir landamæri, þar sem önnur viðmið í þeirri grein munu ná yfir áhrif af atviki á starfsemi aðila á fjármálamarkaði innan einnar lögsögu.
- 8) Þar sem flokkunarviðmiðin eru innbyrðis háð og tengd hvert öðru ætti aðferðin við að greina alvarleg atvik sem ber að tilkynna í samræmi við 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 að byggjast á samsetningu viðmiða þar sem sum viðmið, sem eru nátengd skilgreiningum á atviki sem tengist upplýsinga- og fjarskiptatækni og alvarlegu atviki sem tengist upplýsinga- og fjarskiptatækni eins og sett fram í 8. og 10. mgr. 3. gr. reglugerðar (ESB) 2022/2554, ættu að veita þyngra í flokkun á alvarlegum atvikum en önnur.
- 9) Til að tryggja að skýrslur og tilkynningar um alvarleg atvik sem berast lögbærum yfirvöldum skv. 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 þjóni tilgangi bæði í eftirlitsskyni og til að koma í veg fyrir smitáhrif í fjármálageiranum ættu mikilvægismörkin að gera kleift að fanga alvarleg atvik, m.a. með því að leggja áherslu á áhrifin á einingarsértæka mikilvæga þjónustu, tiltekin algild og hlutfallsleg mörk viðskiptavina eða fjárhagslegra mótaðila, viðskipti sem sýna umtalsverð áhrif á aðila á fjármálamarkaði og þýðingu áhrifanna í öðrum aðildarríkjum.
- 10) Líta ætti á atvik sem hafa áhrif á upplýsinga- og fjarskiptatækniþjónustu eða net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi eða fjármálaþjónustu sem krefst leyfis, eða óheimilan aðgang í illum tilgangi að net- og upplýsingakerfum sem styðja nauðsynlega eða mikilvæga starfsemi, sem atvik sem hafa áhrif á mikilvæga þjónustu aðila á fjármálamarkaði. Óheimill aðgangur í illum tilgangi að net- og upplýsingakerfum sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði hefur í för með sér alvarlega áhættu fyrir þá og ætti alltaf að teljast alvarlegt atvik sem ber að tilkynna, þar sem aðgangurinn getur haft áhrif á aðra aðila á fjármálamarkaði.
- 11) Endurtekin atvik sem virðast tengjast í gegnum svipaðar frumorsakir, sem hvert um sig er ekki alvarlegt atvik, geta bent til verulegra annmarka og veikleika í verklagsreglum aðila á fjármálamarkaði við atvika- og áhættustýringu. Endurtekin atvik ættu því að teljast vera alvarleg ef þau koma ítrekað fyrir yfir tiltekið tímabil.
- 12) Í ljósi þess að netógnir geta haft neikvæð áhrif á aðila á fjármálamarkaði og fjármálageirann ættu þær verulegu netógnir sem aðilar á fjármálamarkaði kunna að tilkynna að gefa til kynna líkurnar á því að þær raungerist og alvarleika mögulegra áhrifa. Til samræmis við það ætti flokkun netógnar sem verulegrar að fara eftir líkunum á því að flokkunarviðmið fyrir alvarleg atvik og viðmiðunarmörk þeirra myndu vera uppfyllt ef ógnin raungerðist, eftir tegund netógnar og eftir þeim upplýsingum sem eru tiltækar fyrir aðila á fjármálamarkaði, til að tryggja skýrt og samræmt mat á þýðingu netóгна.

<sup>(3)</sup> Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2018/959 frá 14. mars 2018 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) nr. 575/2013 að því er varðar tæknilega eftirlitsstaðla um lýsingu á aðferðafræði varðandi mat sem lögbær yfirvöld skulu nota til að heimila stofnunum að nota þróaðar mæliaðferðir fyrir rekstraráhættu (Stjtið. ESB L 169, 6.7.2018, bls. 1, ELI: [http://data.europa.eu/eli/reg\\_del/2018/959/oj](http://data.europa.eu/eli/reg_del/2018/959/oj)).

- 13) Í ljósi þess að tilkynna þarf lögbærum yfirvöldum í öðrum aðildarríkjum um atvik sem hafa áhrif á aðila á fjármálamarkaði og viðskiptavinum í lögsögu þeirra ætti mat á áhrifum í öðru lögsagnarumdæmi í samræmi við 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554 að byggjast á frumorsökum atviksins, á hugsanlegum smitáhrifum í gegnum veitendur sem eru þriðja aðilar og á innviðum fjármálamarkaðar, sem og á áhrifum atviksins á mikilvæga hópa viðskiptavina eða fjárhagslega mótaðila.
- 14) Skýrslugjafar- og tilkynningarferlin sem um getur í 6. og 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554 ættu að gera viðkomandi viðtakendum kleift að leggja mat á áhrifin af atvikunum. Því ættu sendar upplýsingar að ná yfir allar upplýsingar úr atvikaskýrslum sem aðili á fjármálamarkaði sendir til lögbærs yfirvalds.
- 15) Ef atvik felur í sér öryggisbrest við meðferð persónuupplýsinga, samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 <sup>(4)</sup> og tilskipun Evrópuþingsins og ráðsins 2002/58/EB <sup>(5)</sup>, ætti þessi reglugerð ekki að hafa áhrif á skráningar- og tilkynningarskyldur vegna öryggisbrests við meðferð persónuupplýsinga sem settar eru fram í þeim lögum Sambandsins. Lögbær yfirvöld ættu að starfa með og skiptast á upplýsingum um öll viðeigandi mál við þau yfirvöld sem um getur í reglugerð (ESB) 2016/679 og tilskipun 2002/58/EB.
- 16) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem evrópsku eftirlitsstofnanirnar, í samráði við Netöryggisstofnun Evrópusambandsins og Seðlabanka Evrópu hafa lagt fyrir framkvæmdastjórnina.
- 17) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 <sup>(6)</sup>, 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 <sup>(7)</sup> og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 <sup>(8)</sup> hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint hugsanlegan kostnað og ávinning af fyrirhuguðum stöðlum og óskað eftir ráðgjöf hagsmunahóps um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahóps í váttryggingum og hagsmunahóps um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahóps á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.

<sup>(4)</sup> 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 (almenna persónuvemdarreglugerðin) (Stjtið. ESB L 119, 4.5.2016, bls. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

<sup>(5)</sup> Tilskipun Evrópuþingsins og ráðsins 2002/58/EB frá 12. júlí 2002 um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafræna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti) (Stjtið. EB L 201, 31.7.2002, bls. 37, ELI: <http://data.europa.eu/eli/dir/2002/58/oj>).

<sup>(6)</sup> 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 (Stjtið. ESB L 331, 15.12.2010, bls. 12, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

<sup>(7)</sup> Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska váttrygginga- og lífeyrissjóðaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/79/EB (Stjtið. ESB L 331, 15.12.2010, bls. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

<sup>(8)</sup> 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 (Stjtið. ESB L 331, 15.12.2010, bls. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

- 18) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 <sup>(9)</sup> og skilaði hún álit 24. janúar 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

#### I. KAFLI

#### FLOKKUNARVIÐMIÐ

##### 1. gr.

#### Viðskiptavinir, fjárhagslegir mótaðilar og viðskipti

1. Fjöldi viðskiptavina sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal endurspegla fjölda allra viðskiptavina sem verða fyrir áhrifum, óháð því hvort þeir eru einstaklingar eða lögaðilar, sem geta ekki eða gátu ekki nýtt sér þá þjónustu sem aðili á fjármálamarkaði veitti á meðan atvikinu stóð eða sem atvikið hafði neikvæð áhrif á. Sá fjöldi skal einnig taka til þriðju aðila sem falla sérstaklega undir samningsbundið samkomulag á milli aðila á fjármálamarkaði og viðskiptavinarins sem viðtakanda viðkomandi þjónustu.
2. Fjöldi fjárhagslegra mótaðila sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal endurspegla fjölda allra fjárhagslegra mótaðila sem verða fyrir áhrifum og hafa gert samning við viðkomandi aðila á fjármálamarkaði.
3. Í tengslum við mikilvægi viðskiptavina og fjárhagslegra mótaðila sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal viðkomandi aðili á fjármálamarkaði taka tillit til þess að hvaða marki áhrif á viðskiptavin eða fjárhagslegan mótaðila snerta framkvæmd viðskiptamarkmiða aðila á fjármálamarkaði sem og hugsanlegra áhrifa atviksins á skilvirkni markaðar.
4. Í tengslum við fjárhæð eða fjölda viðskipta sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal viðkomandi aðili á fjármálamarkaði taka tillit til allra viðskipta sem verða fyrir áhrifum og fela í sér peningafjárhæð þar sem a.m.k. einn hluti viðskiptanna fer fram í Sambandinu.
5. Ef ekki er hægt að ákvarða raunverulegan fjölda viðskiptavina eða fjárhagslegra mótaðila eða raunverulegan fjölda eða fjárhæð viðskipta sem verða fyrir áhrifum skal aðili á fjármálamarkaði leggja mat á fjöldann eða fjárhæðina miðað við tiltæk gögn frá sambærilegum viðmiðunartímabilum.

##### 2. gr.

#### Áhrif á orðspor

1. Til að skera úr um áhrif atviksins á orðspor, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði líta svo á að áhrif hafi orðið á orðspor ef a.m.k. eitt eftirfarandi viðmið er uppfyllt:
  - a) fjallað hefur verið um atvikið í fjölmiðlum,
  - b) atvikið hefur valdið endurteknum kvörtunum frá mismunandi viðskiptavinum eða fjárhagslegum mótaðilum varðandi þjónustu með beinum samskiptum við viðskiptavini eða mikilvæg viðskiptasambönd,
  - c) aðili á fjármálamarkaði mun ekki geta, eða líklegt er að hann geti ekki, uppfyllt kröfur samkvæmt reglum vegna atviksins,
  - d) aðili á fjármálamarkaði mun, eða er líklegur til að, missa viðskiptavini eða fjárhagslega mótaðila sem hafa umtalsverð áhrif á viðskipti hans vegna atviksins.

<sup>(9)</sup> Reglugerð Evrópuþingsins og ráðsins (ESB) 2018/1725 frá 23. október 2018 um vernd einstaklinga í tengslum við vinnslu meginstofnana, stofnana, skrifstofa og fagstofnana Sambandsins á persónuupplýsingum og um frjálsta miðlun slíkra upplýsinga og um niðurfellingu reglugerðar (EB) nr. 45/2001 og ákvörðunar nr. 1247/2002/EB (Stjtið. ESB L 295, 21.11. 2018, bls. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

2. Við mat á áhrifum atviks á orðspor skulu aðilar á fjármálamarkaði taka tillit til þess hversu sýnilegt það er eða er líklegt til að verða í tengslum við hvert viðmið sem tilgreint er í 1. mgr.

3. gr.

#### **Tímalengd og niðritími þjónustu**

1. Aðilar á fjármálamarkaði skulu mæla tímalengd atviks eins og um getur í 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554 frá því augnabliki sem atvikið átti sér stað og þar til úr því hefur verið leyst.

Ef aðilar á fjármálamarkaði geta ekki ákvarðað hvenær atvikið átti sér stað skulu þeir mæla tímalengd atviksins frá því að það uppgötvaðist. Ef aðilar á fjármálamarkaði komast að því síðar að atvikið hafi átt sér stað áður en það uppgötvaðist skulu þeir mæla tímalengdina frá því að atvikið var skráð í net- eða kerfissskrár eða aðrar gagnalindir.

Ef aðilar á fjármálamarkaði vita ekki enn hvenær leyst verður úr atvikinu eða geta ekki sannprófað skrár í kerfissskrám eða öðrum gagnalindum skulu þeir nota mat.

2. Aðilar á fjármálamarkaði skulu mæla niðritíma þjónustu, eins og um getur í b-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, frá því þegar þjónustan er að öllu leyti eða hluta til óaðgengileg viðskiptavinum, aðilum á fjármálamarkaði eða öðrum innri eða ytri notendum þar til regluleg starfsemi eða rekstur hefur verið færður aftur á sama þjónustustig og var veitt á undan atvikinu. Ef niðritími þjónustu veldur töfum á þjónustustarfsemi eftir að regluleg starfsemi eða rekstur hefur verið færður aftur í sama horf skal mæla niðritímann frá upphafi atviks þangað til að seinkuð þjónusta er aftur veitt að fullu.

Ef aðilar á fjármálamarkaði geta ekki ákvarðað hvenær niðritími þjónustu hófst skulu þeir mæla niðritíma þjónustunnar frá því að það uppgötvaðist.

4. gr.

#### **Landfræðileg útbreiðsla**

Til að ákvarða landfræðilega útbreiðslu að því er varðar svæðin sem atvikið hefur áhrif á, eins og um getur í c-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði leggja mat á hvort atvik hafi, eða hafi haft, áhrif í öðrum aðildarríkjum og einkum þýðingu áhrifanna í tengslum við eftirfarandi:

- a) viðskiptavinum og fjárhagslega mótaðila í öðrum aðildarríkjum,
- b) útibú eða aðra aðila á fjármálamarkaði innan samstæðunnar, sem annast starfsemi í öðrum aðildarríkjum,
- c) innviði fjármálamarkaðar eða veitendur sem eru þriðju aðilar, sem gæti haft áhrif á aðila á fjármálamarkaði í öðrum aðildarríkjum þar sem þeir veita þjónustu, að því marki sem slíkar upplýsingar eru tiltækar.

5. gr.

#### **Tap á gögnum**

Til að ákvarða gagnatapið sem atvik hefur í för með sér, eins og um getur í d-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði taka tillit til eftirfarandi:

- a) í tengslum við tiltækileika gagna, hvort atvikið hafi gert gögn sem aðili á fjármálamarkaði, viðskiptavinir hans eða mótaðilar höfðu óskað eftir tímabundið eða varanlega ótiltæk eða ónothæf,
- b) í tengslum við ósvikni gagna, hvort atvikið hafi skert trúverðugleika gagnalindarinnar,

- c) í tengslum við réttleika gagna, hvort atvikið hafi valdið óheimilaðri breytingu á gögnum sem hafi gert þau ónákvæm eða ófullnægjandi,
- d) í tengslum við leynd gagna, hvort atvikið hafi leitt til þess að óviðkomandi aðili eða kerfi hafi fengið aðgang að gögnum eða fengið þau afhent.

6. gr.

**Mikilvægi þjónustu sem verður fyrir áhrifum**

Til að ákvarða mikilvægi þjónustunnar sem verður fyrir áhrifum, eins og um getur í e-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði meta hvort atvikið:

- a) hafi eða hafi haft áhrif á upplýsinga- og fjarskiptatækniþjónustu eða net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði,
- b) hafi eða hafi haft áhrif á fjármálaþjónustu sem aðili á fjármálamarkaði veitir, sem þarfnast starfsleyfis, skráningar eða sem er undir eftirliti lögbærra yfirvalda,
- c) feli eða hafi falið í sér árangursríkan, óheimilan aðgang í illum tilgangi að net- og upplýsingakerfum aðila á fjármálamarkaði.

7. gr.

**Efnahagsleg áhrif**

1. Til að ákvarða efnahagsleg áhrif atviks, eins og um getur í f-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði taka tillit til eftirfarandi tegunda af beinum og óbeinum kostnaði sem þeir hafa stofnað til vegna atviksins, án þess taka tillit til fjárhagslegrar endurheimtar:

- a) fjármuna eða fjáreigna sem hafa verið tekin eignarnámi og þeir bera ábyrgð á, þ.m.t. eigna sem tapast vegna þjófnaðar,
- b) kostnaðar við að endurnýja eða flytja hugbúnað, vélbúnað eða innviði,
- c) starfsmannakostnaðar, þ.m.t. kostnaðar við að endurnýja eða flytja starfsfólk, ráða starfsfólk til viðbótar, greiða yfirvinnu og endurheimt tapaðrar eða skertrar færni,
- d) gjalda sem hljótast af því að ekki er staðið við samningsbundnar skyldur,
- e) kostnaðar vegna lagfæringa og bóta til viðskiptavina,
- f) taps vegna tapaðra tekna,
- g) kostnaðar sem tengist innri og ytri samskiptum,
- h) ráðgjafarkostnaðar, þ.m.t. kostnaðar sem tengist lögfræðiráðgjöf, tæknirannsóknnum og úrbótum.

2. Kostnaður og tap sem um getur í 1. mgr. skal ekki taka til kostnaðar sem er nauðsynlegur fyrir daglegan rekstur fyrirtækisins, einkum eftirfarandi:

- a) kostnaðar vegna almenns viðhalds á innviðum, búnaði, vélbúnaði og hugbúnaði, og kostnaðar við að viðhalda færni starfsfólks,
- b) innri eða ytri kostnaðar við að styrkja fyrirtækið eftir atvikið, þ.m.t. uppfærslur, endurbætur og framtaksverkefni í áhættumati,
- c) tryggingariðgjalda.

3. Aðilar á fjármálamarkaði skulu reikna út fjárhæð kostnaðar og taps út frá þeim gögnum sem liggja fyrir við skýrslugjöf. Ef ekki er hægt að ákvarða fjárhæð fyrir raunverulegan kostnað og tap skulu aðilar á fjármálamarkaði áætla þá fjárhæð.

4. Við mat á efnahagslegum áhrifum atviksins skulu aðilar á fjármálamarkaði leggja saman þann kostnað og tap sem um getur í 1. mgr.

## II. KAFLI

## ALVARLEG ATVIK OG MIKILVÆGISMÖRK

## 8. gr.

## Alvarleg atvik

1. Atvik skal teljast vera alvarlegt atvik að því er varðar 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 ef það hefur áhrif á nauðsynlega þjónustu, eins og um getur í 6. gr., og ef annaðhvort eftirfarandi skilyrða er uppfyllt:

- a) mikilvægismörkin, sem um getur í b-lið 5. mgr. 9. gr., eru uppfyllt,
- b) tvö eða fleiri af öðrum mikilvægismörkum, sem um getur í 1. til 6. mgr. 9. gr., eru uppfyllt.

2. Endurtekin atvik sem hvert fyrir sig er ekki alvarlegt atvik í samræmi við 1. mgr. skulu teljast eitt alvarlegt atvik ef þau uppfylla öll eftirfarandi skilyrði:

- a) þau hafa átt sér stað a.m.k. tvisvar á 6 mánuðum,
- b) þau hafa sömu augljósu frumorsökina, eins og um getur í b-lið fyrstu undirgr. 20. gr. reglugerðar (ESB) 2022/2554,
- c) þau uppfylla samtals viðmiðin til að teljast alvarlegt atvik eins og sett er fram í 1. mgr.

Aðilar á fjármálamarkaði skulu meta tíðni endurtekinna atvika einu sinni í mánuði.

Þessi málsgrein gildir ekki um örfyrirtæki og aðila á fjármálamarkaði sem eru taldir upp í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554.

## 9. gr.

## Mikilvægismörk til að ákvarða alvarleg atvik

1. Mikilvægismörkum fyrir viðmiðið „viðskiptavinir, fjárhagslegir mótaðilar og viðskipti“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:

- a) fjöldi viðskiptavina sem verða fyrir áhrifum er meiri en 10% af öllum viðskiptavinum sem nota viðkomandi þjónustu,
- b) fjöldi viðskiptavina sem verða fyrir áhrifum og nota viðkomandi þjónustu er meiri en 100 000,
- c) fjöldi fjárhagslegra mótaðila sem verða fyrir áhrifum er meiri en 30% af öllum fjárhagslegum mótaðilum sem annast starfsemi sem tengist veitingu viðkomandi þjónustu,
- d) fjöldi viðskipta sem verða fyrir áhrifum er meiri en 10% af meðalfjölda daglegra viðskipta sem aðili á fjármálamarkaði annast í tengslum við viðkomandi þjónustu,
- e) fjárhæð viðskipta sem verða fyrir áhrifum er hærri en 10% af meðalvirði daglegra viðskipta sem aðili á fjármálamarkaði annast í tengslum við viðkomandi þjónustu,
- f) viðskiptavinir eða fjárhagslegir mótaðilar sem hafa verið auðkenndir sem mikilvægir, í samræmi við 3. mgr. 1. gr., hafa orðið fyrir áhrifum.

Ef ekki er hægt að ákvarða raunverulegan fjölda viðskiptavina eða fjárhagslegra mótaðila eða raunverulegan fjölda eða fjárhæð viðskipta sem verða fyrir áhrifum skal aðili á fjármálamarkaði leggja mat á fjöldann eða fjárhæðina miðað við tiltæk gögn frá sambærilegum viðmiðunartímabilum.

2. Mikilvægismörkum fyrir viðmiðið „áhrif á orðspor“ er náð ef einhver skilyrðanna sem eru sett fram í a- til d-lið 2. gr. eru uppfyllt.

3. Mikilvægismörkum fyrir viðmiðið „tímalengd og niðritími þjónustu“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:

- a) tímalengd atviksins er lengri en 24 stundir,

- b) niðritími þjónustu er lengri en 2 stundir fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.
4. Mikilvægismörkum fyrir viðmiðið „landfræðileg útbreiðsla“ er náð ef atvikið hefur áhrif í tveimur eða fleiri aðildarríkjum í samræmi við 4. gr.
5. Mikilvægismörkum fyrir viðmiðið „gagnatap“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:
- a) öll áhrif eins og um getur í 5. gr. á tiltækileika, ósvikni, réttleika eða leynd gagna hafa eða munu hafa neikvæð áhrif á framkvæmd viðskiptamarkmiða aðila á fjármálamarkaði eða á getu hans til að uppfylla kröfur samkvæmt reglum,
- b) hvers konar árangursríkur og óheimill aðgangur í illum tilgangi að net- og upplýsingakerfum, sem a-liður fjallar ekki um, ef slíkur aðgangur getur valdið gagnatapi.
6. Mikilvægismörkum fyrir viðmiðið „efnahagsleg áhrif“ er náð ef kostnaður og tap sem aðili á fjármálamarkaði hefur stofnað til vegna atviksins hafa farið, eða eru líkleg til að fara, umfram 100 000 evrur.

### III. KAFLI

#### VERULEGAR NETÓGNIR

##### 10. gr.

##### **Há mikilvægismörk til að ákvarða verulegar netógnir**

Að því er varðar 2. mgr. 18. gr. reglugerðar (ESB) 2022/2554 skal netógn teljast veruleg ef öll eftirfarandi skilyrði eru uppfyllt:

- a) ef netógnin raungerist getur hún haft eða gæti hafa haft áhrif á nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði eða haft áhrif á aðra aðila á fjármálamarkaði, veitendur sem eru þriðju aðilar, viðskiptavinir eða fjárhagslega mótaðila, á grundvelli þeirra upplýsinga sem aðila á fjármálamarkaði eru tiltækar,
- b) miklar líkur eru á að netógnin raungerist hjá viðkomandi aðila á fjármálamarkaði eða öðrum aðilum á fjármálamarkaði, að teknu tilliti til a.m.k. eftirfarandi þátta:
- i. gildandi áhættu sem tengist þeirri netógn sem um getur í a-lið, þ.m.t. hugsanlegra veikleika í kerfum aðila á fjármálamarkaði sem hægt er að misnota,
- ii. getu og tilgangs ógnvalda, að því marki sem aðila á fjármálamarkaði er kunnugt um,
- iii. langæi ógnarinnar og hvers kyns uppsafnaðrar vitneskju um atvik sem hafa haft áhrif á aðila á fjármálamarkaði eða veitanda hans sem er þriðji aðili, viðskiptavinir eða fjárhagslega mótaðila,
- c) netógnin gæti, ef hún raungerðist, uppfyllt eitthvert eftirfarandi:
- i. viðmiðið varðandi mikilvægi þjónustunnar sem sett er fram í e-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, eins og tilgreint er 6. gr. þessarar reglugerðar,
- ii. mikilvægismörk sem sett eru fram í 1. mgr. 9. gr.,
- iii. mikilvægismörk sem sett eru fram í 4. mgr. 9. gr.,

Komist aðili á fjármálamarkaði að þeirri niðurstöðu að þau mikilvægismörk sem sett eru fram í 2., 3., 5. og 6. mgr. 9. gr. gætu verið uppfyllt er einnig hægt að taka tillit til þeirra marka, allt eftir gerð netógnar og fyrirbyggjandi upplýsinga.



## IV. KAFLI

**GILDI ALVARLEGRA ATVIKA FYRIR LÖGBÆR YFIRVÖLD Í ÖÐRUM AÐILDARRÍKJUM OG UPPLÝSINGAR Í SKÝRSLUM SEM Á AÐ DEILA MEÐ ÖÐRUM LÖGBÆRUM YFIRVÖLDUM***11. gr.***Gildi alvarlegra atvika fyrir lögbær yfirvöld í öðrum aðildarríkjum**

Mat á því hvort alvarleg atvik hafi gildi fyrir lögbær yfirvöld í öðrum aðildarríkjum, eins og um getur í 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554, skal byggjast á því hvort atvikið eigi sér frumorsök í öðru aðildarríki eða hvort atvikið hafi eða hafi haft umtalsverð áhrif í öðru aðildarríki í tengslum við eitthvert eftirfarandi:

- a) viðskiptavini eða fjárhagslega mótaðila,
- b) útibú aðila á fjármálamarkaði eða annan aðila á fjármálamarkaði innan samstæðunnar,
- c) innviði fjármálamarkaðar eða veitanda sem er þriðji aðili sem gæti haft áhrif á aðila á fjármálamarkaði sem þeir veita þjónustu.

*12. gr.***Upplýsingar um alvarleg atvik sem ber að deila með öðrum lögbærum yfirvöldum**

Upplýsingar um alvarleg atvik sem lögbærum yfirvöldum ber að senda öðrum lögbærum yfirvöldum í samræmi við 6. mgr. 19. gr. reglugerðar (ESB) 2022/2554 og tilkynningamar sem Evrópska bankaeftirlitsstofnunin, Evrópska verðbréfamarkaðseftirlitsstofnunin eða Evrópska váttrygginga- og lífeyrissjóðaeftirlitsstofnunin og Seðlabanki Evrópu verða að senda til viðkomandi lögbærra yfirvalda í öðrum aðildarríkjum í samræmi við 7. mgr. 19. gr. þeirrar reglugerðar skulu innihalda sömu upplýsingar, án nokkurs nafnleysis, og tilkynningar og skýrslur um alvarleg atvik sem berast frá aðilum á fjármálamarkaði í samræmi við 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554.

## V. KAFLI

**LOKAÁKVÆÐI***13. gr.***Gildistaka**

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í Stjórnartíðindum Evrópusambandsins.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 13. mars 2024.

*Fyrir hönd framkvæmdastjórnarinnar,*

Ursula VON DER LEYEN

*forseti.*