

Fylgiskjal 2.**FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1773**

frá 13. mars 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina ítarlegt innihald stefnunnar varðandi samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu

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 ⁽¹⁾, einkum þriðju undirgrein 10. mgr. 28. gr.

og að teknu tilliti til eftirfarandi:

- 1) Með ramma um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálagæirann, sem komið er á fót með reglugerð (ESB) 2022/2554, er þess krafist að aðilar á fjármálamarkaði setji sér tilteknar meginreglur til að stýra upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, sem er einkar mikilvægt þegar aðilar á fjármálamarkaði eru í samstarfi við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að styðja við nauðsynlega eða mikilvæga starfsemi þeirra.
- 2) Aðilar á fjármálamarkaði verða að taka upp og endurskoða reglulega stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, sem hluta af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Í samræmi við 2. mgr. 28. gr. reglugerðar (ESB) 2022/2554 skal sú stefnuáætlun fela í sér stefnu um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Hún skal gilda á einingagrundvelli og, þar sem við á, undirsamstæðu- og samstæðugrunni.
- 3) Aðilar á fjármálamarkaði eru afar mismunandi að því er varðar stærð, uppbyggingu og innra skipulag og eðli og flækjustig starfssemi þeirra og rekstrar. Nauðsynlegt er að taka tillit til þessarar fjölbreytni við setningu tiltekinna réttarfarslegra grundvallarkrafna sem eiga við um alla aðila á fjármálamarkaði við mótun stefnu varðandi samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu („stefnan“), og tryggja að þessum kröfum sé beitt á hlutfallslegan hátt.
- 4) Ef aðilar á fjármálamarkaði tilheyra samstæðu ætti móðurfyrirtækið sem ber ábyrgð á að gera samstæðu- eða undirsamstæðureikningsskil fyrir samstæðuna því að tryggja að stefnunni sé beitt á samræmdan og samfelldan hátt innan samstæðunnar.
- 5) Við beitingu stefnunnar ætti að líta á veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu, þ.m.t. þá sem eru að öllu leyti eða sameiginlega í eigu aðila á fjármálamarkaði innan sama stofnanaverndarkerfis, sem þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Áhættan sem stafar af veitendum upplýsinga- og fjarskiptatækniþjónustu innan samstæðu getur verið mismunandi en kröfum sem gilda um þá eru þær sömu skv. reglugerð (ESB) 2022/2554. Að sama skapi ætti stefnan að gilda um undirverktaka sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða veigamikla hluta hennar til þriðju aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, ef keðja af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu er til staðar.
- 6) Endanleg ábyrgð stjórnar og/eða framkvæmdastjórnar aðila á fjármálamarkaði á stýringu upplýsinga- og fjarskiptatækniáhættu er grundvallarmeginregla sem gildir einnig um notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu. Þessi ábyrgð ætti að endurspeglast í áframhaldandi þátttöku stjórnar og/eða framkvæmdastjórnar í eftirliti með og vöktun á áhættustýringu í upplýsinga- og fjarskiptatækni, þ.m.t. við samþykkt og endurskoðun stefnunnar a.m.k. einu sinni á ári.

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

- 7) Til að tryggja viðeigandi skýrslugjöf til stjórnar og/eða framkvæmdastjórnar ætti stefnan að setja skýrt fram og skilgreina innri skyldur vegna samþykkis, stjórnunar, eftirlits með og skjalfestingar samningsbundins fyrirkomulags um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („samningsbundið fyrirkomulag“), þ.m.t. upplýsinga- og fjarskiptatækniþjónusta sem veitt er samkvæmt samningunum sem um getur a-lið 1. mgr. 28. gr. reglugerðar (ESB) 2022/2554.
- 8) Til að taka tillit til allrar hugsanlegrar áhættu sem getur skapast þegar samið er um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi ætti uppbygging stefnunnar að fylgja öllum skrefum í hverjum meginfasa lífsferils samningsbundins fyrirkomulags við veitendur sem eru þriðju aðilar.
- 9) Til að draga úr áhættu sem greinst hefur ætti stefnan að kveða á um skipulagningu samningsbundins fyrirkomulags, þ.m.t. áhættumat, áreiðanleikakönnun og samþykkisferli fyrir nýjar eða veigamiklar breytingar á samningsbundna fyrirkomulaginu. Til að stýra áhættunni sem getur skapast áður en gert er samningsbundið fyrirkomulag við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu ætti stefnan að tiltaka viðeigandi og hlutfallslegt ferli til að velja og leggja mat á hæfi væntanlegra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og krefjast þess að aðili á fjármálamarkaði taki tillit til lista, sem ekki er tæmandi, yfir þætti sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu ættu að hafa til staðar. Listinn ætti að innihalda þætti sem tengjast orðsþori þjónustuveitenda, fjármagni, mannauði og tækni-úræðum þeirra, upplýsingaöryggi, stjórnskipulagi, þ.m.t. áhættustýringu, og innra eftirliti þeirra.
- 10) Til að tryggja trausta áhættustýringu við veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ætti stefnan að innihalda upplýsingar um framkvæmd, vöktun og stjórnun samningsbundins fyrirkomulags, þ.m.t. á samstæðu- og undirsamstæðugrunni, eftir atvikum. Þetta felur í sér kröfur um samningsákvæði um gagnkvæmar skuldbindingar aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem ætti að setja fram skriflega. Til að tryggja skilvirkt eftirlit og stuðla að viðnámi ef breytingar verða á viðskiptalíkani eða viðskiptaumhverfi ætti stefnan að tryggja réttindi aðilans á fjármálamarkaði eða tilnefndra þriðju aðila og lögbærra yfirvalda til að skoða og hafa aðgang að upplýsingum, auk þess að skýra frekar útgönguáætlanir og uppsagnarferli.
- 11) Að því marki sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu vinna með persónuupplýsingar er þessi stefna og hvers kyns samningsbundið fyrirkomulag með fyrirvara um, og ætti að vera viðbót við, skuldbindingar samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 ⁽²⁾, eins og að hafa skriflegan samning til staðar sem lýsir vinnslu persónuupplýsinga, kröfu um að tryggja öryggi við vinnslu persónuupplýsinga og ákvörðun um alla aðra þætti sem kraftur er samkvæmt þeirri reglugerð.

(²) 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 persónuverndarreglugerðin) (Stjtið. ESB L 119, 4.5.2016, bls. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

- 12) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ⁽³⁾, 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ⁽⁴⁾ og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ⁽⁵⁾ 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 hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahópsins í váttryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.
- 13) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ⁽⁶⁾ og skilaði hún álit 24. janúar 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Heildaráhættusnið og flækjustigi

Stefnan um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („stefnan“) skal taka mið af stærð og heildaráhættusniði aðila á fjármálamarkaði, og eðli, umfangi og þáttum sem auka eða draga úr flækjustigi þjónustu hans, starfsemi og rekstri, þ.m.t. þáttum sem tengjast:

- a) tegund upplýsinga- og fjarskiptatækniþjónustu sem fellur undir samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („samningsbundið fyrirkomulag“) milli aðila á fjármálamarkaði og þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,
- b) staðsetningu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða staðsetningu móðurfélagsins,
- c) hvort upplýsinga- og fjarskiptatækniþjónustan sem styður nauðsynlega eða mikilvæga starfsemi sé veitt af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í aðildarríki eða í þriðja landi, einnig að teknu tilliti til staðarins sem upplýsinga- og fjarskiptatækniþjónustan er veitt frá og staðarins þar sem gögnin eru unnin og geymd,
- d) eðli gagnanna sem er deilt með þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,
- e) hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé hluti af sömu samstæðu og sá aðili á fjármálamarkaði sem þjónustan er veitt,

⁽³⁾ Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska bankaftirlitsstofnunin), 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>).

⁽⁴⁾ 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>).

⁽⁵⁾ 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>).

⁽⁶⁾ 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 fjálssa 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>).

- f) notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru með starfsleyfi, eru skráðir eða falla undir eftirlit eða tilsjón lögbærs yfirvalds aðildarríkis eða lúta eftirlitsramma skv. II. þætti V. kafla reglugerðar (ESB) 2022/2554, og notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem ofangreint gildir ekki um,
- g) notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru með starfsleyfi, eru skráðir eða falla undir eftirlit eða tilsjón eftirlitsstofnunar í þriðja landi, og notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem ofangreint gildir ekki um,
- h) hvort veiting upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi einskorðist við stakan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða lítinn fjölda slíkra þjónustuveitenda,
- i) flytjanleika upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi til annars þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. vegna tæknisértækra eiginleika,
- j) hugsanlegum áhrifum truflana á veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi á samfellu í starfsemi aðila á fjármálamarkaði og framboð á þjónustu hans.

2. gr.

Beiting á samstæðugrunni

Ef þessi reglugerð gildir á undirsamstæðu- eða samstæðugrunni skal móðurfyrirtækið sem ber ábyrgð á því að gera samstæðu- eða undirsamstæðureikningsskil fyrir samstæðuna tryggja að stefnunni sé framfylgt á samræmdan hátt hjá öllum aðilum á fjármálamarkaði sem eru hluti samstæðunnar og að hún sé fullnægjandi til að unnt sé að beita reglugerðinni á öllum stigum samstæðunnar á skilvirkan hátt.

3. gr.

Fyrirkomulag stjórnarháttanna

1. Stjórn og/eða framkvæmdastjórn skal fara yfir stefnuna a.m.k. einu sinni á ári og uppfæra hana eftir því sem nauðsyn krefur. Breytingar sem gerðar eru á stefnunni skulu innleiddar tímanlega og eins fljótt og auðið er innan viðkomandi samningsbundins fyrirkomulags. Aðilinn á fjármálamarkaði skal skjalfesta áætlaða tímalínu fyrir innleiðinguna.
2. Stefnan skal setja fram eða vísa til aðferðafræði til að ákvarða hvaða upplýsinga- og fjarskiptatækniþjónusta styður nauðsynlega eða mikilvæga starfsemi. Í stefnunni skal einnig koma fram hvenær þetta mat skuli gert og endurskoðað.
3. Stefnan skal fela í sér skýra úthlutun á innri ábyrgð vegna samþykkis, stjórnunar, eftirlits og skjalfestingar á viðkomandi samningsbundnu fyrirkomulagi og tryggja að aðilinn á fjármálamarkaði viðhaldi viðeigandi færni, reynslu og þekkingu til að hafa skilvirkt eftirlit með viðkomandi samningsbundnu fyrirkomulagi, þ.m.t. upplýsinga- og fjarskiptatækniþjónustu sem er veitt samkvæmt þessu fyrirkomulagi.
4. Með fyrirvara um endanlega ábyrgð aðilans á fjármálamarkaði á því að hafa skilvirkt eftirlit með viðeigandi samningsbundnu fyrirkomulagi skal stefnan innihalda kröfur um að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé metinn hafa nægjanleg tilföng til að tryggja að aðili á fjármálamarkaði fari að öllum kröfum samkvæmt lögum og reglum varðandi veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.
5. Í stefnunni skal skilgreina með skýrum hætti hvaða staða eða háttsettur stjórnandi ber ábyrgð á vöktun á viðkomandi samningsbundnu fyrirkomulagi. Í stefnunni skal einnig tilgreint hvernig samstarfi stöðunnar eða háttsetta stjórnandans við eftirlits-einingarnar skal háttáð, nema viðkomandi sé hluti þeirra, og koma á boðleiðum til stjórnar og/eða framkvæmdastjórnar, þ.m.t. eðli þeirra upplýsinga sem á að tilkynna og skjölin sem leggja ber fram. Í henni skal einnig setja fram tíðni slíkrar skýrslugjafar.

6. Stefnan skal tryggja að samningsbundið fyrirkomulag samræmist eftirfarandi:
- a) áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 6. gr. reglugerðar (ESB) 2022/2554,
 - b) stefnu um upplýsingaöryggi sem um getur í 4. mgr. 9. gr. reglugerðar (ESB) 2022/2554,
 - c) stefnu um rekstrarsamfellu upplýsinga- og fjarskiptatækni sem um getur í 11. gr. reglugerðar (ESB) 2022/2554,
 - d) kröfum um tilkynningar um atvik sem settar eru fram í 19. gr. reglugerðar (ESB) 2022/2554.
7. Stefnan skal fela í sér kröfur um að upplýsinga- og fjarskiptatækniþjónusta sem styður nauðsynlega eða mikilvæga starfsemi sem veitt er af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu falli undir sjálfstæða endurskoðun og sé hluti af endurskoðunaráætluninni.
8. Í stefnunni skal skýrt tekið fram að samningsbundna fyrirkomulagið:
- a) leysi aðilann á fjármálamarkaði og stjórn og/eða framkvæmdastjórn hans ekki undan lögbundnum skuldbindingum sínum og skyldum gagnvart viðskiptavinum,
 - b) megi ekki koma í veg fyrir skilvirkt opinbert eftirlit með aðila á fjármálamarkaði, né stangast á við neinar takmarkanir á eftirliti með þjónustu og starfsemi,
 - c) verði að innihalda kröfur um að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafi samstarf við lögbær yfirvöld,
 - d) verði að innihalda kröfur um að aðilinn á fjármálamarkaði, endurskoðendur hans og lögbær yfirvöld hafi virkan aðgang að gögnum og athafnasvæði í tengslum við notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

4. gr.

Meginfasar í lífsferli samningsbundins fyrirkomulags að því er varðar samþykkt og notkun

Stefnan skal tilgreina kröfur, þ.m.t. reglur, ábyrgð og ferla, fyrir sérhvern meginfasa í lífsferli samningsbundins fyrirkomulags, sem ná a.m.k. yfir eftirfarandi:

- a) ábyrgð stjórnar og/eða framkvæmdastjórnar, þ.m.t. þátttaka hennar, eins og við á, í ákvarðanatökuferli um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,
- b) skipulagningu samningsbundins fyrirkomulags, þ.m.t. áhættumat, áreiðanleikakönnun eins og sett er fram í 5. og 6. gr. og samþykkisferli varðandi nýjar eða umtalsverðar breytingar á samningsbundnu fyrirkomulagi, eins og sett er fram í 4. mgr. 8. gr.,
- c) aðkomu rekstrareininga, innra eftirlits og annarra viðeigandi eininga að því er varðar samningsbundið fyrirkomulag,
- d) innleiðingu, vöktun og stjórnun samningsbundins fyrirkomulags, eins og um getur í 7., 8. og 9. gr., þ.m.t. á samstæðu- og undirsamstæðugrunni, eftir atvikum,
- e) skjalfestingu og skráahald, að teknu tilliti til krafna að því er varðar skráningu upplýsinga sem mælt er fyrir um í 3. mgr. 28. gr. reglugerðar (ESB) 2022/2554,
- f) útgönguáætlanir og uppsagnarferli, eins og sett er fram í 10. gr.

5. gr.

Fyrirframáhættumat

1. Stefnan skal innihalda kröfur um að viðskiptaþarfir aðila á fjármálamarkaði séu skilgreindar áður en samningsbundið fyrirkomulag er gert.
2. Stefnan skal innihalda kröfur um að gert sé áhættumat á stigi aðila á fjármálamarkaði og, eftir atvikum, á samstæðu- og undirsamstæðugrunni áður en samningsbundið fyrirkomulag er gert.

Áhættumatið skal taka tillit til allra viðeigandi krafna sem mælt er fyrir um í reglugerð (ESB) 2022/2554 og gildandi geirasértækri löggjöf Sambandsins. Með því skal einkum meta þau áhrif sem þjónusta þriðju aðila, sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi, hefur á aðila á fjármálamarkaði og alla þá áhættu sem skapast af veitingu þriðju aðila á þeirri upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi, þ.m.t. eftirfarandi:

- a) rekstraráhættu,
- b) lagalegri áhættu,
- c) upplýsinga- og fjarskiptatækniáhættu,
- d) orðsporsáhættu,
- e) áhættu sem tengist vernd trúnaðar- eða persónuupplýsinga,
- f) áhættu sem tengist aðgengi að gögnum,
- g) áhættu sem tengist þeirri staðsetningu þar sem gögn eru unnin og geymd,
- h) áhættu sem tengist staðsetningu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,
- i) upplýsinga- og fjarskiptatækniáhættu á einingastigi.

6. gr.

Áreiðanleikakönnun

1. Stefnan skal setja fram viðeigandi og hlutfallslegt ferli fyrir val og mat á líklegum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu að teknu tilliti til þess hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé veitandi upplýsinga- og fjarskiptatækniþjónustu innan samstæðu og gera kröfu um að áður en aðili á fjármálamarkaði gerir samningsbundið fyrirkomulag, meti hann hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu:
 - a) hafi viðskiptalegt orðspor, fullnægjandi getu, sérfræðiþekkingu og fullnægjandi fjármagn, mannauð og tækniúrræði, upplýsingaöryggisstaðla, viðeigandi stjórnskipulag, áhættustýringu og innra eftirlit og, ef við á, áskilin starfsleyfi eða skráningar til að veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi á áreiðanlegan og faglegan hátt,
 - b) hafi getu til að vakta viðeigandi tækniþróun og bera kennsl á leiðandi aðferðir í upplýsinga- og fjarskiptatækniöryggi og innleiða þær þar sem við á, til að hafa skilvirkan og traustan ramma fyrir stafrænan rekstrarlegan viðnámsþrótt,
 - c) noti eða hyggist nota undirverktaka í upplýsinga- og fjarskiptatækni til að sinna upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða umtalsverðan hluta hennar,
 - d) sé staðsettur eða vinni eða geymi gögn í þriðja landi og, ef svo er, hvort sú framkvæmd hafi áhrif á umfang rekstrar- eða orðsporsáhættu eða hættuna á því að verða fyrir áhrifum af takmarkandi ráðstöfunum, þ.m.t. viðskiptabönnum og refsiaðgerðum, sem kunna að hafa áhrif á getu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að veita upplýsinga- og fjarskiptatækniþjónustuna eða aðila á fjármálamarkaði til að fá þá upplýsinga- og fjarskiptatækniþjónustu,
 - e) samþykki samningsbundið fyrirkomulag sem tryggir að aðilinn á fjármálamarkaði sjálfur, tilnefndir þriðju aðilar og lögbær yfirvöld geti framkvæmt úttektir, þ.m.t. vettvangsathuganir, á skilvirkan hátt hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. á staðnum,

- f) komi fram á siðferðislega og samfélagslega ábyrgan hátt, virði mannréttindi og réttindi barna, þ.m.t. bann við barnavinnu, virði gildandi meginreglur um umhverfisvernd og tryggi viðunandi vinnuskilyrði.
2. Stefnan skal tilgreina áskilið fullvissustig varðandi skilvirkni áhættustýringarramma þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Stefnan skal innihalda kröfur um að áreiðanleikaferlið feli í sér mat á því hvort ráðstafanir séu til staðar til áhættumildunar og rekstrarsamfellu og hvernig tryggt sé að þær virki hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.
3. Stefnan skal ákvarða áreiðanleikaferlið fyrir val og mat á þriðju aðilum sem til greina kemur að veiti upplýsinga- og fjarskiptatækniþjónustu og tilgreina hverjum eftirfarandi þátta eigi að beita fyrir tilskilið fullvissustig á frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu:
- a) úttekt eða sjálfstætt mat sem aðili á fjármálamarkaði gerir sjálfur eða er gert fyrir hans hönd,
 - b) notkun óháðra endurskoðunarskýrsla sem unnar eru að beiðni þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,
 - c) notkun endurskoðunarskýrsla sem gerðar eru af deild innri endurskoðunar hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,
 - d) notkun viðeigandi vottana þriðja aðila,
 - e) notkun annarra viðeigandi upplýsinga sem eru aðgengilegar aðilanum á fjármálamarkaði eða annarra upplýsinga frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.
4. Aðilar á fjármálamarkaði skulu tryggja viðeigandi fullvissustig fyrir frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, að teknu tilliti til þáttanna sem eru settir fram í a- til e-lið 3. mgr. Nota skal fleiri en einn þátt sem taldir eru upp í þessum liðum, eftir því sem við á.

7. gr.

Hagsmunaárekstrar

1. Stefnan skal tilgreina viðeigandi ráðstafanir til að skilgreina, koma í veg fyrir og stjórna raunverulegum eða mögulegum hagsmunaárekstrum sem stafa af notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, sem gera verður áður en viðkomandi samningsbundið fyrirkomulag er gert og skal kveða á um áframhaldandi vöktun á slíkum hagsmunaárekstrum.
2. Ef veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi skal stefnan tilgreina að ákvarðanir um skilyrði, þ.m.t. fjárhagsleg skilyrði, fyrir upplýsinga- og fjarskiptatækniþjónustunni verði að taka á hlutlægan hátt.

8. gr.

Samningsákvæði

1. Í stefnunni skal tilgreint að viðkomandi samningsbundið fyrirkomulag eigi að vera á skriflegu formi og innihalda öll atriði sem um getur í 2. og 3. mgr. 30. gr. reglugerðar (ESB) 2022/2554. Í stefnunni skulu einnig koma fram atriði varðandi kröfurnar sem um getur í a-lið 1. mgr. 1. gr. reglugerðar (ESB) 2022/2554, sem og annarra viðeigandi laga Sambandsins og landslaga eins og við á.
2. Í stefnunni skal tilgreint að viðkomandi samningsbundið fyrirkomulag verði að fela í sér rétt aðila á fjármálamarkaði til að hafa aðgang að upplýsingum, framkvæma skoðanir og úttektir og gera prófanir á upplýsinga- og fjarskiptatækni. Í því skyni skal þess krafist í stefnunni að aðili á fjármálamarkaði noti eftirfarandi aðferðir, með fyrirvara um endanlega ábyrgð aðila á fjármálamarkaði:
- a) eigin innri úttekt eða úttekt tilnefnds þriðja aðila,

- b) eftir því sem við á, samsettar úttektir og samsettar prófanir á upplýsinga- og fjarskiptatækni, þ.m.t. ógnamiðuð innbrotsprófun, sem eru skipulagðar í sameiningu með öðrum samningsbundnum aðilum á fjármálamarkaði eða fyrirtækjum sem nota upp-
lýsinga- og fjarskiptatækniþjónustu frá sama þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og sem þessi samningsbundnu aðilar á fjármálamarkaði eða fyrirtæki eða þriðji aðili sem þau hafa tilnefnt framkvæma,
- c) eftir því sem við á, vottanir þriðja aðila,
- d) eftir því sem við á, innri endurskoðunarskýrslur eða endurskoðunarskýrslur þriðja aðila frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.
3. Aðili á fjármálamarkaði skal ekki til lengri tíma reiða sig eingöngu á vottanirnar sem um getur í c-lið 2. mgr. eða endurskoðunarskýrslur sem um getur í d-lið þeirrar málsgreinar. Stefnan skal aðeins heimila notkun aðferðanna sem um getur í c- og d-lið 2. mgr. ef aðili á fjármálamarkaði:
- a) telur endurskoðunaráætlun þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu fullnægjandi fyrir viðkomandi samningsbundið fyrirkomulag,
- b) tryggir að umfang vottana eða endurskoðunarskýrslna nái yfir kerfin og lykilstýringar sem hann hefur skilgreint og tryggir að farið sé að viðeigandi kröfum samkvæmt reglum,
- c) gerir ítarlegt mat á efni vottana eða endurskoðunarskýrslna á áframhaldandi grundvelli og sannprófar að skýrslur eða vottanir séu ekki úreltar,
- d) tryggir að fjallað sé um helstu kerfi og stýringar í síðari útgáfum vottunar eða endurskoðunarskýrslu,
- e) telur færni vottunar- eða endurskoðunarfyrirtækis vera fullnægjandi,
- f) er fullviss um að vottanirnar séu gefnar út og úttektirnar gerðar á grundvelli almennt viðurkenndra viðeigandi fagstaðla og feli í sér prófun á rekstrarskilvirkni þeirra lykilstýringa sem er til staðar,
- g) hefur samningsbundinn rétt til að óska, eins oft og sanngjarnt og lögmætt þykir út frá sjónarmiði áhættustýringar, eftir breytingum á umfangi vottunar eða endurskoðunarskýrslna á öðrum viðeigandi kerfum og eftirliti,
- h) hefur samningsbundinn rétt til að framkvæma stakar og samsettar úttektir að eigin ákvörðun með tilliti til samningsbundins fyrirkomulags og nýta þau réttindi í samræmi við umsamda tíðni.
4. Stefnan skal tryggja að umtalsverðar breytingar á samningsbundnu fyrirkomulagi séu gerðar á formlegan hátt í skriflegu skjali sem er dagsett og undirritað af öllum aðilum og skal tilgreina endurnýjunarferli fyrir samningsbundið fyrirkomulag.

9. gr.

Vöktun á samningsbundnu fyrirkomulagi

1. Í stefnunni skal krefjast að samningsbundið fyrirkomulag tilgreini þær ráðstafanir og helstu vísa sem á að vakta á áframhaldandi grundvelli, frammistöðu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. ráðstafanir til að vakta hlítina við kröfur varðandi trúnað, tiltækileika, heilleika og ósvikni gagna og upplýsinga og hlítina þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu við viðeigandi stefnur og verklagsreglur aðila á fjármálamarkaði. Í stefnunni skulu einnig tilgreindar ráðstafanir sem gilda þegar þjónustusamningar eru ekki uppfylltir, þ.m.t. samningsbundin viðurlög, eftir því sem við á.
2. Stefnan skal tilgreina hvernig aðili á fjármálamarkaði skal meta hvort þeir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru notaðar fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi uppfylli viðeigandi frammistöðu- og gæðastaðla í samræmi við samningsbundið fyrirkomulag og eigin stefnur aðila á fjármálamarkaði. Með stefnunni skal einkum tryggja eftirfarandi:
- a) að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skili viðeigandi skýrslum um aðgerðir sínar og þjónustu til aðilans á fjármálamarkaði, þ.m.t. reglubundnum skýrslum, atvikaskýrslum, þjónustuskýrslum, skýrslum um öryggi í upplýsinga- og fjarskiptatækni og skýrslum um rekstrarsamfellu og prófun,

- b) að frammistaða þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sé metin með lykilárangursvísunum, lykilstýringarvísunum, úttektum, sjálfvottunum og óháðum úttektum í samræmi við áhættustýringarramma aðila á fjármálamarkaði,
- c) að aðili á fjármálamarkaði fái aðrar viðeigandi upplýsingar frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,
- d) að aðila á fjármálamarkaði sé tilkynnt, eftir því sem við á, um atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik,
- e) að framkvæmd sé óháð úttekt og endurskoðun til að sannreyna að farið sé að öllum kröfum samkvæmt lögum og reglum og stefnum.

3. Í stefnunni skal tilgreint að skjalfesta skuli matið sem um getur í 2. mgr. og að nota eigi niðurstöður þess til að uppfæra áhættumat aðila á fjármálamarkaði sem um getur í 6. gr.

4. Með stefnunni skal koma á fót viðeigandi ráðstöfunum sem aðili á fjármálamarkaði þarf að grípa til ef hann uppgötvar annmarka á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik, í tengslum við veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða í samræmi við samningsbundið fyrirkomulag eða lagakröfur. Jafnframt skal tilgreina hvernig vakta eigi framkvæmd slíkra ráðstafana til að tryggja að þeim sé framfylgt með skilvirkum hætti innan tiltekins tímaramma, að teknu tilliti til þess hversu alvarlegir annmarkarnir eru.

10. gr.

Útganga úr og uppsögn á samningsbundnu fyrirkomulagi

Stefnan skal fela í sér kröfur um skjalfesta útgönguáætlun fyrir sérhvert samningsbundið fyrirkomulag og um reglubundna endurskoðun og prófun á skjalfestu útgönguáætluninni. Þegar útgönguáætlun er komið á fót skal taka skal tillit til eftirfarandi:

- a) ófyrirsjáanlegra og viðvarandi truflana á þjónustu,
- b) óviðeigandi eða misheppnaðrar veitingar á þjónustu,
- c) óvæntar uppsagnar á samningsbundnu fyrirkomulagi,

Útgönguáætlunin skal vera raunhæf, framkvæmanleg, byggjast á trúverðugum sviðsmyndum og raunhæfum forsendum og vera með áætlaðan framkvæmdatíma sem er í samræmi við útgöngu- og uppsagnarskilmálana sem komið er á með samningsbundna fyrirkomulaginu.

11. 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.