

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), um netöryggisvottun upplýsinga- og fjarskiptatækni og um niðurfellingu reglugerðar (ESB) nr. 526/2013 (gerð um netöryggi), sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 10 frá 12. febrúar 2026, 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. tölul. 4. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2016/1148 frá 6. júlí 2016 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu og 1. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
2. *Evrópskt netöryggisvottorð*: Skjal sem gefið er út af viðeigandi stofu og staðfestir að samræmi tiltekinna upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferla við sértækar öryggiskröfur sem mælt er fyrir um í evrópsku netöryggisvottunarkerfi hafi verið metið.
3. *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 fjarskiptatæknivörum, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferlum.
4. *Faggilding*: Faggilding eins og hún er skilgreind í 10. tölul. 2. gr. reglugerðar Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggilding og markaðseftirlit í tengslum við markaðssetningu á vörum og niðurfellingu reglugerðar (EBE) nr. 339/93 og 1. tölul. 2. gr. laga um faggilding o.fl., nr. 24/2006.
5. *Faggildingarstofa í aðildarríki*: Faggildingarstofa í aðildarríki eins og hún er skilgreind í 11. tölul. 2. gr. reglugerðar Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggilding og markaðseftirlit í tengslum við markaðssetningu á vörum og niðurfellingu reglugerðar (EBE) nr. 339/93.

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 fjarskiptatækniferli hefur verið metið en mælir ekki sem slíkt öryggi þeirrar upplýsinga- og fjarskiptatæknivöru, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferlis 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 fjarskiptatækniferlum.
8. *Landsbundin stefnuáætlun um öryggi net- og upplýsingakerfa*: Landsbundin stefnuáætlun um öryggi net- og upplýsingakerfa eins og hún er skilgreind í 3. tölul. 4. gr. tilskipunar (ESB) 2016/1148.
9. *Meðhöndlun atvika*: Meðhöndlun atvika eins og hún er skilgreind í 8. tölul. 4. gr. tilskipunar (ESB) 2016/114 og 12. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
10. *Net- og upplýsingakerfi*: Net- og upplýsingakerfi eins og það er skilgreint í 1. tölul. 4. gr. tilskipunar (ESB) 2016/1148 og 15. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
11. *Netógn*: Allar hugsanlegar aðstæður, atburðir eða aðgerðir sem gætu valdið skaða eða 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. *Rekstraraðili nauðsynlegrar þjónustu*: Rekstraraðili nauðsynlegrar þjónustu eins og hann er skilgreindur í 4. tölul. 4. gr. tilskipunar (ESB) 2016/1148 og 18. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
14. *Samræmismat*: Samræmismat eins og það er skilgreint í 12. tölul. 2. gr. reglugerðar (ESB) nr. 765/2008 og 6. tölul. 2. gr. laga um faggildingu o.fl., nr. 24/2006.
15. *Samræmismatsstofa*: Aðili sem annast samræmismat, sbr. 13. tölul. 2. gr. reglugerðar (ESB) nr. 765/2008.
16. *Sjálfsmat á samræmi*: Aðgerð sem framkvæmd er af framleiðanda eða veitanda upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónustu eða upplýsinga- og fjarskiptatækniferla sem metur hvort þessar upplýsinga- og fjarskiptatæknivörur, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækniferli uppfylli kröfur tiltekins evrópsks netöryggisvottunarkerfis.
17. *Staðall*: Staðall eins og hann er skilgreindur í 1. tölul. 2. gr. reglugerðar (ESB) nr. 1025/2012 frá 25. október 2012 um evrópska stöðlun og breytingu á tilskipun ráðsins 89/686/EBE og 93/15/EBE og tilskipunum Evrópuþingsins og ráðsins 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB og 2009/105/EB og niðurfellingu á ákvörðun ráðsins 87/95/EBE og ákvörðun Evrópuþingsins og ráðsins nr. 1673/2006/EB og 23. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.
18. *Tækniforskrift*: Skjal sem mælir fyrir um tæknilegar kröfur sem upplýsinga- og fjarskiptatæknivara, upplýsinga- og fjarskiptatækniþjónusta eða upplýsinga- og fjarskiptatækniferli skal uppfylla eða samræmismatsaðferðir þar að lútandi.

19. *Upplýsinga- og fjarskiptatækniþerli*: Starfsemi sem felst í að hanna, þróa, afhenda eða viðhalda vöru eða þjónustu á sviði upplýsinga- og fjarskiptatækni.
20. *Upplýsinga- og fjarskiptatæknivara*: Hluti eða hlutar net- eða upplýsingakerfis.
21. *Upplýsinga- og fjarskiptatækniþjónusta*: Þjónusta sem felst að öllu eða mestu leyti í því að senda, geyma, endurheimta eða vinna upplýsingar með net- og upplýsingakerfum.
22. *Veitandi stafrænnar þjónustu*: Veitandi stafrænnar þjónustu eins og hann er skilgreindur í 6. tölul. 4. gr. tilskipunar (ESB) 2016/1148 frá 6. júlí 2016 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu og 28. tölul. 6. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, 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 netöryggisvottorða hér á landi þegar við á samkvæmt ákvæðum reglugerðarinnar.

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

4. gr.

Útvistun.

Fjarskiptastofa getur á grundvelli samnings útvistað verkefnum sem varða útgáfu netöryggisvottorða og eftirlit á grundvelli laga þessara eða reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881, að hluta eða í heild, til skemmri eða lengri tíma, þ.m.t. til 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 útgáfu evrópsks netöryggisvottorðs skal greiddur af þeim aðila sem óskar netöryggisvottunar.

5. gr.

Eftirlit.

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

Fjarskiptastofa getur kafið faggildingarsvið Hugverkastofu, samræmismatsstofur, handhafa evrópskra netöryggisvottorða og útgefendur ESB-samræmisýfirlýsinga um allar upplýsingar og gögn sem nauðsynleg þykja svo að hún geti sinnt verkefnum sínum. Skulu upplýsingar og gögn afhent innan hæfilegs frests sem stofnunin setur eða reglubundið samkvæmt fyrirmælum stofnunarinnar.

Fjarskiptastofu er heimilt að gera 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, reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881, reglna settra samkvæmt þeim eða skilyrðum netöryggisvottunarkerfis.

Fjarskiptastofa getur krafist afturköllunar á evrópsku netöryggisvottorði sem landsbundin netöryggisvottunaryfirvöld hafa gefið út eða evrópskum netöryggisvottorðum sem samræmis-matsstofur hafa gefið út ef slík vottorð uppfylla ekki skilyrði reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881 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.

7. gr.

Alþjóðlegt samstarf.

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

Fjarskiptastofa er tengiliður íslenskra stjórnvalda í neti landsbundinna 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 sem 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 skv. 8. gr. eftir alvarleika og mikilvægi mála.

10. gr.

Réttarúrræði vegna kvartana.

Einstaklingar og lögaðilar geta skotið til dómstóla ákvörðunum sem teknar eru vegna kvartana skv. 8. gr. vegna ófullnægjandi útgáfu, vanrækslu á að gefa út eða viðurkenna evrópskt netöryggisvottorð sem þeir einstaklingar eða lögaðilar eru handhafar að, og er máls-höfðunarfrestur þrír mánuðir frá því að ákvörðun er tekin.

Hið sama gildir um vanrækslu Fjarskiptastofu á að bregðast við kvörtun skv. 8. gr. Ákvarðanir Fjarskiptastofu eru endanlegar á stjórnarsýslustigi. Málshöfðun frestar ekki réttar-áhrifum ákvarðana stofnunarinnar.

11. gr.

Þagnarskylda.

Starfsmenn Fjarskiptastofu eru bundnir þagnarskyldu skv. X. kafla stjórnarsýslulaga, nr. 37/1993. Þagnarskyldan helst þótt látið sé af störfum.

Þrátt fyrir 1. mgr. má veita netöryggisvottunaryfirvöldum í aðildarríkjum á Evrópska efnahagssvæðinu, Evrópskum netöryggisvottunarhópi, Netöryggisstofnun Evrópusambandsins

(ENISA) og Eftirlitsstofnun EFTA upplýsingar sé það liður annaðhvort í samstarfi ríkjanna samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881 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 því 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) 2019/881, ákvörðunum eða stjórnvaldsfyrirmælum Fjarskiptastofu, skilyrðum evrópskra netöryggisvottana, veitir ekki þær upplýsingar sem honum er skylt að afhenda stofnuninni eða fer ekki að öðrum kröfum stofnunarinnar er henni heimilt að leggja á og innheimta dagsektir til að tryggja að farið sé eftir fyrirmælum hennar. Ákvarðaðar dagsektir eru aðfararhæfar skv. 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. Sektir geta numið allt að 1.000.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að kröfum eða fyrirmælum sé fylgt eða gögn afhent skv. 1. mgr. Önnheimtar dagsektir falla ekki niður þótt aðili verði síðar við kröfu eftirlitsstjórnvalds 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:

- evrópskum netöryggisvottunarkerfum,
- þriðja bálki reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881,
- skyldu til að afhenda Fjarskiptastofu réttar, fullnægjandi og uppfærðar upplýsingar,
- stjórnvaldsákvörðunum og -fyrirmælum,
- reglum settum á grundvelli laga þessara.

Sektir skv. 1. mgr. geta numið frá 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 fjárhæð. Við ákvörðun á fjárhæð sekta skal hafa hliðsjón af eðli og umfangi brota, hvað brot hafa staðið lengi yfir 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.

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

14. gr.

Reglugerðarheimildir.

Ráðherra er heimilt að kveða á um nánari framkvæmd laga þessara og reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881 í reglugerðum sem fjalla nánar um:

- a. framkvæmd eftirlits Fjarskiptastofu,
- b. framkvæmdarreglugerðir,
- c. netöryggisvottunarkerfi,
- d. tilkynningar Fjarskiptastofu til framkvæmdarstjórnar Evrópusambandsins,
- e. samræmismöt,
- f. starfsemi Netöryggisstofnunar Evrópu.

15. gr.

Gildistaka.

Lög þessi öðlast þegar gildi.

16. gr.

Breytingar á öðrum lögum.

Við gildistöku laga þessara verða eftirfarandi breytingar á lögum um Fjarskiptastofu, nr. 75/2021:

- a. Við 1. mgr. 2. gr. laganna bætist nýr stafliður, svohljóðandi: framkvæmd laga um netöryggisvottun á sviði upplýsinga- og fjarskiptatækni.
- b. Við 2. málsl. 11. mgr. 21. gr. laganna bætist: auk útgáfu evrópsks netöryggisvottorðs.
- c. F-liður 1. mgr. 30. gr. laganna fellur brott.

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) 2019/881 frá 17. apríl 2019 um Netöryggisstofnun Evrópusambandsins (ENISA), um netöryggisvottun upplýsinga- og fjarskiptatækni og um niðurfellingu reglugerðar (ESB) nr. 526/2013 (gerð um netöryggi).

Netöryggisgerðin var samþykkt 19. apríl 2019 og kom til framkvæmda 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 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 (sem inniheldur skrána sem kveðið er á um í 101. gr.) við EES-samninginn, að undangengnu samráði við utanríkismálanefnd Alþingis með vísan til reglna um þinglega meðferð EES-mála.

Frumvarpið var lagt fram á 157. löggjafarþingi en náði ekki fram að ganga og fékk litla umfjöllun (571. mál). Frumvarpið er lagt fram að nýju með smávægilegum lagfæringum og orðalagsbreytingum.

2. Tilefni og nauðsyn lagasetningar.

2.1. Gerð um netöryggi.

Framkvæmdarstjórnin lagði fram frumvarp til netöryggisgerðarinnar í september 2017 sem hluta af viðtækum aðgerðum til að takast á við netárásir sem og til að byggja upp sterkt netöryggi innan Evrópusambandsins. Meginmarkmið reglugerðar (ESB) 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 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 netöryggisvottunarhópur (e. European Cybersecurity Certification Group – ECCG), netöryggisvottunarhópur hagsmunaaðila (e. Stakeholder Cybersecurity Certification Group – SCCG) og ríki innan Evrópska efnahagssvæðisins fara með mismunandi hlutverk. ENISA fer með yfirumsjón með innleiðingu og framkvæmd vottunarferlisins, en ríki innan Evrópska efnahagssvæðisins sinna eftirliti vottana og, í ákveðnum tilvikum, útgáfu vottana. Reglugerðin gerir kröfu um að aðildarríki tilnefni stjórnvald sem netöryggisvottunarstjórnvald sem fer með eftirlit, prófanir og vottanir evrópskra netöryggisvottunarkerfa á landsvísu sem og upplýsinga-skipti 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 vörum/þjónustum/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/ferla. Fimm árum frá samþykkt reglugerðarinnar hafa engin áform verið birt um slíka vottunarskyldu. Í nýrri reglugerð (ESB) nr. 37/2025, sem breytir reglugerð (ESB) nr. 2019/811, verður gildissvið reglugerðarinnar víkkað þannig að hún nái einnig til stýrðrar öryggisþjónustu. Hinn 11. apríl 2025 hóf framkvæmdastjórnin samráð vegna mögulegrar endurskoðunar á reglugerðinni. Er það m.a. liður í verkefnum framkvæmdastjórnarinnar um að einfalda regluverk. Við endurskoðunina á að einbeita sér að því að gera hlutverk ENISA skýrt og bæta evrópska netöryggisvottunarkerfið til að ná betri viðnámsþrótti. Einnig á með endurskoðuninni að straumlínulaga, einfalda og bæta gerðina til þess að gera evrópska netöryggisvottunarkerfisins notendavænna. Endurskoðunin á einnig að fela í sér forgangsröðun aðgerða sem styðja við markmið Evrópusambandsins sem varða þróun örugga og viðnámsþolinna birgjakæðja, þ.m.t. evrópskan netöryggisiðnaðargrunn.

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) 2019/881. Sú heimild hefur þó ekki verið nýtt. Þar sem reglugerðin tilgreinir margvíslegar skyldur og heimildir stjórnvalda til upplýsingaöflunar og álagningar 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) 2019/881 er annars vegar að tryggja ENISA varanlegan starfsgrundvöll og efla starfsemi hennar á sviði netöryggis. Hins vegar er markmið reglugerðarinnar að koma á fót samræmdu evrópsku vottunarferli fyrir vörur, þjónustu og ferla á

sviði upplýsinga- og fjarskiptatækni, 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 öryggisþjónustuveitenda (e. managed security services providers).

3.2. Netöryggisstofnun Evrópusambandsins.

3.2.1. Inngangur.

Netöryggisstofnun Evrópusambandsins, 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 stuðlar m.a. að auknu trausti á stafrænum vörum, þjónustu og ferlum með því að þróa vottunarkerfi fyrir netöryggi, sem miða að því að samræma öryggisstaðla 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 eflingar viðbragðsgetu stofnunarinnar sem stuðningsaðila við aðrar stofnanir Evrópusambandsins sem 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. kafli II. bálks reglugerðarinnar fjallar um umboð og markmið stofnunarinnar. ENISA er sérfræðistofnun á sviði netöryggis sem veitir faglega ráðgjöf og stuðning við stofnanir Evrópusambandsins og aðildarríki. Hún styður við þróun stefnu, eflingu getu og bætir viðbragðsgetu við netógnunum innan Evrópusambandsins. 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 nánar hver verkefni stofnunarinnar eru en hún skal m.a. stuðla að þróun og framkvæmd stefnu og laga Evrópusambandsins, byggja upp færni þess í netöryggismálum, styðja við rekstrarsamstarf milli aðildarríkja. Í 3. kafla II. bálks reglugerðarinnar er gerð grein fyrir uppbyggingu og skipulagi netöryggisstofnunarinnar en skv. 13. gr. reglugerðarinnar samanstendur ENISA af stjórn, framkvæmdastjórn, framkvæmdastjóra, ráðgjafarhópi og neti landsbundinna tengifulltrúa. Stjórn ENISA á að tryggja að stofnunin uppfylli verkefni sín á skilvirkan hátt samkvæmt reglugerðinni. Framkvæmdastjórn ENISA undirbýr ákvarðanir sem eru samþykktar af stjórninni. Framkvæmdastjóri ENISA ber ábyrgð á stjórnun stofnunarinnar og er sjálfstæður í störfum sínum. Net landsbundinna tengifulltrúa greiðir fyrir upplýsingaskipti milli ENISA og aðildarríkja sambandsins. Ráðgjafarhópurinn aðstoðar ENISA við að móta starfsáætlun sína og stefnumótandi markmið og eiga samskipti við aðalhagsmunaaðila. Þá er í 4. kafla II. bálks reglugerðarinnar fjallað um framkvæmd og efnisskipan fjárlaga ENISA 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, svo sem ákvæði um réttarstöðu stofnunarinnar, bótaábyrgð, tungumál og samstarf við þriðju lönd og alþjóðastofnanir.

3.3. Evrópsk netöryggisvottunarkerfi.

Samkvæmt 46. gr. reglugerðarinnar á evrópska netöryggisvottunarkerfið að bæta skilyrði fyrir starfsemi innri markaðar með því að auka netöryggisstig innan Evrópusambandsins og greiða fyrir samhæfðri nálgun, svo sem varðandi kröfur til vottana, á vettvangi þess í því skyni að skapa stafrænan innri markað fyrir vörur, þjónustu og ferla á sviði upplýsinga- og fjarskiptatækni. Evrópska netöryggisvottunarkerfið á að þjóna tvíþættum tilgangi, í fyrsta lagi að stuðla að meira trausti á upplýsinga- og fjarskiptatækniþjónustu, vörur og ferla sem hafa nú þegar hlotið vottun samkvæmt evrópskum netöryggisvottunarkerfum. Í öðru lagi á 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 evrópskum netöryggisvottunarkerfum sem staðfesta að upplýsinga- og fjarskiptatæknivörur, þjónusta og ferli, sem metin hafa verið í samræmi við slík kerfi, uppfylli tilgreindar öryggis-kröfur. Tilgangur þeirra öryggiskrafna er almennt 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 þeirra.

Evrópskt netöryggisvottunarkerfi á að byggjast á því sem nú þegar er til á alþjóðlegum og innlendum vettvangi og, ef þörf krefur, á tæknilýsingum samtökum eða öðrum aðilum, og með því að læra af styrkleikum, meta veikleika og bæta úr þeim. Tilgangur evrópska netöryggisvottunarkerfisins er að tryggja að upplýsinga- og fjarskiptatæknivörur, þjónusta eða ferlar sem hljóta slíka vottun uppfylli kröfur sem miða að því að vernda aðgengi, áreiðanleika, réttleika og leynd gagna og tengdra aðgerða eða þjónustu á líftíma þeirra. Þó er ekki unnt að skilgreina nákvæmlega samræmdar kröfur í reglugerðinni sökum fjölbreytileika í upplýsingatæknilausnum. Því byggist 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 framkvæmdastjórn óskað eftir því að ENISA útbúi og þrói evrópsk netöryggisvottunarkerfi. Evrópsku netöryggisvottunarkerfin sem 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-samræmisýfirlýsingum.

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

gagnsætt samráðsferli við alla hagsmunaaðila og aðildarríki. Í fjórða lagi skal framkvæmdastjórnin taka tillit til allra innleiðingarfresta, bráðabirgðaráðstafana og tímabila, einkum með tilliti til mögulegra áhrifa á framleiðendur og veitendur upplýsingatæknivara, upplýsingatæknipjónustu og upplýsingatækniferla, þar með talið lítil og meðalstór fyrirtæki. Að lokum, í fimmta lagi, skal framkvæmdastjórnin leggja til leið sem telja má fljótlega og skilvirka til að fara úr valfrjálsum 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 sem tilgreind eru í 51. gr. reglugerðarinnar. Í fyrsta lagi að vernda gögn sem eru geymd, send eða unnin á annan hátt gegn óleyfilegri geymslu, vinnslu, aðgangi eða birtingu á öllum líftíma upplýsinga- og fjarskiptatækivara, þjónustu og ferla, sbr. a-lið 1. mgr. 51. gr. reglugerðarinnar. Í öðru lagi að vernda gögn sem eru geymd, send eða unnin á annan hátt óleyfilegri eyðileggingu, tapi eða breytingu eða skorti á aðgengi á öllum líftímanum, 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 aðgangs-réttur 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, þjónusta 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 fjarskiptatæknivörur, þjónusta og ferlar feli ekki í sér 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 atvik kemur upp, sbr. h-lið 1. mgr. 51. gr. reglugerðarinnar. Í áttunda lagi að upplýsinga- og fjarskiptatæknin sé örugg og samkvæmt hönnun, sbr. i-lið 1. mgr. 51. gr. reglugerðarinnar. Að lokum, í níunda lagi, að hugbúnaðurinn og vélbúnaðurinn sé uppfærður og innihaldi ekki þekkta veikleika og sé með kerfi fyrir öruggar uppfærslur, sbr. j-lið 1. mgr. 51. gr. reglugerðarinnar.

3.3.2. Fullvissustig evrópskra netöryggisvottunarkerfa.

Evrópsk netöryggisvottunarkerfi geta tilgreint eitt eða fleiri fullvissustig sem skiptast í „lágt“, „verulegt“ eða „hátt“, sbr. 52. gr. reglugerðarinnar. Fullvissustigunum er ætlað að vera í samræmi við það áhættustig sem tengist fyrirhugaðri notkun, með tillit til hversu líklegt atvik er og áhrif þess. Evrópsk netöryggisvottorð og ESB-samræmisýfirlýsingar skulu vísa til þess fullvissustigs sem tilgreint er í evrópska netöryggisvottunarkerfinu þar sem evrópsk netöryggisvottorðið eða ESB-samræmisýfirlýsingar eru gefnar út. Öryggiskröfur samsvara hverju fullvissustigi og eru skilgreindar í viðkomandi evrópsku netöryggisvottunarkerfi, þar á meðal viðeigandi öryggisráðstafanir og hversu umfangsmikið matið eigi að vera. Netöryggisvottorðið eða ESB-samræmisýfirlýsingar eiga 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 tryggja viðeigandi öryggiskröfur, þ.m.t. öryggiseiginleika, og að þau hafi verið metin á stigi sem ætlað er til að lágmarka þekkta grunnáhættu atvika og netarása. Við mat á því hvort uppfyllt séu skilyrði fyrir fullvissustigið „lágt“ skal a.m.k. yfirfara tæknileg gögn. Þegar slík yfirferð er ekki viðeigandi skal framkvæmt annars konar matsferli með sambærilegum áhrifum.

Evrópsk netöryggisvottorð sem vísa til fullvissustigsins „verulegt“ skulu tryggja viðeigandi öryggiskröfur, þ.m.t. öryggiseiginleika, og að þau hafi verið metin á því stigi sem ætlað er að lágmarka þekkta netöryggisá hættu og hættu á atvikum og netárásum framkvæmdum af aðilum með takmarkaða færni og úrræði. Matstengdar aðgerðir sem framkvæma á skulu a.m.k. fela í sér yfirferð til að sýna fram á að ekki séu til staðar þekktir veikleikar og prófanir til að sýna að nauðsynlegir öryggiseiginleikar hafi verið innleiddir rétt er varða upplýsinga- og fjarskiptatæknivörur, þjónustu og ferla. Þegar slík matsferli eru ekki viðeigandi skal framkvæmt annars konar matsferli með sambærilegum áhrifum.

Evrópsk netöryggisvottorð sem vísa til fullvissustigsins „hátt“ skulu tryggja viðeigandi öryggiskröfur, þar á meðal öryggiseiginleika, og að þau hafi verið metin á stigi sem er ætlað til að lágmarka hættuna á háþrúðum netárásum framkvæmdum af aðilum með verulega færni og úrræði. Matstengdar aðgerðir og prófanir sem skulu framkvæmdar eiga a.m.k. að fela í sér yfirferð til að sýna fram á að þekktir veikleikar séu ekki fyrir hendi og að nauðsynlegir öryggiseiginleikar hafi verið innleiddir rétt er varða upplýsinga- og fjarskiptatæknivörur, þjónustu og ferla í samræmi við nýjustu tækniþróun og mat á viðnámi þeirra gegn hæfum árársaðilum með notkun innbrotspófana. Þegar 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 vottunina séu uppfylltar. Matið er framkvæmt af óháðum þriðja aðila. Ef skilyrðin eru uppfyllt ætti að gefa út evrópskt netöryggisvottorð. 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 einkaaðili eða opinber aðili eigi að gefa út evrópska netöryggisvottorðið. Samræmismat og samræmisvottun tryggja ekki ein og sér að andlag vottunarinnar búi yfir nægilegu netöryggi. Þess í stað eru þetta aðferðir og tæknileg aðferðafræði til að staðfesta prófanir og að tiltekna netöryggiskröfur sé uppfylltar, svo sem þær sem mælt er fyrir um annars staðar, t.d. í tæknistöðlum.

Samkvæmt 4. mgr. 56. gr. reglugerðarinnar skulu samræmismatsstofur skv. 60. gr. reglugerðarinnar gefa út evrópsk netöryggisvottorð á fullvissustigunum „lágt“ eða „verulegt“ á grundvelli viðmiða sem eru í evrópska netöryggisvottunarkerfinu sem framkvæmdastjórnin hefur samþykkt skv. 49. gr. reglugerðarinnar. Þó geta verið ákveðnar undantekningar frá því sem tilgreindar eru í 5. mgr. 56. gr. reglugerðarinnar. Þegar krafist er fullvissustigsins „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 að sjálfsmat á samræmi sá á ábyrgð framleiðanda eða veitanda. Sjálfsmat á samræmi skal eingöngu heimilað fyrir upplýsinga- og fjarskiptatæknivörur, þjónustu og ferla sem fela í sér litla áhættu og samsvara fullvissustiginu „lágt“. Í slíkum tilvikum ætti að nægja að framleiðandi eða veitandi framkvæmi sjálfur allar nauðsynlegar athuganir til að tryggja að viðkomandi vörur, þjónusta eða ferlar séu í samræmi við evrópska netöryggisvottunarkerfið. Framleiðandi eða veitandi 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 ábyrgð á því að þær kröfur sem fram eru settar í viðkomandi vottunarkerfi séu uppfylltar. Framleiðandi eða veitandi skal gera ESB-

samræmisýfirlýsinguna, tæknileg skjöl og allar aðrar viðeigandi upplýsingar 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-samræmisýfirlýsingunni sent til landsbundinnar netöryggisvottunarstofnunar og ENISA. Þá er útgáfa ESB-samræmisýfirlýsingar valkvæð nema annað komi fram í lögum Evrópusambandsins eða landslögum aðildarríkis. Auk þess skulu ESB-samræmisýfirlýsingar viðurkenndar í öllum aðildarríkjum. Samræmismat og vottun tryggir ekki í sjálfu sér að andlag vottunar sé að fullu öruggt með tilliti til 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 lágmarkspætti sem evrópsk netöryggisvottunarkerfi þurfa að hafa. Sem dæmi verður evrópsk netöryggiskerfi að innihalda viðfangsefni og umfang vottunarkerfis, þ.m.t. þá tegund eða flokka 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 byggjast á samræmdri löggjöf Evrópusambandsins. Ef samræmd löggjöf Evrópusambandsins er ekki fyrir hendi er heimild fyrir því að í löggjöf aðildarríkis sé kveðið 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-samræmisýfirlýsing 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 netöryggisvottorð eða ESB-samræmisýfirlýsing fellur úr gildi, sbr. 2. mgr. 55. gr. reglugerðarinnar.

3.4. *Netöryggisvottun.*

Líkt og tilgreint er í 2. mgr. 56. gr. reglugerðarinnar skal netöryggisvottun fyrir aðila vera valkvæð nema annað sé tekið fram, annaðhvort ef það leiðir af lögum Evrópusambandsins eða af landslögum aðildarríkisins. Ef upplýsinga- og fjarskiptatæknivörur, þjónusta og ferlar hafa verið vottaðir 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 en skv. 4. mgr. 56. gr. reglugerðarinnar eiga þær að gefa út evrópsk netöryggisvottorð sem vísa til fullvissustiga, annars vegar „lágt“ og hins vegar „verulegt“ á grundvelli viðmiða sem eru í evrópska netöryggisvottunarkerfinu sem framkvæmdastjórnin hefur samþykkt skv. 49. gr. reglugerðarinnar. Þó geta, að vissum skilyrðum uppfylltum, netöryggisvottunarkerfi kveðið á um að evrópsk netöryggisvottorð, sem leiðir 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, þarf að hafa fullvissustigið „hátt“ 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.

Kveðið er á um samræmismatsstofur í 60. gr. reglugerðarinnar. Samræmismatsstofur er hafa hlotið faggildingu skulu uppfylla skilyrði viðauka reglugerðarinnar. Skv. 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 skv. 2. mgr. 60. gr. reglugerðarinnar 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 um faggildingu o.fl., 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 og á sviðum þar sem aðilum er í sjálfsvald sett að láta faggilda starfsemi sína.

3.6. Landsbundin netöryggisvottunaryfirvöld.

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 landsbundin netöryggisvottunaryfirvöld með staðfestu í því aðildarríki til að bera ábyrgð á eftirlitsverkefnum í tilnefningaraðildarríkinu. Aðildarríkin skulu svo upplýsa framkvæmdastjórn Evrópusambandsins um hvaða stjórnvöld verða landsbundin netöryggisvottunaryfirvöld og ef aðildarríki tilnefnir fleiri en eitt yfirvald skal það jafnframt upplýsa um verkaskiptingu þeirra. Aðildarríkin verða að tryggja að 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. gr. 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 upplýsinga- og fjarskiptatæknivara, þjónustu og ferla sé fylgt eftir og framfylgt þeim sem hafa komið á fót á viðkomandi yfirráðasvæði og framkvæma sjálfsmat á samræmi, og skal einkum fylgjast með því að slíkir framleiðendur eða veitendur uppfylli þau skilyrði sem sett 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 á virkan hátt við eftirlit með starfsemi samræmismatsstofnana sem og að hafa eftirlit með starfsemi opinberra stofnana sem kveðið er á um í 5. mgr. 56. gr. reglugerðarinnar. Einnig skulu innlend netöryggisvottunaryfirvöld bregðast við kvörtunum einstaklinga eða lögaðila í tengslum við evrópsk netöryggisvottorð sem hafa verið gefin út af innlendum netöryggisvottunaryfirvöldum.

Innlend netöryggisvottunaryfirvöld skulu árlega leggja fram yfirlitsskýrslu um þá starfsemi sem fer fram skv. b-, c- og d-lið 7. mgr. 58. gr. reglugerðarinnar eða skv. 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 í 8. mgr. 58. gr. reglugerðarinnar kveðið á um lágmarksvaldheimildir innlendra netöryggisvottunaryfirvalda. Þar kemur m.a. fram að þau geti krafist tiltekna aðila um upplýsingar, framkvæmt úttektir, gert viðeigandi ráðstafanir til þess að tryggja að samræmismatsstofnanir, handhafar evrópska netöryggisskírteina og útgefendur ESB-samræmisyfirlýsinga uppfylli skilyrði reglugerðarinnar eða evrópskra netöryggisvottunarkerfa, afturkallað evrópsk netöryggisvottorð og beitt viðurlögum. Skv. f- lið 7. mgr. 58. gr. eiga netöryggisvottunaryfirvöld að hafa heimild til þess að beita refsiaðkvæðum í samræmi við landslög og krefjast þess að brot gegn skyldunum sem settar eru fram í reglugerðinni verði stöðvuð án tafar. Skv. 65. gr. reglugerðarinnar skulu aðildarríki setja reglur um viðurlög við brotum gegn rammaákvæðum um netöryggisvottun samkvæmt 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 hvert með öðru og með framkvæmdastjórninni, m.a. hvað varðar upplýsingaskipti og tæknileg atriði.

3.6.2. Jafningjarýni.

Í 59. gr. reglugerðarinnar er kveðið á um jafningjarýni sem komið var á með það markmið í huga að ná jafngildum stöðlum innan Evrópusambandsins að því er varðar evrópsk netöryggisvottorð og ESB-samræmisyfirlýsingar og því skulu innlend netöryggisvottunaryfirvöld sæta jafningjarýni. Jafningjarýnin fer fram á grundvelli traustra og gagnsærra matsviðmiða og verklagsreglna, einkum hvað varðar uppbyggingu, mannauðs- og ferlacröfur, 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 fjarskiptatæknivörum, þjónustu og ferlum 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“ fullvissustig skv. 6. mgr. 56. gr. reglugerðarinnar hafi viðeigandi sérfræðipækkingu. Jafningjarýnin skal gerð af a.m.k. tveimur netöryggisvottunaryfirvöldum annarra aðildarríkja og framkvæmdastjórninni á a.m.k. fimm ára fresti auk þess sem ENISA getur tekið þátt í jafningjarýnni.

3.6.3. Tilkynningar.

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 fullvissustigum 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 evrópsku netöryggisvottorði sem samræmismatsstofa gefur út þegar hún starfar í samræmi við 6. mgr. 56. gr. hjá viðeigandi landsbundnu netöryggisvottunaryfirvaldi. Skv. 2. mgr. 63. gr. reglugerðarinnar skal netöryggisvottunaryfirvaldið eða samræmismatsstofan, þar sem kvörtunin er lögð fram, upplýsa þann sem kvartaði um framvindu málsmeðferðarinnar og þá ákvörðun sem tekin er og skal upplýsa þann sem kvartaði um rétt til skilvirks réttarúrræðis sem um getur í 64. gr. reglugerðarinnar.

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

Samkvæmt 65. gr. reglugerðarinnar ber aðildarríkjum skylda til 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 er einnig lögð skylda á aðildarríkin að tilkynna framkvæmdastjórninni án tafar um reglurnar um viðurlög og ráðstafanir vegna brota á ákvæðum reglugerðarinnar eða netöryggisvottana. Þá skulu aðildarríkin einnig tilkynna framkvæmdastjórninni um allar síðari breytingar sem hafa áhrif á reglurnar.

3.8. Evrópski netöryggisvottunarhópurinn.

Samkvæmt 62. gr. reglugerðarinnar skal Evrópski netöryggisvottunarhópurinn (ECCG) 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:

- að ráðleggja og aðstoða framkvæmdastjórnina við það að tryggja samræmda framkvæmd og beitingu netöryggisvottunarkerfa,
- að aðstoða, veita ráðgjöf og starfa með Netöryggisstofnun Evrópusambandsins vegna undirbúnings á tillögukerfi skv. 49. gr. reglugerðarinnar,
- að biðja ENISA um að undirbúa tillögukerfi skv. 2. mgr. 48. gr.,
- að samþykkja álit sem beint er til framkvæmdastjórnarinnar varðandi viðhald og endurskoðun fyrirliggjandi 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.

Samkvæmt 23. gr. reglugerðarinnar skal hvert aðildarríki tilnefna einn fulltrúa í net landsbundinna tengifulltrúa. Landsbundnir tengifulltrúar skulu greiða fyrir upplýsingaskiptum, niðurstöðum og ráðleggingum til viðeigandi hagsmunaaðila í Evrópusambandinu, 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 sameiginlegru 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 gerir grein fyrir hlutverki og starfsgrundvelli ENISA sem og netöryggisvottunarkerfi fyrir vörur, þjónustu og ferla á sviði upplýsinga- og fjarskiptatækni. Ekki er svigrúm til að víkja frá efnisákvæðum reglugerðarinnar sem fjalla um netöryggisvottunarkerfi, sérstök réttarúrræði eða starfsemi ENISA en aðildarríki geta þó sjálf ákveðið hvaða innlendu aðilum verður úthlutað ákveðnum verkefnum og hlutverkum á grundvelli reglugerðarinnar. Reglugerðin kveður ekki heldur nákvæmlega á um þær viðurlagaheimildir eða sektir sem netöryggisvottunaryfirvöld skulu hafa heldur er eingöngu kveðið á um að ríki skuli 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-lið 8. mgr. 58. gr. reglugerðarinnar. Vísast til nánari umfjöllunar í skýringum við 5. gr. og kafla 3.6.1 og 3.7.

Reglugerðin kveður ekki á um fjárhæðarviðmið dagsekta eða stjórnvaldssekta, sem stundum á við í Evrópuverðum. Því er um landsbundna útfærslu ákvæða um stjórnsýsluviðurlög að ræða. Lagt er til að hámarksfjárhæðarviðmið dagsekta vegna brota, m.a. gegn ákvæðum reglugerðarinnar, verði skilgreind í samræmi við nærtækar fyrirmyndir á málefnasviðinu, þ.e. allt að 1.000.000 kr. fyrir hvern dag, sbr. 12. gr. frumvarpsins. Sem dæmi um nærtæka fyrirmynd er hægt að vísa til 19. gr. laga um Fjarskiptastofu, nr. 75/2021. Lagt er til að hámarksfjárhæðarviðmið stjórnvaldssekta vegna brota, m.a. gegn ákvæðum reglugerðarinnar, verði skilgreind í samræmi við nærtækar fyrirmyndir á málefnasviðinu, þ.e. 10.000–10.000.000 kr. eða allt að 4% af heildarveltu síðasta rekstrarárs hjá hverjum þeim aðila sem aðild á að broti ef það leiðir af sér hærri fjárhæð, sbr. 13. gr. frumvarpsins. Dæmi um nærtæka fyrirmynd er 23. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019.

3.11. Breytingar á öðrum lögum.

Með frumvarpinu eru lagðar til breytingar á lögum um Fjarskiptastofu, nr. 75/2021, enda leysir frumvarpið, verði það að lögum, reglugerðarheimildarákvæði laga um Fjarskiptastofu af hólmi. Vísast til skýringa við 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 vottanir samkvæmt frumvarpinu eru valkvæðar verður ekki talið að frumvarpið setji atvinnufrelsi skorður. 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 skerði ekki atvinnufrelsi samkvæmt stjórnarskrárákvæðinu. Frumvarpið felur í sér upptöku á efnisákvæðum reglugerðarinnar í íslenskan rétt. Verkefni og heimildir netöryggisvottunaryfirvalds samkvæmt reglugerðinni verður í höndum Fjarskiptastofu. Innleiðing reglugerðarinnar er talin samræmast 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 faggildingarviðs Hugverkastofu. Áform um lagasetningu voru birt í samráðsgátt stjórnvalda (mál nr. S-137/2025) frá 19. júlí 2025 til 9. ágúst 2025 og bárust umsagnir frá Opnum kerfum og Advania auk sameiginlegrar umsagnar frá Samtökum iðnaðarins og Samtökum upplýsingatæknifyrirtækja. Í umsögn Opinna kerfa sagði að mikilvægt væri að ekki yrði gengið lengra en þörf krefði við innleiðingu reglugerðarinnar, að netöryggisvottunarkerfið ætti að vera valkvætt og að reglugerð (ESB) 2019/881 hefði tekið breytingum hjá Evrópusambandinu en að áhrif þeirra breytinga hefðu ekki verið metin í áformunum. Í umsögn Advania sagði að mikilvægt væri að í frumvarpinu yrði tekið tillit til smæðar landsins, að það hefði ekki neikvæð áhrif á samkeppnishæfni íslenska markaðarins og að netöryggisvottunin ætti að vera valkvæð. Í umsögn Samtaka iðnaðarins og Samtaka upplýsingatæknifyrirtækja sagði að ekki ætti að ganga lengra en þörf krefði við innleiðinguna, að netöryggisvottun ætti að vera valkvæð og breytingarreglugerð (ESB) 2025/37, sem breytir reglugerð (ESB) 2019/881, mundi hafa áhrif á hluta af smærri íslenskum fyrirtækjum og því yrði sérstaklega að meta efnahagsáhrif þeirrar gerðar.

Drög að frumvarpi voru birt í samráðsgátt (mál nr. S-256/2025) frá 19. desember 2025 til 15. janúar 2026, en engar umsagnir bárust um frumvarpsdrögin.

6. Mat á áhrifum.

Markmið frumvarpsins er að tryggja fullnægjandi stig netöryggis fyrir upplýsinga- og fjarskiptatækni sem og að koma í veg fyrir ósamræmi á innri markaðnum varðandi vottunarkerfi á þessu sviði. Að auki ber að nefna að með netöryggisvottuninni eykst traust og öryggi. Verður að teljast lykilsenda fyrir öflugum innri stafrænum markaði að almenningur og fyrirtæki treysti því að slíkar vörur, þjónusta og ferli veiti tiltekið stig netöryggis. Einnig aðstoða evrópsk netöryggisvottorð endanlega notendur við að taka upplýstar ákvarðanir. Við undirbúning frumvarpsins var horft til sjónarmiða um meðalhóf og jafnræði.

Líkt og fram hefur komið er í reglugerðinni ekki lögð sú krafa 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 beinar íþyngjandi kröfur á aðila á markaði. 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 netöryggisvottunarskema til að efla traust á þeim. 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 aðilar kjósi að afla sér netöryggisvottunar eða ekki. En jafnvel þótt óljóst sé hver verði ásókn aðila hér á landi til að afla sér netöryggisvottunar og því sé erfitt að meta áhrif á starfsemi Fjarskiptastofu er ljóst að til staðar þarf að vera ákvæðin umgjörð og þekking hjá stofnuninni til að sinna lögbundnum verkefnum á grundvelli reglugerðarinnar. Þá er einnig ljóst að reglugerðin kveður á um þá skyldu að netöryggisvottunaryfirvöld geti framkvæmt samræmis- mat og uppfyllt skilyrði faggildingar. Það getur verið áskorun í fámennu samfélagi líkt og á Íslandi að tryggja strax slíka getu og sérþekkingu. Því er lagt til í frumvarpinu að Fjarskipta- stofa geti úthýst verkefnum sem leiðir af ákvæðum reglugerðarinnar, hvort sem er að hluta eða heild. Aftur á móti er ljóst að Fjarskiptastofa mun bera ábyrgð á verkefnum þrátt fyrir að til útivistunar komi. Því þarf ávallt að eiga sér stað þekkingaruppbygging og geta hvað þetta varðar og verða því áhrif frumvarpsins á fjárheimildir Fjarskiptastofu metin með reglubundn- um hætti. Frumvarpið gerir ráð fyrir að sá aðili sem sækist eftir vottun standi straum af kostnaði við framkvæmd vottunar sem hann sækist eftir.

Innleiðing reglugerðarinnar kann einnig að hafa áhrif á starfsemi faggildingarsviðs Hug- verkastofu vegna hlutverks þess sem áskilið er að hún taki að sér samkvæmt reglugerðinni. En í lögum um faggildingu o.fl., nr. 24/2006, er faggildingarsviði Hugverkastofu falið 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 um að netöryggisvottunaryfirvald sé tilkynningar- aðili fyrir faggiltar samræmismatsstofur en samkvæmt lögum um faggildingu o.fl. er það á forræði hlutaðeigandi ráðherra. Því eru gerðar smávægilegar breytingar hvað varðar tilkynningu á faggiltum samræmismatsstofum á grundvelli reglugerðarinnar til innleiðingar á 1. mgr. 61. gr. hennar þannig að faggildingarsviðið tilkynni Fjarskiptastofu um faggildingu á aðila sem og allar mögulegar breytingar sem kunna að vera þar á, sbr. 6. gr. frumvarpsins.

Frumvarp þetta hefur að markmiði að bæta netöryggi á Íslandi. Áhrif aukins netöryggis eru jákvæð fyrir öll kyn, en kannanir fjölmiðlanefndar benda þó til þess að kynin upplifi ógnir á netinu með mismunandi hætti. Við forgangsstöðun aðgerða um aukið netöryggi verður lögð áhersla á aðgerðir sem jafna stöðu kynja og þjóðfélagshópa.

Um einstakar greinar frumvarpsins.

Um 1. gr.

Í greininni er lagt til að ákvæði reglugerðar (ESB) 2019/881 eins og hún hefur verið aðlöguð og tekin upp í EES-samninginn með ákvörðunum sameiginlegu EES-nefndarinnar nr. 22/2023 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 yferráðasvæða og ríkisborgara aðildarríkja Evrópusambandsins eigi við um yferráðasvæði og ríkis- borgara 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 reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/881. Fjarskiptastofa er það stjórnvald hér á landi sem býr yfir hvað mestri tæknilegri og faglegri þekkingu sem mun nýta 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 innleiddu tilskipun (ESB) 2016/1148 (NIS-1 tilskipun). Vert er að nefna að mörg aðildarríki Evrópusambandsins, t.d. Finnland, Tékkland og Belgía, hafa farið þessa sömu leið sem lögð er til í frumvarpi þessu og úthlutað þeim stofnunum heima fyrir hlutverki samhæfingarstjórnvalds en þessar stofnanir fara með sambærilegt hlutverk og Fjarskiptastofa hefur á grundvelli 13. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019, sem og 27. gr. laga um Fjarskiptastofu, nr. 75/2021. Að auki tekur stofnunin þegar þátt í alþjóðlegu samstarfi á sviði netöryggis, þ.m.t. með ENISA og aðildarríkjum Evrópusambandsins, á grundvelli laga um öryggi net- og upplýsingakerfa mikilvægra innviða, 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 traustþjónustu á grundvelli laga um lykilupplýsingaskjöl vegna tiltekinna fjárfestingarafurða fyrir almenna fjárfesta, nr. 55/2021. Þetta hefur ákveðna tengingu við þá reglugerð sem innleiða á samkvæmt lagafrumvarpi þessu en unnið er að vottunarkerfi fyrir stafrænt auðkenningarveski sem sett er á laggimar með nýrri reglugerð Evrópuþingsins og ráðsins (ESB) 2024/1183 frá 11. apríl 2024 sem breytir reglugerð (ESB) nr. 910/2014 um að koma á rafrænni auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum. Slík veski munu lúta eftirliti á grundvelli þeirrar reglugerðar. Þá er hýsir stofnunin Eyvöru sem er hæfnisetur Íslands í netöryggi. Eyvör er stofnað á grundvelli reglugerðar (ESB) 2021/887 og mun vinna í nánú samstarfi við Hæfnisetur Evrópu í netöryggi. Setrið styður íslenska aðila úr atvinnulífinu, rannsóknasamfélaginu og hinu opinbera við 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.

Reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881 gerir þá kröfu að ríki skuli tryggja að netöryggisvottunaryfirvöldin hafi tilföng til að beita valdheimildum sínum og sinna verkefnum sínum á árangursríkan og skilvirkkan 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 netöryggisvottunaryfirvaldanna koma fram í 7. mgr. 58. gr. reglugerðarinnar. Visast til nánari umfjöllunar í kafla 3.6.1. 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 sérfræðiþekkingu 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. 8. gr. frumvarpsins og 63. gr. reglugerðarinnar.

Í 2. mgr. ákvæðisins er ákvæði 3. og 4. mgr. 58. gr. reglugerðarinnar innleitt. Samkvæmt því skulu landsbundin netöryggisvottunaryfirvöld vera óháð þeim aðilum sem þau hafa eftirlit með og sú starfsemi þeirra sem 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.

Ákvæðið heimilar Fjarskiptastofu að útvista verkefnum á grundvelli frumvarpsins og/eða reglugerðarinnar til ytri aðila. Opnað er fyrir 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. 3. gr. frumvarpsins er lagt til að farin sé sú leið að Fjarskiptastofa sé tilnefnt netöryggisvottunaryfirvald hér á landi en lagt til að stofnuninni verði veitt heimild til að útvista, á grundvelli samnings, verkefnum, að hluta eða í heild, til skemmri og/eða lengri tíma, til ytri aðila, þ.m.t. faggiltra samræmismatsstofa eða netöryggisvottunaryfirvalds innan Evrópska efnahagssvæðisins. Þessi leið þykir heppileg í ljósi smæðar landsins og til að tryggja aðgengi að sérfræðiþekkingu sem mögulega væri af skornum skammti hér á landi sem og í ljósi smæðar stofnunarinnar ef til að mynda 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 og framkvæmd eftirlits eða annarra verkefna. Þessi nálgun ætti að tryggja að fagleg sjónarmið séu tryggð þegar við á í einstaka verkefnum og er mikilvægur liður í að tryggja fullan aðskilnað milli hlutverka stofnunarinnar við útgáfu netöryggisvottorða og eftirlits með aðilum.

Þá kveður 2. mgr. á um að allur kostnaður sem hlýst af framkvæmd netöryggisvottunar skuli greiddur af viðkomandi aðila sem óskar eftir netöryggisvottun. Mikilvægt er að ef aðili kys að afla sér slíkrar vottunar sé skýrt kveðið á um að hann skuli bera allan kostnað sem af því hlýst. Fjarskiptastofa skal því innheimta umræddan kostnað frá aðila. Undir þennan kostnað fellur allur kostnaður sem hlýst 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. 1. mgr., skal sá kostnaður jafnframt borinn af viðkomandi aðila.

Um 5. gr.

Ákvæðið byggist aðallega á 8. mgr. 58. gr. reglugerðarinnar sem mælir fyrir um þær valdheimildir sem netöryggisvottunaryfirvaldið skal a.m.k. hafa svo að það geti sinnt þeim verkefnum sem því er skylt að gera skv. 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) 2019/881 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 hennar. Að auki er tilgreint í ákvæðinu að upplýsingar og gögn skuli vera afhent innan hæfilegs frests sem stofnunin setur eða með reglubundnum hætti samkvæmt fyrirmælum stofnunarinnar. Er þar um að ræða þá valdheimild sem Fjarskiptastofa skal hafa skv. 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-lið 7. mgr. 58. gr. reglugerðarinnar.

Í samræmi við b- og d-lið 8. mgr. 58. gr. reglugerðarinnar er í 3. mgr. lagt til að Fjarskiptastofu verði heimilt gera úttektir, rannsóknir, prófanir og vettvangsskoðanir til að sinna verkefnum sínum. Skv. b-lið 8. mgr. 58. gr. reglugerðarinnar skulu netöryggisvottunaryfirvöld hafa valdheimildir til þess að gera 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 Evrópusambandsins eða aðildarríkis um málsmeðferð.

Í samræmi við c- og f-lið 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, verði frumvarpið samþykkt, reglugerðarinnar eða reglna settra samkvæmt þeim sem og skilyrðum netöryggisvottunarkerfa. Skv. 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 reglugerðarinnar 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 reglugerðinni verði stöðvuð án tafar. Skv. 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 á dagsektir, sem og stjórnvaldsektir, sbr. 12. og 13. 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 hafa gefið út eða evrópsk netöryggisvottorð sem samræmismatsstofur hafa gefið út ef slík vottorð uppfylla ekki skilyrði reglugerðarinnar eða netöryggisvottunarkerfisins. Slík ákvörðun verður einungis tekin á grundvelli ítarlegrar málsmeðferðar af hálfu Fjarskiptastofu. Skv. 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 reglugerðinni eða eru ekki í samræmi við evrópska netöryggisvottunarkerfið.

Um 6. gr.

Í ákvæðinu er lagt til að faggildingarsvið Hugverkastofu skuli upplýsa Fjarskiptastofu um faggildingu sem gefin verður út samkvæmt frumvarpinu, auk allra breytinga sem kunna að verða gerðar á henni. Er það gert til að uppfylla skilyrði 1. mgr. 61. gr. 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 skýrar kröfur reglugerðarinnar og því er lagt til að faggildingarsvið Hugverkastofu tilkynni Fjarskiptastofu um slíkar faggildingar. Vísast til umfjöllunar í 3. 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. Skv. 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 verkefni eru að veita framkvæmdastjórninni ráðgjöf og aðstoð við vinnu hennar sem miðar að því að tryggja samræmda framkvæmd og beitingu evrópska netöryggisvottunarrammans, að aðstoða og starfa náið með ENISA við undirbúning tillagna um evrópsk netöryggisvottunarkerfi, 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 gefa út evrópsk netöryggisvottorð.

Í 2. mgr. ákvæðisins er lagt til að Fjarskiptastofa fari með hlutverk tengiliðs íslenskra stjórnvalda í neti landsbundinna tengifulltrúa. Skv. 23. gr. reglugerðarinnar er hlutverk nets landsbundinna tengifulltrúa að greiða fyrir upplýsingaskiptum og samstarfi 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 Sambandsins á grundvelli laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019. 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 evrópsks netöryggisvottorðs eða til netöryggisvottunaryfirvalds þegar kvörtunin varðar útgáfu evrópsks netöryggisvottorðs sem samræmismatsstofa gefur út skv. 6. mgr. 56. gr. reglugerðarinnar. Þegar slík vottorð sýna fullvissustigið „hátt“ ættu netöryggisvottunaryfirvöldin 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 sem tekur við kvörtuninni að upplýsa þann sem kvartaði um réttarúrræði skv. 9. gr. frumvarpsins.

Um 9. gr.

Ákvæðið heimilar Fjarskiptastofu að taka mál til meðferðar eftir ábendingu eða kvörtun er varðar ákvæði laga þessara og reglugerðar (ESB) 2019/881. Ákvæðið er í samræmi við c-lið 58. gr. reglugerðarinnar sem mælir fyrir um að netöryggisvottunaryfirvaldið skuli hafa völd til þess að gera viðeigandi ráðstafanir, í samræmi við landslög, til að tryggja að samræmis-matsstofur, handhafar evrópskra netöryggisvottorða og útgefendur ESB-samræmisýfirlýsinga fari að reglugerðinni eða sé í samræmi við evrópskt netöryggisvottunarkerfi.

Í 2. mgr. er Fjarskiptastofu veitt heimild til að forgangsraða meðferð mála vegna ábendinga og kvartana skv. 8. gr. frumvarpsins eftir alvarleika og mikilvægi þeirra.

Um 10. gr.

Í samræmi við 64. gr. reglugerðarinnar er kveðið á um heimild einstaklinga og lögaðila til þess að skjóta til dómstóla ákvörðunum sem netöryggisvottunaryfirvald eða útgefandi netöryggisvottana tekur vegna kvartana skv. 8. gr. frumvarpsins. Þær ákvarðanir sem hægt er að bera undir dómstóla eru þær ákvarðanir netöryggisvottunaryfirvalda eða samræmismatsstofa sem varða ófullnægjandi útgáfu, vanrækslu á útgáfu eða viðurkenningu á evrópskri netöryggisvottun sem einstaklingurinn eða lögaðilinn er handhafi að. Slíkt hið sama gildir um vanrækslu Fjarskiptastofu til þess að bregðast við kvörtunum er lagðar eru fram skv. 8. gr. frumvarpsins. Mál skal höfðað í því ríki þar sem netöryggisvottunaryfirvaldið eða útgefandi netöryggisvottorðsins er staðsett.

Þá er kveðið á um það að ákvarðanir Fjarskiptastofu séu endanlegar á stjórnsýslustigi og að aðili máls geti skotið ákvörðun stofnunarinnar til dómstóla. Er sérstaklega tilgreint að málshöfðunarfrestur sé þrír mánuðir frá því að ákvörðun er tekin. Málshöfðun frestar ekki réttaráhrifum ákvarðana stofnunarinnar. Almennu eru ákvarðanir Fjarskiptastofu kærnanlegar til úrskurðarnefndar fjarskipta- og póstmála, sbr. 20. gr. laga um Fjarskiptastofu, 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 lagður til sami rammi fyrir málshöfðun og tilgreindur er í framangreindu ákvæði laga um Fjarskiptastofu, en aðilar hafa almennt heimild á grundvelli þeirra laga til 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 málshöfðunarfrestur þrír mánuðir og var horft til þess við samningu frumvarpsins sem og þess að réttaráhrifum ákvarðana væri 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. laga um Fjarskiptastofu, nr. 75/2021.

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

Um 12. gr.

Í samræmi við 65. gr. reglugerðarinnar er lagt er til að kveðið verði á um heimild Fjarskiptastofu til álagningar dagsektar til þess að knýja á um fylgni við ákvæði laganna, reglugerðarinnar, skilyrði evrópskra netöryggisvottana, ákvarðanir netöryggisvottunaryfirvalds, stjórnvaldsfyrirmæli, upplýsinga-, gagna- og aðgangsbeiðnir sem og önnur fyrirmæli netöryggisvottunaryfirvalds í einstaka málum. Með hugtakinu stjórnvaldsfyrirmæli í 1. mgr. er átt við afleidd lög sem geta hvort tveggja verið reglugerðir eða reglur sem netöryggisvottunaryfirvaldið eða ráðherra gefur út á grundvelli laganna.

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

Í 3. mgr. er sérstaklega tekið fram að ef ákvörðun um dagsektir samkvæmt ákvæðinu er skotið til dómstóla byrji þær ekki að falla á fyrr en dómur er endanlegur. Þá er nauðsynlegt að tiltaka að dagsektir renna í ríkissjóð og eru aðfararhæfar án undangengins dóms eða sáttar.

Um 13. gr.

Í samræmi við 65. gr. reglugerðarinnar kveður 13. gr. á um heimild Fjarskiptastofu til álagningar stjórnvaldssektar vegna brota gegn ákvæðum laganna, reglugerðarinnar eða netöryggisvottunarkerfa. Skv. 65. gr. reglugerðarinnar skulu viðurlögin vera skilvirk, í réttu hlutfalli við brotið og hafa letjandi áhrif.

Í 2. mgr. er fjallað um sektarramma stjórnvaldssektar. Viðmið um hámarksfjárhæð stjórnvaldssektar er af tvennum toga, þ.e. annars vegar föst krónutala en hins vegar 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 fjárhæðar. Lagt er til að horft verði til sömu viðmiða og eru í 2. mgr. 103. gr. laga um fjarskipti, nr. 70/2022.

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 renni í ríkissjóð að fráregnum 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. laga um fjarskipti.

Ákvæði 4. mgr. þarfnast ekki skýringar.

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

Um 14. gr.

Í ákvæðinu heimild ráðherra til að setja reglugerðir um nánari framkvæmd laganna, nái frumvarpið fram að ganga, og reglugerðarinnar. Mikilvægt er að mælt sé fyrir um almenna reglugerðarheimild sem veitir víðtæka heimild til reglugerðarsetningar. Að auki er að finna í reglugerðinni sjálfri heimild framkvæmdastjórnar til setningar framkvæmdarreglugerða, þ.e. 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 framkvæmdarreglugerðanna. Nú þegar hafa verið gefnar út þrjár framkvæmdarreglugerðir, þ.e. framkvæmdarreglugerð (ESB) nr. 2024/3143 sem gefin var út á grundvelli 5. mgr. 61. gr. og kveður nánar á um kringumstæður, sniðmát og verklagsreglur fyrir tilkynningar, framkvæmdarreglugerð (ESB) nr. 2024/482 um innleiðingu á netöryggisvottunarkerfi sem byggist á almennum evrópskum kröfum, 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 um Fjarskiptastofu, nr. 75/2021. Verið er að uppfæra ákvæði 2. gr. laganna vegna nýs hlutverks Fjarskiptastofu. Þá er verið að bæta inn heimild um að innheimta kostnað sem hlýst af útgáfu evrópsks netöryggisvottorðs með breytingu á 11. mgr. 21. gr. laganna. Loks er í f-lið 1. mgr. 30. gr. laganna 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 brott þann staflið.