

156. löggjafarþing 2025.

Þingskjal x — x. mál.

Stjórnarfrumvarp.

Frumvarp til laga

um netöryggisvottun á sviði upplýsinga- og fjarskiptatækni.

Frá innviðaráðherra.

1. gr.

Lögfesting.

Ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881 frá 17. apríl 2019 um Netöryggisstofnun Evrópusambandsins (ENISA) og netöryggisvottunarkerfi upplýsinga- og samskiptatækja og niðurfellingu á reglugerð (ESB) 526/2016, sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 75 frá 19. október 2023, skulu hafa lagagildi hér á landi með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar nr. 22/2023 frá 3. febrúar 2023, sbr. einnig bókun 1 um altæka aðlögun við samninginn um Evrópska efnahagssvæðið, sbr. lög um Evrópska efnahagssvæðið, nr. 2/1993, þar sem bókunin er lögfest.

2. gr.

Orðskýringar.

Merking orða í lögum þessum er sem hér segir:

1. *Atvik*: atvik eins og það er skilgreint í 7. lið 4. gr. tilskipunar (ESB) 2016/1148 og 1. tl. 6. gr. laga nr. 78/2019.
2. *Evrópskt netöryggisvottunarkerfi*: heildarbálgur reglna, tæknilegra krafna, staðla og verklagsreglna sem þróaðar eru og komið er á fót á vettvangi Sambandsins og sem gilda um vottun eða samræmismat á tilteknum upplýsinga- og fjarskipta-tæknivörum, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferlum.
3. *Evrópskt netöryggisvottorð*: skjal sem gefið er út af viðeigandi stofu og staðfestir að samræmi tiltekinna upplýsinga- og fjarskiptatæknivara, upp lýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferla við sértækar öryggis-kröfur sem mælt er fyrir um í evrópsku netöryggisvottunarkerfi hafi verið metið.
4. *Faggilding*: faggilding eins og hún er skilgreind í 10. lið 2. gr. reglugerðar (ESB) nr. 765/2008 og 1. tl. 2. gr. laga nr. 24/2006.
5. *Faggildingarstofa í aðildarríki*: faggildingarstofa í aðildarríki eins og hún er skilgreind í 17. lið 2. gr. reglugerðar (ESB) nr. 765/2008.
6. *Fullvissustig*: grundvöllur fyrir tiltrú á því að upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækniferli uppfylli öryggiskröfur tiltekins evrópsks netöryggisvottunarkerfis, gefur til kynna að hvaða marki upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækni-ferli hefur verið metið en mælir ekki sem slíkt öryggi þeirrar upplýsinga-

og fjarskiptatæknivöru, upplýsinga- og fjarskipta-tækniþjónustu eða upplýsinga- og fjarskiptatækniþjónustu sem um er að ræða.

7. *Landsbundið netöryggisvottunarkerfi*: heildarbálgur reglna, tæknilegra krafna, staðla og verklagsreglna sem þróaðar eru og komið er á fót á vettvangi opinbers landsyfirvalds og sem gilda um vottun eða samræmismat á tilteknum upplýsinga- og fjarskiptatæknivörum, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniþjónustu.

8. *Landsbundin stefnuáætlun um öryggi net- og upplýsingakerfa*: landsbundin stefnuáætlun um öryggi net- og upplýsinga-kerfa eins og hún er skilgreind í 3. lið 4. gr. tilskipunar (ESB) 2016/1148.

9. *Meðhöndlun atvika*: meðhöndlun atvika eins og hún er skilgreind í 8. lið 4. gr. tilskipunar (ESB) 2016/114 og 12. tl. 6. gr. laga nr. 78/2019.

10. *Net- og upplýsingakerfi*: net- og upplýsingakerfi eins og skilgreint er í 1. lið 4. gr. tilskipunar (ESB) 2016/1148 og 15. tl. 6. gr. laga nr. 78/2019.

11. *Netógn*: allar hugsanlegar aðstæður, atburðir eða aðgerðir sem gætu valdið skaða, röskun eða haft á annan hátt neikvæð áhrif á net- og upplýsingakerfi, notendur slíkra kerfa og aðra einstaklinga.

12. *Netöryggi*: sú starfsemi sem nauðsynleg er til að vernda net- og upplýsingakerfi, notendur slíkra kerfa og aðra einstaklinga sem verða fyrir netógnum.

13. *Upplýsinga- og fjarskiptatæknivara*: hluti eða hlutar net- eða upplýsingakerfis.

14. *Upplýsinga- og fjarskiptatækniþjónusta*: þjónusta sem felst að öllu eða mestu leyti í því að senda, geyma, endurheimta eða vinna upplýsingar með net- og upplýsingakerfum.

15. *Upplýsinga- og fjarskiptatækniþjónusta*: starfsemi sem framkvæmd er til að hanna, þróa, afhenda eða viðhalda vöru eða þjónustu á sviði upplýsinga- og fjarskiptatækni.

16. *Rekstraraðili nauðsynlegrar þjónustu*: rekstraraðili nauðsynlegrar þjónustu eins og hann er skilgreindur í 4. lið 4. gr. tilskipunar (ESB) 2016/1148 og 17. tl. 6. gr. laga nr. 78/2019.

17. *Samræmismat*: samræmismat, eins og það er skilgreint í 12. lið 2. gr. reglugerðar (ESB) nr. 765/2008 og 4. tl. 2. gr. laga nr. 24/2006.

18. *Samræmismatsstofa*: samræmismatsstofa, eins og hún er skilgreind í 13. lið 2. gr. reglugerðar (ESB) nr. 765/2008.

19. *Sjálfsmat á samræmi*: aðgerð sem framkvæmd er af framleiðanda eða veitanda upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniþjónustu, sem metur hvort þessar upplýsinga- og fjarskipta-tæknivörur, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækniþjónusta uppfylli kröfur tiltekins evrópsks netöryggisvottunarkerfis.

20. *Staðall*: staðall í skilningi 1. liðar 2. gr. reglugerðar (ESB) nr. 1025/2012.

21. *Tækniforskrift*: skjal sem mælir fyrir um tæknilegar kröfur sem upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækniþjónusta skal uppfylla eða samræmismatsaðferðir þar að lútandi.

22. *Veitandi stafrænnar þjónustu*: veitandi rafrænnar þjónustu eins og hann er skilgreindur í 6. lið 4. gr. tilskipunar (ESB) 2016/1148 og 27. tl. 6. gr. laga nr. 78/2019.

3. gr.

Landsbundið netöryggisvottunaryfirvald.

Fjarskiptastofa fer með hlutverk landsbundins netöryggisvottunaryfirvalds á Íslandi samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881. Skal stofnunin annast útgáfu netöryggisvörðna hér á landi þegar við á samkvæmt ákvæðum reglugerðarinnar.

Fjarskiptastofa skal vera sjálfstæð frá þeim aðilum er stofnunin hefur eftirlit með. Starfsemi Fjarskiptastofu er tengist útgáfu evrópskra netöryggisvottorða skal vera aðskilin þeirri starfsemi sem sinnir eftirliti með netöryggisvottunum.

4. gr.

Útvistun.

Fjarskiptastofa getur á grundvelli samnings úthýst verkefnum er varða útgáfu netöryggisvottorða og/eða eftirlits á grundvelli laga þessara og/eða reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881, að hluta eða heild, til skemmri og/eða lengri tíma, til ytri aðila, þ.m.t. faggiltra samræmismatsstofa eða annarra netöryggisvottunaryfirvalda innan Evrópska efnahagssvæðisins. Með samningi skal tryggt að Fjarskiptastofa hafi aðgang að öllum þeim gögnum sem liggja til grundvallar útgáfu netöryggisvottorðs.

Kostnaður sem hlýst af vegna útgáfu evrópsks netöryggisvottorðs skal greiddur af þeim aðila sem óskar netöryggisvottunar.

5. gr.

Eftirlit.

Fjarskiptastofa skal viðhafa eftirlit á grundvelli laga þessara og/eða reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2019/881 og sinna öðrum verkefnum landsbundins netöryggisvottunaryfirvalds.

Fjarskiptastofa getur krafið faggildingarsvið Hugverkastofu, samræmismatsstofur, handhafa evrópskra netöryggisvottorða og útgefendur ESB-samræmisýfirlýsinga um allar upplýsingar og gögn sem nauðsynlegar þykja til að sinna verkefnum sínum. Skulu upplýsingar og gögn afhent innan hæfilegs frests sem stofnunin setur eða með reglubundnum hætti samkvæmt fyrirmælum stofnunarinnar.

Fjarskiptastofu er heimilt að framkvæma úttektir, rannsóknir, prófanir og vettvangsskoðanir til að sinna verkefnum sínum.

Fjarskiptastofa getur mælt fyrir um nauðsynleg tilmæli, fyrirmæli um úrbætur, beitt viðurlögum og lagt bann við háttsemi eftir því sem við getur átt hverju sinni gagnvart þeim sem brjóta gegn ákvæðum laga þessara, reglugerðarinnar, reglna settra samkvæmt þeim eða skilyrðum netöryggisvottunarkerfis.

Fjarskiptastofa getur krafist afturköllunar á evrópsku netöryggisvottorði sem landsbundin netöryggisvottunaryfirvöld gefa út eða evrópsk netöryggisvottorð sem samræmismatsstofur gefa út ef slík vottorð uppfylla ekki skilyrði reglugerðarinnar eða netöryggisvottunarkerfisins.

6. gr.

Tilkynning um faggildingu

Faggildingasvið Hugverkastofu skal upplýsa Fjarskiptastofu um faggildingu sem gefin er út samkvæmt lögum þessum, auk allra breytinga sem kunna að vera gerðar á henni. Fjarskiptastofa annars tilkynningu slíkra faggilda aðila lögunum.

7. gr.

Alþjóðlegt samstarf.

Fjarskiptastofa tekur þátt í starfi evrópsks netöryggisvottunarhóps sem landsbundið netöryggisvottunaryfirvald Íslands samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) nr. 2019/881.

Fjarskiptastofa er tengiliður íslenskra stjórnvalda í neti landsbundna tengifulltrúa samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881.

8. gr.

Réttur til kvörtunar.

Einstaklingar og lögaðilar geta lagt inn kvartanir til útgefanda evrópsks netöryggisvottorðs eða til Fjarskiptastofu þegar um er að ræða vottorð er hefur fullvissustigið hátt.

9. gr.

Málsmeðferð.

Fjarskiptastofa getur að eigin frumkvæði eða eftir ábendingu eða kvörtun tekið mál til meðferðar er varðar ákvæði laga þessara og reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881.

Ef þörf krefur er stofnuninni heimilt að forgangsraða ábendingum og kvörtunum samkvæmt 7. gr. laganna eftir alvarleika og mikilvægi mála.

10. gr.

Réttarúrræði vegna kvartana.

Einstaklingar og lögaðilar geta skotið ákvörðun er teknar eru vegna kvartana samkvæmt 7. gr. laganna vegna ófullnægjandi útgáfu, vanrækslu á að gefa út eða viðurkenna evrópskt netöryggisvottorð sem þeir einstaklingar eða lögaðilar eru handhafar að, til dómstóla og er málshöfðunarfrestur þrír mánuðir frá því að ákvörðun var tekin. Hið sama gildir um vanrækslu Fjarskiptastofu til þess að bregðast við kvörtun samkvæmt 7. gr. laganna. Ákvarðanir Fjarskiptastofu eru endanlegar á stjórnsýslustigi. Málshöfðun frestar ekki réttaráhrifum ákvarðana stofnunarinnar.

11. gr.

Þagnarskylda

Starfsmenn Fjarskiptastofu eru bundnir þagnarskyldu skv. X. kafla stjórnsýslulaga. Þagnarskyldan helst þótt látið sé af starfi.

Þrátt fyrir lagaákvæði um þagnarskyldu má veita netöryggisvottunaryfirvöldum í aðildarríkjum á Evrópska efnahagssvæðinu, Evrópskum netöryggisvottunarahópi, Netöryggisstofnun Evrópusambandsins (ENISA) og Eftirlitsstofnun EFTA, upplýsingar sé það liður annaðhvort í samstarfi ríkjanna samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) nr. 2019/881 frá 17. apríl 2019, eða við úrlausn einstakra mála og slík upplýsingagjöf er nauðsynleg til að unnt sé að framfylgja lögmæltu eftirliti eða verkefnum. Ákvæði þessarar málsgreinar gilda einnig um skipti á upplýsingum við eftirlitsstjórnvöld hér á landi. Fjarskiptastofu er aðeins heimilt að veita eftirlitsstjórnvöldum upplýsingar samkvæmt þessari málsgrein að sá sem upplýsingarnar fær sé háður sams konar þagnarskyldu.

12. gr.

Dagsektir.

Þegar aðili fer ekki að ákvæðum laga þessara, reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2019/881 frá 17. apríl 2019, ákvörðunum eða stjórnvaldsfyrirmælum Fjarskiptastofu, skilyrðum evrópskra netöryggisvottana, veitir ekki þær upplýsingar sem honum er skylt að afhenda stofnuninn eða fer ekki að öðrum kröfum stofnunarinnar er henni heimilt að leggja á og innheimta dagsektir til að tryggja að eftir fyrirmælum stofnunarinnar sé

farið. Ákvarðaðar dagsektir eru aðfararhæfar samkvæmt 5. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989 og renna í ríkissjóð að frádregnum kostnaði við innheimtuna.

Fjárhæð dagsektar skal ákvörðuð með hliðsjón af eðli brotsins. Dagsektir geta numið allt að 1.000.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að kröfur eða fyrirmælunum sé fylgt eða gögn afhent skv. 1. mgr. Önnheimtar dagsektir falla ekki niður þótt aðili verði síðar við kröfu eftirlitstjórnvalds nema sérstök sjónarmið eigi við og Fjarskiptastofa ákveði það sérstaklega.

Ef ákvörðun um dagsektir skv. 1. mgr. er skotið til dómstóla byrja dagsektir ekki að falla á fyrr en dómur er endanlegur. Dagsektir renna í ríkissjóð og má gera aðför til fullnustu þeirra án undangengins dóms eða sáttar.

13. gr.

Stjórnvaldssektir.

Fjarskiptastofa getur lagt stjórnvaldssekt á lögaðila sem brýtur gegn:

- a. evrópskum netöryggisvottunarkerfum,
- b. þriðja bákl reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2019/881 frá 17. apríl 2019,
- c. skyldu til að afhenda Fjarskiptastofu réttar, fullnægjandi og uppfærðar upplýsingar,
- d. stjórnvaldsákvörðunum og -fyrirmælum eða
- e. reglum settum á grundvelli þessara laga.

Sektir skv. 1. mgr. geta numið allt að 4% af heildarveltu síðasta rekstrarárs hjá hverjum þeim aðila sem aðild á að broti ef það leiðir af sér hærri upphæð. Við ákvörðun á fjárhæð sekta skal hafa hliðsjón af eðli og umfangi brota, hvað brot hafa staðið lengi og hvort um ítrekað brot er að ræða.

Ákvarðaðar stjórnvaldssektir eru aðfararhæfar skv. 5. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989, og renna í ríkissjóð að frádregnum kostnaði við innheimtuna. Sé stjórnvaldssekt ekki greidd innan mánaðar frá ákvörðun Fjarskiptastofu skal greiða dráttarvexti af fjárhæð sektarinnar. Um ákvörðun og útreikning dráttarvaxta fer eftir lögum um vexti og verðtryggingu.

Stjórnvaldssektum verður beitt óháð því hvort lögbrot eru framin af ásetningi eða gáleysi. Falla má frá sektarákvörðun teljist brot óverulegt eða af öðrum ástæðum sé ekki talin þörf á slíkum sektum til að stuðla að framgangi ákvæða laga þessara.

Ákvörðun Fjarskiptastofu er endanleg á stjórnarsýslustigi. Aðili máls getur skotið ákvörðun um stjórnvaldssekt til dómstóla og er málshöfðunarfrestur þrír mánuðir frá því að ákvörðun var tekin. Málskot frestar aðför.

14. gr.

Reglugerðarheimildir.

Ráðherra er heimilt að kveða á um nánari framkvæmd laga þessara og reglugerðar (ESB) nr. 2019/881 í reglugerðum er m.a., en ekki einvörðungu, fjalla með nánari hætti um:

- a. framkvæmd Fjarskiptastofu,
- b. framkvæmdareglugerðir,
- c. netöryggisvottunarkerfi,
- d. tilkynningar Fjarskiptastofu til framkvæmdarstjórnar ESB,
- e. samræmismöt,
- f. Netöryggisstofnun Evrópu.

15. gr.
Gildistaka.

Lög þessi öðlast þegar gildi.

16. gr.
Breytingar á öðrum lögum.

Við gildistöku laga þessara verða eftirfarandi breytingar á öðrum lögum:

1. Lög um Fjarskiptastofu nr. 75/2021:

- a. f. liður 1. mgr. 30. gr. laganna fellur brott.
- b. Við 1. mgr. 2. gr. laganna bætist nýr stafliður, er verður f. liður, og orðast svo:
Framkvæmd laga nr. xx/xxxx, um netöryggisvottun á sviði upplýsinga- og fjarskiptatækni

Greinargerð.

1. Inngangur.

Frumvarp þetta til heildarlaga um netöryggisvottun á sviði upplýsinga- og fjarskiptatækni var samið af innviðaráðuneytinu. Markmið með framlagningu þess er að innleiða í íslenskan rétt ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2019/881 um Netöryggisstofnun Evrópusambandsins (hér eftir ENISA), um netöryggisvottun upplýsinga- og fjarskiptatækni og um niðurfellingu reglugerðar (ESB) nr. 526/2013 (hér eftir gerð um netöryggi, netöryggisgerðin eða CSA).

Netöryggisgerðin var samþykkt 19. apríl 2019 og kom í framkvæmd í aðildarríkjum Evrópusambandsins 27. júní 2019. Hún var tekin upp í upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 22/2023 frá 3. febrúar 2023 að undangengnu samráði við utanríkismálanefnd Alþingis með vísan til reglna um þinglega meðferð EES-mála. Á fundum sameiginlegu EES-nefndarinnar eru teknar ákvarðanir um hvort viðkomandi gerðir Evrópusambandsins verði felldar inn í EES samninginn. Þegar sameiginlega EES-nefndin hefur tekið ákvörðun um að taka gerð upp í EES-samninginn er gerðin orðin hluti samningsins. EFTA-ríkjunum ber þá að taka hana upp í landsrétt sinn eftir efni og aðlögun að EES-samningnum.

2. Tilefni og nauðsyn lagasetningar.

2.1. Gerð um netöryggi

Framkvæmdarstjórnin lagði fram frumvarp til netöryggisgerðarinnar í september 2017 sem hluta af víðtækum aðgerðum til að takast á við netárásir sem og til að byggja upp sterkt netöryggi innan Sambandsins. Meginmarkmið reglugerðar (ESB) nr. 2019/881 er annars vegar að tryggja ENISA, varanlegan starfsgrundvöll og efla starfsemi hennar á sviði netöryggis og hins vegar að koma á fót samræmdu evrópsku vottunarferli fyrir vörur, þjónustu og ferla á sviði upplýsinga- og fjarskiptatækni (e. Information and Communication Technology- ICT), til þess m.a. að vernda aðgengi, réttleika eða leynd gagna eða tengdrar virkni eða þjónustu sem boðið er upp á með slíkum vörum, þjónustu eða ferlum.

Reglugerðin setur fram margþætt kerfi þar sem framkvæmdastjórn ESB, ENISA, evrópskur netöryggisvottunarahópur (e. European Cybersecurity Certification Group – ECCG), netöryggisvottunarahópur hagsmunaaðila (e. Stakeholder Cybersecurity Certification Group – SCCG) og ríki innan EES svæðisins fara með mismunandi hlutverk. ENISA fer með yfirumsjón með innleiðingu og framkvæmd vottunarferlisins, en ríki innan EES svæðisins sinna eftirliti vottana og í ákveðnum tilvikum, útgáfu vottana. Reglugerðin gerir kröfu um að aðildarríki tilnefni stjórnvald sem netöryggisvottunarstjórnvald er fer með eftirlit, prófanir og vottanir evrópskra netöryggisvottunarkerfa á landsvísi sem og upplýsingaskipti á á evrópskum vettvangi.

Samkvæmt reglugerðinni er það valkvætt fyrir aðila sem bjóða upp á vörur, þjónustu eða ferla á sviði upplýsinga- og fjarskiptatækni að afla vottunar á vöruna/þjónustuna/ferlana. Reglugerðin kveður hins vegar á um að framkvæmdastjórn Evrópusambandsins muni reglulega leggja mat á vottunarferlið og hvort nauðsynlegt sé að gera það að skyldu fyrir ákveðnar vörur/þjónustur/ferli. Fimm árum frá samþykkt reglugerðarinnar hafa engin áform verið birt um að skylda slíka vottun. Í nýrri reglugerð (ESB) nr. 37/2025, gerir breytingar á reglugerð (ESB) nr. 2019/811, verður gildissvið reglugerðarinnar víkkað þannig að hún nái einnig til stýrðrar öryggisþjónustu (e. managed security services). Þann 11. apríl 2025 opnaði framkvæmdarstjórnin samráð vegna mögulegrar endurskoðunar á reglugerðinni. Er það m.a. liður í verkefnum framkvæmdarstjórnarinnar um að einfalda reglugverk. Endurskoðunin á að einbeita sér að því að skýra umboð ENISA og bæta evrópska netöryggisvottunarkerfið (e. European Cybersecurity Certification Framework) til að ná betri viðnámsþrótti. Einnig á endurskoðunin að straumlínulaga, einfalda og bæta gerðina til þess að gera innleiðingu evrópska netöryggisvottunarkerfisins notenda- og viðskiptavænna. Endurskoðunin á einnig að kveða á um forgangsriðun aðgerða er styðja við markmið Evrópusambandsins er varða þróun öruggra og viðnámsþolinna birgjakæða, þ.m.t. evrópskan netöryggis iðnaðargrunn (e. industrial base).

2.2. Mat á nauðsyn og mögulegar leiðir við lagasetningu

Við setningu laga um fjarskiptastofu nr. 75/2021, var ráðherra veitt heimild í f.-lið, 1. mgr. 30. gr. laganna til að setja reglugerð til innleiðingar á umræddri reglugerð Evrópuþingsins og ráðsins (ESB) nr. 2019/881. Þeirri heimild hefur þó ekki verið nýtt. Þar sem að reglugerðin tilgreinir margvíslegar skyldur og heimildir stjórnvalda til upplýsingaöflunar og álagningu viðurlaga er nauðsynlegt að kveða skýrt á um slíkar heimildir stjórnvalda í lögum, en ekki eingöngu reglugerð.

3. Meginefni frumvarpsins.

3.1. Samantekt.

Meginmarkmið reglugerðar (ESB) nr. 2019/881 er annars vegar að tryggja ENISA, varanlegan starfsgrundvöll og efla starfsemi hennar á sviði netöryggis. Hins vegar er markmið reglugerðarinnar einnig að koma á fót samræmdu evrópsku vottunarferli fyrir vörur, þjónustu og ferla á sviði upplýsinga- og fjarskiptatækni (e. Information and Communication Technology – ICT), til þess m.a. að vernda aðgengi, réttleika eða leynd gagna eða tengdrar virkni eða þjónustu sem boðið er upp á með slíkum vörum, þjónustu eða ferlum. Í kjölfarið á breytingarreglugerð (ESB) nr. 2025/37 mun gildissvið reglugerðarinnar einnig ná til öryggisþjónustutaka (e. managed security services providers).

3.2 Netöryggisstofnun Evrópusambandsins (e. European Union Agency for Cybersecurity - ENISA)

3.2.1. Inngangur

ENISA var stofnuð árið 2004 með það að markmiði að efla netöryggi innan aðildarríkja Evrópusambandsins og styðja við þróun og framkvæmd laga og reglna á sviði netöryggis. Stofnunin m.a. stuðlar að auknu trausti á stafrænum vörum, þjónustu og ferlum með því að þróa vottunarkerfi fyrir netöryggi, sem miða að því að samræma öryggis staðla og tryggja að stafrænar lausnir uppfylli strangar netöryggiskröfur. ENISA starfar í nánú samstarfi við aðildarríki og stofnanir þeirra og gegnir lykilhlutverki í að styrkja netöryggisumgjörð Evrópu. Með gildistöku reglugerðarinnar í Evrópu var ENISA gefið varanlegt umboð og var sérstaklega horft til þess að efla viðbragðsgetu stofnunarinnar sem stuðningsaðila við aðrar stofnanir Evrópusambandsinssem og ríki á Evrópska efnahagssvæðinu. Meðal hlutverka ENISA er að stuðla að auknu viðbúnaðarstigi, byggja upp getu, framkvæma reglubundnar æfingar vegna netógnna, taka á móti tilkynningum frá ríkjum um öryggisatvik, hýsa samráðsvettvang landstengiliða netöryggissveita, veita ráðgjöf og gefa út leiðbeiningar. ENISA á að verða þekkingarmiðstöð um netöryggismál, beita sér fyrir almennri fræðslu á því sviði og aðstoða ríki á Evrópska efnahagssvæðinu við að stuðla að vitund borgara um netöryggi.

3.2.2. Kaflar reglugerðarinnar er fjalla um ENISA

II. bálkur reglugerðarinnar fjallar um ENISA en 1. kafla II. bálks reglugerðarinnar fjallar um umboð og markmið stofnunarinnar. Líkt og kom fram í kafla 3.2.1. frumvþarsins er ENISA er sérfræðistofnun á sviði netöryggis er veitir faglega ráðgjöf og stuðning við stofnanir Evrópusambandsins og aðildarríki. Hún styður við þróun stefnu, eflingu getu og bætir viðbragðsgetu við netógnunum innan sambandsins. ENISA stuðlar að samstarfi og upplýsingamiðlun milli opinberra og einkaaðila í netöryggismálum. Hún vinnur einnig að innleiðingu evrópsks vottunarkerfis og eflingu netöryggisvitundar meðal almennings, fyrirtækja og stofnana.

Í 2. kafla II. bálks reglugerðarinnar er tilgreint með nánari hætti hver verkefni stofnunarinnar eru en hún skal m.a. stuðla að þróun og framkvæmd stefnu og laga Evrópusambandsins, byggja upp færni þess, styðja við rekstrarsamstarf (e. operational cooperation) milli aðildarríkja. Í 3. kafla II. bálks reglugerðarinnar er gerð grein fyrir uppbyggingu og skipulagi netöryggisstofnunarinnar en sbr. 13. gr. reglugerðarinnar samanstendur ENISA af stjórn (e. Management board), framkvæmdarstjórn (e. Executive Board), framkvæmdastjóra (e. The Executive Director), ráðgjafarhópi (e. Advisory Group (AG)) og neti landsbundinna tengifulltrúa (e. National Liaison Officers Network (NLOs)). Stjórn ENISA að tryggja að stofnunin uppfylli verkefni sín við viðeigandi aðstæður til að starfa á skilvirkan hátt samkvæmt reglugerðinni. Framkvæmdarstjórn ENISA undirbýr ákvarðanir sem að verða samþykktar af stjórninni. Framkvæmdastjóri ENISA ber ábyrgð á stjórnun stofnunarinnar og sinnir störfum sínum sjálfstætt. Net landsbundinna tengifulltrúa greiða fyrir upplýsingaskipti milli ENISA og aðildarríkja sambandsins. Ráðgjafarhópurinn aðstoðar ENISA við að móta starfsáætlun sína, stefnumótandi markmið sín og eiga samskipti við aðal hagsmunaaðila (e. key stakeholders). Þá er í 4. kafla II. bálks reglugerðarinnar fjallað um framkvæmd og efnisskipan fjárlaga ENISA sem og í 5. kafla II. bálks reglugerðarinnar er fjallað um starfsfólk ENISA. Að lokum er í 6. kafla II. bálks að finna almenn ákvæði um ENISA líkt og ákvæði um réttarstöðu stofnunarinnar, bótaábyrgð, tungumálanotkun og samstarf við þriðju lönd og alþjóðastofnanir.

3.3. Evrópsk netöryggisvottunarkerfi (e. European cybersecurity certification framework)

Samkvæmt 46. gr. reglugerðarinnar á evrópska netöryggisvottunarkerfið að bæta skilyrði fyrir starfsemi innri markaðar með því að auka netöryggisstig innan Evrópusambandsins sem og greiða fyrir samhæfða nálgun á vettvangi Evrópusambandsins í því skyni að skapa stafrænan innri markað fyrir vörur, þjónustu og ferli á sviði upplýsinga- og fjarskiptatækni. Evrópska netöryggisvottunarkerfið á að þjóna tvíþættum tilgangi, í fyrsta lagi að stuðla að auknu trausti á upplýsinga- og fjarskiptatækniþjónustu, vörur- eða ferla sem hafa nú þegar hlotið vottun samkvæmt evrópskum netöryggisvottunarkerfum. Í öðru lagi ætti það að koma í veg fyrir margföldun á innlendum netöryggisvottunarkerfum sem stangast á eða skarast og þar með draga úr kostnaði fyrir fyrirtæki sem starfa innan stafræna innri markaðarins.

Evrópska netöryggisvottunarkerfið skal kveða á um fyrirkomulag til þess að koma á fót evrópskum netöryggisvottunarkerfum sem staðfesta að upplýsinga- og fjarskiptatæknivörur-, þjónustu - og ferli, sem metin hafa verið í samræmi við slík kerfi, uppfylli tilgreindar öryggiskröfur í þeim tilgangi að vernda aðgengileika, sannvottaðan uppruna, réttleika eða leynd vistaðra, sendra eða unninna gagna eða tengdrar virkni eða þjónustu sem boðin er eða er aðgengileg í gegnum þessar vörur, þjónustu eða ferli á líftíma (e. life cycle) þeirra.

Evrópskt netöryggisvottunarkerfi á að byggja á því sem nú þegar er til staðar á alþjóðlegum og innlendum vettvangi, og ef þörf krefur, á tæknilýsingum frá vettvöngum og samtökum, með því að læra af þeim styrkleikum sem nú þegar eru fyrir hendi og meta og leiðrétta veikleika. Tilgangur evrópskra netöryggisvottunarkerfa er að tryggja að upplýsinga- og fjarskiptatæknivörur-, þjónusta- eða ferlar sem hljóta slíka vottun uppfylli tilteknar kröfur sem miða að því að vernda aðgengi, áreiðanleika, réttleika og leynd gagna og tengdra aðgerða eða þjónustu yfir líftíma þeirra. Þó er ekki unnt að skilgreina nákvæmlega samræmdar kröfur í reglugerðinni sökum fjölbreytileika í upplýsingatæknilausnum. Því byggir reglugerðin á víðtækri og almennri skilgreiningu á netöryggi í vottunarskyni sem studd er af tilteknum öryggismarkmiðum sem hafa skal til hliðsjónar við hönnun vottunarkerfa.

Samkvæmt 48. gr. reglugerðarinnar getur framkvæmdarstjórn óskað eftir því að ENISA útbúi og þrói evrópsk netöryggisvottunarkerfi. Evrópsku netöryggisvottunarkerfin er ENISA útbýr skulu uppfylla skilyrði 51., 52., og 54. gr. reglugerðarinnar en 49. gr. reglugerðarinnar fjallar um ferli undirbúnings, samþykkis og endurskoðun evrópskra netöryggisvottunarkerfa.

Samkvæmt 50. gr. reglugerðarinnar skal ENISA halda úti sérstöku vefsetri þar sem veittar eru upplýsingar um og vakin er athygli á evrópskum netöryggisvottunarkerfum, evrópskum netöryggisvottorðum og ESB-samræmisyfirlýsingum.

Þá er það í höndum framkvæmdarstjórnarinnar að meta reglulega skilvirkni og notkun samþykktra evrópskra netöryggiskerfa auk þess að leggja mat á það hvort gera eigi sérstakt evrópskt netöryggisvottunarkerfi að skyldu með viðeigandi lögum Evrópusambandsins til þess að tryggja fullnægjandi netöryggi slíkra vara, þjónustu og ferla í Evrópusambandinu og með því bæta virkni innri markaðarins. Mat á þessu skal framkvæmt á að minnsta kosti tveggja ára fresti. Við undirbúning á matinu skal framkvæmdarstjórnin í fyrsta lagi taka tillit til þeirra áhrifa sem aðgerðirnar hafa á framleiðendur eða veitendur upplýsinga- og fjarskiptatækni vara-, þjónustu- eða ferla og á notendur með tilliti til kostnaðar við þær ráðstafanir og samfélagsleg eða efnahagslegs ávinnings sem stafar af væntanlegu auknu öryggisstigi fyrir slíkar vörur, þjónustu eða ferla. Í öðru lagi skal framkvæmdarstjórnin við undirbúning matsins taka tillit til tilvistar og framkvæmda viðeigandi laga aðildarríkis og þriðja lands. Í þriðja lagi þarf framkvæmdarstjórnin að framkvæma opið, gagnsætt og innifalið samráðsferli við alla viðeigandi hagsmunaaðila og aðildarríki. Í fjórða lagi skal framkvæmdarstjórnin taka tillit til

allra innleiðingarfesta, bráðabirgðaráðstafana og tímabila, einkum með tilliti til mögulegra áhrifa ráðstöfunarinnar á framleiðendur eða veitendur upplýsingatæknivara, upplýsingatækniþjónustu eða upplýsingatækniþjónustu, þar með talið lítil og meðalstór fyrirtæki. Að lokum, í fimmta lagi, skal framkvæmdarstjórnin leggja til leið sem verður talin fljótleg og skilvirk til að færa úr fjálsum vottunarkerfum yfir í lögboðin vottunarkerfi

3.3.1. Öryggismarkmið evrópskra netöryggisvottunarkerfa:

Evrópsk netöryggisvottunarkerfi skulu vera hönnuð til þess að ná, eftir því sem við á, a.m.k. eftirfarandi öryggismarkmiðum er tilgreind eru í 51. gr. reglugerðarinnar. Í fyrsta lagi að vernda geymd, send eða á annan hátt unnin gögn gegn slysi eða óleyfilegri geymslu, vinnslu, aðgangi eða birtingu á öllum líftíma af upplýsinga- og fjarskiptatæki vöru-, þjónustur- og ferla, sbr. a-lið 1. mgr. 51. gr. reglugerðarinnar. Í öðru lagi vernda geymd, send eða unnin á annan hátt gögn gegn slysi eða óleyfilegri eyðileggingu, tapi eða breytingu eða skorti á aðgengi á öllum líftíma upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferla, sbr. b-lið 1. mgr. 51. gr. reglugerðarinnar. Í þriðja lagi að viðurkenndir aðilar, forrit eða vélar geti aðeins fengið aðgang að gögnum, þjónustu eða aðgerðum sem aðgangsréttur þeirra vísar til, sbr. c-lið 1. mgr. 51. gr. reglugerðarinnar. Í fjórða lagi að bera kennsl á og skjalfesta þekkt hæði (e. known dependencies) og veikleika, sbr., d-lið 1. mgr. 51. gr. reglugerðarinnar. Í fimmta lagi að gert sé mögulegt að athuga hvaða gögn, þjónustu eða aðgerðir hafa verið opnaðar, notaðar eða unnar á annan hátt, á hvaða tímum og af hverjum, sbr. e-lið 1. mgr. 51. gr. reglugerðarinnar. Í sjötta lagi að sannreyna að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar innihaldi ekki þekkta veikleika, sbr. f-lið 1. mgr. 51. gr. reglugerðarinnar. Í sjöunda lagi að endurheimta framboð og aðgang að gögnum, þjónustu og aðgerðum tímanlega ef líkamlegt eða tæknilegt atvik kemur upp, sbr. h-lið 1. mgr. 51. gr. reglugerðarinnar. Í áttunda lagi að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar séu öruggir sjálfgefið og í hönnun (e. secure by default and by design), sbr. i-lið 1. mgr. 51. gr. reglugerðarinnar. Að lokum, í níunda lagi, að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar séu búnir uppfærðum hugbúnaði og vélabúnaði sem inniheldur ekki þekktra veikleika og sé með kerfi fyrir öruggar uppfærslur, sbr. j-lið 1. mgr. 51. gr. reglugerðarinnar.

3.3.2. Fullvissustig (e. assurance levels) evrópskra netöryggisvottunarkerfa

Evrópsk netöryggisvottunarkerfi geta tilgreint eitt eða fleiri fullvissustig fyrir upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferla sem skiptast í „lágt“ (e. basic), „verulegt“ (e. substantial) eða „hátt“ (e. high) sbr. 52. gr. reglugerðarinnar. Fullvissustigunum er ætlað að vera í samræmi við það áhættustig sem tengist fyrirhugaðri notkun upplýsinga- og fjarskiptatækni vöru-, þjónustu- og ferla, með tilliti til líkinda og áhrifa atviks. Evrópsk netöryggisvottorð og ESB-samræmisýfirlýsingar (e. statements of conformity) skulu vísa til hvers kyns fullvissustig sem tilgreint er í evrópska netöryggisvottunarkerfinu þar sem evrópsk netöryggisvottorðið eða ESB-samræmisýfirlýsingin er gefin út. Öryggiskröfurnar samsvara hverju fullvissustigiog eru þær veittar í viðkomandi evrópsku netöryggisvottunarkerfi, þar á meðal samsvarandi öryggisaðgerðir og samsvarandi nákvæmni og umfang matsins sem upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar eiga að gangast undir. Netöryggisvottorðið eða ESB-samræmisýfirlýsingin á að vísa í tækniforskriftir, staðla og verklagsreglur sem tengjast þeim, þ.m.t. tæknilegt eftirlit, sem hefur þann tilgang að draga úr hættu á eða koma í veg fyrir netöryggisatvik.

Evrópsk netöryggisvottorð sem eru með fullvissustigið „lágt“ skulu veita tryggingu fyrir því að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sem vottorðin gilda um,

uppfylli samsvarandi öryggiskröfur, þ.m.t. öryggiseiginleika, og að þau hafi verið metin á stigi sem ætlað er til að lágmarka þekkta grunnáhættu atvika og netárása. Matstengdar aðgerðir sem skulu a.m.k. fela í sér yfirferð á tæknilegum gögnum. Þar sem slík yfirferð er ekki viðeigandi skal framkvæmt annars konar matsferli með sambærilegum áhrifum.

Evrópsk netöryggisvottorð sem vísa til fullvissustigsins „verulegt“ skulu veita tryggingu fyrir því að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sem vottorðið gildir um, uppfylli viðeigandi öryggiskröfur, þ.m.t. öryggiseiginleika, og að þau hafi verið metin á því stigi sem ætlað er að lágmarka þekkta netöryggisáhættu og hættu á atvikum og netárásam framkvæmdum af aðilum með takmarkaða færni og úrræði. Matstengdar aðgerðir sem skulu vera framkvæmdar skulu að minnsta kosti fela í sér yfirferð til að sýna fram á fjarveru opinberra veikleika og prófanir til að sýna að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar innleiði rétt nauðsynlega öryggiseiginleika. Þar sem slík matsferli eru ekki viðeigandi skal framkvæmt annars konar matsferli með sambærilegum áhrifum.

Evrópsk netöryggisvottorð sem vísa til fullvissustigs „hátt“ skulu veita tryggingu fyrir því að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sem vottorðin gilda um, uppfylli viðeigandi öryggiskröfur, þar á meðal öryggiseiginleika, og að þau hafi verið metin á því stigi sem er ætlað til að lágmarka áhættuna á háþrúðum netárásam framkvæmdum af aðilum með verulega færni og úrræði. Matstengdar aðgerðir sem skulu framkvæmdar eiga að minnsta kosti fela í sér yfirferð til að sýna fram á fjarveru opinberra veikleika, prófanir til að sýna upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar innleiði rétta nauðsynlega öryggiseiginleika í samræmi við nýjustu tækniþróun, og mat á viðnámi þeirra gegn hæfum árársaðilum með notkun innbrotsprófana. Þar sem slík matsferli eru ekki viðeigandi skal framkvæmt annars konar matsferli með jafngildum áhrifum.

3.3.3. Samræmismat

Samræmismat er ferli sem felur í sér mat á því hvort tiltekna kröfur sem gilda um upplýsinga- og fjarskiptatæknivörur-, þjónustu- eða ferla séu uppfylltar. Sú aðferð er framkvæmd af óháðum þriðja aðila sem er ekki framleiðandi eða veitandi upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækni ferla sem verið er að meta. Gefa ætti út evrópskt netöryggisvottorð eftir að upplýsinga- og fjarskiptatæknivara, -þjónusta eða -ferli hefur staðist mat. Evrópskt netöryggisvottorð ætti að teljast vera staðfesting á því að matið hafi farið fram á tilhlýðilegan hátt. Með hliðsjón af fullvissustiginu ætti evrópskt netöryggisvottunarkerfi að gefa til kynna hvort að einkaaðili eða opinber aðili eigi að gefa út evrópska netöryggisvottorðið. Samræmismat og samræmisvottun tryggja ekki ein og sér að upplýsinga- og fjarskiptatæknivörur, upplýsinga- og fjarskiptatækniþjónusta og upplýsinga- og fjarskiptatækni ferli sem hafa hlotið vottun búi yfir nægilegu netöryggi. Þess í stað eru þetta aðferðir og tæknileg aðferðafræði til að staðfesta að upplýsinga- og fjarskiptatæknivörur, þjónusta og ferli hafi verið prófuð og að þau uppfylli tiltekna öryggiskröfur sem mælt er fyrir um annars staðar, t.d. í tæknistöðlum.

Samkvæmt 4. mgr. 56. gr. reglugerðarinnar skulu samræmismatsstofur samkvæmt 60. gr. reglugerðarinnar skulu gefa út evrópsk netöryggisvottorð er samsvara fullvissustigi „lág“ eða „verulegt“ á grundvelli viðmiða sem eru innifalin í evrópska netöryggisvottunarkerfinu sem framkvæmdastjórnin hefur samþykkt samkvæmt 49. gr. reglugerðarinnar. Þó geta verið ákveðnar undantekningar frá því er tilgreindar eru í 5. mgr. 56. gr. reglugerðarinnar. Þegar krafist er fullvissustigs „hátt“ í evrópsku netöryggisvottunarkerfi sem samþykkt er skv. 49. gr. reglugerðarinnar, eiga einungis landsbundin netöryggisvottunaryfirvöld að gefa út evrópskt

netöryggisvottorð samkvæmt því kerfi, eða samræmismatsstofur í tilteknum tilfellum sbr. 6. mgr. 56. gr. reglugerðarinnar.

Samkvæmt 53. gr. reglugerðarinnar getur evrópskt netöryggisvottunarkerfi heimilað sjálfsmat á samræmi á ábyrgð framleiðanda eða veitanda upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferla. Sjálfsmat á samræmi skal eingöngu heimilað fyrir upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sem fela í sér litla áhættu og samsvara fullvissustigi „lágt.“ Í slíkum tilvikum ætti að nægja að framleiðandi eða veitandi framkvæmi sjálfur allar nauðsynlegar athuganir til að tryggja að viðkomandi vörur, þjónustur eða ferlar séu í samræmi við evrópska netöryggisvottunarkerfið. Framleiðandi eða veitandi upplýsinga- og fjarskiptatækni vöru-, þjónustu- og ferla getur gefið út ESB-samræmisfirlýsingu þar sem fram kemur að staðfest hafi verið að kröfur sem settar eru fram í vottunarkerfinu séu uppfylltar. Með því að gefa út slíka yfirlýsingu tekur framleiðandi eða veitandi á sig ábyrgð á því að upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sé í samræmi við þær kröfur sem fram eru settar í viðkomandi vottunarkerfi. Framleiðandi eða veitandi upplýsinga- og fjarskiptatækni vöru-, þjónustu- og ferlar skal gera ESB-samræmisfirlýsinguna, tæknileg skjöl og allar aðrar viðeigandi upplýsingar um samræmi upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar við vottunarkerfið aðgengilegar fyrir landsbundin netöryggisvottunaryfirvöld, sem kveðið er á um í 58. gr. reglugerðarinnar, á því tímabili sem tilgreint er í viðeigandi evrópsku netöryggisvottunarkerfi. Auk þess skal afrit af ESB-samræmisfirlýsingunni sent til landsbundins netöryggisvottunarstofnunar og ENISA. Þá er útgáfa ESB-samræmisfirlýsingar valkvæð nema annað komi fram í lögum Evrópusambandsins eða landslögum aðildarríkis. Auk þess skulu ESB-samræmisfirlýsingar viðurkenndar í öllum aðildarríkjum. Samræmismat og vottun tryggir ekki í sjálfu sér að vottuð upplýsinga- og fjarskiptatæknivara, þjónusta- eða ferli sé að fullu öruggt m.t.t. netöryggis. Hins vegar staðfestir það að viðkomandi vara, þjónusta eða ferli hafi verið prófað og uppfylli tilteknar netöryggiskröfur sem skilgreindar eru.

Í 54. gr. reglugerðarinnar er kveðið er á um lágmarksþætti sem evrópsk netöryggisvottunarkerfi þurfa að innihalda. Sem dæmi um slíkt er að evrópsk netöryggiskerfi verði að innihalda viðfangsefni og umfang vottunarkerfis, þ.m.t. tegund eða flokka upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferlar sem falla undir það, skýra lýsingu á tilgangi kerfisins og hvernig slíkir staðlar sem hafa orðið fyrir valinu, matsaðferðir og fullvissustig samsvara þörfum fyrirhugaðra notenda kerfisins, vísun í fullvissustig þar sem við á og skýringar á því hvort sjálfsmat á samræmi sé heimilt innan kerfisins. Tilgreindar kröfur evrópsks netöryggisvottunarkerfis skulu vera í samræmi við öll viðeigandi lagaleg skilyrði, einkum þær kröfur sem byggja á samræmdri löggjöf Evrópusambandsins. Ef samræmd löggjöf Evrópusambandsins er ekki fyrir hendi er heimild fyrir löggjöf aðildarríkis um að kveða á um að evrópskt netöryggisvottunarkerfi sé notað til að staðfesta samræmi við lagalegar kröfur.

3.3.4. *Upplýsingar um netöryggi*

Samkvæmt 1. mgr. 55. gr. reglugerðarinnar skulu framleiðendur og veitendur upplýsinga- og fjarskiptatæknivara, þjónustu eða ferla sem eru vottuð eða upplýsinga- og fjarskiptatæknivara, þjónustu og ferla sem ESB-samræmisfirlýsing hefur verið gefin út fyrir gera ákveðnar viðbótarupplýsingar um netöryggi aðgengilegar öllum. Þessar upplýsingar skulu vera aðgengilegar á rafrænu formi og skulu haldast aðgengilegar og vera uppfærðar a.m.k. þar til samsvarandi evrópskt netöryggis-vottorð eða ESB-samræmisfirlýsing fellur úr gildi sbr. 2. mgr. 55. gr. reglugerðarinnar.

3.4. Netöryggisvottun (e. *Cybersecurity certification*)

Líkt og tilgreint er í 2. mgr. 56. gr. reglugerðarinnar skal netöryggisvottun fyrir aðila vera valfrjálts nema annað sé tekið fram, annað hvort ef það leiðir af lögum Evrópusambandsins eða af landslögum aðildarríkisins. Ef upplýsinga- og fjarskiptatæknivörur-, þjónustur- og ferlar hafa verið vottaðar samkvæmt evrópsku netöryggisvottunarkerfi í samræmi við 49. gr. reglugerðarinnar, er gert ráð fyrir að þeir uppfylli kröfur til slíks kerfis sbr. 1. mgr. 56. gr. reglugerðarinnar.

Í 60. gr. reglugerðarinnar er kveðið á um samræmismatsstofur (e. the conformity assessment bodies) en samkvæmt 4. mgr. 56. gr. reglugerðarinnar eiga þær að gefa út evrópsk netöryggisvottorð sem vísa til fullvissustiga, annars vegar „lágt“ (e. basic) og hins vegar „verulegt“ (e. substantial) á grundvelli viðmiða sem eru innifalin í evrópska netöryggisvottunarkerfinu sem framkvæmdarstjórnin hefur samþykkt samkvæmt 49. gr. reglugerðarinnar. Þó geta, að vissum skilyrðum uppfylltum, netöryggisvottunarkerfi kveðið á um að evrópsk netöryggisvottorð, sem leiða af því kerfi, skuli einungis vera gefin út af landsbundnu netöryggisvottunaryfirvaldi eða opinberum aðila sem hefur faggildingu sem samræmismatsstofa, sbr. 5. mgr. 56. gr. gerðarinnar.

Ef netöryggiskerfi, sem samþykkt hefur verið í samræmi við 49. gr. reglugerðarinnar, krefst „hátt“ (e. high) fullvissustigs, þá skal evrópska netöryggisvottorðið samkvæmt því kerfi einungis gefið út af innlendu netöryggisvottunaryfirvaldi eða í ákveðnum tilfellum, af samræmismatsstofu, sbr. 6. mgr. 56. gr. reglugerðarinnar.

3.5. Samræmismatsstofur

Líkt og fram kemur í kafla 3.4. er kveðið á um samræmismatsstofur í 60. gr. reglugerðarinnar. Samræmismatsstofur er hafa hlotið faggildingu skulu uppfylla skilyrði viðauka reglugerðarinnar. Samkvæmt 1. og 4. mgr. 60 gr. skulu samræmismatsstofur hljóta faggildingu landsbundinna faggildingastofa sem gildir að hámarki til fimm ára. Að liðnum fimm árum er hægt að endurnýja faggildinguna með sömu skilyrðum, að því tilskildu að samræmismatsstofan uppfylli enn þá kröfurnar. Ef landsbundið netöryggisvottunaryfirvald gefur út evrópskt netöryggisvottorð skal það einnig hljóta faggildingu samkvæmt 2. mgr. 60. gr. reglugerðinni með sömu skilyrðum. Faggildingarstofur í aðildarríkjum ættu að takmarka, fella tímabundið úr gildi eða afturkalla faggildingu samræmismatsstofu ef skilyrðin fyrir faggildingunni hafa ekki verið uppfyllt eða eru ekki lengur uppfyllt, eða ef samræmismatsstofan brýtur í bága við reglugerðina.

Samkvæmt 1. mgr. 3. gr. laga nr. 24/2006 annast Faggildingarsvið Hugverkastofu faggildingu sem hinn opinberi faggildingaraðili á Íslandi og hefur með höndum allar tegundir faggildinga, bæði þar sem er lagaleg krafa um faggildingu sem og á sviðum þar sem aðilum er í sjálfsvald sett að láta faggilda starfsemi sína.

3.6. Landsbundin netöryggisvottunaryfirvöld (e. *national cybersecurity certification authorities*)

Samkvæmt 58. gr. reglugerðarinnar skal hvert aðildarríki tilnefna eitt eða fleiri landsbundin netöryggisvottunaryfirvöld á yfirráðasvæði sínu eða, með samþykki annars aðildarríkis, tilnefna eitt eða fleiri landbundin netöryggisvottunaryfirvöld með staðfestu í því aðildarríki til að bera ábyrgð á eftirlitsverkefnum í tilnefningaraðildarríkinu. Aðildarríkin skulu svo upplýsa framkvæmdarstjórn Evrópusambandsins um hvaða stjórnvöld verða landsbundin netöryggisvottunaryfirvöld, auk þess ef aðildarríki tilnefnir fleiri en eitt yfirvald þá skulu aðildarríkin upplýsina um verkefnaskiptingu þeirra. Þörf er fyrir aðildarríkin að

tryggja starfsemi netöryggisvottunaryfirvalda, sem tengist netöryggisvottorði sem kveðið er á um í 56. gr. reglugerðarinnar, sé haldið algerlega aðskilinni frá eftirlitsstarfsemi þeirra sem sett er fram í 58. grein og að öll starfsemi fari fram óháð annarri starfsemi. Þá skulu aðildarríkin tryggja að landsbundin netöryggisvottunaryfirvöld hafi nægileg tilföng til að beita valdheimildum sínum og sinna verkefnum sínum á árangursríkan og skilvirkan hátt. Auk þess skulu landsbundin netöryggisvottunaryfirvöld taka þátt í evrópska netöryggisvottunarhópnum með virkum, árangursríkum, skilvirkum og öruggum hætti.

3.6.1. Hlutverk og valdheimildir innlendra netöryggisvottunaryfirvalda

Í 7. mgr. 58. gr. reglugerðarinnar er kveðið á um hvað innlend netöryggisvottunaryfirvöld skuli gera. Í fyrsta lagi má nefna að innlend netöryggisvottunaryfirvöld skulu hafa umsjón með og framfylgja reglum sem fylgja evrópskum netöryggisvottunarkerfum, skv. j.-lið 1. mgr. 54. gr. reglugerðarinnar. Þá skulu innlend netöryggisvottunaryfirvöld hafa eftirlit með því að framleiðendur eða veitendur upplýsingar- og fjarskiptatækni vara, þjónusta- eða ferla sé fylgt eftir og framfylgt þeim sem hafa komið á fót á viðkomandi yfirlitssvæði og framkvæma sjálfsmat á samræmi, og skal einkum fylgjast með því að farið sé að og framfylgja skyldum slíkra framleiðenda eða veitenda sem settar eru fram í 2. og 3. mgr. 53. gr. reglugerðarinnar.

Þá skulu innlend netöryggisvottunaryfirvöld, með fyrirvara um 3. mgr. 60. gr., aðstoða og styðja innlendar faggildingarstofur (e. national accreditation bodies) á virkan hátt við eftirlit með starfsemi samræmismatstofnanna sem og fylgjast með og hafa eftirlit með starfsemi opinberra stofnana sem kveðið er á um í 5. mgr. 56. gr. reglugerðarinnar. Einnig skulu innlend netöryggisvottunaryfirvöld sjá um kvartanir einstaklinga eða lögaðila í tengslum við evrópsk netöryggisvottorð sem hafa verið gefin út af innlendum netöryggisvottunaryfirvöldum eða til evrópsk netöryggisvottorðs gefin út af samræmismatsstofum í samræmi við 6. mgr. 56. gr. reglugerðarinnar eða í tengslum við samræmisýfirlýsingar Evrópusambandsins sem gefnar eru út skv. 53. gr.

Að lokum skulu innlend netöryggisvottunaryfirvöld leggja fram árlega yfirlitsskýrslu um þá starfsemi sem fer fram samkvæmt b-, c- og d.-liðs 7. mgr. 58. gr. reglugerðarinnar eða samkvæmt 8. mgr. 58. gr. reglugerðarinnar til ENISA og ECCG, vinna með öðrum netöryggisvottunaryfirvöldum eða öðrum opinberum yfirvöldum, þ.m.t. með upplýsingaskiptum, og fylgjast með viðeigandi þróun á sviði netöryggisvottunar.

Þá er kveðið á um í 8. mgr. 58. gr. reglugerðarinnar lágmarks valdheimildir innlendra netöryggisvottunaryfirvalda en þar kemur m.a. fram að þau geti krafist tiltekna aðila um upplýsinga, framkvæmt úttektir, geta viðeigandi ráðstafanir til þess að tryggja að samræmismatsstofnanir, handhafar evrópska netöryggisskírteina og útgefendur ESB-samræmisýfirlýsinga uppfylli skilyrði reglugerðarinnar eða evrópskra netöryggisvottunarkerfa, afturkalla evrópsk netöryggisvottorð og beitt viðurlögum. Samkvæmt f.-liði 7. mgr. 58. gr. eiga netöryggisvottunaryfirvöld að hafa heimild til þess að beita refsíákvæðum í samræmi við landslög og krefjast þess að brot gegn skyldunum sem settar eru fram í þessari reglugerð verði stöðvuð án tafar. Samkvæmt 65. gr. reglugerðarinnar skulu aðildarríki setja reglur um viðurlög við brotum gegn rammaákvæðum um netöryggisvottun skv. reglugerðinni sem og gegn evrópskum netöryggisvottunarkerfum og gera allar nauðsynlegar ráðstafanir til að tryggja að þeim sé beitt. Viðurlögin skulu vera skilvirk, í réttu hlutfalli við brotið og hafa letjandi áhrif en aðildarríki skulu án tafar tilkynna framkvæmdastjórninni um þessar reglur og þessar ráðstafanir og skulu tilkynna henni um allar síðari breytingar sem hafa áhrif á þær. Að lokum skulu netöryggisvottunaryfirvöld vinna

saman með hvort öðru og með framkvæmdarstjórninni m.a. hvað varðar upplýsingaskipti og tæknileg atriði.

3.6.2. Jafningjarýni

Í 59. gr. reglugerðarinnar er kveðið á um jafningjarýni (e. peer review) sem komið var á með það markmið í huga að ná jafngildum stöðlum (e. equivalent standards) innan Evrópusambandsins að því er varðar evrópsk netöryggisvottorð og ESB-samræmisýfirlýsingar og því skulu innlend netöryggisvottunaryfirvöld sæta jafningjarýni. Jafningjarýnin fer fram á grundvelli trausta og gagnsærra matsviðmiða og verklagsreglna, einkum hvað varðar uppbyggingu, mannauðs- og ferlacröfur (e. human resource and process requirements), trúnað og kvartanir. Þá skal m.a. leggja mat á hvort starfsemi innlendra netöryggisvottunaryfirvalda sem tengist útgáfu evrópskra netöryggisvottana sem kveðið er á um í a-lið 5. mgr. 56. gr. reglugerðarinnar, verklagsreglur um hvort eftirlit og framfylgd reglna um eftirlit með upplýsinga- og fjarskiptatækni vara, þjónusta og ferla séu í samræmi við evrópsk netöryggisvottorð skv. a-lið 7. mgr. 58. gr., verklagsreglur um eftirlit og leyfi um starfsemi samræmismatsstofnana og eftir því sem við á, hvort starfsfólk yfirvalda eða stofnana sem gefa út vottorð fyrir „hátt“ fullvissutíg skv. 6. mgr. 56. gr. reglugerðarinnar hafi viðeigandi sérfræðipækkingu. Jafningjarýnin skal framkvæmd af a.m.k. tveimur netöryggisvottunaryfirvöldum annarra aðildarríkja og framkvæmdarstjórninni á að minnsta kosti fimm ára fresti auk þess sem ENISA getur tekið þátt í ritryni.

3.6.3. Tilkygningar

Samkvæmt 61. gr. reglugerðarinnar skulu landsbundnu netöryggisvottunaryfirvöldin tilkynna framkvæmdastjórninni fyrir hvert evrópskt netöryggisvottunarkerfi um þær samræmismatsstofur sem hafa hlotið faggildingu og, eftir atvikum, fengið heimild skv. 3. mgr. 60. gr. til að gefa út evrópsk netöryggisvottorð á tilgreindum fullvissustígum eins og um getur í 52. gr. Að auki skulu landsbundnu netöryggisvottunaryfirvöldin tilkynna framkvæmdastjórninni um allar síðari breytingar sem því tengjast án ástæðulausrar tafar.

3.7. Kvartanir og viðurlög

Samkvæmt 63. gr. reglugerðarinnar skulu einstaklingar og lögaðilar hafa rétt að leggja fram kvörtun hjá útgefanda evrópsks netöryggisvottorðs eða ef kvörtunin tengist evrópska netöryggisvottorði sem samræmismatsstofa gefur út þegar hún starfar í samræmi við 6. mgr. 56. gr. hjá viðeigandi landsbundnu netöryggisvottunaryfirvaldi. Samkvæmt 2. mgr. 63. gr. reglugerðarinnar skal netöryggisvottunaryfirvaldið eða samræmismatsstofan þar sem kvörtunin er lögð fram, upplýsa kvörtunaraðilann um framvindu málsmeðferðarinnar og þá ákvörðun sem tekin er og skal upplýsa kvörtunaraðilann um réttinn til skilvirks réttarúræðis sem um getur í 64. gr. reglugerðarinnar.

Þá kveður 64. gr. reglugerðarinnar á um rétt einstaklinga og lögaðila til skilvirks réttarúræðis vegna ákvarðana sem og vanrækslu á að bregðast við kvörtunum sem teknar eru á grundvelli 63. gr. reglugerðarinnar.

Samkvæmt 65. gr. reglugerðarinnar ber aðildarríkjum skylda til þess að setja reglur um viðurlög vegna brota á ákvæðum reglugerðarinnar eða netöryggisvottana. Þá segir í f. lið 8. mgr. 58. gr. reglugerðarinnar að landsbundin netöryggisvottunaryfirvöld skuli hafa vald til að leggja á viðurlög. Auk þess skulu aðildarríkin gera allar nauðsynlegar ráðstafanir til að tryggja að slíkum viðurlögum verði beitt en þau skulu vera skilvirk, í réttu hlutfalli við brotið og hafa letjandi áhrif. Í 65. gr. reglugerðarinnar leggur einnig skylda á aðildarríkin til þess að tilkynna

framkvæmdastjórninni án tafar um þær reglur og ráðstafanir vegna brota á ákvæðum reglugerðarinnar eða netöryggisvottana, sem og aðildarríkin skulu einnig tilkynna framkvæmdastjórninni um allar síðari breytingar sem hafa áhrif á þær.

3.8. Evrópski netöryggisvottunarhópurinn (ECCG)

Samkvæmt 62. gr. reglugerðarinnar skal Evrópski netöryggisvottunarhópurinn vera skipaður fulltrúum innlendra netöryggisvottunaryfirvalda eða fulltrúum annarra viðeigandi landsyfirvalda. Hver aðili að ECCG á þó ekki að vera fulltrúi fleiri en tveggja aðildarríkja. Helstu verkefni evrópska netöryggisvottunarhópsins eru tilgreind í 4. mgr. 62. gr. reglugerðarinnar eru að:

- að ráðleggja og aðstoða framkvæmdastjórnina við það að tryggja samræmda framkvæmd og beitingu netöryggisvottunarkerfa,
- að aðstoða, veita ráðgjöf og starfa með vegna undirbúnings á tillögukerfi skv. 49. gr. reglugerðarinnar,
- að biðja ENISA um að undirbúa tillögukerfi skv. 2. mgr. 48. gr.,
- samþykkja álit sem beint er til framkvæmdastjórnarinnar varðandi viðhald og endurskoðun fyrirbyggjandi evrópskra netöryggisvottunarkerfa,
- að rannsaka viðeigandi þróun á sviði netöryggisvottorða og skiptast á upplýsingum og góðum starfsvenjum um netöryggisvottunarkerfi,
- að greiða fyrir samstarfi og upplýsingaskiptum milli landsbundinna netöryggisvottunaryfirvalda,
- að stuðla að framkvæmd fyrirkomulags fyrir jafningamat í samræmi við reglurnar sem settar eru í evrópsku netöryggisvottunarkerfi skv. u-lið 1. mgr. 54. gr.,
- að greiða fyrir því að evrópsk netöryggisvottunarkerfi samræmist viðurkenndum alþjóðlegum stöðlum.

3.9. Net landsbundinna tengifulltrúa (e. National Liaison Officers Network)

Samkvæmt 23. gr. reglugerðarinnar skal hvert aðildarríki tilnefna einn fulltrúa í net landsbundinna tengifulltrúa. Landsbundnir tengifulltrúar skulu greiða fyrir upplýsingaskipti milli ENISA og aðildarríkjanna en tengifulltrúinn skal styðja ENISA við að miðla starfsemi, niðurstöðum og ráðleggingum hennar til viðeigandi hagsmunaaðila í Sambandinu sbr. 2. mgr. 23. gr. reglugerðarinnar. Landsbundnu tengifulltrúarnir skulu einnig vera tengiliðir á landsbundnum vettvangi til að greiða fyrir samstarfi milli ENISA og landsbundinna sérfræðinga í tengslum við framkvæmd árlegrar starfsáætlunar ENISA sbr. 3. mgr. 23. gr. reglugerðarinnar.

3.10. Svigrúm við innleiðingu

Með frumvarpinu er lagt til að reglugerðin, með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar nr. 22/2023 um upptöku hennar í EES-samninginn og bókun 1 um altæka aðlögun við samninginn, skuli hafa lagagildi hér á landi. Reglugerðin verði þannig, í samræmi við a-lið 1. mgr. 7. gr. EES-samningsins, tekin í heild upp í landsrétt. Reglugerðin leggur fram umboð og starfsgrundvöll ENISA sem og leggur fram netöryggisvottunarferli fyrir vörur, þjónustu og ferla á sviði upplýsinga- og fjarskiptatækni. Ekki er svigrúm til að víkja frá efnisákvæðum reglugerðarinnar er fjalla um

netöryggisvottunarkerfi, sérstök réttarúrræði eða starfsemi ENISA en aðildarríki geta þó sjálf ákveðið hvaða innlendu aðilum verður úthlutað ákveðin verkefni og hlutverk á grundvelli reglugerðarinnar. Reglugerðin kveður ekki heldur á með nákvæmum hætti um þær viðurlagaheimildir eða sektir er netöryggisvottunaryfirvöld skulu hafa heldur er eingöngu kveðið á að ríki skulu setja reglur um viðurlög vegna brota á ákvæðum reglugerðarinnar eða netöryggisvottana sem og að landsbundin netöryggisvottunaryfirvöld skuli hafa vald til að leggja á viðurlög sbr. 65. gr. og f. liður 8. mgr. 58. gr. reglugerðarinnar. Vísast til nánari umfjöllunar í skýringum við 5. gr og kafla 3.6.1 og 3.7 í greinagerð þessari. Reglugerðin kveður ekki á um fjárhæðarviðmið dagsekta eða stjórnvaldssekta, sem stundum á við í Evrópuþerðum. Því er um landsbundna útfærslu ákvæða um stjórnsýsluviðurlög að ræða með frumvarpinu. Lagt er til að hámarksfjárhæðarviðmið dagsekta vegna brota gegn m.a. ákvæðum reglugerðarinnar verði skilgreind í samræmi við nærtækar fyrirmyndir á málefnasviðinu, þ.e. 1.000.000 kr. fyrir hvern dag, sbr. 11. gr. frumvarpsins. Dæmi um nærtæka fyrirmynd er hægt að vísa til 19. gr. laga nr. 75/2021. Lagt er til að hámarksfjárhæðarviðmið stjórnvaldssekta vegna brota gegn m.a. ákvæðum reglugerðarinnar verði skilgreind í samræmi við nærtækar fyrirmyndir á málefnasviðinu, þ.e. annaðhvort 10.000 kr. til 10.000.000 kr. eða allt að 4% af heildarveltu síðasta rekstrarárs hjá hverjum þeim aðila sem aðild á að broti ef það leiðir af sér hærri upphæð, sbr. 12. gr. frumvarpsins. Dæmi um nærtæka fyrirmynd er hægt að vísa til 23. gr. laga nr. 78/2019.

3.11. Breytingar á öðrum lögum.

Með frumvarpinu eru lagðar til breytingar lögum nr. 75/2021, um Fjarskiptastofu enda leysir frumvarpið, verði það að lögum, reglugerðarheimildarákvæði laga um Fjarskiptastofu af hólmi. Vísast til umfjöllunar um 16. gr. frumvarpsins.

4. Samræmi við stjórnarskrá og alþjóðlegar skuldbindingar.

Atvinnufrelsi nýtur verndar 1. mgr. 75. gr. stjórnarskrár Lýðveldisins Íslands, nr. 33/1944. Þessu frelsi má þó setja skorður með lögum, enda krefjist almannahagsmunir þess og gætt sé jafnræðis, sbr. 1. mgr. 65. gr. stjórnarskrárinnar. Þar sem að vottanir samkvæmt frumvarpinu eru valkvæðar er því ekki þörf á að meta sérstaklega hvort að frumvarpið fullnægi kröfum stjórnarskrárinnar. Aftur á móti verður að telja líklegt í ljósi þeirra ógna sem skortur á netöryggi getur haft á starfsemi aðila, mikilvægra innviða og samfélagið allt, að samræmdar lagakröfur til netöryggis upplýsinga- og fjarskitpataækni vara, -þjónustu og -ferla geti ekki talist skerða atvinnufrelsi skv. stjórnarskrárákvæðinu. Frumvarpið felur í sér upptöku á efnisákvæðum reglugerðarinnar í íslenskan rétt. Verkefni og heimildir netöryggisvottunarsamkvæmt reglugerðinni verður í höndum Fjarskiptastofu. Innleiðing reglugerðarinnar samræmist skuldbindingum Íslands skv. 7. gr. EES-samningsins og er ekki talin brjóta í bága við þjóðréttarlegar skuldbindingar Íslands.

5. Samráð.

Frumvarpið var samið í innviðaráðuneytinu og samráð viðhaft við fulltrúa Fjarskiptastofu við undirbúning þess. Á vinnslustigi var ráðuneytið m.a. í samskiptum við og átti fundi með fulltrúum Faggingingarsviðs Hugverkastofu. Áform um lagasetningu voru birt í samráðsgátt stjórnvalda þann 19. júlí 2025 og bárust umsagnir frá Opnum kerfum, Advania auk sameiginlegrar umsagnar frá Samtökum iðnaðarins og Samtaka upplýsingatæknifyrirtækja. Í umsögn Opinna kerfa segir að mikilvægt sé að ekki verði gengið lengra heldur en þörf krefur við innleiðingu reglugerðarinnar, að netöryggisvottunarkerfið eigi að vera valkvæmt og að

reglugerð 2019/881 hafi tekið breytingum hjá Evrópusambandi en að áhrif þeirra breytinga hafi ekki verið metnar í áformunum. Í umsögn Advania segir að mikilvægt sé að frumvarp muni taka tillit til smáðar landsins, að það hafi ekki neikvæð áhrif á samkeppnishæfni íslenska markaðarins og að netöryggisvottunin eigi að vera valkvæð. Í umsögn Samtaka iðnaðarins og Samtaka upplýsingatæknifyrirtækja segir að ekki eigi að ganga lengra heldur en þörf krefur við innleiðinguna, að netöryggisvottun eigi að vera valkvæð og að við innleiðingu breytingareglugerðar (ESB) 2025/37 sem breytir reglugerð (ESB) 2019/881 hafi áhrif á hluta af smærri íslenskum fyrirtækjum og þurfi því sérstaklega að meta efnahagsáhrif þeirrar gerðar.

[Kafllinn er í vinnslu]

6. Mat á áhrifum.

Markmið frumvarpsins er að tryggja fullnægjandi stig netöryggis fyrir upplýsinga- og fjarskiptatækni vöru-, þjónustur- og ferla sem og að koma í veg fyrir ósamræmi á innri markaðinum varðandi vottunarkerfi á þessu sviði. Að auki ber að nefna að með netöryggisvottuninni eykst traust og öryggi gagnvart upplýsinga- og fjarskiptatæknivörum, -þjónustu og -ferlum. Verður það að teljast lykiforsenda fyrir því að öflugum innri stafrænum markaði að almenningur og fyrirtæki treysti að því að slíkar vörur, þjónusta og ferli veiti tiltekið stig netöryggis. Einnig aðstoða evrópsk netöryggisvottorð endanlegum notendum að taka upplýstar ákvarðanir. Við undirbúning frumvarpsins var horft til sjónarmiða um meðalhóf og jafnræði.

Líkt og fram hefur komið þá leggur reglugerðin ekki þá kröfu á aðila að afla sér netöryggisvottunar heldur er slík vottun valkvæð. Kveður frumvarp þetta ekki á um annað fyrirkomulag. Verði frumvarpið að lögum mun það ekki setja beina kröfur á aðila á markaði með íþyngjandi hætti. Aðilar hafa fullt vald til að meta hvort þeir vilji afla sér viðeigandi netöryggisvottunar út frá regluverkinu. Það getur þó verið ákveðinn ávinningur fyrir aðila að afla sér vottunar samkvæmt þessu netöryggisvottunarskemum til að efla traust aðila á þeim upplýsinga- og fjarskiptatæknivöru, -þjónustu og- ferli sem hann býður. Slíkt getur bætt samkeppnishæfni viðkomandi á markaði.

Áformuð lagasetning mun fela í sér aukin verkefni fyrir Fjarskiptastofu sem netöryggisvottunaryfirvald. Óljóst er þó hversu umfangsmikil þau verkefni verða enda fara þau eftir því hvort að aðilar kjósi að afla sér netöryggisvottunar eða ekki.

Að auki gæti innleiðing reglugerðarinnar haft áhrif á Faggildingarsvið Hugverkastofu vegna hlutverk þeirra sem faggildingarstofa samkvæmt reglugerðinni. En í lögum um faggildingu nr. 24/2006, er faggildingarsviði Hugverkastofu falið það hlutverk að annast faggildingu og aðra þá starfsemi sem um getur í 1. gr. laganna, fyrir hönd íslenskra stjórnvalda. Frumvarpi þessu er ekki ætlað að hreyfa við því lögbundna verkefni. Aftur á móti er ljóst að gerð er krafa í þessari reglugerð að netöryggisyfirvald sé tilkynningaraðila fyrir faggiltar samræmismatsstofur en skv. lögum um faggildingu er slíkt á forræði hlutaðeigandi ráðherra. Því eru gerðar smávægilegar breytingar hvað varðar tilkynningu á faggiltum samræmismatsstofum á grundvelli þessarar reglugerðar til innleiðingar á 1. mgr. 61. gr. reglugerðarinnar, með þeim hætti að faggildingarsviðið tilkynni Fjarskiptastofu um faggildingu á aðila sem og allar mögulegar breytingar sem kunna að vera þar á, sbr. 7. gr. frumvarpsins.

[Kafllinn er í vinnslu]

Um einstakar greinar frumvarpsins.

Um 1. gr.

Í greininni er lagt til að ákvæði reglugerðar (ESB) nr. 2019/881 eins og hún hefur verið aðlöguð og tekin upp í EES-samninginn með ákvörðunum sameiginlegu EES-nefndarinnar nr. 22 frá 3. febrúar 2023, skuli hafa lagagildi hér á landi. Altækar aðlaganir eru aðlaganir sem eiga við um allar gerðir sem eru teknar upp í EES-samninginn og er ætlað að tryggja að efni gerða taki mið af eðli samningsins. Þær fela í sér atriði á borð við að vísanir til yfirráðasvæða og ríkisborgara aðildarríkja Evrópusambandsins eigi við um yfirráðasvæði og ríkisborgara aðildarríkja EES-samningsins. Aðlaganir í ákvörðun sameiginlegu EES-nefndarinnar taka fyrst og fremst mið af tveggja stöða kerfinu, ekki síst að því er varðar vísanir til hlutverks evrópsku netöryggisvottunaryfirvaldanna sem eftirlitsaðila og tilheyrandi valdheimilda.

Um 2. gr.

Í ákvæðinu er að finna skilgreiningar á hugtökum reglugerðarinnar. Ákvæðið þarfnast ekki skýringa.

Um 3. gr.

Samkvæmt 1. mgr. ákvæðisins er lagt til að Fjarskiptastofa verði landsbundið netöryggisvottunaryfirvald fyrir Ísland og skal stofnunin annast útgáfu netöryggisvottorða hér á landi þegar við á í samræmi við ákvæði reglugerðarinnar. Fjarskiptastofa er það stjórnvald hér á landi sem býr yfir hvað mestri tæknilegri og faglegri þekkingu er mun nýttast í verkefnum netöryggisvottunaryfirvalds samkvæmt reglugerðinni. Meðal núverandi verkefna Fjarskiptastofu á grundvelli annarra laga er m.a. að annast stjórnsýslu og eftirlit með framkvæmd fjarskipta- og netöryggismála, sbr. 2. gr. laga um Fjarskiptastofu nr. 75/2021. Einnig fer Fjarskiptastofa með hlutverk samhæfingarstjórnvalds samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða nr. 78/2019 en þau lög innleiða tilskipun (ESB) nr. 2016/1148 (NIS-1 tilskipun). Vert er að nefna að mörg aðildarríki, t.d. Finnland, Tékkland og Belgía, hafa úthlutað þeim stofnunum er fara með sambærilegt hlutverk og Fjarskiptastofu hefur á grundvelli 13. gr. laga nr. 78/2019 sem og 27. gr. laga nr. 75/2021. Að auki tekur stofnunin þegar þátt alþjóðlegu samstarfi á sviði netöryggis, þ.m.t. með ENISA og öðrum aðildarríkjum Evrópusambandsins, á grundvelli laga nr. 78/2019. Eins hefur stofnunin haft eftirlit með grunnkröfum fjarskiptabúnaðar um áralangt skeið á grundvelli fjarskiptalaga. Stofnunin er jafnframt eftirlitsstjórnvald með rafrænum auðkenningum og traustþjónustum á grundvelli laga nr. 55/2021. Þetta hefur ákveðna tengingu við þá reglugerð sem innleiða á með lagafrumvarpi þessu en unnið er að vottunarkerfi fyrir stafrænt auðkenningarveski sem sett er á laggirnar með nýrri reglugerð Evrópusambandsins nr. 2024/1183. Slík veski munu lúta eftirliti á grundvelli þeirrar reglugerðar. Þá er hýsir stofnunin Eyvöru, sem er hæfnissetur Íslands í netöryggi. Markmið þess er að efla netöryggisgetu á landsvísu og styðja við íslenskt netöryggissamfélag sem og að tryggja öflugt Evrópusamstarf á sviði netöryggismála. Eyvör er stofnað á grundvelli reglugerðar (ESB) nr. 2021/887 og mun vinna í nánú samstarfi við Hæfnisetur Evrópu í netöryggi (e. European Cybersecurity Competence Centre – ECCC). Eyvör mun markvisst styðja við íslenska aðila úr atvinnulífinu, rannsóknasamfélaginu og hinu opinbera í að efla rannsóknir og auka hæfni, þekkingu og þróun á sviði netöryggis. Eyvör mun m.a. sjá um rekstur netöryggisstyrkja og auðvelda íslenskum hagsmunaaðilum aðgengi að alþjóðlegum sóknarfærum.

Reglugerðin gerir þá kröfu að ríki skuli tryggja að netöryggisvottunaryfirvöldin hafi tilföng til að beita valdheimildum sínum og sinna verkefnum sínum á árangursríkan og skilvirkan hátt

sbr. 5. mgr. 58. gr. reglugerðarinnar. Þegar aðildarríki hefur tilnefnt aðila sem landsbundið netöryggisvottunaryfirvald skal það án tafar upplýsa framkvæmdastjórnina um það sbr. 2. mgr. 58. gr. reglugerðarinnar. Verkefni landsbundnu netöryggisvottunaryfirvaldsins koma fram í 7. mgr. 58. gr. reglugerðarinnar. Vísast til umfjöllunar í kafla 3.6.1 í frumvarpi þessu. En netöryggisvottunaryfirvaldið skal m.a. hafa eftirlit með og framfylgja reglum sem eru hluti af evrópskum netöryggisvottunarkerfum skv. j.-lið 1. mgr. 54. gr. reglugerðarinnar. Þá skal það aðstoða landsbundnar faggildingarstofur við vöktun og framfylgd með því að veita þeim sérfræðipækkingu og viðeigandi upplýsingar. Eins skal það fylgjast með viðeigandi þróun á sviði netöryggisvottunar og sjá um meðferð kvartana sem einstaklingar eða lögaðilar leggja fram í tengslum við evrópsk netöryggisvottorð sbr. 7. gr. laganna og 63. gr. reglugerðarinnar.

Í 2. mgr. ákvæðisins er ákvæði 3. og 4. mgr. 58. gr. reglugerðarinnar innleitt. Samkvæmt því skulu landsbundin netöryggisvottunaryfirvöld að vera óháð þeim aðilum er þau hafa eftirlit með. Sem og að starfsemi þeirra er lýtur að útgáfu evrópskra netöryggisvottorða skal vera aðskilin eftirlitsstarfsemi þeirra með netöryggisvottorðum. Í ákvæði 58. gr. reglugerðarinnar er m.a. kveðið á um að starfsemi landsbundinna netöryggisvottunaryfirvalda, sem tengist útgáfu evrópskra netöryggisvottorða sem um getur í a-lið 5. mgr. 56. gr. og í 6. mgr. 56. gr., sé haldið aðskilinni frá eftirlitsstarfsemi þeirra sem sett er fram í þessari grein og að öll starfsemi fari fram óháð annarri starfsemi. Tilgangur ákvæðisins er að tryggja að netöryggisvottunaryfirvaldið sé sjálfstætt frá þeim aðilum sem það hefur eftirlit með. En í ákveðnum tilfellum geta netöryggisvottunaryfirvöld einnig gefið út vottanir með fullvissustigið hátt og því geta komið upp tilfelli þar sem tryggja þarf hlutleysi í störfum netöryggisvottunaryfirvaldsins.

Um 4. gr.

Í 4. gr. frumvarpsins að finna ákvæði sem heimilar Fjarskiptastofu að úthýsa verkefnum á grundvelli laganna og/eða reglugerðarinnar til ytri aðila. Reglugerðin opnar á slíka heimild í 58. gr. reglugerðarinnar þegar kemur að eftirliti. Samkvæmt þeirri grein geta aðildarríki einnig tilnefnt yfirvöld er hafa staðfestu í öðru aðildarríki til þess að bera ábyrgð á eftirlitsverkefnum ef samþykki fæst frá þriðja ríkinu. Í 1. mgr. greinarinnar er lagt til að farin sé sú leið að Fjarskiptastofa sé tilnefnt netöryggisvottunaryfirvald hér á landi en lagt til að stofnuninni sé veitt heimild til að úthýsa, á grundvelli samnings, verkefnum, að hluta eða heild, til skemmri og/eða lengri tíma, til ytri aðila eða netöryggisvottunaryfirvalds innan Evrópska efnahagssvæðisins. Þessi leið þykir heppileg í ljósi smæðar landsins og til að tryggja aðgengi að sérfræðipækkingu sem mögulega væri af skornum skammti hér á landi sem og í ljósi smæðar stofnunarinnar ef t.a.m. tryggja þarf hlutleysi og aðgreiningu verkefna svo sem hvað varðar útgáfu evrópsks netöryggisvottorðs. Þá nær þessi heimild til hvort tveggja vinnu við samræmismat til útgáfu netöryggisvottorða sem og framkvæmd eftirlits eða annarra verkefna. Þessi nálgun ætti að tryggja að fagleg sjónarmið séu tryggð þegar við á í einstaka verkefnum sem og er mikilvægur liður til að tryggja fullan aðskilnað milli hlutverki stofnunarinnar við útgáfu netöryggisvottorða og eftirlits með aðilum.

Þá kveður 2. mgr. ákvæðisins einnig á um að allur kostnaður sem hlýst af framkvæmd netöryggisvottunar skuli greidd af viðkomandi aðila sem óskar eftir netöryggisvottun. Mikilvægt er að ef aðili kys að afla sér slíkrar vottunar að skýrt sé kveðið á um að hann skuli bera allan kostnað af sem af því hlýst. Fjarskiptastofa skal því innheimta umræddan kostnað frá aðila. Innan þessa kostnaðar skal falla allur kostnaður af undirbúningi, framkvæmd samræmis og útgáfu sem og annar kostnaður sem til kann að falla og er sannanlega liður í því að gefa út netöryggisvottun. Vert er að tilgreina að kjósi Fjarskiptastofa að útvista slíku

verkefni á grundvelli samnings, sbr. 4. mgr., skal sá kostnaður jafnframt borinn af viðkomandi aðila.

Um 5. gr.

Ákvæðið byggir á almennt á 8. mgr. 58. gr. reglugerðarinnar er mælir fyrir um þær valdheimildir er netöryggisvottunaryfirvaldið skal að minnsta kosti hafa svo hún geti sinnt þeim verkefnum er henni er skylt að gera samkvæmt 7. mgr. 58. gr. reglugerðarinnar. Í 1. mgr. ákvæðisins er sérstaklega tilgreint að Fjarskiptastofa skuli viðhafa eftirlit á grundvelli laga þessara og/eða reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 2019/881 frá 17. apríl 2019 og sinna öðrum verkefnum landsbundins netöryggisvottunaryfirvalds. Er hér einkum um að ræða vísun til 7. mgr. 58. gr. reglugerðarinnar.

Í samræmi við a. lið 8. mgr. 58. gr. reglugerðarinnar er í 2. mgr. lagt til að Fjarskiptastofu verði heimilt að krefja samræmismatsstofur, handhafa evrópskra netöryggisvottorða og útgefendur ESB-samræmisýfirlýsinga um allar upplýsingar sem nauðsynlegar þykja til að sinna verkefnum sínum. Þær upplýsingar sem afhentar eru stofnuninni skv. ákvæðinu skulu vera réttar, fullnægjandi og uppfærðar. Að auki tilgreinir ákvæðið að upplýsingar og gögn skulu vera afhent innan hæfilegs frests sem stofnunin setur eða með reglubundnum hætti samkvæmt fyrirmælum stofnunarinnar. Er þar um að ræða þá valdheimild er Fjarskiptastofa skal hafa samkvæmt a lið 8. mgr. 58. gr. reglugerðarinnar en þessi valdheimild er einkum mikilvæg þegar netöryggisvottunaryfirvaldið m.a. sinnir hlutverki sínu sbr. a, b og f liðum 7. mgr. 58. gr. reglugerðarinnar

Í samræmi við b og d liði 8. mgr. 58. gr. reglugerðarinnar er í 3. mgr. lagt til að Fjarskiptastofu verði heimilt framkvæma úttektir, rannsóknir, prófanir og vettvangsskoðanir til að sinna verkefnum sínum. Samkvæmt b. lið 8. mgr. 58. gr. reglugerðarinnar skulu netöryggisvottunaryfirvöld hafa valdheimildir til þess að framkvæma rannsóknir, í formi úttekta, á samræmismatsstofum, handhöfum evrópskra netöryggisvottorða og útgefendum ESB-samræmisýfirlýsinga í þeim tilgangi að sannprófa að þau fari að ákvæðum III. bálks reglugerðarinnar. Í d lið 8. mgr. 58. gr. reglugerðarinnar er tilgreint að netöryggisvottunaryfirvöld skuli hafa valdheimildir til þess að fá aðgang að athafnasvæðum allra samræmismatsstofa eða handhafa evrópskra netöryggisvottorða í þeim tilgangi að framkvæma rannsóknir í samræmi við lög Sambandsins eða aðildarríkis um málsmeðferð.

Í samræmi við c og f liði 8. mgr. 58. gr. reglugerðarinnar er í 4. mgr. lagt til að Fjarskiptastofa geti mælt fyrir um nauðsynleg tilmæli, fyrirmæli um úrbætur, beitt viðurlögum og lagt bann við háttsemi eftir því sem við getur átt hverju sinni gagnvart þeim sem brjóta gegn ákvæðum laga þessara, reglugerðarinnar eða reglna settra samkvæmt þeim sem og skilyrðum netöryggisvottunarkerfa. Samkvæmt c lið 8. mgr. 58. gr. reglugerðarinnar skulu netöryggisvottunaryfirvöld hafa valdheimildir til að gera viðeigandi ráðstafanir, í samræmi við landslög, til að tryggja að samræmismatsstofur, handhafar evrópskra netöryggisvottorða og útgefendur ESB-samræmisýfirlýsinga uppfylli kröfur þessarar reglugerðar eða evrópsks netöryggisvottunarkerfis. Í f lið 8. mgr. 58. gr. reglugerðarinnar er tilgreint að netöryggisvottunaryfirvöld skuli hafa valdheimildir til þess að beita refsíákvæðum í samræmi við landslög eins og kveðið er á um í 65. gr. reglugerðarinnar og krefjast þess að brot gegn skyldunum sem settar eru fram í þessari reglugerð verði stöðvuð án tafar. Samkvæmt 65. gr. reglugerðarinnar skulu viðurlögin vera skilvirk, í réttu hlutfalli við brotið og hafa letjandi áhrif og því hafa netöryggisvottunaryfirvöldin heimild til þess að leggja dagsektir sem og stjórnvaldsektir, sbr. 11. og 12. gr. frumvarpsins.

Í samræmi við e lið 8. mgr. 58. gr. reglugerðarinnar er í 5. mgr. lagt til að Fjarskiptastofa geti krafist afturköllunar á evrópsku netöryggisvottorði sem landsbundin netöryggisvottunaryfirvöld gefa út eða evrópsk netöryggisvottorð sem samræmismatsstofur gefa út ef slík vottorð uppfylla ekki skilyrði reglugerðarinnar eða netöryggisvottunarkerfisins. Slík ákvörðun verður einungis tekin á grundvelli ítarlegrar málsmeðferðar af hálfu Fjarskiptastofu. Samkvæmt e lið 8. mgr. 58. gr. reglugerðarinnar skulu netöryggisvottunaryfirvöld hafa valdheimildir til þess að afturkalla í samræmi við landslög evrópsk netöryggisvottorð sem landsbundin netöryggisvottunaryfirvöld gefa út eða evrópsk netöryggisvottorð sem samræmismatsstofur gefa út í samræmi við 6. mgr. 56. gr. reglugerðarinnar ef slík vottorð fara ekki að þessari reglugerð eða evrópsku netöryggisvottunarkerfi.

Um 6. gr.

Í ákvæðinu er lagt til að faggildingarsviði Hugverkastofu skuli upplýsa Fjarskiptastofu um faggildingu sem gefin er út samkvæmt lögum þessum, auk allra breytinga sem kunna að verða gerðar á henni og að Fjarskiptastofu skuli annars tilkynningar slíkra faggildra aðila. Er það gert til að uppfylla skilyrði 1. mgr. 61. mgr., reglugerðarinnar en samkvæmt henni skulu netöryggisvottunaryfirvöld tilkynna Evrópusambandinu um þær samræmismatsstofur er hafa hlotið fullgildingu sem og allar þær breytur sem verða á fullgildingu þeirra. Fram til þessa hefur sú nálgun tíðkast að viðkomandi fagráðherra tilkynni um slíkar samræmismatsstofur en slíkt er ekki talið uppfylla skýra kröfur reglugerðarinnar og því er lagt til að faggildingarsvið Hugverkastofu tilkynni Fjarskiptastofu um slíkar faggildingar. Visast til umfjöllunar í 6. kafla hvað þetta varðar.

Um 7. gr.

Í 1. mgr. ákvæðisins er lagt til að Fjarskiptastofa taki þátt í starfi evrópsks netöryggisvottunarhóps en hún fer með hlutverk netöryggisvottunaryfirvalds hér á landi sbr. 3. gr. laganna. Samkvæmt 6. mgr. 58. gr. reglugerðarinnar skulu landsbundin netöryggisvottunaryfirvöld taka þátt í evrópska netöryggisvottunarhópnum með virkum, árangursríkum, skilvirkum og öruggum hætti. Evrópski netöryggisvottunarhópurinn skal vera skipaður fulltrúum landsbundinna netöryggisvottunaryfirvalda sbr. 2. mgr. 62. gr. reglugerðarinnar. Helsta hlutverk hópsins er að styðja við samræmda innleiðingu evrópskrar netöryggisvottunar þvert á öll aðildarríki. Verkefni netöryggisvottunarhópsins eru talin upp í 4. mgr. 62. gr. reglugerðarinnar en helstu verkefnin eru að veita framkvæmdastjórninni ráðgjöf og aðstoð við vinnu hennar sem miðar að því að tryggja samræmda framkvæmd og beitingu evrópska netöryggisvottunarrámmans, að aðstoða og starfa náið með ENISA við undirbúning tillagna um evrópsk netöryggisvottunarkerfi, að óska eftir því að ENISA undirbúi tillögukerfi í tilhlýðilega rökstuddum tilvikum, samþykkja álit sem beint er til ENISA um tillögukerfi og að samþykkja álit sem beint er til framkvæmdastjórnarinnar um viðhald og endurskoðun á fyrirliggjandi evrópskum netöryggisvottunarkerfum. Að auki ætti evrópski netöryggisvottunarhópurinn að greiða fyrir gagnkvæmri miðlun góðra starfsvenja og sérfræðipækkingar milli mismunandi landsbundinna netöryggisvottunaryfirvalda sem bera ábyrgð á að veita samræmismatsstofum heimildir og að gefa út evrópsk netöryggisvottorð.

Í 2. mgr. ákvæðisins er lagt til að Fjarskiptastofa fari með hlutverk tengiliðs íslenskra stjórnvalda í neti landsbundna tengifulltrúa. Samkvæmt 23. gr. reglugerðarinnar er hlutverk net landsbundinna tengifulltrúa að greiða fyrir upplýsingaskipti og samstarfs milli aðildarríkja og ENISA. Fjarskiptastofa er nú þegar í virku samstarfi við Netöryggisstofnun

Evrópusambandsins sem og aðrar stofnanir aðildarríkja á grundvelli hlutverks hennar sem tengiliður stjórnvalda hér á landi vegna eftirlits með net- og upplýsingaöryggi mikilvægra innviða og framkvæmd tilskipunar (ESB) 2016/1148 um ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan Evrópska efnahagssvæðisins á grundvelli laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða. Það er því eðlilegt að samhæfa þessi hlutverk innan íslenskrar stjórnsýslu.

Um 8. gr.

Í samræmi við 63. gr. reglugerðarinnar fjallar ákvæðið um rétt einstaklinga og lögaðila til þess að leggja fram kvörtun til útgefanda (e. issuer) evrópsks netöryggisvottorðs eða til netöryggisvottunaryfirvalds, þegar kvörtunin varðar útgáfu evrópsks netöryggisvottorðs sem að samræmismatsstofa gefur út samkvæmt 6. mgr. 56. gr. reglugerðarinnar. Þegar slík vottorð sýna fullvissustigið „hátt“ ættu netöryggisvottunaryfirvaldin að rannsaka, að því marki sem viðeigandi er, viðfangsefni kvörtunarinnar og upplýsa kvartanda um framvindu og útkomu rannsóknarinnar innan hæfilegs tíma. Að auki ætti aðilinn er tekur við kvörtuninni að upplýsa kvartandann um réttarráðgjafi samkvæmt 9. gr. frumvarpsins.

Um 9. gr.

Ákvæðið heimilar Fjarskiptastofu að taka mál eftir ábendingu eða kvörtun, til meðferðar er varðar ákvæði laga þessara og reglugerðar (ESB) nr. 2019/881. Ákvæðið er í samræmi við c lið 58. gr. reglugerðarinnar er mælir fyrir um að netöryggisvottunaryfirvaldið skal hafa völd til þess að gera viðeigandi ráðstafanir, í samræmi við landslög, til að tryggja að samræmismatsstofur, handhafar evrópskra netöryggisvottorða og útgefendur ESB-samræmisvottunaryfirlýsinga fari að þessari reglugerð eða að evrópsku netöryggisvottunarkerfi.

Í 2. mgr. ákvæðisins er Fjarskiptastofu veitt heimild til að forgangsraða meðferð mála vegna ábendinga og kvartana skv. 7. gr. frumvarpsins og 63. gr. reglugerðarinnar eftir alvarleika og mikilvægi mála.

Um 10. gr.

Í samræmi við 64. gr. reglugerðarinnar leggur ákvæðið fram heimild einstaklinga og lögaðila til þess að skjóta ákvörðunum er netöryggisvottunaryfirvald eða útgefandi netöryggisvottana taka vegna kvartana skv. 7. gr. frumvarpsins, til dómstóla. Þær ákvarðanir sem hægt er að bera undir dómstóla eru þær ákvarðanir netöryggisvottunaryfirvalda eða samræmismatsstofa, er varða ófullnægjandi útgáfu, vanrækslu á útgáfu eða viðurkenningu á evrópsku netöryggisvottun er einstaklingurinn eða lögaðilinn eru handhafar af. Slíkt hið sama gildir um vanrækslu Fjarskiptastofu til þess að bregðast við kvörtunum er lagðar eru fram skv. 7. gr. frumvarpsins. Málsmeðferð kvartana skal vera lögð fyrir dómstóla þess ríkis þar sem að netöryggisvottunaryfirvaldið eða útgefandi netöryggisvottorðsins er staðsett.

Þá er kveðið á um það í ákvæðinu að ákvarðanir Fjarskiptastofu séu endanlegar á stjórnsýslustigi og að aðili máls geti skotið ákvörðun stofnunarinnar til dómstóla. Er sérstaklega tilgreint að málshöfðunarfrestur séu þrír mánuðir frá því að ákvörðun er tekin. Málshöfðun frestar ekki réttaráhrifum ákvarðana stofnunarinnar. Almennu eru ákvarðanir Fjarskiptastofu kærarlegar til úrskurðarnefndar fjarskipta- og póstmála sbr. 20. gr. laga nr. 75/2021 og því er lagt til að innleiða sérstakt ákvæði sem víkur frá þeirri framkvæmd. Er slíkt í samræmi við ákvæði 64. gr. reglugerðarinnar. Þó er hafður sami rammi fyrir málshöfðun og tilgreindur er í framgreindu ákvæði laga um Fjarskiptastofu, en aðilar hafa almennt heimild á grundvelli þeirra laga að bera ákvarðanir Fjarskiptastofu beint undir dómstóla án þess að mál

sé fyrst borið undir úrskurðarnefnd. Í 4. mgr. 20. gr. laga um Fjarskiptastofu er málfhjöfðunarfrestur þrír mánuðir og var horft til þess við samningu frumvarpsins sem og þess að réttaráhrifum ákvarðana sé ekki frestað þrátt fyrir slíka málshöfðun.

Um 11. gr.

Í ákvæðinu er kveðið á um þagnarskyldu starfsfólks Fjarskiptastofu, en ákvæðið er efnislega samhljóða 1. mgr. 25. gr. gildandi laga um Fjarskiptastofu.

Þá er í 2. mgr. að finna undanþágu frá almenntri þagnarskyldu netöryggisvottunaryfirvalda vegna samskipta og upplýsingaskipta, þ.m.t. almennra persónuupplýsinga, er netöryggisvottunaryfirvaldinu er skylt að gera samkvæmt a og g liðum 7. mgr. og 9. mgr. 58. gr. reglugerðarinnar. Ákvæðið er samhljóða 4. mgr. 25. gr. gildandi laga um Fjarskiptastofu.

Um 12. gr.

Í samræmi við 65. gr. reglugerðarinnar er lagt er til að í ákvæðinu verði kveðið á um heimild Fjarskiptastofu til álagninga dagsekta til þess að knýja á um fylgni við ákvæði laganna, reglugerðar, skilyrðum evrópskra netöryggisvottunarfyrirvalda, ákvarðanir netöryggisfyrirvalds, stjórnvaldsfyrirmælum og upplýsinga, gagna og aðgangsbeiðnir og aðrar kröfur netöryggisvottunaryfirvalds í einstaka málum. Með hugtakinu stjórnvaldsfyrirmæli í 1. mgr. ákvæðins er átt við afleiðd lög sem geta hvort tveggja verið reglugerðir eða reglur sem netöryggisvottunaryfirvaldið eða ráðherra gefur út á grundvelli laganna.

Í 2. mgr. ákvæðisins er lagt til að hámark dagsekta verði 1.000.000 kr. á dag, en það er sama hámark og er á dagsektum skv. 19. gr. laga nr. 75/2021 um Fjarskiptastofu. Í 2. mgr. ákvæðisins er einnig tilgreint að óinnheimtar dagsektir falli ekki á brott þótt skyldan hafi verið efnd en það er í samræmi við þá réttarþróun er hefur verið á á síðari árum en sem dæmi um slík ákvæði má nefna 2. mgr. 45. gr. laga nr. 140/2018 um aðgerðir gegn peningabætti og fjármögnun hryðjuverka og ákvæði 3. mgr. 58. gr. laga nr. 14/2022 um dýralyf.

Í 3. mgr. er sérstaklega tekið fram að ef ákvörðun um dagsektir skv. ákvæðinu er skotið til dómstóla þá byrji þær ekki að fylla fyrir en dómur er endanlegur. Þá er nauðsynlegt að tiltaka að dagsektir renni í ríkissjóð og eru aðfararhæfar án undangengins dóms eða sáttar.

Um 13. gr.

Í samræmi við 65. gr. reglugerðarinnar kveður 12. gr. á um heimild Fjarskiptastofu til álagningar stjórnvaldssekta vegna brota gegn ákvæðum laganna, reglugerðarinnar eða netöryggisvottunarkerfa. Samkvæmt 65. gr. reglugerðarinnar skulu viðurlögin vera skilvirk, í réttu hlutfalli við brotið og hafa letjandi áhrif.

Í 2. mgr. er fjallað um sektarramma stjórnvaldssekta. Viðmið um hámarksupphæð stjórnvaldssekta er af tvennum toga, þ.e. annars vegar föst krónutala eða sem hlutfall af veltu viðkomandi aðila á alþjóðavísu miðað við síðasta almanaksár. Gert er ráð fyrir því að sektarramminn ráðist af því hvort viðmiðið leiðir til hærri upphæðar. Lagt er til að horft verði til sömu viðmiða og eru í 2. mgr. 103. gr. nr. 70/2022, um fjarskipti.

Í 3. mgr. ákvæðisins er tilgreint að ákvarðaðar stjórnvaldssektir séu aðfararhæfar skv. 5. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989, og renna í ríkissjóð að frádregnum kostnaði við innheimtuna. Þá er sérstaklega kveðið á um að sé stjórnvaldssekt ekki greidd innan mánaðar frá ákvörðun Fjarskiptastofu skuli greiddir dráttarvextir af fjárhæð sektarinnar. Um

ákvörðun og útreikning dráttarvaxta fer eftir lögum um vexti og verðtryggingu. Hér er því einnig lagt til að horft verði til 2. mgr. 103. gr. fjarskiptalaga.

Í 4. mgr. kemur fram að stjórnvaldssektum verði beitt óháð því hvort lögbrot eru framin af ásetningi eða gáleysi. Þá er sett fram heimild til Fjarskiptastofu um að falla frá sektarákvörðun teljist brot óverulegt eða af öðrum ástæðum sé ekki talin þörf á slíkum sektum til að stuðla að framgangi markmiða frumvarpsins.

Að lokum er í 5. mgr. tilgreint að ákvörðun Fjarskiptastofu er endanleg á stjórnsýslustigi en aðilar geti skotið ákvörðun um stjórnvaldssekt til dómstóla. Lagt er til að málshöfðunarfrestur sé einnig þrír mánuðir líkt og við á um aðrar ákvarðanir Fjarskiptastofu á grundvelli frumvarpsins. Sérstaklega er tekið fram að málskot aðila fresti aðför.

Um 14. gr.

Ákvæðið kveður á um heimild ráðherra til að setja reglugerðir um nánari framkvæmd laganna og/eða reglugerðarinnar. Mikilvægt er að lögin mæli fyrir um almenna reglugerðarheimild sem veitir víðtæka heimild til reglugerðarsetningar. Upptalning í staflíðum a-f er því ekki tæmandi. Að auki er að finna í reglugerðinni sjálfri síðan heimild framkvæmdarstjórnar til setningu framkvæmdargerða í 7. mgr. 49. gr., 5. mgr. 59. gr og 5. mgr. 61. gr. reglugerðarinnar og því getur reglugerðin sjálf einnig leitt til þess að nauðsynlegt sé að setja frekari reglugerðir til innleiðingar framkvæmdareglugerðanna. Nú þegar hafa verið gefnar út þrjár framkvæmdargerðir, þ.e. framkvæmdareglugerð (ESB) nr. 2024/3143, er gefin var út á grundvelli 5. mgr. 61. gr. er kveður nánar á um kringumstæður, sniðmát og verklagsreglur fyrir tilkynningar. Einnig hefur verið gefin út framkvæmdarreglugerð (ESB) nr. 2024/482 innleiðingu á netöryggisvottunarkerfi er byggir á almennum evrópskum kröfum (e. European Common Criteria-based cybersecurity certification scheme (EUCC)), sem gefin var út á grundvelli 7. mgr. 49. gr. reglugerðarinnar og framkvæmdarreglugerð (ESB) nr. 2024/3144 er leiðréttir og lagfærir framkvæmdarreglugerð (ESB) nr. 2024/482.

Um 15. gr.

Ákvæðið þarfnast ekki skýringa.

Um 16. gr.

Með ákvæðinu eru lagðar til nauðsynlegar breytingar á lögum nr. 75/2021, um Fjarskiptastofu. Einungis er um afleiddar breytingar að ræða en eðlilegt þykir að uppfæra ákvæði 2. gr. laganna vegna þessa nýja hlutverks Fjarskiptastofu. Þá er í f. lið 1. mgr. 30. gr. laganna er að finna heimild til handa ráðherra að innleiða reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881 með setningu reglugerðar. Í lagafrumvarpi þessu er umrædd reglugerð Evrópusambandsins innleidd og því er rétt að fella á brott áður nefndan staflíð.