149. löggjafarþing 2018–2019.
Þingskjal xx — xx. mál.
Stjórnarfrumvarp.

Frumvarp til laga

um öryggi net- og upplýsingakerfa mikilvægra innviða.

Frá samgöngu- og sveitarstjórnarráðherra.

I. KAFLI
Markmið, orðskýringar og gildissvið.

1. gr.
Markmið.

Markmið laga þessara er að stuðla að háu öryggisstigi net- og upplýsingakerfa mikilvægra innviða eins og þeir eru skilgreindir í lögum þessum. Í því felst m.a. að:

1. samhæfa aðgerðir og skilgreina hlutverk stjórnvalda,
2. samþykkja stefnu stjórnvalda um öryggi net- og upplýsingakerfa,
3. efla hlutverk netöryggissveitar,
4. koma á öryggiskröfum og tilkynningarskyldu um atvik og
5. styrkja alþjóðasamstarf.

2. gr.
Orðskýringar.

Merking orða í lögum þessum og reglugerðum settum á grundvelli þeirra er sem hér segir:

Atvik: Hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa.

Áhætta: Aðstæður eða atburðir sem eru sanngreinanleg með fullnægjandi hætti og hafa mögulega skaðleg áhrif á öryggi net- og upplýsingakerfa.

Bankaþjónusta: Lánastofnanir eins og skilgreint er í 1. lið 4. gr. reglugerðar (ESB) 575/2013.

Eftirlitsstjórnvald: Stjórnvald sem sinnir eftirliti með öryggi net- og upplýsingakerfarekstraraðila mikilvægra innviða hvert á sínu sviði.

Fjármálamarkaðir: Rekstraraðilar viðskiptavettvangs eins og skilgreint er í 24. lið 4. gr. tilskipunar 2014/65/ESB og mikilvægir mótaðilar (CCPs) eins og skilgreint er í 1 lið 2. gr. reglugerðar (ESB) 648/2012.

Flutningar: Flutningar á lofti; flugrekendur eins og skilgreint er í 4. lið. 3. gr. reglugerðar (EB) 300/2008, framkvæmdarstjórnir flugvalla eins og skilgreint er í 2. lið 2. gr. tilskipunar 2009/12/EB, flugvellir eins og skilgreint er í 1. lið 2. gr. tilskipunar 2009/12/EB þ.m.t. flugvellir í grunneti sem skráðir eru í 2. þætti II. viðauka reglugerðar (ESB) 1315/2013 og einingar sem starfrækja viðbúnað sem staðsettur er innan flugvalla, kerfisstjórar umferðarstjórnunar sem veita flugstjórnarþjónustu (ATC) eins og skilgreint er í 1. lið 2. gr. reglugerðar (EB) 549/2004. Járnbrautarflutningar; stjórnendur grunnvirkja eins og skilgreint er í 2. lið 3. gr. tilskipunar 2012/34/EB og járnbrautarfyrirtæki eins og skilgreint er í 1. lið 3. gr. tilskipunar 2012/34/ESB þ.m.t. rekstraraðilar þjónustuaðstöðu eins og skilgreint er í 12. lið

3. gr. tilskipunar 2012/34/ESB. Flutningar á sjó og vatnaleiðum; fyrirtæki sem sjá um vatna-, millilanda- og strandsiglingar með farþega og vöruflutninga á sjó og vatnaleiðum eins og skilgreint er fyrir flutninga á sjó í I. viðauka reglugerðar (EB) 725/2004 að frátöldum einstökum skipum sem þau fyrirtæki gera út, hafnarstjórnir eins og skilgreint er í í 1. lið 3. gr. tilskipunar 2005/65/EB þ.m.t. hafnaraðstöður þeirra eins og skilgreint er í 1.lið 2. gr. reglugerðar (EB) 725/2004 og einingar sem annast mannvirki og búnað sem staðsett eru innan hafna og rekstraraðilar skipaumferðarþjónustu eins og skilgreint er í o. lið 3. gr. tilskipunar 2002/59/EB. Flutningar á vegum; vegamálayfirvöld eins og skilgreint er í 12. lið 2. gr. framseldar reglugerðar (ESB) 2015/962 sem bera ábyrgð á umferðarstjórnun og rekstraraðilar skynvæddra flutningakerfa eins og skilgreint er í 1. lið 4. gr. tilskipunar 2010/40/ESB.

Forskrift: Tækniforskrift í skilningi 4. liðar 2. gr. reglugerðar (ESB) 1025/2012.

Fulltrúi eftirlitsstjórnvalds: Sérfræðingur í net- og upplýsingaöryggi sem eftirlitsstjórnvald gerir samning við um afmarkaða þætti eftirlits með net- og upplýsingaöryggi mikilvægra innviða.

Heilbrigðisgeiri: Veitendur heilbrigðisþjónustu, þ.m.t. spítalar og einkareknar læknastofur, eins og skilgreint er í g. lið 3. gr. tilskipunar 2011/24/EB.

Landsbundin stefnuáætlun um öryggi net- og upplýsingakerfa: Rammi sem m.a. kemur á fót stefnumótandi markmiðum og forgangsröðun varðandi öryggi net- og upplýsingakerfa á landsvísu.

Leitarvél á Netinu: Stafræn þjónusta sem leyfir notendum að framkvæma leit, að meginreglu til, að öllum vefsvæðum eða vefsvæðum á tilteknu tungumáli á grundvelli fyrirspurnar um alls konar viðfangsefni í formi lykilorðs, orðasambands eða annars konar gagna færð inn í tölvu og skilar tenglum þar sem finna má upplýsingar sem varða efnið sem óskað er eftir.

Lénsheitakerfi (DNS): Stigskipt dreift gagnasafn í netkerfi sem annast fyrirspurnir um lénsheiti.

Meðhöndlun atvika: Allt það verklag sem styður við að koma upp um, greina og afmarka atvik og viðbrögð við þeim.

Mikilvægir innviðir: Rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur eins og þeir eru skilgreindir í lögum þessum.

Netmarkaður: Stafræn þjónusta sem leyfir neytendum og/eða seljendum, eins og þeir eru skilgreindir í a. og b. liðum 1. mgr. 4. gr. tilskipunar 2013/11/ESB, að gera sölu- og þjónustusamninga á Netinu við seljendur annað hvort á vefsvæði netmarkaðarins eða á vefsvæði seljandans sem notar þjónustu á sviði gagnaumferðar í gegnum netmarkaðinn.

Nauðsynleg þjónusta: Þjónusta sem er af tegund sem greind er í II. viðauka tilskipunar 2016/1148/ESB.

Net- og upplýsingakerfi: Rafræn fjarskiptanet í skilningi a. liðar 2. gr. tilskipunar 2002/21/EB, tæki eða samsafn innbyrðis tengdra eða skyldra tækja þar sem í einu þeirra eða fleiri fer fram sjálfvirk stafræn gagnavinnsla eftir forriti, eða stafræn gögn sem eru geymd, unnin, sótt eða send fyrir tilstilli þátt sem falla undir framangreint að því er varðar starfrækslu þeirra, notkun, verndun og viðhald.

Orkuveitur: Rafmagn; raforkufyrirtæki eins og skilgreint er í 35. lið 2. gr. tilskipunar 2009/72/EB sem sinna hlutverki „afhendingar“ eins og skilgreint er í 19. lið 2. gr. hennar, dreifikerfisstjórar eins og skilgreint er í 6. lið 2. gr. tilskipunar 2009/72/EB og flutningakerfisstjórar eins og skilgreint er í 4. lið 2. gr. tilskipunar 2009/72/EB. Olía; rekstraraðilar flutningsleiðslna fyrir olíu og rekstraraðilar olíuframleiðslu, olíuhreinsunar- og meðhöndlunarstöðva, olíugeymslu- og flutnings. Gas; afhendingarfyrirtæki eins og skilgreint

er í 8. lið 2. gr. tilskipunar 2009/73/EB, dreifikerfisstjórar eins og skilgreint er í 6. lið 2. gr. tilskipunar 2009/73/EB, flutningakerfisstjórar eins og skilgreint er í 4. lið 2. gr. tilskipunar 2009/73/EB, geymslukerfisstjórar eins og skilgreint er í 10. lið 2. gr. tilskipunar 2009/72/EB, kerfisstjórar með fljótandi jarðgas eins og skilgreint er í 12. lið 2. gr. tilskipunar 2009/73/EB, jarðgasfyrirtæki eins og skilgreint er í 1. lið 2. gr. tilskipunar 2009/73/EB og kerfisstjórar hreinsunar og meðhöndlunarstöðva fyrir jarðgas.

Rekstraraðili nauðsynlegrar þjónustu: Er opinber eða einkaaðili, birtur í skrá skv. lögum þessum, sem veitir þjónustu sem nánar er skilgreind í lögunum.

Samhæfingarstjórnvald: Stjórnvald sem m.a. samhæfir eftirlit eftirlitsstjórnvalda, tekur þátt í alþjóðasamstarfi og starfrækir netöryggissveit.

Skráningarstofa höfuðléna: Aðili sem annast og vinnur að skráningu lénsheita á Netinu undir sérstöku höfuðléni (TLD).

Skýjavinnsluþjónusta: Stafræn þjónusta sem veitir aðgang að skjalanlegum og sveigjanlegum brunni tölvunargetu sem hægt er að deila.

Spillikóði; Sérhver kóði, þ.e. runa skipana og/eða gagna, sem er ætlaður til að leiða til óæskilegra áhrifa, öryggisrofs eða skemmda á kerfum.

Stafræn þjónusta: Þjónusta í skilningi b. liðar 1. mgr. 1. gr. tilskipunar 2015/1535/ESB sem er af tegund sem greind er í III. viðauka tilskipunar 2016/1148/ESB.

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

Stafræn grunnvirki: Tengi- og skiptipunktar (IXPs), þjónustuveitendur lénsheitakerfis og skráningarstofur höfuðléna.

Stafrænn þjónustuveitandi: Sérhver lögaðili með höfuðstöðvar þ.e. aðalskrifstofu, eða staðfestu, hérlendis sem veitir stafræna þjónustu eða fulltrúi hans með staðfestu hérlendis.

Tegundir stafrænnar þjónustu: Netmarkaður, leitarvél á Netinu og skýjavinnsluþjónusta.

Tengi- og skiptipunktur (IXP): Netvirki sem gerir kleift að samtengja fleiri en tvö sjálfstæð og sjálfstýrð kerfi, fyrst og fremst í þeim tilgangi að greiða fyrir miðlun Netumferðar, tengi- og skiptipunkturinn veitir einungis samtengingu fyrir sjálfstýrð kerfi, tengi- og skiptipunkturinn gerir ekki kröfu um að Netumferð sem fer á milli tveggja hlutaðeigandi sjálfstýrðra kerfa fari í gegnum þriðja sjálfstýrða kerfið, né breytir hún eða truflar slíka umferð,

Vatnsveitur: Birgjar og dreifingaraðilar neysluvatns, eins og skilgreint er í a. lið 1. liðar 2. gr. tilskipunar 98/83/EB. Á ekki við þegar dreifing neysluvatns er einungis hluti af almennri starfsemi þeirra sem felur í sér dreifingu annarra verslunarvara og varnings sem telst ekki vera nauðsynleg þjónusta.

Öryggi net- og upplýsingakerfa: Geta net- og upplýsingakerfis til að standast, með tilteknu öryggisstigi, allar aðgerðir sem stofna í hættu aðgengi, sannvottuðum uppruna, réttleika og leynd vistaðra, sendra eða unninna gagna eða tengdrar þjónustu sem boðin er eða er aðgengileg um þessi net- og upplýsingakerfi.

Þjónustuveitandi lénsheitakerfis: Aðili sem veitir þjónustu fyrir lénsheitakerfi á Netinu.

3. gr.

Gildissvið.

Lög þessi taka til net- og upplýsingakerfa mikilvægra innviða eins og þeir eru skilgreindir í lögum þessum, í reglugerðum settum samkvæmt þeim og í auglýsingu í B-deild Stjórnartíðinda skv. 4. mgr. 5. gr.

Lög þessi taka til net- og upplýsingaöryggis stjórnarráðs Íslands hvað varðar vöktun atvika og viðbrögð við atvikum í net- og upplýsingakerfum eins og nánar greinir í lögunum og reglugerðum settum samkvæmt þeim.

Lögin gilda ekki um stafræna þjónustuveitendur sem teljast örfélög eða lítil félög í skilningi laga um ársreikninga nr. 3/2006.

4. gr.

Almannavarnir.

Sé net- og upplýsingaöryggi ógnað með þeim hætti að upp komi neyðarástand sem kann að ógna lífi og heilsu almennings, umhverfi og/eða eignum í skilningi laga um almannavarnir nr. 82/2008 fer um viðbrögð stjórnvalda á grundvelli þeirra laga.

II. KAFLI

Rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur.

5. gr.

Rekstraraðilar nauðsynlegrar þjónustu.

Rekstraraðili nauðsynlegrar þjónustu veitir þjónustu á einhverju eftirtaldra sviða:

1. orkuveitur,
2. flutningar,
3. bankaþjónusta,
4. fjármálamarkaðir,
5. heilbrigðisþjónusta,
6. vatnsveitur og
7. stafræn grunnvirki.

Þjónusta skv. 1. mgr. skal vera nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi, veiting þjónustu er háð net- og upplýsingakerfum og atvik myndu hafa veruleg skerðandi áhrif á veitingu þjónustu.

Ráðherra skal með reglugerð mæla nánar fyrir um viðmiðanir til auðkenningar rekstraraðila nauðsynlegrar þjónustu þar sem m.a. er yfirlit yfir þá þjónustu sem er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi og hvað flokkast til verulega skerðandi áhrifa í skilningi 2. mgr.

Ráðherra skal halda opinbera skrá yfir rekstraraðila nauðsynlegrar þjónustu, með starfsstöð hérlendis, með auglýsingu í B-deild Stjórnartíðinda. Skal skráin vera uppfærð á a.m.k. tveggja ára fresti.

6. gr.

Stafrænir þjónustuveitendur.

Stafrænn þjónustuveitandi veitir eftirfarandi stafræna þjónustu:

1. netmarkaður,
2. leitarvél á Netinu eða
3. skýjavinnsluþjónusta.

Ráðherra getur með reglugerð mælt nánar fyrir um viðmiðanir við auðkenningu stafrænna þjónustuveitenda.

III. KAFLI

Stefna og hlutverk stjórnvalda, samvinna og gjaldtaka.

7. gr.

Stefna um net- og upplýsingaöryggi.

Ráðherra skal marka stefnu um net- og upplýsingaöryggi þar sem m.a. eru greind markmið og ráðstafanir stjórnvalda sem eru nauðsynleg til að stuðla að háu öryggisstigi net- og

upplýsingakerfa mikilværa innviða og eftir atvikum annarra aðila. Stefnan skal endurskoðuð með reglubundnum hætti.

Stefnan skal unnin af ráðherra að höfðu samráði, m.a. við netöryggisráð, eftirlitsstjórnvöld, netöryggissveit og samráðshóp netöryggissveitar. Ráðherra skal með reglugerð mæla nánar fyrir um til hvaða þátta stefnan skal taka og um gildissvið hennar.

8. gr.

Eftirlitsstjórnvöld öryggis net- og upplýsingakerfamála.

Eftirfarandi stjórnvöld sinna eftirliti með öryggi net- og upplýsingakerfamála rekstraraðila nauðsynlegrar þjónustu hvert á sínu sviði:

1. Orkustofnun vegna orkuveitna,
2. Samgöngustofa vegna flutninga,
3. Fjármálaeftirlitið vegna bankaþjónustu,
4. Fjármálaeftirlitið vegna fjármálamarkaða,
5. Embætti landlæknis vegna heilbrigðisþjónustu,
6. Umhverfisstofnun vegna vatnsveitna og
7. Póst- og fjarskiptastofnun vegna stafrænna grunnvirkja.

Póst- og fjarskiptastofnun sinnir eftirliti með öryggi net- og upplýsingakerfa stafrænna þjónustuveitenda.

Þau stjórnvöld sem tiltekin eru í 1.-7. tölul. 1. mgr. geta gert með sér þjónustusamning um að eitt þeirra sinni afmörkuðu eftirliti með öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu á sviði annars. Þá geta þau gert samninga við sérfræðinga, svokallaða fulltrúar eftirlitsstjórnvalds í skilningi laga þessara og reglugerða settra á grundvelli þeirra, um aðstoð við afmarkað eftirlit.

Ráðherra skal með reglugerð mæla nánar fyrir um hlutverk eftirlitsstjórnvalda og gerð þjónustusamninga og samninga við sérfræðinga skv. 3. mgr.

9. gr.

Samhæfingarstjórnvald öryggis net- og upplýsingakerfa.

Póst- og fjarskiptastofnun samhæfir eftirlit stjórnvalda skv. 8. gr. með öryggi net- og upplýsingakerfa og starfrækir netöryggissveit skv. 10. gr.

Ráðherra skal með reglugerð mæla nánar fyrir um hlutverk samhæfingarstjórnvalds.

10. gr.

Netöryggissveit.

Netöryggissveit gegnir hlutverki viðbragðsteymis vegna atvika er varðar netöryggi, svokallað CSIRT-teymi fyrir Ísland. Netöryggissveitin skal sinna sólarhrings vöktun atvika í net- og upplýsingakerfum mikilvægra innviða sem falla undir starfsemi sveitarinnar skv. lögum þessum, reglugerð og birtri skrá, auk sólarhrings vöktunar atvika í net- og upplýsingakerfum Stjórnarráðs Íslands. Þá sinnir hún þjónustu við aðra aðila skv. 13. gr. Netöryggissveitin skal leitast við að greina öryggisatvik á frumstigi og skal hún senda út snemmviðvaranir og viðvörunarmerki í þeim tilgangi. Skal netöryggissveitin tilkynna og miðla upplýsingum til hlutaðeigandi hagsmunaaðila um áhættur og atvik, bregðast við atvikum og veita virka greiningu á áhættum og atvikum.

Ráðherra skal með reglugerð mæla nánar fyrir um starfsemi netöryggissveitar þar sem m.a. er fjallað um:

a. hlutverk, skipulag og verkefni netöryggissveitarinnar

b. mönnun og hæfi starfsmanna netöryggissveitarinnar, þ.m.t. um öryggisvottun starfsmanna,
c. miðlun upplýsinga til erlendra samstarfsaðila og viðeigandi öryggisráðstafanir þar að lútandi,
d. aðgang netöryggissveitar að upplýsingum,
e. vinnslu persónuupplýsinga, þ.m.t. öflun þeirra, hámarks varðveislutíma, miðlun og eyðingu,
f. upplýsingagjöf til almennings vegna netógna,
g. miðlun upplýsinga til tiltekinna hópa og flokkun trúnaðarstigs þeirra,
h. alþjóðasamstarf,
i. starf samráðshóps netöryggissveitar og sviðshópa hennar,
j. samninga netöryggissveitar við rekstraraðila mikilvægra innviða og stjórnarráð Íslands um vöktunarþjónustu,
k. þjónustusamninga netöryggissveitar við aðra aðila,
l. fyrirkomulag tilmæla vegna bráðrar netógnar og
m. skýrslugjöf um starfsemi netöryggissveitarinnar,

11. gr.

Samráðshópar netöryggissveitar.

Netöryggissveitinni er heimilt að koma á samráðshópi netöryggissveitar í þeim tilgangi að efla tengsl og samstarf á milli rekstraraðila mikilvægra innviða og sveitarinnar.

Þá skal netöryggissveit setja á laggirnar sérstaka sviðshópa fyrir hvert svið nauðsynlegrar þjónustu, skv. 1. mgr. 5. gr., fyrir hverja tegund stafrænna þjónustuveitenda skv. 1. mgr. 6. gr. og stjórnarráð Íslands. Sviðshópar skulu vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði net- og upplýsingaöryggis, m.a. til að greina ógnir og samræma viðbrögð. Í slíkum sviðshópum skulu eiga sæti, auk fulltrúa netöryggissveitar, tæknilegir fulltrúar rekstraraðila mikilvægra innviða og tæknilegir fulltrúar stjórnarráðs Íslands.

Um þær upplýsingar sem ræddar eru á fundum samráðshópsins og sviðshópanna skal ríkja trúnaður og þau gögn sem unnin eru eða afhent hópnum skulu teljast til vinnugagna í skilningi 2. og 3. tölul. 2. mgr. 8. gr. upplýsingalaga nr. 140/2012 sem réttur almennings til aðgangs tekur ekki til sbr. 5. tölul. 6. gr. sömu laga.

12. gr.

Alþjóðasamstarf.

Samhæfingarstjórnvald tekur þátt í alþjóðasamstarfi er varðar efni laga þessara.

Netöryggissveit tekur þátt í alþjóðasamstarfi netöryggissveita til að stuðla að trausti og samstarfi ríkja á þessu sviði.

Ráðherra skal með reglugerð mæla nánar fyrir um alþjóðasamstarf m.a. um afhendingu upplýsinga til erlendra stjórnvalda, eftirlitsaðila eða aðila sem sinna net- og upplýsingaöryggi.

13. gr.

Samningar og þjónustugjöld.

Aðilar sem ekki falla undir gildissvið laganna geta gert samninga við netöryggissveit um ráðgjöf, aðstoð og viðbúnað til að verjast mögulegum netárásum á net- og upplýsingakerfi

þeirra sem gerðar eru í þeim tilgangi að gera þau óvirk, valda skemmdum á þeim eða til öflunar ólögmæts fjárhagsleg ávinnings, svo sem með þjófnaði á gögnum eða peningum.

Netöryggissveit er heimilt að taka þjónustugjöld af þeim aðilum sem nýta sér þjónustu hennar án þess að vera það skylt skv. lögum þessum og hafa ekki gert samning skv. 1. mgr. Ráðherra getur með reglugerð mælt fyrir um fjárhæð þjónustugjalda og önnur atriði í tengslum við þjónustugjöld skv. ákvæði þessu.

IV. KAFLI
Öryggi net- og upplýsingakerfa.

14. gr.
Skipulag net- og upplýsingaöryggis.

Rekstraraðilar mikilvægra innviða skulu gera viðeigandi og hóflegar tæknilegar og skipulagslegar ráðstafanir til að stýra þeirri áhættu sem steðjar að öryggi net- og upplýsingakerfa sem þeir nota í starfsemi sinni svo stuðla megi að háu öryggisstigi að teknu tilliti til þeirrar áhættu sem getur skapast. Skulu þeir skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, framkvæma áhættumat og ákveða öryggisráðstafanir á grundvelli þess.

Rekstraraðilar mikilvægra innviða skulu gera viðeigandi ráðstafanir til að tryggja samfelldan og órofinn rekstur þeirrar þjónustu sem þeir veita og lágmarka áhrif af atvikum á öryggi net- og upplýsingakerfa með það fyrir augum að tryggja samfellu þjónustunnar.

Ráðherra skal með reglugerð, mæla nánar fyrir um skipulag net- og upplýsingaöryggis og virkni net- og upplýsingakerfa rekstraraðila mikilvægra innviða. Skal þar m.a. tekið tillit til eftirfarandi þátta eins og við á:

1. hvernig skjalfesta skuli skipulag net- og upplýsingaöryggis, þ.e. öryggi kerfa og búnaðar auk stjórnunar rekstrarsamfellu,
2. samræmingu fyrir stafræna þjónustuveitendur,
3. notkun alþjóðlegra staðla eða forskrifta,
4. framkvæmd innra eftirlits, t.a.m. eftirlits, endurskoðunar og prófana,
5. gerð skriflegrar neyðaráætlunar, s.s. um meðferð atvika,
6. raunlæg vernd net- og upplýsingakerfa vegna stjórnunar rekstrarsamfellu,
7. tilkynningar vegna öryggis- og/eða þjónusturofs og
8. helstu öryggisráðstafanir sem til greina koma.

15. gr.
Eftirlit og afhending upplýsinga.

Eftirlitsstjórnvöld hver á sínu sviði hafa eftirlit með því að rekstraraðilar mikilvægra innviða viðhafi viðeigandi ráðstafanir og að öryggiskröfum, skv. 14. gr. sé fullnægt.

Rekstraraðilar mikilvægra innviða skulu afhenda hlutaðeigandi eftirlitsstjórnvaldi, eða fulltrúa þess, allar upplýsingar um skipulag upplýsingaöryggis, þ.m.t. öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum, neyðaráætlun, skýrslur um innra eftirlit og niðurstöður öryggisúttekta og/eða prófana, þegar hlutaðeigandi eftirlitsstjórnvald óskar eftir því. Þá má kalla sömu aðila á fund til að veita munnlegar upplýsingar og skýringar varðandi atriði sem lög þessi taka til.

Eftirlitsstjórnvöldum, hverju á sínu sviði, eða fulltrúum þeirra, er heimilt að framkvæma úttektir og prófanir á því hvort rekstraraðilar nauðsynlegrar þjónustu uppfylli kröfur 14. gr. og reglugerðar skv. 3. mgr. greinarinnar.

Ráðherra getur með reglugerð mælt nánar fyrir um inntak eftirlits skv. 1. mgr., afhendingu gagna skv. 2. mgr. og um úttektir og prófanir skv. 3. mgr.

16. gr.

Tilkynningar um atvik.

Rekstraraðilar mikilvægra innviða skulu tilkynna annars vegar eftirlitsstjórnvaldi á viðkomandi sviði og hins vegar netöryggissveit um atvik sem hafa veruleg áhrif á þjónustu sem þeir veita. Við mat á verulegum áhrifum skal m.a. horfa til eftirfarandi þátta eins og við á:

1. fjölda þeirra notenda sem atvik hefur áhrif á,
2. hversu lengi atvikið stendur yfir,
3. stærð þess svæðis sem atvikið hefur áhrif á,
4. umfang atviks á virkni þjónustunnar og
5. umfang áhrifa atviks á efnahagslega og samfélagslega starfsemi.

Þegar rekstraraðili nauðsynlegrar þjónustu reiðir sig á stafrænan þjónustuveitanda sem er þriðji aðili til að veita þjónustu sem er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar eða efnahagslegrar starfsemi skal sá rekstraraðili tilkynna um öll veruleg áhrif á samfellu nauðsynlegrar þjónustu vegna atviks sem hefur áhrif á stafræna þjónustuveitandann.

Ráðherra skal með reglugerð mæla fyrir um þær upplýsingar sem eiga að koma fram í tilkynningu m.a. upplýsingar um hvort áhrifa atviks gæti yfir landamæri og nánar um þá þætti sem hafa áhrif á mat á verulegum áhrifum.

Stjórnarráð Íslands skal með sama hætti og um getur í 1. og 2. mgr. tilkynna atvik sem hafa veruleg áhrif á þjónustu til netöryggissveitar.

17. gr.

Atviks gætir yfir landamæri.

Ef áhrifa atviks gætir yfir landamæri skal netöryggissveit tilkynna viðkomandi ríki, og eftir atvikum alþjóðastofnun, um atvikið og hvort það hafi veruleg áhrif á nauðsynlega þjónustu í því ríki.

Þegar við á skal netöryggissveit veita þeim rekstraraðila mikilvægra innviða, sem tilkynnti um atvik sem gætir yfir landamæri, viðeigandi upplýsingar um eftirfylgni við tilkynningu skv. 1. mgr. ef þær geta stutt við skilvirka meðhöndlun atviks.

Samhæfingarstjórnvald skal afhenda hlutaðeigandi fulltrúum ríkja þar sem atviks gætir afrit tilkynningar rekstraraðila mikilvæga innviða telji netöryggissveit slíkt nauðsynlegt.

Ráðherra getur með reglugerð mælt nánar fyrir um tilkynningar um atvik sem gætir yfir landamæri m.a. um tilkynningar til alþjóðastofnana.

18. gr.

Valfrjálsar tilkynningar.

Aðilar sem falla utan gildissiðs laga þessara geta að eigin frumkvæði tilkynnt netöryggissveit um atvik sem hafa umtalsverð áhrif á samfellu þeirrar þjónustu sem þeir veita.

Um meðferð tilkynninga skv. 1. mgr. fer eftir lögum þessum og reglugerðum settum á grundvelli þeirra eins og við á en netöryggissveit er heimilt að veita skyldubundnum tilkynningum forgang umfram valfrjálsar tilkynningar.

Ráðherra getur með reglugerð mælt nánar fyrir um meðferð valfrjálsra tilkynninga.

19. gr.

Samningar netöryggissveitar

Rekstraraðilar mikilvægra innviða og stjórnarráð Íslands skulu, að beiðni netöryggissveitarinnar, gera samning við sveitina um vöktunarþjónustu fyrir net- og upplýsingakerfi sín í þeim tilgangi að greina hættur og ummerki um árásir, spillikóða og aðrar vísbendingar um aðstæður sem gætu skapað hættu fyrir viðkomandi rekstraraðila mikilvægra innviða og stjórnarráðið.

Samningar samkvæmt 1. mgr. skulu að lágmarki innihalda ákvæði er varða:

a. tegund þjónustu og búnað sem tengdur er í vöktun netöryggissveitar,
b. tegund og vinnslu þeirra gagna, þ.m.t. persónuupplýsinga, sem safnað er, meðferð þeirra, vistun og eyðingu,

Ráðherra skal í reglugerð kveða nánar á um gerð samninga, rekstur búnaðar og vinnslu gagna og persónuupplýsinga samkvæmt samningunum.

20. gr.

Aðgangur netöryggissveitar að upplýsingum

Rekstraraðilum mikilvægra innviða og stjórnarráði Íslands er skylt, að beiðni netöryggissveitarinnar að afhenda henni upplýsingar, skriflegar skýringar og gögn, þ.m.t. umferðaskrár netbúnaðar og -þjóna, sem nauðsynleg eru að mati netöryggissveitarinnar til að bregðast við atvikum og tryggja með sem bestum hætti vernd mikilvægra innviða samkvæmt lögum þessum. Þá má kalla sömu aðila á fund til að veita munnlegar upplýsingar og skýringar varðandi atriði sem lög þessi taka til.

Rekstraraðilar mikilvægra innviða og stjórnarráðið skulu afhenda netöryggissveit umbeðnar upplýsingar og gögn eins fljótt og við verður komið og eigi síðar en 12 klukkustundum eftir að beiðni netöryggissveitar berst.

Réttur stjórnvalda skv. þessu ákvæði eða ákvæði 15. gr. verður ekki takmarkaður með vísan til reglna um þagnarskyldu.

Ráðherra skal með reglugerð mæla nánar fyrir um öflun upplýsinga, ráðstafanir til að tryggja öryggi og eyðingu gagna og aðrar ráðstafanir sem eru nauðsynlegar vegna þessa ákvæðis m.a. til að tryggja friðhelgi einkalífs.

21. gr.

Tilmæli netöryggissveitar um viðbrögð við ógnum

Rekstraraðilum mikilvægra innviða og stjórnarráði Íslands er skylt að bregðast án tafar við tilmælum netöryggissveitar um aðgerðir gegn bráðri aðsteðjandi netógn, hvort sem sú ógn steðjar að mikilvægum innviði eins rekstraraðila, sviði rekstraraðila eða öllum rekstraraðilum mikilvægra innviða, stjórnarráði Íslands í heild eða hluta.

Ráðherra skal í reglugerð fjalla um meðferð atvika og áhættu hjá netöryggissveitinni sem m.a. skal innihalda flokkunarkerfi fyrir atvik, áhættu, upplýsingar og framsetningu tilmæla.

V. KAFLI
Upplýsingar og þagnarskylda.

22. gr.

Upplýsingar veittar almenningi.

Netöryggissveit skal, að upplýstu eftirlitsstjórnvaldi á viðkomandi sviði, að höfðu samráði við rekstraraðila mikilvægra innviða og/eða stjórnarráð Íslands tilkynna um atvik, upplýsa almenning um einstök atvik þar sem almenningsvitundar er þörf til að koma í veg fyrir eða takast á við atvik og þegar upplýsingagjöf um atvik er af öðrum ástæðum nauðsynleg í þágu almannahagsmuna. Þá er netöryggissveit heimilt að tilkynna almenningi um veikleika og almennar hættur ef það er nauðsynlegt í þágu almannahagsmuna.

Ráðherra getur með reglugerð mælt nánar fyrir um tilkynningar skv. 1. mgr.

23. gr.

Þagnarskylda.

Sérstök þagnarskylda, umfram þá sem greinir í 18. gr. laga um réttindi og skyldur starfsmanna ríkisins nr. 70/1996, skal ríkja um þær upplýsingar sem eftirlitsstjórnvöld hvert á sínu sviði eða fulltrúar þess, samhæfingarstjórnvald og netöryggissveit afla frá mikilvægum innviðum í tengslum við eftirlit með öryggi net- og upplýsingakerfa eða vegna meðferðar atvika. Þagnarskyldan helst þótt látið sé af starfi.

24. gr.

Undanþágur frá þagnarskyldu.

Ákvæði laga þessara um þagnarskyldu standa því ekki í vegi að eftirlitsstjórnvöld hvert á sínu sviði, samhæfingarstjórnvald og netöryggissveit veiti upplýsingar eða taki við upplýsingum frá lögreglu eða persónuverndaryfirvöldum ef þær upplýsingar varða net- og upplýsingaöryggi, almannavarnir eða persónuvernd.

Ákvæði laga þessara um þagnarskyldu standa því ekki í vegi að eftirlitsstjórnvöld hvert á sínu sviði, samhæfingarstjórnvald og netöryggissveit veiti upplýsingar eða taki við upplýsingum frá erlendum stjórnvöldum, eftirlitsaðilum eða öðrum aðilum eða sérfræðingum sem sinna net- og upplýsingaöryggi þegar slíkt er nauðsynlegt vegna skipulagðrar alþjóðasamvinnu sem hefur það markmið að stuðla að eða framkvæma aðgerðir til að tryggja öryggi net- og upplýsingakerfa.

Við upplýsingaskipti skv. 1. og 2. mgr. skal gæta trúnaðar um öryggis- og viðskiptahagsmuni hlutaðeigandi rekstraraðila mikilvægra innviða og þagnarskylda skv. 23. gr. skal ríkja um þær upplýsingar sem veittar eru eða tekið er á móti skv. 1. og 2. mgr.

25. gr.

Vinnsla persónuupplýsinga.

Netöryggissveitinni er heimil vinnsla persónuupplýsinga að því marki sem nauðsynlegt er til að hún geti sinnt hlutverki sínu á grundvelli þessara laga. Í því felst m.a. móttaka persónuupplýsinga frá aðilum sem falla undir gildissvið laganna og öðrum aðilum á grundvelli 18. gr., sem og miðlun þeirra til viðeigandi þriðju aðila, án samþykkis hins skráða, meti sveitin það nauðsynlegt í þágu þjóðaröryggis eða almannahagsmuna og miðlunin sé til þess að upplýsa um aðsteðjandi ógnir, koma í veg fyrir netárás eða önnur alvarleg öryggisatvik eða til að takmarka útbreiðslu eða draga úr tjóni vegna slíkra tilvika

Netöryggissveitinni er heimil vinnsla persónuupplýsinga og viðkvæmra persónuupplýsinga sem henni berast, t.a.m. vegna öryggisatvika, þ.m.t. að miðla þeim til viðeigandi þriðju aðila, án samþykkis hins skráða, meti hún það nauðsynlegt í þágu almannahagsmuna eða í þágu hagsmuna hins skráða til að koma í veg fyrir eða takmarka mögulegt tjón sem viðkomandi getur orðið fyrir.

Öll vinnsla persónuupplýsinga á grundvelli laga þessara skal vera í samræmi við ákvæði laga um persónuvernd og vinnslu persónuupplýsinga og reglna settra á grundvelli þeirra.

Ákvæði 17. og 20.-23. gr. laga um persónuvernd og vinnslu persónuupplýsinga, sbr. ákvæði 12.-22. og 34. gr. reglugerðarinnar, sbr. 1. tölul. 3. gr. framangreindra laga, gilda ekki um starfsemi netöryggissveitarinnar samkvæmt lögum þessum.

Ráðherra skal í reglugerð, að fengnu áliti Persónuverndar, kveða á um vinnslu persónuupplýsinga hjá netöryggissveitinni, meðferð þeirra og eyðingu, rétt skráðra einstaklinga og takmörkun á rétti þeirra. Í reglugerðinni skal, eftir því sem við á, a.m.k. fjalla um:

a) Tilgang vinnslunnar
b) Tegundir persónuupplýsinga
c) Meðferð, geymslu og eyðingu persónuupplýsinga
d) Gildissvið takmarkana sbr. 4. mgr.
e) Verndarráðstafanir til að koma í veg fyrir misnotkun eða ólögmætan aðgang eða miðlun,
f) Áhættu fyrir réttindi og frelsi skráðra einstaklinga

VI. KAFLI
Bindandi fyrirmæli, viðurlög og önnur ákvæði.

26. gr.
Bindandi fyrirmæli.

Í kjölfar eftirlits með öryggi net- og upplýsingakerfa á grundvelli 15 gr. getur eftirlitsstjórnvald hvert á sínu sviði gefið bindandi fyrirmæli er varða skipulag net- og upplýsingaöryggis, þ.m.t. um tilteknar lágmarks öryggisráðstafanir rekstraraðila mikilvægra innviða. Skylt er að verða við þeim fyrirmælum án tafar. Vanræki viðkomandi aðili að fara að fyrirmælunum getur eftirlitsstjórnvaldið látið vinna verkið á kostnað viðkomandi rekstraraðila mikilvægra innviða. Krafa um kostnað vegna þessa er aðfararhæf skv. 5. tölul. 1. mgr. 1. gr. laga um aðför nr. 90/1989.

Ráðherra getur með reglugerð mælt nánar fyrir um málsmeðferð vegna bindandi fyrirmæla.

27. gr.
Dagsektir.

Ef ekki er farið að fyrirmælum eftirlitsstjórnvalds skv. 26. gr. eða ósk þess eða netöryggissveitar um afhendingu upplýsinga skv. 15. og 20. gr. getur hlutaðeigandi eftirlitsstjórnvald ákveðið að leggja dagsektir á þann sem fyrirmælin beinast að og þar til úr verður bætt að mati eftirlitsstjórnvaldsins og eftir atvikum að höfðu samráði við netöryggissveit. Sektir geta numið allt að 500.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælum sé fylgt.

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 án undangengins dóms gera aðför til fullnustu þeirra.

28. gr.
Refsingar.

Brot á ákvæðum laga þessara og reglugerða settra samkvæmt þeim varða fésektum eða fangelsi allt að tveimur árum nema þyngri refsins liggi við samkvæmt öðrum lögum. Sama refsing liggur við ef ekki er farið að fyrirmælum eftirlitsstjórnvalds eða netöryggissveitar. Gáleysisbrot skulu eingöngu varða sektum.

Nú er brot skv. 1. mgr. framið í starfsemi lögaðila og má þá gera lögaðilanum fésekt skv. II. kafla A almennra hegningarlaga nr. 19/1940.

Tilraun og hlutdeild í brotum á lögum þessum og reglum settum samkvæmt þeim eru refsiverð skv. III. kafla almennra hegningarlaga.

29. gr.

Bótaábyrgð.

Tilkynning um atvik til netöryggissveitar skal ekki hafa áhrif á eða auka mögulega bótaskyldu vegna atviksins.

VII. KAFLI
Gildistaka o.fl.

30. gr.

Innleiðing.

Lög þessi fela í sér innleiðingu á tilskipun Evrópuþingsins og ráðsins 2016/1148/ESB frá 6. júlí 2016 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu.

31. gr.

Reglugerðarheimild.

Ráðherra getur í reglugerð mælt nánar fyrir um önnur atriði en greinir í einstökum greinum laganna í tengslum við framkvæmd laga þessara eins og nánar greinir í lögunum.

32. gr.

Gildistaka.

Lög þessi öðlast gildi 1. janúar 2019.

33. gr.

Breytingar á öðrum lögum.

Við gildistöku laga þessara breytist eftirfarandi ákvæði laga sem hér segir:

1. *Lög um fjarskipti nr. 81/2003*, með síðari breytingum:
    a. Eftirfarandi breytingar verða á 3. gr.:
        i. 20., 23., 27. og 37. töluliðir falla brott.
        ii. 24. töluliður orðast svo: *Netöryggissveit Póst- og fjarskiptastofnunar* eða *netöryggissveitin:* Öryggis- og viðbragðshópur sem starfar á vegum Póst- og fjarskiptastofnunar vegna netógna í netumdæmi Íslands.
        iii. Við bætist nýr töluliður, 22. töluliður, er orðast svo, og breytist röð annarra liða samkvæmt því: *Netógn:* Atburður eða atburðir í tölvu og/eða netkerfum sem geta ógnað einstökum notendum þeirra, einstökum kerfum eða kerfunum í heild. Til slíkra atburða geta talist

alvarlegir og nýtanlegir öryggisgallar sem og notkun á spillihugbúnaði í þeim tilgangi að ná stjórn á kerfum.

b. Í stað 47. gr. a koma þrjár greinar, 47. gr. a – 47. gr. c, er orðast svo, ásamt fyrirsögnum:

47. gr. a

Netöryggissveit.

Póst- og fjarskiptastofnun skal starfrækja netöryggissveit sem gegna skal hlutverki öryggis- og viðbragðshóps hér á landi. Netöryggissveitin skal vera CSIRT-teymi fyrir Ísland og skal hún taka þátt í og gegna hlutverki tengiliðar íslenskra stjórnvalda í innlendu og alþjóðlegu samstarfi um viðbragðsvarnir vegna netógna, hættu og atvika á Internetinu.

Netöryggissveitin skal greina og meðhöndla ógnir, hættur og atvik í net- og upplýsingakerfum fjarskiptafyrirtækja og fyrirbyggja og draga úr hættu á öryggisatvikum eins og kostur er og sporna við og lágmarka tjón aðila sem af slíku kann að hljótast. Netöryggissveitin skal sinna sólarhrings vöktun atvika í net- og upplýsingakerfum fjarskiptafyrirtækja, sbr. 47. gr. b.

Netöryggissveitin skal leitast við að greina öryggisatvik á frumstigi og skal hún senda út snemmviðvaranir í þeim tilgangi. Skal netöryggissveitin tilkynna og miðla upplýsingum til hlutaðeigandi hagsmunaaðila um áhættur og atvik, bregðast við atvikum og veita virka greiningu á áhættum og atvikum. Netöryggissveitin veitir ráðgjöf um varnir og viðbúnað og kemur upplýsingum á framfæri við almenning ef þurfa þykir.

Netöryggissveitin skal aðstoða fjarskiptafyrirtæki við forvarnir, leiðbeina þeim og styðja við skjót viðbrögð gegn aðsteðjandi hættu. Við útbreitt öryggisatvik samhæfir netöryggissveitin aðgerðir aðila þeirra gegn aðsteðjandi hættu til að lágmarka tjón og reisa við óvirk kerfi. Fjarskiptafyrirtækjum er skylt að bregðast án tafar við tilmælum netöryggissveitar um aðgerðir gegn bráðri aðsteðjandi netógn, hvort sem sú ógn steðjar að net- og upplýsingakerfum fjarskiptafyrirtækis eða fjarskiptafyrirtækja.

Netöryggissveit skal setja á laggirnar samstarfshóp með fjarskiptafyrirtækjum fyrir tæknilegt samráð og upplýsingaskipti á sviði net- og upplýsingaöryggis, m.a. til að greina ógnir og samræma viðbrögð.

Ráðherra skal í reglugerð fjalla nánar um starfsemi netöryggissveitarinnar. Skal m.a. fjalla um meðferð atvika og áhættu hjá netöryggissveitinni sem m.a. skal innihalda flokkunarkerfi fyrir atvik, áhættu, upplýsingar og framsetningu tilmæla, og samstarf við ríkislögreglustjórna.

47. gr. b

Samningar netöryggissveitar og fjarskiptafyrirtækja.

Fjarskiptafyrirtæki og netöryggissveit skulu, að beiðni netöryggissveitarinnar, gera með sér samning um uppsetningu og rekstur vöktunarþjónustu fyrir net- og upplýsingakerfi fjarskiptafyrirtækisins í þeim tilgangi að greina hættur og ummerki um árásir, spillikóða og aðrar vísbendingar um aðstæður sem gætu skapað hættu fyrir net- og upplýsingakerfi viðkomandi fjarskiptafyrirtækis.

Samningar samkvæmt 1. mgr. skulu a.m.k. innihalda ákvæði er varða:

a. Búnað og netkerfi sem tengdur er í vöktun netöryggissveitar,
b. tæknilegar lausnir sem beitt er við vöktun,
c. tegund og vinnslu þeirra gagna, þ.m.t. persónuupplýsinga, sem safnað er, meðferð þeirra, vistun og eyðingu.

Fjarskiptafélögum er skylt að hýsa og samtengjast þeim búnaði netöryggissveitarinnar sem nauðsynlegur er vegna vöktunarþjónustu endurgjaldslaust.

Hvorki er heimilt að persónugreina netumferð, né skima einstaka netpakka eða flæði, sem netöryggissveitin kann að nema í almennum netkerfum fjarskiptafyrirtækja. Netöryggissveit er þó heimilt að móttaka upplýsingar um almenna netumferð, þ.m.t. á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar.

47. gr. c

Aðgangur að upplýsingum, þagnarskylda og vinnsla persónuupplýsinga.

Um aðgang netöryggissveitar að gögnum og upplýsingum, um sértæka þagnarskyldu og undanþágur frá slíkri skyldu og um meðferð persónuupplýsinga skal, að breyttu breytanda, fara eftir ákvæðum 20., 23.-25. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða.

2. *Lög um Póst- og fjarskiptastofnun nr. 69/2003,* með síðari breytingum:
   a. 2. mgr. 1. gr. orðast svo: Póst- og fjarskiptastofnun er sjálfstæð stofnun sem heyrir stjórnarfarslega undir ráðherra.
   b. Við 1. mgr. 3. gr. bætist nýr töluliður, 8 töluliður, er orðast svo: Annast málefni öryggis net- og upplýsingakerfa mikilvægra innviða og samkvæmt lögum þar um, þ.m.t.
      i. samhæfingarhlutverk,
      ii. eftirlit með stafrænum grunnvirkjum og
      iii. eftirlit með stafrænum þjónustuveitendum.

G r e i n a r g e r ð .

1. Inngangur.

Frumvarp þetta var samið í samgöngu- og sveitarstjórnarráðuneytinu. Með frumvarpinu og reglugerðum settum á grundvelli þess er stefnt að því að innleiða reglur um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu eins og þeir eru skilgreindir í tilskipun sem Evrópuþingið og ráðið samþykkti 6. júlí 2016, tilskipun 2016/1148/ESB um ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan Evrópska efnahagssvæðisins (þjónustan sem um ræður er á eftirtöldum sviðum; orkuveitur, flutningar, bankaþjónusta, fjármálamarkaðir, heilbrigðisþjónusta, vatnsveitur og stafræn grunnvirki) og stafrænna þjónustuveitenda til að tryggja hátt öryggisstig þessara kerfa, viðbrögð við atvikum o.fl.

Hátt öryggisstig þeirra kerfa sem um ræðir og áreiðanleiki þeirra skiptir sköpum fyrir efnahagslega- og samfélagslega starfsemi. Það skiptir miklu máli fyrir trúverðugleika þeirrar þjónustu sem um ræðir, bæði innanlands og erlendis. Verði frumvarpið að lögum verður í

fyrsta skipta í gildi heildstæð löggjöf um net- og upplýsingaöryggi sem tekur til allra þeirra aðila sem falla undir frumvarpið.

2. Tilefni og nauðsyn lagasetningar.

Frumvarpið felur í sér innleiðingu tilskipunar sem Evrópuþingið og ráðið samþykktu 6. júlí 2016 tilskipun 2016/1148/ESB um ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan EES. Ríkjum ber skv. tilskipuninni að tryggja þeim stjórnvöldum sem fara með verkefni á grundvelli hennar nægt fjármagn til að annast á árangursríkan og skilvirkan hátt þau verkefni sem þeim eru falin svo markmiðum tilskipunarinnar verði náð.

Við vinnslu frumvarpsins voru nokkrar leiðir skoðaðar vegna rúms gildissviðs tilskipunar 2016/1148/ESB. Aðallega komu tvær leiðir til greina. Annars vegar að smíða heildstæða löggjöf um innleiðingu tilskipunarinnar og eftir atvikum gera nauðsynlegar aðrar umfangsminni lagabreytingar og hins vegar að bæta við þá fjölmörgu lagabálka sem gilda nú um þá aðila sem falla undir gildissvið tilskipunarinnar, ákvæðum um net- og upplýsingaöryggi. Vegna þess hversu rúmt gildissvið tilskipunarinnar er og þar sem hún teygir anga sína inn á fjölmörg svið sem fæst hafa heildstæðar reglur um öryggi net- og upplýsingakerfa varð sú leið fyrir valinu að smíða eina löggjöf sem nær utan um efni tilskipunarinnar. Virtist sú leið í senn einföldust og skýrust og best til þess fallin að ná til þess fjölbreytta hóps einka- og opinberra aðila sem falla undir gildissvið hennar.

Tilskipunin kveður á um vernd net- og upplýsingakerfa tiltekinna aðila, þ.e. rekstraraðila þeirra nauðsynlegu þjónustu sem að tilskipunin skilgreinir og stafræna þjónustuveitendur. Þótt eitt yfirlýst markmið tilskipunarinnar sé að tryggja hátt stig öryggis fyrir net- og upplýsingakerfi innan Evrópusambandsins er tilskipunin miðuð að framangreindum aðilum. Tilskipunin kveður því ekki á um almenna netheilsu Evrópusambandsins í heild eða aðildarríkja, þ.e. um það hvaða starfsemi geti verið til staðar í netlögsögu þess eða aðildarríkja.

3. Meginefni frumvarpsins.

Með frumvarpinu er stefnt að því að innleiða eftirfarandi meginmarkmið tilskipunar 2016/1148/ESB og/eða búa þannig um hnútana, þar sem það var unnt, að fyrir hendi sé heimild ráðherra til að setja reglugerð þar sem hluta þessara markmiða er náð. Meginmarkmið tilskipunarinnar eru þríþætt:

1. Að auka hæfni aðildarríkja til að bæta netöryggi og bregðast við aðstæðum þar sem netöryggi er raskað.
- Aðildarríki þurfa að setja sér stefnu um net- og upplýsingaöryggi.
- Aðildarríki þurfa að fela stjórnvöldum umsjón og eftirlit með því að farið sé eftir ákvæðum tilskipunarinnar og tilnefna tengilið sem hefur m.a. samskipti við önnur ríki.
- Aðildarríki þurfa að setja á fót netöryggissveit.
2. Bæta samvinnu aðildarríkja á sviði netöryggis.
- Samstarfshópi aðildarríkja komið á fót í því skyni að styðja og auðvelda stefnumótandi samstarf, skapa traust og miðla upplýsingum.
- Samstarfsneti netöryggissveita aðildarríkja komið á fót í því skyni að stuðla að trausti milli ríkja og skjótri og árangursríkri samvinnu.
3. Styrkja stoðir rekstraraðila mikilvægra innviða og stafrænna þjónustuveitenda þar sem netöryggi kemur við sögu.
- Aðildarríki þurfa að skilgreina þá sem falla undir tilskipunina.
- Tilskipunin kemur á öryggiskröfum og tilkynningarskyldu fyrir þessa aðila.

4. Samræmi við stjórnarskrá og alþjóðlegar skuldbindingar.

Með upptöku tilskipun 2016/1148/ESB í EES-samninginn verður Ísland skuldbundið samkvæmt samningnum til að innleiða tilskipunina.

Frumvarpið gaf tilefni til að skoða samræmi við ákvæði 71. gr. stjórnarskrár um friðhelgi einkalífs auk ákvæða laga um persónuvernd og vinnslu persónupplýsinga nr. /2018, og var gætt að þeim sjónarmiðum sem þar koma fram við útfærslu ákvæða frumvarpsins.

5. Samráð.

Frumvarpið varðar samfélagið í heild, en helstu hagsmunaaðilar eru allir rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur í skilningi tilskipunar 2016/1148/ESB hvort sem um er að ræða einka- eða opinbera aðila. Almenningur sem nýtir þá þjónustu sem um ræðir hefur að auki ríka hagsmuni af háu öryggisstigi net- og upplýsingakerfa enda notendur þeirrar þjónustu sem um ræðir.

Net- og upplýsingaöryggi fellur undir málefnasvið samgöngu- og sveitarstjórnarráðuneytis en nokkur skörun er við málefnasvið atvinnuvega- og nýsköpunarráðuneytis, fjármála- og efnahagsráðuneytis, umhverfisráðuneytis og velferðarráðuneytis vegna þeirra aðila sem falla undir gildissvið tilskipunarinnar. Við vinnslu frumvarpsins var viðhaft náið samráð við ráðuneytin og önnur stjórnvöld sem starfa á þeim málefnasviðum sem frumvarpið tekur til. Fundað hefur verið með þeim ráðuneytum og öðrum stjórnvöldum um tilskipunina, auk þess sem fyrirhuguð lagasetning var kynnt á ráðstefnum og ýmsum fundum m.a. á UT-messunni í Hörpu í febrúar 2018. Þá var haldinn opinn samráðsfundur þann 17. maí 2018 þar sem öllum hagsmunaaðilum var boðið að taka þátt. Á þeim fundi voru þær hugmyndir sem frumvarp þetta byggir á kynntar og í framhaldinu átti sér stað virk umræða við hagsmunaaðila.

Áform um lagasetningu og frummat á áhrifum fóru í kynningu innan ráðuneytanna og þá fóru sömu skjöl í opið samráð við almenning á vef ráðuneytisins í samræmi við samþykkt ríkisstjórnarinnar um undirbúning og frágang stjórnarfrumvarpa og stjórnartillaga frá mars 2017.

Drög að frumvarpi fóru í kynningu í samráðsgátt stjórnarráðsins í júní 2018.

6. Mat á áhrifum.

Verði frumvarp þetta að lögum er ljóst að lagðar verða kröfur á rekstraraðila mikilvægra innviða um ákveðið skipulag á öryggi net- og upplýsingakerfa þeirra sem og að þeir munu sæta eftirliti af hálfu stjórnvalda. Hér eru því lagðar íþyngjandi kröfur á viðkomandi aðila að viðlögðum refsingum. Aftur á móti byggja þessar kröfur á mikilvægum almannahagsmunum, þ.e. að sú þjónusta sem talin er samfélagslega og efnahagslega mikilvæg fái ákveðna vernd gegn utanaðkomandi ógnum. Þannig vegast á hagsmunir viðkomandi rekstraraðila og almannahagsmunir. Hefur löggjafi Evrópusambandsins metið það svo að umræddir almannahagsmunir vegi þyngra en þær íþyngjandi kröfur sem að lagðar eru á rekstraraðila mikilvægra innviða. Hins vegar er í þessu ljósi nauðsynlegt að horfa til þess að umræddum rekstraraðilum er jafnframt tryggð mikilvæg þjónusta í formi viðbragðsteymis vegna netógna og atvika. Fá þeir aðgang að sólarhringsþjónustu slíks CSIRT-teymis, aðgengi að hópi sérfræðinga á þessu sviði sem og, með óbeinum hætti í gegnum þá sérfræðinga, upplýsingar eða viðvaranir um ógnir sem að einungis netöryggissveit hefur aðgang að. Það er því ekki einungis um að ræða íþyngjandi skyldur, heldur er jafnframt stuðlað að hærra öryggisstigi þeirra eigin net- og upplýsingakerfa. Það er því ljóst að ávinningur með samþykkt frumvarps þessa er mikill fyrir veitingu samfélagslega og efnahagslega mikilvæga þjónustu hér á landi.

Frumvarpið mun stuðla að auknu öryggi þessarar þjónustu sem og þeirra upplýsinga sem að rekstraraðilar þjónustunnar hafa yfir að ráða. Slíkar upplýsingar geta verið mjög margþættar og falið í sér upplýsingar um rekstur viðkomandi aðila, rekstraruppbyggingu og áætlanir sem og almennar jafnt sem viðkvæmar persónuupplýsingar.

Eins er ljóst að með frumvarpinu er kveðið á um hlutverk eftirlitsstjórnvalda þegar kemur að öryggisskipulagi net- og upplýsingakerfa rekstraraðila mikilvægra innviða. Við samningu frumvarpsins var talið skynsamlegast að þau stjórnvöld sem nú þegar sinna ákveðnu eftirlitshlutverki með umræddum aðilum sinni einnig því eftirliti sem kveðið er á um í frumvarpi þessu. Er sú leið valin, umfram þá að hafa einungis eitt eftirlitsstjórnvald, sökum þeirrar þekkingar sem þegar er til staðar innan viðkomandi stjórnvalda. Sú viðbót sem hér um ræðir ætti því ekki að vera mjög íþyngjandi fyrir viðkomandi stjórnvöld, sér í lagi m.t.t. þeirrar samhæfingar sem mun eiga sér stað um framkvæmd eftirlitsins á vegum Póst- og fjarskiptastofnunar. Sú stofnun sker sig nokkuð úr hvað varðar eftirlitsstjórnvöld. Stofnunin hefur fram til þessa einungis haft eftirlit með fjarskiptafyrirtækjum hér á landi. Með frumvarpinu er stofnuninni falin ný hlutverk, þ.e. auk þess að vera samhæfingarstjórnvald skal stofnunin nú hafa eftirlit með skipulagi öryggis net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja og stafrænum þjónustuveitendum. Starfsemi stofnunarinnar mun því aukast hvað það varðar. Þá er ljóst að hlutverk netöryggissveitar Póst- og fjarskiptastofnunar mun margfaldast. Í dag sinnir sveitin fjarskiptamarkaðinum og stjórnarráði Íslands, sbr. samning þar um. Við samþykkt frumvarpsins mun þjónustuhópur sveitarinnar því stækka gríðarlega og ná til þeirra rekstraraðila mikilvægra innviða sem undir gildisvið laganna falla. Þá fær sveitin skýrari heimildir og hlutverk er varða samræmingu viðbragða við netógnum og atvikum, upplýsingagjöf o.fl.

Verði frumvarpið óbreytt að lögum er áætlað að sá kostnaður sem hlýst við innleiðingu NIS tilskipunar á næstu fimm árum, eða á tíma fjármálaáætlunar ríkisstjórnarinnar 2019-2023, verði um 2.853 m.kr., þar af er áætlað um 471 m.kr. á árinu 2019. Sá kostnaðarliður, sem vegur hvað þyngst er vegna rannsóknartækja, eða um 233 m.kr. af 471 m.kr. Áætlað er að innleiða verkefni skv. tilskipuninni í þrepum og verði þau að fullu innleidd árið 2022. Á árinu 2020 er áætlaður heildarkostnaður um 509 m.kr. og hækkar 38 m.kr. milli ára. Á árunum 2021-2023 er áætlaður kostnaður vegna innleiðingar samtals um 1,9 ma.kr. yfir 3 ár. Ekki hefur verið gert ráð fyrir þessum auknu útgjöldum á málefnasviði 11 hjá samgöngu- og sveitarstjórnaráðuneyti, í málaflokki fjarskipta, í gildandi fjármálaáætlun. Ekki er gert ráð fyrir auknum útgjöldum umfram gildandi fjárlög þar sem áætlað er að lögin taki gildi 2019.

Um einstakar greinar frumvarpsins.

Um 1. gr.

Í ákvæðinu eru helstu markmið frumvarpsins sett fram í fimm töluliðum en með því er ætlunin að ná utan um 1. gr. tilskipunar 2016/1148/ESB auk þess sem fram kemur í inngangsorðum tilskipunarinnar um markmið hennar. Megin markmið tilskipunarinnar er að koma á sameiginlegu öryggisstigi í net- og upplýsingakerfum innan Evrópusambandsins í því skyni að bæta starfsemi innri markaðarins. Svo stuðla megi að háu öryggisstigi net- og upplýsingakerfa mikilvægra innviða hérlendis, þ.e. rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda, þurfa stjórnvöld að samhæfa aðgerðir og skilgreina hlutverk sitt, samþykkja stefnu um öryggi net- og upplýsingakerfa, efla hlutverk netöryggissveitar, koma á öryggiskröfum og tilkynningarskyldu um atvik og styrkja alþjóðasamstarf. Í öðrum greinum

frumvarpsins og reglugerðum settum á grundvelli þess eru og verða markmiðin fimm skilgreind nánar.

Um 2. gr.

Ákvæðið 2. gr. þarfnast ekki sérstakrar skýringar en það felur í sér orðskýringar á helstu orða eða orðasamböndum sem notuð eru í frumvarpinu. Í ákvæðinu eru að mestu teknar upp þær skilgreiningar sem fram koma í 4. gr. tilskipunar 2016/1148/ESB auk annarra orðskýringa sem þóttu nauðsynlegar samhengisins vegna. Ákvæðið tekur jafnt til ákvæða frumvarpsins og þeirra reglugerða sem skylt er eða heimilt verður að setja á grundvelli þess.

Um 3. gr.

Í ákvæðinu er gildissvið frumvarpsins afmarkað. Frumvarpinu er ætlað ná til sömu aðila og þeirra sem falla undir tilskipun 2016/1148/ESB en taka að auki til annarra aðila eins og skýrt verður nánar.

Í 1. mgr. kemur fram að frumvarpið taki til net- og upplýsingakerfi mikilvægra innviða. Mikilvægir innviðir er yfirheiti yfir annars vegar rekstraraðila nauðsynlegrar þjónustu og hins vegar stafræna þjónustuveitendur en þessir aðilar eru nánar skilgreindir í frumvarpinu, sbr. 2., 5. og 6. gr. auk reglugerða sem settar verða á grundvelli frumvarpsins

Í 2. mgr. er kveðið á um að frumvarpið taki einnig til net- og upplýsingaöryggis Stjórnarráðs Íslands hvað varðar vöktun atvika og viðbrögð við atvikum í net- og upplýsingakerfum eins og nánar greinir í frumvarpinu og reglugerðum settum á grundvelli þess. Net- og upplýsingaöryggi Stjórnarráðs Íslands fellur ekki með beinum hætti undir tilskipun 2016/1148/ESB en þó þykir eðlilegt að hluti þeirra reglna sem kveðið er á um í frumvarpinu taki einnig til Stjórnarráðs Íslands. Í gildi er sérstakur samningur Stjórnarráðs Íslands við netöryggissveit Póst- og fjarskiptastofnunar sem undirritaður var í janúar 2018. Markmið samningsins var að styrkja stjórnsýsluna til að verjast öryggisatvikum og takast á við netárásir og hliðstæðar ógnir með sérhæfðri þjónustu Netöryggissveitarinnar. Samkvæmt samningnum veitir netöryggissveitin stjórnsýslunni, og þá sérstaklega ráðuneytunum, netöryggisþjónustu sem er sérsniðin að þörfum hins opinbera, svonefnda GovCERT þjónustu. Netöryggissveitinni ber, samkvæmt núgildandi lögum, fyrst og fremst að þjóna skilgreindum þjónustuhópi sínum. Í þeim hópi eru fjarskiptafélögin, en aðrir rekstraraðilar ómissandi upplýsingainnviða geta einnig notið þjónustu netöryggissveitarinnar á grunni samninga. Ákvæði 2. mgr. er ætlað að koma í stað þess að Stjórnarráð Íslands þurfi að gera sérstakan samning við netöryggissveitina um þjónustu tengda net- og upplýsingaöryggi.

Í 3. mgr. er tekið fram að utan gildissvið frumvarpsins falla stafrænir þjónustuveitendur sem teljast örfélög í skilningi laga um ársreikninga nr. 3/2006. En stafrænir þjónustuveitendur eru annar flokkur nauðsynlegra innviða af tveimur, hinn flokkurinn eru rekstraraðilar nauðsynlegrar þjónustu, og eru þeir í 2. gr. skilgreindir sem sérhver lögaðili með höfuðstöðvar þ.e. aðalskrifstofu, eða staðfestu, hérlendis sem veitir stafræna þjónustu eða fulltrúi hans með staðfestu hérlendis. Er málsgreininni ætlað að ná utan um 3. mgr. 1. gr. tilskipunarinnar þar sem fram kemur að öryggiskröfur og tilkynningarskyldan sem tilskipunin kveður á um skulu ekki gilda um fyrirtæki sem falla undir kröfur 13. gr. a og 13. gr. b í tilskipun 2002/21/EB eða um veitendur traustþjónustu sem falla undir kröfur 19. gr. í reglugerð (ESB) nr. 910/2014.

Um 4. gr.

Með ákvæðinu er tekið af skarið um að í þeim tilvikum þegar net- og upplýsingaöryggi er ógnað með þeim hætti að upp komi neyðarástand sem kann að ógna lífi og heilsu almennings,

umhverfis og/eða eignum eins og fjallað er um þessi atriði í lögum um almannavarnir nr. 82/2008 skulu stjórnvöld bregðast við á grundvelli þeirra laga. Ákvæðinu er ekki ætlað að koma í veg fyrr viðbrögð á grundvelli ákvæða frumvarpsins heldur taka af skarið um að þegar þessi staða kemur upp verði einnig að gæta að framangreindum lögum.

Af ákvæðum tilskipunar 201671148/ESB sbr. t.d. 6. mgr. 1. gr. er ljóst að tilskipuninni er ekki ætlað að hafa áhrif á aðgerðir sem stjórnvöld hafa gripið til sem vernda grundvallarhlutverk ríkja. Er þar einkum átt við þjóðaröryggi þ.m.t. aðgerðir sem vernda upplýsingar þar sem talið verður að birting sé talin andstæð mikilvægum öryggishagsmunum og til að halda uppi lögum og reglu t.a.m. vegna rannsókna og saksóknar refsiverðra brota.

Um 5. gr.

Undir gildissvið frumvarpsins skv. 1. mgr. 3. gr. falla mikilvægir innviðir en þeir eru skv. orðskýringum 2. gr. annars vegar rekstraraðilar nauðsynlegrar þjónustu og hins vegar stafrænir þjónustuveitendur. Fjallað er um þá fyrrnefndu í ákvæðinu. Í orðskýringum 2. gr. frumvarpsins eru rekstraraðilar nauðsynlegrar þjónustu skilgreindir sem opinber eða einkaaðili, birtur í skrá skv. lögunum og veitir þjónustu sem nánar er skilgreind í lögunum. Ákvæðið, reglugerð og skrá sett á grundvelli ákvæðisins fela í sér innleiðingu á 5. gr., 6. gr. og II. viðauka við tilskipun 2016/1148/ESB. Í 5. gr. tilskipunarinnar er fjallað um auðkenningu rekstraraðila nauðsynlegrar þjónustu, í 6. gr. er fjallað um hvað fellst í verulega skerðandi áhrifum og í II. viðauka við tilskipunina er gefið yfirlit yfir tegundir aðila sem flokkast geta til rekstraraðil nauðsynlegrar þjónustu. Um er að ræða sjö tegundir aðila og/eða þjónustu, sbr. nánari umfjöllun um 1. mgr.

Í 1. mgr. er fjallað um rekstraraðila nauðsynlegrar þjónustu en þeir geta hvort sem heldur er verið opinberir aðilar eða einkaaðilar eins og nánar er getið. Tiltekið er í sjö töluliðum á hvaða sviðum þjónustan er sem um ræðir. Sviðin eru; orkuveitur, flutningar, bankaþjónusta, fjármálamarkaðir, heilbrigðisþjónusta, vatnsveitur og stafræn grunnvirki og hafa þeir aðilar verið skilgreindir nánar í orðskýringum 2. gr. frumvarpsins, sbr. einnig II. viðauka við tilskipunina þar sem sviðin tilgreind með nánari hætti eins og fram hefur komið. og

Í 2. mgr. kemur fram að sú þjónusta sem rekstraraðilar nauðsynlegrar þjónustu veita skuli vera nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi, veiting þjónustunnar þarf að verða háð net- og upplýsingakerfum og atvik þurfa að hafa verulega skerðandi áhrif á veitingu þjónustunnar. Í 6. gr. tilskipunarinnar eru sett fram viðmið um til hvaða þátta skuli taka tillit til við mat á því hvað teljist til verulega skerðandi áhrifa. Er hér um að ræða þau viðmið sem fram koma í a.-c. liðum 2. mgr. 5. gr. tilskipunar 2016/1148/ESB.

Með 3. mgr. er ráðherra gert skylt að setja reglugerð þar sem mælt er fyrir um við hvað eigi að miða þegar rekstraraðilar nauðsynlegrar þjónustu eru auðkenndir. Þar þarf m.a. að koma fram hvaða þjónusta er nauðsynleg fyrir viðhald mikilværar samfélagslegrar og efnahagslegrar starfsemi og hvað flokkast til verulega skerðandi áhrifa. Útfæra þarft í reglugerðinni það sem fram kemur í 5. gr., 6. gr. og II. viðauka við tilskipunina og ekki hefur verið innleitt með frumvarpinu.

Í 3. mgr. er gert ráð fyrir því að ráðherra haldi opinbera skrá yfir rekstraraðila nauðsynlegrar þjónustu sem hafa starfstöð hér á landi. Skrána skal birta með auglýsingu í B-deild Stjórnartíðinda og skal hún vera uppfærð á a.m.k. tveggja ára fresti. Ef breytingar eru tíðar á þeim aðilum sem uppfylla þau viðmið sem mælt verður fyrir um á grundvelli 2. mgr. getur ráðherra uppfært skránna tíðar en á tveggja ára fresti enda er sú uppfærsla einungis lágmarks uppfærsla skrárinnar.

Um 6. gr.

Undir gildissvið frumvarpsins skv. 1. mgr. 3. gr. falla mikilvægir innviðir en þeir eru skv. orðskýringum 2. gr. annars vegar rekstraraðilar nauðsynlegrar þjónustu og hins vegar stafrænir þjónustuveitendur. Fjallað er um þá síðarnefndu í ákvæðinu. Í orðskýringum 2. gr. frumvarpsins eru stafrænir þjónustuveitendur skilgreindir sem sérhver lögaðili með höfuðstöðvar þ.e. aðalskrifstofu, eða staðfestu, hérlendis sem veitir stafræna þjónustu eða fulltrúi hans með staðfestu hérlendis. Í III. viðauka tilskipunar 2016/1148/ESB eru tegundir stafrænnar þjónustu tilgreindar en þær eru netmarkaður, leitarvélar á Netinu og skýjavinnsluþjónusta og eru tegundirnar skilgreindar nánar í orðskýringum í 2. gr. frumvarpsins. Ákvæði 6. gr. felur í sér innleiðingu þess sem fram kemur í viðaukanum.

Í þremur töluliðum í 1. mgr. eru tilgreindar tegundir stafrænnar þjónustu og í 2. mgr. er gert ráð fyrir að ráðherra geti með reglugerð mælt nánar fyrir um auðkenningu stafrænna þjónustuveitenda. Um er að ræða heimildarákvæði en ekki skyldu til setningar reglugerðar sem ráðherra getur nýtt telji hann þörf á reglusetningu um framangreint.

Um 7. gr.

Eitt af markmiðum frumvarpsins skv. 1. gr., sbr. 1. gr. tilskipunar 2016/1148/ESB, er að mörkuð verði stefna um öryggi net- og upplýsingakerfa. Ákvæðinu er ætlað að innleiða 7. gr. tilskipunarinnar sem fjallar með ítarlegum hætti um landsbundnar stefnuáætlanir um öryggi net- og upplýsingakerfa þeirra aðila sem falla aðila sem falla undir gildissvið tilskipunarinnar.

Í 1. mgr. er mælt fyrir um skyldu ráðherra til að marka stefnu um öryggi net- og upplýsingakerfa mikilvægra innviða og eftir atvikum annarra aðila. Í stefnunni þarf að greina markmið og ráðstafanir stjórnvalda sem eru nauðsynlegar til að ná og viðhalda háu öryggisstig net- og upplýsingakerfa. Þá er mælt fyrir um stefnan skuli endurskoðuð með reglubundnum hætti. Stefnur sem heyra undir samgöngu- og sveitarstjórnarráðuneytið eru nú til 5 og 15 ára og gert er ráð fyrir að samræmi sé gætt milli málaflokka og er þessi stefna ekki undanskilin. Stefnunni er ætlað að ná til verndar mikilvægra innviða landsins og nauðsynlegra viðbragða vegna vaxandi netógna sem steðja að stjórnvöldum, viðskiptalífi og borgurum. Í stefnunni er að finna framtíðarsýn til ársins 2026 um net- og upplýsingaöryggi og sett eru fram fjögur meginmarkmið til að ná þeirri sýn: *Efld geta.* Almenningur, fyrirtæki og stjórnvöld búi yfir þeirri þekkingu, getu og tækjum sem þarf til að verjast netógnum. *Aukið áfallaþol.* Bætt geta til greiningar, viðbúnaðar og viðbragða eru lykilþættir í bættu áfallaþoli. Áfallaþol upplýsingakerfa samfélagsins og viðbúnaður verði aukinn þannig að hann standist samanburð við áfallaþol upplýsingakerfa á Norðurlöndum og öryggi verði órjúfanlegur þáttur í þróun og viðhaldi net- og upplýsingakerfa. *Bætt löggjöf.* Íslensk löggjöf sé í samræmi við alþjóðlegar kröfur og skuldbindingar á sviði netöryggis og persónuverndar. Jafnframt styðji löggjöfin við nýsköpun og uppbyggingu þjónustu sem byggir á öryggi, t.d. hýsingu. *Traust löggæsla.* Lögregla búi yfir eða hafi aðgang að faglegri þekkingu, hæfni og búnaði til að leysa úr málum er varða net- og upplýsingaöryggi. Til þess að fylgja eftir innleiðingu stefnunnar stofnaði þáverandi innanríkisráðherra Netöryggisráð skipað fulltrúum innanríkisráðuneytis (nú samgöngu- og sveitarstjórnarráðuneytis og dómsmálaráðuneytis), fjármála- og efnahagsráðuneytis, utanríkisráðuneytis, mennta- og menningarmálaráðuneytis, atvinnuvega- og nýsköpunarráðuneytis, Póst- og fjarskiptastofnunar, netöryggissveitar Póst- og fjarskiptastofnunar, Ríkislögreglustjóra og Persónuverndar. Jafnframt var myndaður Samstarfshópur um net- og upplýsingaöryggi, þar sem fulltrúar hagsmunaaðila eiga fulltrúa.

Í 2. mgr. er ráðherra gert skylt að setja reglugerð þar sem mælt er nánar fyrir til hvaða þátta stefnunni er ætlað að taka, hverja skuli haft samráð við og um gildissvið hennar. Með þeirri reglugerð þarf m.a. að mæla fyrir um þau atriði eða þá þætti sem fram koma í 7. gr. tilskipunar 2016/1148/ESB, s.s. a.-g. liði 1. mgr. 7. gr. og 3. mgr. 7. gr., sem ekki þótti nauðsynlegt að færa sérstaklega inn í ákvæði frumvarpsins. Auk þess að mæla fyrir um önnur atriði sem eðlilegt þykir að stefnan taki til.

Um 8. gr.

Í tilskipun 2016/1148/ESB eru tilgreindar þrjár tegundir stjórnvalda sem hafa hlutverki að gegna við að tryggja net- og upplýsingaöryggi þeirra aðila sem falla undir gildissvið tilskipunarinnar. Um er að ræða i) lögbær yfirvöld en þau geta verið eitt eða fleiri stjórnvöld, þau fylgjast með öryggi net og upplýsingakerfa og beitingu tilskipunarinnar á landsvísu. Saman taka þau til þeirra aðila og þeirrar þjónustu sem fellur undir gildissvið tilskipunarinnar. Þá er gert ráð fyrir ii) sameiginlegum tengilið en ef lögbært yfirvald er bara eitt er það sjálfkrafa sameiginlegur tengiliður en annars skal tilnefna eitt stjórnvald til að sinna samræmingar- og samráðshlutverki. Þá er gert ráð fyrir iii) netöryggissveit sem getur verið ein eða fleiri og heimilt er að koma netöryggissveit á fót innan lögbærs yfirvalds. Í dag er starfrækt á vegum Póst- og fjarskiptastofnunar netöryggissveit (hýst hjá lögreglunni á höfuðborgarsvæðinu) en undir hana falla ómissandi upplýsingainnviðir. Ákvæðinu er ætlað að innleið 8. gr. tilskipunar hvað varðar lögbær landsyfirvöld.

Í 1.-7. tölul. 1. mgr. er kveðið á um að tiltekin stjórnvöld sinni eftirlit með öryggi net- og upplýsingakerfamála rekstraraðila nauðsynlegrar þjónustu hvert á sínu sviði. Sviðin eru mismunandi og framangreint fyrirkomulag gerir það að verkum að sú þekking sem skapast hefur innan hvers stjórnvalds fyrir sig með sérhæfðum kerfum helst í stað þess að fela einu stjórnvaldi allt eftirlit sem myndi gera það að verkum að sérfræðiþekking myndi tapast. Þau stjórnvöld sem um ræður eru Orkustofnun vegna orkuveitna, Samgöngustofa vegna flutninga, Fjármálaeftirlitið vegna bankaþjónustu og fjármálamarkaða, Umhverfisstofnun vegna vatnsveitna og Póst- og fjarskiptastofnun vegna stafrænna grunnvirkja. Þá er í 2. mgr. kveðið á um Póst og fjarskiptastofnun sinni eftirlit með öryggi net- og upplýsingakerfamála stafrænna þjónustuveitenda.

Ljóst er að þau stjórnvöld sem falið hefur verið eftirlitshlutverk á grundvelli 1. mgr. eru misvel í stakk búin til að sinna því. Því er í 3. mgr. kveðið á um að þau geti gert með sér þjónustusamning um að eitt þeirra sinni eftirlit með öryggi net- og upplýsingakerfarekstraraðila nauðsynlegrar þjónustu á sviði annars. Þessi möguleiki er fyrir hendi þrátt fyrir að telja verið eðlilegt að þau stjórnvöld sem um ræðir byggi upp þekkingu á net- og upplýsingaöryggi og sinni framangreindu eftirliti þegar þeirri uppbyggingu er lokið. Þá er jafnframt í 3. mgr. kveðið á um að framangreindum stjórnvöldum sé heimilt að gera samninga við sérfræðinga um aðstoð við afmarkað eftirlit. Um er að ræða svokallaða fulltrúa eftirlitsstjórnvalds í skilningi frumvarpsins og reglugerða settra á grundvelli þess. Hlutverki fulltrúa er ekki ætlað að koma í stað hlutverks eftirlitsstjórnvalds heldur einungis styðja við það hlutverk þegar það getur átt við s.s. vegna umfangs eftirlits eða sérhæfð eftirlits.

Í 4. mgr. er kveðið á um að ráðherra skuli með reglugerð mæla nánar fyrir um hlutverk eftirlitsstjórnvalda og gerð þjónustusamninga og samninga við sérfræðinga skv. 3. mgr. Er reglugerðinni m.a. ætlað að taka til þeirra þátta tilskipunar 2016/1148/ESB sem lúta að lögbærum yfirvöldum þ.e. eftirlitsstjórnvaldi, m.a. í 8. gr., sem ekki þykir ástæða til að mæla fyrir með beinum hætti í frumvarpinu.

Um 9. gr.

Eins og fram kemur í athugasemdum við 8. gr. frumvarpsins eru í tilskipun 2016/1148/ESB tilgreindar þrjár tegundir stjórnvalda sem hafa hlutverki að gegna við að tryggja net- og upplýsingaöryggi þeirra aðila sem falla undir gildissvið tilskipunarinnar. Eitt þeirra er svokallaður sameiginlegur tengiliður. Þegar lögbær yfirvöld eru fleiri en eitt, sbr. 8. gr., skal tilnefna eitt stjórnvald til að sinna samræmingar- og samráðshlutverki. Ákvæðinu er ætlað að innleiða 8. gr. tilskipunarinnar hvað varðar sameiginlegan tengilið.

Í 1. mgr. kemur fram að Póst- og fjarskiptastofnun samhæfir eftirlit stjórnvalda skv. 8. gr. með öryggi net- og upplýsingakerfa og starfrækir netöryggissveit skv. 10. gr. sem skal gegna hlutverki viðbragðsteymis vegna atvika er varða netöryggi til verndar mikilvægum innviðum gegn netárásum. Innan Póst- og fjarskiptastofnunar er gríðarleg þekking á net- og upplýsingaöryggi og þykir stofnunin vera það starfandi stjórnvald sem best er í stakk búið til að sinna þessu hlutverki. Hlutverk samhæfingarstjórnvalds á a.m.k. að taka til þriggja meginþátta, þ.e. i) stefnumörkun stjórnvalda á eftirliti með lögum þessum, ii) aðstoð við framkvæmd og samræmingu eftirlitsins og iii) alþjóðasamvinnu.

Hvað varðar stefnumörkun við eftirlit er eðlilegt að gerð verði samræmd stefna þegar kemur að eftirliti eftirlitsstjórnvalda samkvæmt frumvarpinu við eftirlit með öryggi net- og upplýsingakerfa rekstraraðila mikilvægrar þjónustu. Slík stefnumótun er grundvallarforsenda þess að eftirlit ríkisins með aðilum sem falla undir gildissviðs laganna verði, eftir eðli máls og aðstæðum á hverjum markaði fyrir sig, samræmt og leggist með jöfnum hætti á aðila, þ.e. að jafnræðis- og meðalhófsreglum stjórnsýslulaga og stjórnskipunarréttarins gagnvart aðilum sé uppfyllt. Á þetta hvort tveggja við um framkvæmd eftirlits, gerð bindandi fyrirmæla og heimfærslu á viðurlagaákvæði frumvarpsins. Gerð stefnumótunar sem þessarar er umfangsmikil vinna og krefst töluverðar þekkingaruppbyggingar. Greina þarf á milli úttektarstefnu fyrir a) raunlægt öryggi og b) kerfislægt öryggi (*cyber*). Í því felst t.a.m. greining á mismunandi andlagi úttekta og vali á úttektaraðferðum m.t.t. hlutaðeigandi andlags og mögulegra lágmarkskrafna. Slíkt getur verið mismunandi eftir sviðum nauðsynlegrar þjónustu. Þá geta úttektaraðferðir verið með mjög mismunandi hætti og fullnægt mismunandi þörfum og kröfum. Þannig geta úttektir verið allt frá sjálfsmati, skrifborðsúttektum, viðtalsúttektum til ítarlegra vettvangsskoðana. Hér þarf því að móta aðferðarfræði úttekta miðað við tiltekið úttektarandlag. Í þessu samhengi er nauðsynlegt að líta til þeirra vinnu sem fram hefur farið á vegum netöryggisstofnunar Evrópusambandsins (*ENISA*).

Aðstoð við eftirlit og samræming þess er, líkt og áður segir, gríðarlega mikilvæg til að tryggja jafnræði gagnvart þeim aðilum sem undir lögin falla. Þannig er eðlilegt samhæfingarstjórnvaldið sinna ákveðinni eftirfylgni á stefnumörkun við framkvæmd eftirlits. Slíkt væri fyrst og fremst í formi aðstoðar við eftirlitsstjórnvöld við undirbúning, framkvæmd og eftirfylgni úttekta m.t.t. þeirra stefnumörkunar sem fram hefur farið. Það yrði hlutverk samhæfingarstjórnvaldsins að leiðbeina og aðstoða eftir fremsta megni önnur eftirlitsstjórnvöld svo að heildrænt og samræmt eftirlit náist.

Hvað varðar alþjóðlega samvinnu, gerir tilskipunin kröfu um þátttöku stjórnvalda í slíkri vinnu en með henni er settur á laggirnar samstarfshópur til að styðja og greiða fyrir stefnumótandi samstarfsverkefnum og upplýsingasamskiptum milli aðildarríkja. Reynsla stjórnvalda, m.t.t. starfsemi netöryggissveitar, hefur sýnt að alþjóðleg samvinna er gríðarlega mikilvæg þegar kemur að net- og upplýsingaöryggi mikilvægra innviða. Netógnir, -hættur og -atvik fylgja ekki hefðbundnum landamærum og því er nauðsynlegt að samhæfingarstjórnvald á þessu sviði sé vel tengt með þeim hætti að það geti hvort tveggja fengið mikilvægar

upplýsingar frá öðrum ríkjum og aðilum þegar kemur að þessum málaflokki sem og gefið af sér í þessari samvinnu.

Í 2. mgr. er kveðið á um að ráðherra skuli með reglugerð mæla nánar fyrir um hlutverk samhæfingarstjórnvalds. Er reglugerðinni m.a. ætlað að taka til þeirra þátta tilskipunar 2016/1148/ESB sem lúta að sameiginlegum tengilið þ.e. samhæfingarstjórnvaldi, m.a. í 8. gr., sem ekki þykir ástæða til að mæla fyrir með beinum hætti í frumvarpinu.

Um 10. gr.

Með tilskipuninni er gert ráð fyrir veigamiklu hlutverki viðbragðsteyma. Í 9. gr. tilskipunarinnar er aðildarríkjum gert skylt að hafa viðbragðsteymi, eitt eða fleiri, vegna váatvika er varða netöryggi sem jafnframt uppfyllir þær kröfur sem settar eru fram í 1. lið viðauka I við tilskipunina og skal ná til a.m.k. þeirra geira sem um getur í viðauka II og þeirra þjónustu sem um getur í viðauka III., þ.e. til rekstraraðila mikilvægra innviða eins og þeir eru skilgreindir í frumvarpi þessu. Viðbragðsteymið skal bera ábyrgð á meðhöndlun á áhættu og atvikum í samræmi við vel skilgreint ferli. Ber aðildarríkjum að tryggja nægjanlegt fjármagn til slíkra teyma til að það geti annast þau verkefni sem sett eru fram í 2. lið viðauka I við tilskipunina. Þótt ekki sé með beinum hætti taldar upp hvaða heimildir netöryggissveitir skuli hafa í NIS-tilskipuninni eru settar fram kröfur um starfsumhverfi slíks teymis í framangreindum viðauka I við tilskipunina, en þar segir að teymin skuli:

1. tryggja hátt stig tiltækileika þjónustu sinnar og tryggðar skulu leiðir fyrir aðila að hafa samband við teymin, og þau við aðra, hvenær sem er,
2. hafa öruggt athafnasvæði og stuðningsupplýsingakerfi,
3. hafa tryggða rekstrarsamfellu með því að m.a.:
    a. vera búin viðeigandi kerfi til að stjórna og beina beiðnum til að auðvelda yfirfærslu,
    b. hafa yfir að ráða fullnægjandi fjölda starfsmanna til að tryggja að þau séu ávallt tiltæk og
    c. treysta á innviði þar sem samfella er tryggð.
4. hafa möguleika á að taka þátt, þegar þau óska þess, í alþjólegum samstarfsnetum.

Í frumvarpi þessu hefur verið valin sú leið að netöryggissveit Póst- og fjarskiptastofnunar sinni hlutverki viðbragðsteymis fyrir alla mikilvæga innviði samkvæmt frumvarpinu. Verkefni sveitarinnar eru þannig útvíkkuð með lögbundnum hætti til fleiri innviða hér á landi en fjarskiptamarkaðar líkt og nú er. Því verður í frumvarpi þessu að tryggja sveitinni viðeigandi heimildir til að uppfylla kröfur tilskipunarinnar. Líkt og áður segir eru verkefni viðbragðsteyma, líkt og netöryggissveitarinnar, sett fram í 2. lið viðauka I við tilskipunina. En þar segir að verkefni þeirra skuli fela í sér:

1. vöktun atvika á landsstigi,
2. sendingu snemmviðvörunar, viðvörunarmerkja, tilkynninga og miðlun upplýsinga til hlutaðeigandi hagsmunaaðila um áhættur og atvik,
3. að bregðast við atvikum,
4. að veita virka greiningu á áhættum og atvikum og næmni á aðstæðum,
5. að taka þátt í neti viðbragsteyma vegna váatvika er varða netöryggi.

Auk framangreindra verkefna þá skulu viðbragðsteymin koma á fót samstarfstengslum við einkageirann sem og að stuðla að samþykkt og notkun á algengum og stöðluðum starfsvenjum varðandi meðferð atvika og áhættu sem og flokkunarkerfi fyrir atvik, áhættu og upplýsingar.

Lagt er til í frumvarpinu að starfandi CSIRT-teymi, þ.e. netöryggissveit Póst- og fjarskiptastofnunar sinni ein hlutverki viðbragðsteyma vegna váatvika samkvæmt tilskipuninni. En samkvæmt henni geta aðildarríki ákveðið að slík teymi sé starfandi fyrir hvern þátt nauðsynlegrar þjónustu. Að mati ráðuneytisins er slíkt ekki æskilegt hér á landi m.a. vegna smæðar landsins. Með því að starfrækja eitt slíkt teymi er hægt að byggja upp öflugan hóp sérfræðinga sem sinnir framangreindu hlutverki samkvæmt tilskipuninni. Þá er ljóst að mikil þekking hefur byggst upp innan netöryggissveitar Póst- og fjarskiptastofnunar á starfsemi viðbragðsteyma sem þessara sem og að hún hefur sterk alþjóðatengsl í gegnum þá alþjóðasamvinnu sem átt hefur sér stað frá stofnun sveitarinnar.

Í 1. mgr. frumvarpsins er að finna lýsingu á þeim verkefnum sem netöryggissveitin skal sinna á grundvelli þess. Er hér um að ræða þau verkefni sem að tilskipunin setur viðbragðsteymum.

Í 2. mgr. er kveðið á um skyldu ráðherra til að setja reglugerð um starfsemi netöryggissveitarinnar. Í dag er í gildi reglugerð nr. 475/2013 um málefni sveitarinnar þar sem kveðið er á um verkefni hennar, meðferð persónuupplýsinga, gerð þjónustusamninga o.fl. Ljóst er að með samþykkt frumvarps þessa mun starfsemi sveitarinnar aukast til mikilla muna enda munu vera lögbundnir samningar gerðir við rekstraraðila mikilvægra innviða. Það er því mikilvægt að við setningu reglugerðarinnar verði vandað vel til verka og fjallað með ítarlegum hætti um þau verkefni sem sveitin mun hafa með höndum, hvernig uppbygging hennar verður, hvernig vinnslu persónuupplýsinga sé háttað, upplýsingagjöf til almennings, tilmæla til rekstraraðila vegna bráðra netógna o.s.frv.

Um 11. gr.

Með ákvæðinu er kveðið á um samráðshóp netöryggissveitar og sérstökum sviðshópum fyrir hvert svið nauðsynlegrar þjónustu.

Í 1. mgr. kemur fram að tilgangur með skipan samráðshóps netöryggissveitar sé að efla tengsl og samstarf á milli rekstraraðila mikilvægra innviða og sveitarinnar. Hópnum er ekki markað tæmandi hlutverk í frumvarpinu og getur jafnframt nýst sem vettvangur fyrir samráð og upplýsingaskipti í tengslum við greiningu ógna og samræmingu viðbragða við þeim ógnum. Samráðshópurinn mun m.a. hafa það hlutverk að upplýsa og samræma aðgerðir þegar aðkallandi ógnir eru taldar geta haft áhrif á fleiri en eitt svið rekstraraðila nauðsynlegra innviða. Þannig verður hópurinn kallaður saman eftir þörfum af hálfu netöryggissveitarinnar.

Í 2. mgr. er fjallað um skipan sérstakra sviðshópa fyrir hvert svið nauðsynlegrar þjónustu og fyrir stafræna þjónustuveitendur, sbr. 1. mgr. 5. gr. og 1. mgr. 6. gr. frumvarpsins og skal hann vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði net- og upplýsingaöryggis, m.a. til að greina ógnir og samræma viðbrögð. Þar skulu eiga sæti, auk fulltrúa netöryggissveitar, fulltrúar rekstraraðila nauðsynlegrar þjónustu skv. opinni skrá ráðherra skv. 3. mgr. 5. gr., og fulltrúar hvers flokks starfrænna þjónustuveitenda skv. 1. mgr. 6. gr., sbr. þó 2. mgr. 3. gr. laganna. Hlutverk sviðshópa getur verið m.a. að skiptast á upplýsingum við netöryggissveit um stöðu aðila og þeirra áherslur í öryggismálum, ráðleggja aðilum hópsins um öryggismál, miðla upplýsingum um aðsteðjandi ógnir og aðferðum til að verjast þeim, miðla samræmdum upplýsingum um atvik sem átt hafa sér stað hjá aðilum hópsins, innan þeirra marka sem trúnaður við einstaka aðila leyfir, vera vettvangur fyrir upplýsingaskipti í trúnaði á milli aðila og fjalla um áherslur í fræðslu og leggja línur um forgangsröðun verkefna í uppbyggingu öryggismála. Hóparnir geta verið kallaðir saman, einn eða fleiri, eftir því sem netöryggissveit telur nauðsynlegt hverju sinni. Hópur sem þessi er nú þegar starfandi vegna fjarskiptageirans og hefur reynst mikilvægur og nauðsynlegur

vettvangur. Það er því lagt til að lögfest verði ákvæði um tilvist slíks vettvangs fyrir þær tegundir þjónustur sem ákvæði frumvarpsins og tilskipunarinnar ná til. Markmið með sviðshópum er t.a.m. að skiptast á upplýsingum við netöryggissveit um stöðu aðila og þeirra áherslur í öryggismálum, ráðleggja aðilum hópsins um öryggismál, miðla upplýsingum um ógnir og mögulegar aðferðir til að verjast þeim sem og vera vettvangur fyrir upplýsingaskipti í trúnaði. Þá skulu hóparnir jafnframt fjalla um áherslu í fræðslu og leggja línur um forgangsröðun verkefna í uppbyggingu öryggismála. Fundir sviðshópa og umræður um ógnir og ráðstafanir hafa ekki áhrif á heimild netöryggissveitarinnar til að gefa aðilum sem falla undir gildissvið laganna tilmæli um viðbrögð við bráðri aðsteðjandi netógn, sbr. 22. gr. Í 3. mgr. kemur fram að trúnaður skuli ríkja um þær upplýsingar sem ræddar eru á fundum samráðshóps sviðshópanna og þau gögn sem unnin eru eða afhent hópnum skulu teljast til vinnugagna í skilningi 2. og 3. tölul. 2. mgr. 8. gr. upplýsingalaga nr. 140/2012 sem réttur almennings tekur ekki til sbr. 5. tölul. 6. gr. sömu laga. Ákvæðinu er ekki ætlað að fela í sér reglu um sérstaka þagnarskyldu gagnvart upplýsingalögum heldur árétta þau ákvæði sem þar koma fram. Hópnum er eftir sem áður skylt, ef við á, að afhenda gögn á grundvelli 3. mgr. 8. gr. upplýsingalaga og er heimilt að afhenda gögn umfram skyldu enda standi aðrar lagareglur því ekki í vegi, þar á meðal ákvæði laga um þagnarskyldu og persónuvernd sbr. 1. mgr. 11. gr. upplýsingalaga.

Um 12. gr.

Ákvæðið kveður á um þátttöku stjórnvalda í alþjóðasamstarfi enda eitt af markmiðum frumvarpsins sbr. 1. gr. og tilskipunar 2016/1148/ESB að styrkja alþjóðasamstarf.

Í 1. mgr. er kveðið almennt á um að samhæfingarstjórnvald taki þátt í alþjóðasamstarfi er varðar efni laganna og í 2. mgr. að netöryggissveit taki þátt í alþjóðasamstarfi netöryggissveita til að stuðla að trausti og samstarfi ríkja á þessu sviði. Þrátt fyrir að kveðið sé sérstaklega á um framangreint alþjóðasamstarf er alveg ljóst að eftirlitsstjórnvöld, hvert á sínu sviði, taka eðlilega einnig þátt í hinu ýmsa alþjóðasamstarfi innan sín sviðs.

Í 3. mgr. kemur fram að ráðherra skuli með reglugerð mæla nánar fyrir um alþjóðasamstarf m.a. um afhendingu upplýsinga til erlendra stjórnvalda eða eftirlitsaðila sem sinna net- og upplýsingaöryggi. Tilskipunin gerir ráð fyrir skilum á skýrslum sem Ísland þarf að skila til eftirlitsstofnana og þarf í reglugerðinni að tiltaka þau skil m.a. til að koma í veg fyrir að þau misfarist.

Um 13. gr.

Í ákvæðinu er kveðið á um samninga við netöryggissveit og töku þjónustugjalda í tilviki aðila sem ekki falla undir gildissvið frumvarpsins. Í 20. gr. tilskipunar 2016/1148/ESB er kveðið á um valfrjálsa tilkynningu aðila sem hvorki eru rekstraraðilar nauðsynlegrar þjónustu né veitendur stafrænnar þjónustu um atvik sem hafa umtalsverð áhrif á samfellu þeirra þjónustu sem þeir veita. Í 18. gr. frumvarpsins er kveðið á um valfrjálsar tilkynningar.

Í 1. mgr. kemur fram að þeir aðilar sem ekki falla undir gildissvið laganna geti gert samninga við netöryggissveit um ráðgjöf, aðstoð og viðbúnað til að verjast mögulegum netárásum á net- og upplýsingakerfi þeirra sem gerðar eru í þeim tilgangi að gera þau óvirk, valda skemmdum á þeim eða til öflunar ólögmæts fjárhagsleg ávinnings, svo sem með þjófnaði á gögnum eða peningum.

Í 2. mgr. kemur fram að ráðherra er heimilt með reglugerð að mælt fyrir um heimildir netöryggissveitar til töku þjónustugjalda. Er hér um að ræða gjöld sem sveitinni er heimilt að taka af þeim aðilum sem velja að nýta sér þjónustu sveitarinnar án þess að vera það skylt skv.

lögunum og hafa ekki gert samninga skv. 1. mgr. ákvæðisins. Gjaldinu er ætlað að standa straum af þeim kostnaði sem hlýst af veitingu þjónustunnar.

Um 14. gr.

Í 14. gr. frumvarpsins er fjallað um skipulag net- og upplýsingaöryggis. Með ákvæðinu eru lagðar kröfur á rekstraraðila nauðsynlegrar þjónustu og stafræna þjónustuveitendur um ákveðið skipulag fyrir net- og upplýsingaöryggi þeirra. Líkt og fram kemur í formálsorðum NIS-tilskipunarinnar skiptir áreiðanleiki og öryggi net- og upplýsingakerfa og -þjónustna sköpum fyrir efnahagslega og samfélagslega starfsemi innri markaðarins. Tíðni váatvika, umfang þeirra og þau áhrif sem þau hafa er vaxandi og hefur í för með sér hættu fyrir mikilvæga innviða innan Evrópusambandsins. Skaðlegum aðgerðum, sem framkvæmdar eru af ásetningi, gegn umræddum innviðum geta valdið miklum skaða og truflað rekstur þjónustunnar og hamlað þannig atvinnustarfsemi, valdið fjárhagstjóni, grafið undan trausti notenda og valdið miklu tjóni á efnahag viðkomandi ríkis sem og Evrópusambandsins í heild. Í 44. og 46. liða formálsorða tilskipunarinnar er kveðið skýrt á um það að ábyrgðin á að tryggja öryggi net- og upplýsingakerfa hvílir að miklu leyti á rekstraraðilum mikilvægra innviða. Þannig ætti að þróa áhættustýringarmenningu sem felur í sér áhættumat og framkvæmd öryggisráðstafana sem eiga við þá áhættu sem staðið er frammi fyrir með viðeigandi regluföstum kröfum og valfrjálsum starfsvenjum í atvinnugreininni. Áhættustýringarráðstafanir fela í sér ráðstafanir til að auðkenna áhættu á atvikum, og til að koma í veg fyrir, greina og meðhöndla og draga úr áhrifum þeirra.

Í 1. mgr. ákvæðisins er kveðið á um að rekstraraðilar mikilvægra innviða skuli gera viðeigandi og hóflegar tæknilegar og skipulagslegar ráðstafanir til að stýra þeirri áhættu sem steðjar að öryggi net- og upplýsingakerfa sem þeir nota í starfsemi sinni svo stuðla megi að háu öryggisstigi að teknu tilliti til þeirra áhættu sem getur skapast. Ákvæðinu er ætla að innleiða þau markmið og kröfur sem endurspeglast í framangreindum formálasorðum tilskipunarinnar sem og að ákvæðið byggir á 14. og 16. gr. tilskipunarinnar og tekur jafnt til rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda. Í ákvæðinu er sérstaklega tilgreint að aðilarnir skuli skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, framkvæma áhættumat og ákveða öryggisráðstafanir á grundvelli þess. Um er að ræða nálgun um skipulag upplýsingaöryggis sem byggir á þekktum stöðlum hvað það varðar, þ.e. ISO 27001:2005 Upplýsingatækni – Öryggistækni – Stjórnkerfi upplýsingaöryggis – Kröfur, er það í samræmi við markmið tilskipunarinnar en í 66. lið formálasorða hennar er sérstaklega tekið fram að aðildarríki ættu að hvetja til þess að farið sé að ákvæðum tilgreindra staða eða samræmis sé gætt við þá til að tryggja hátt öryggisstig net- og upplýsingakerfa innan sambandsins.

Í málsgreininni er gerð krafa um að skipulagi því sem mælt er fyrir um í framangreindum staðli, og skyldum stöðlum, sé fylgt. Er þannig gert ráð fyrir að stjórnendur þeirra fyrirtækja sem teljast til mikilvægra innviða samkvæmt frumvarpinu móti sér öryggisstefnu þar sem fram komi afstaða þeirra til upplýsingavinnslunnar ásamt helstu áherslum í tengslum við öryggi hennar. Í áhættumati skal skilgreina þær hættur sem steðja að öryggi net- og upplýsingakerfum þeirra, meta líkindi þess að slíkar hættur verði að veruleika og afmarka umfang hugsanlegs tjóns af völdum þeirra. Til þess að draga úr eða mögulega sporna við slíkum hættum skal skjalfesta til hvaða öryggisráðstafana verður gripið. Er hér átt við tæknilegar og skipulagslegar ráðstafanir sem ná skulu jafnt til innra og ytra öryggis í rekstri fyrirtækjanna. Eðlilegt er að slíkar ráðstafanir tryggi nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, að teknu tilliti til nýjustu tækni og kostnaðar við framkvæmd þeirra. Eigendur

net- og upplýsingakerfa, þ.e. rekstraraðilar þjónustu og þjónustuveitendur, eru best til þess fallnir að meta þá áhættu sem fylgir viðkomandi net- og upplýsingakerfum, og þeirrar þjónustu sem þeir veita. Þannig er það lagt í hendur þeirra sjálfra að áhættumeta kerfi sín og velja þær ráðstafanir í samræmi við niðurstöður slíks áhættumats. Aftur á móti er eðlilegt að setja þá kröfu á aðilanna að við val á öryggisráðstöfunum skuli höfð hliðsjón af nýjustu tækni á sviði slíkra ráðstafana. Rétt er að taka fram að öryggisskipulag sem kveðið er á um í málsgreininni skal jafnframt ná til raunlægrar verndar þeirra rýma sem búnaður er hýstur. Er hér um gríðarlega mikilvægan þátt í vernd hvort tveggja kerfanna sem og þjónustunnar að ræða enda ljóst að raunlægt öryggi spilar jafnframt stóran sess í öryggi umræddrar þjónustu. Jafnvel þótt að tíðni netárása fari vaxandi er ljóst að ef að raunlæg vernd umræddra kerfa er ekki tryggð með sem bestum hætti er mikil hætta á að til þjónusturofs geti komið. Til nánari afmörkunar á raunlægu öryggi hvað varðar gildissvið þessa frumvarps er nauðsynlegt að taka það fram að um er að ræða raunlægt öryggi þeirra rýma sem að nauðsynlegur búnaður fyrir net- og upplýsingakerfisins er hýstur. Með raunlægu öryggi er hér t.a.m. átt við aðgengi að rými, innbrotskerfi, brunavarnakerfi, slökkvikerfi, mikilvæga nema til varnar fyrir viðkomandi búnað líkt og vatnsnema, rakanema og hitanema. Auk framangreinds er ljóst að áhætta getur stafað af því ef varaafl til keyrslu búnaðar er ekki tryggt. Hér er ekki um tæmandi talningu að ræða og kemur reglugerð ráðherra ekki til með að kveða á um allar þær raunlægu öryggisráðstafanir sem mögulegar eru. Fer það allt eftir viðkomandi búnaði og rými. Það er jafnframt á ábyrgð viðkomandi rekstraraðila að velja viðeigandi öryggisráðstafanir hvað þetta varðar.

Í 2. mgr. ákvæðisins er lögð sú krafa á rekstraraðila mikilvægra innviða að tryggja með sem bestum hætti samfelldan og órofinn rekstur þeirrar þjónustu sem þeir veita og að lágmarka áhrif af atvikum á öryggi net- og upplýsingakerfa. Hér er í raun sett fram sú krafa að tryggja skuli rekstur þjónustunnar með sem bestum hætti, t.d. með gerð neyðaráætlunar. Í slíkri neyðaráætlun er eðlilegt og nauðsynlegt að fjallað sér sérstaklega um það hvernig rekstraraðili hyggst viðhalda þjónustu eða koma henni aftur á. Hér er um tæknilegar ráðstafanir að ræða sem varða t.a.m. um endurræsingu kerfa, gerð afrita þeirra, endurheimt upplýsinga o.s.frv. Þannig ætti neyðaráætlun í raun að taka á því hvernig koma megi þjónustu á aftur á sem skemmstum tíma, leiði atvik til þjónusturofs, og til að lágmarka áhrif atviks á þjónustuna sem og þær upplýsingar sem að net- og upplýsingakerfi þeirra hafa að geyma. Ljóst er að prófun neyðaráætlunar, eftirlit með henni og endurmat er hér mikilvægur liður í öryggi net- og upplýsingakerfa rekstraraðila. Hér er um mikilvægan þátt að ræða í veitingu þjónustu rekstraraðila mikilvægs innviðar og lýtur í senn að gæðum þjónustunnar og öryggi hvort tveggja neta þeirra sem og þeirra upplýsinga sem þar eru geymdar.

Í 3. mgr. ákvæðisins er kveðið á um skyldu ráðherra til að setja reglugerð þar sem nánar er mælt fyrir um skipulag net- og upplýsingaöryggis og virkni kerfanna hjá rekstraraðilum mikilvægra innviða. Slík reglugerðarsetning er nauðsynleg til að fjalla með ítarlegri hætti um þær kröfur sem felast í 1. og 2. mgr. ákvæðisins, sem nær þá hvort tveggja til öryggisskipulagsins og vernd kerfanna, þ.m.t. raunlægri vernd sem nauðsynleg er til að tryggja umrædd kerfi, fyrir hvort tveggja rekstraraðila nauðsynlegrar þjónustu og stafræna þjónustuveitendur. Þótt vissulega sé gerð skriflegrar öryggisstefnu, framkvæmdar áhættumats og val á öryggisráðstöfunum á höndum rekstraraðila er jafnframt ljóst að slíkar öryggisráðstafanir þurfa að byggja á því sem að best gerist á hverjum tíma. Það er því nauðsynlegt að í reglugerð sé kveðið á um ákveðnar lágmarksráðstafanir sem nauðsynlegar eru. Þótt kveðið sé á um slíkar ráðstafanir verður ábyrgðin þó ekki tekin af viðkomandi rekstraraðila að byggja vernd kerfa sinna með hliðstjón af nýjustu tækni. Hér er því um að

ræða lágmarksráðstafanir sem geta átt við í flestum tilvikum en ávallt verður að vera svigrúm til ákveðins mats á því hvað er eðlilegt m.t.t. þeirra áhættu og eðli þjónustu og kerfis. Í 1. tölul. er kveðið á um skjalfestingu á skipulagi upplýsingaöryggisins, sbr. einnig 1. mgr. ákvæðisins. Hér er því kveðið á um að allt öryggisskipulag rekstraraðila þurfi að vera skriflegt enda er slíkt nauðsynlegt til að nægjanleg og víðtæk yfirsýn náist yfir öryggisskipulagið. Þetta felur jafnframt í sér skriflegt áhættumat og skriflegar öryggisráðstafanir. Í 2. tölul. er tiltekið að fjalla skuli um samræmingu fyrir stafræna þjónustuveitendur. Í formálsorðum tilskipunarinnar, sbr. 44. – 49. liði þeirra kemur m.a. fram að í raun sé áhættustig fyrir rekstraraðila nauðsynlegrar þjónustu en fyrir stafræna þjónustuveitendur enda er þjónusta þeirra of nauðsynleg til að halda uppi mikilvægri samfélagslegri og efnahagslegri þjónustu. Hins vegar styðjast þeir oft á tíðum við stafræna þjónustu. Slík þjónusta ná yfir landamæri þá ættu þeir að falla undir samhæfðari nálgun á vettvangi Evrópusambandsins. Hefur Evrópusambandið nú þegar gefið út reglugerð nr. 2018/151 varðandi framkvæmd NIS-tilskipunarinnar varðandi þjónustuveitendur. Er eðlilegt að reglugerð ráðherra sé litið til þessarar reglugerðar sem og mögulegra annarra gerða Evrópusambandsins hvað þetta varðar. Í 3. tölul. er á ný vísað til staðla á þessu sviði en eins og áður segir byggjast þær kröfur sem settar eru fram í greininni á ISO 27001 og munu kröfur í reglugerð ráðherra jafnframt byggjast á honum. Í 4. tölul. er gerð krafa um að í reglugerð ráðherra verði fjallað um framkvæmd innra eftirlits, svo sem endurskoðun á öryggisskipulagi og neyðaráætlun sem og gerð prófanna. Er slíkt mikilvægt svo að heildstæð og raunveruleg mynd náist af stöðu verndar net- og upplýsingaöryggis, sem og þeirra þjónustu sem á að vernda fyrir árásum eða atvikum. Í 5. tölul. er svo tilgreint að reglugerð ráðherra skuli enn fremur fjalla um skriflega neyðaráætlunar, sbr. einnig umfjöllun um 2. mgr. ákvæðisins. Í 6. tölul. er gert að skyldu að ráðherra fjalli um raunlæga vernd net- og upplýsingakerfanna. Raunlæg vernd þeirra rýma sem hýsa búnað net- og upplýsingakerfis skal vera hluti af öryggisskipulagi rekstraraðila mikilvægs innviðar, sbr. 1. mgr. ákvæðisins. Hvað varðar reglugerð ráðherra þá er nauðsynlegt að hér sé jafnframt kveðið á um ákveðnar lágmarksráðstafanir. Líkt og áður þá geta slíkar ráðstafanir verið mismunandi eftir rýmum og tegundum búnaðar og verður að meta m.t.t. þess. Árétta ber þó að raunlæg vernd og gerð áhættumats þar um sem og val á öryggisráðstöfunum eru ávallt á ábyrgð viðkomandi rekstraraðila. Í 7. tölul. ákvæðisins kemur fram að í reglugerðinni skuli fjallað um tilkynningar vegna atvika. Vísast til umfjöllunar um 16. gr. frumvarpsins hvað það varðar. Í 8. tölul. er tilgreint sérstaklega að ráðherra skuli kveða á um helstu öryggisráðstafanir sem til greina koma við vernd net- og upplýsingakerfa og þeirra þjónustu sem fellur undir gildisvið frumvarpsins. Vísast til framangreindrar umfjöllunar hvað það varðar.

Um 15. gr.

Í ákvæðinu er fjallað um eftirlit stjórnvalda með rekstraraðilum mikilvægra innviða og rétt þeirra til upplýsinga. Líkt og fram hefur komið fara mismunandi stjórnvöld með eftirlit með mismunandi rekstraraðilum. Þessi stjórnvöld eru svo kölluð lögbær yfirvöld samkvæmt tilskipuninni og ber þeim að fylgjast náið með beitingu tilskipunarinnar á landsvísu. Þannig ber þeim að fylgjast með öryggi net- og upplýsingakerfa þeirra aðila sem falla undir gildissvið tilskipunarinnar. Ákvæðið byggir á 15. og 17. gr. tilskipunarinnar en fyrrgreinda ákvæðið nær til framkvæmdar og fullnustu gagnvart rekstraraðilum nauðsynlegrar þjónustu en hið síðarnefnda til framkvæmdar og fullnustu gagnvart stafrænum þjónustuveitendum.

Þótt vissulega séu gerðar sömu kröfur til allra rekstraraðila mikilvægra innviða er varðar skipulag öryggis net- og upplýsingakerfa samkvæmt frumvarpinu er ljóst að ákveðin

sérsjónarmið geta átt við um stafræna þjónustuveitendur enda ber Evrópusambandinu, sbr. 8. mgr. 17. gr. að samþykkja framkvæmdagerðir til að tilgreina nánar um þætti sem tilgreindir eru í 1. mgr. ákvæðisins, þ.e. um ráðstafanir varðandi öryggi kerfa og búnaðar, meðferðar atvika, stjórnunar rekstrarsamfellu o.fl., sbr. stafliði 1. mgr. greinarinnar. Hvað varðar eftirlit með þessum tveimur tegundum rekstraraðila mikilvægra innviða þá er því ekki eins farið. Ákvæði tilskipunarinnar gera ráð fyrir ex-ante eftirliti með rekstraraðilum mikilvægrar þjónustu og ex-post eftirliti með stafrænum þjónustuveitendum. Þannig er kveðið á um það í 15. gr. tilskipunarinnar að eftirlitsyfirvald geti krafist allra nauðsynlegra upplýsinga til að meta öryggi net- og upplýsingakerfi þeirra sem og sannanna fyrir skilvirkri framkvæmd á öryggisreglum. Það er því gert ráð fyrir því að eftirlitsstjórnvöld geti framkvæmt úttektir til þess að ganga úr skugga skjalfestingu skipulags öryggis net- og upplýsingakerfa sem og staðreynt slíkt öryggisskipulag að sínu eigin frumkvæði. Ekki þarf því að hafa orðið atvik eða öryggisbrestur svo eftirlitshlutverk verði virkt. Þegar kemur að stafrænum þjónustuveitendum er staðan frábrugðin þessu en í tilskipuninni skal eftirlitsyfirvald grípa til aðgerða, með eftir á eftirlitsráðstöfunum, þegar sönnunargögn eru lögð fram fyrir því að stafrænn þjónustuveitandi uppfylli ekki kröfurnar sem ákvæði tilskipunarinnar kveða á um. Þannig skal eftirlitsyfirvaldið geta óskað nauðsynlegra upplýsinga til meta öryggi net- og upplýsingakerfa þeirra og krafist þess að þeir bæti úr öllum tilvikum þar sem kröfur eru ekki uppfylltar. Hér þarf því að vera ákveðinn rökstuddur grunur um að viðkomandi stafræni þjónustuveitandi sé ekki að fara að kröfum laganna. Slíkur rökstuddur grunur getur komið frá stafræna þjónustuveitandanum, frá öðru eftirlitsyfirvaldi eða af hálfu notenda þjónustunnar.

Í 1. mgr. ákvæðisins er að finna almennt ákvæði um að eftirlitsstjórnvöld, hvert á sínu sviði, skuli hafa eftirlit með rekstraraðilum mikilvægra innviða og að þeir uppfylli þær kröfur sem á þá eru lagðar samkvæmt ákvæðum frumvarpsins. Hlutaðeigandi stjórnvöld eru skilgreind í 8. gr. frumvarpsins.

Í 2. mgr. ákvæðisins, sem nær til allra rekstraraðila mikilvægra innviða, er kveðið á um upplýsingaöflun eftirlitsstjórnvalda þegar kemur að framkvæmd eftirlits. Ákvæðið tekur með jöfnum hætti til rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda og byggir á a. lið 2. mgr. 15. gr. tilskipunarinnar, hvað varðar rekstraraðila nauðsynlegrar þjónustu, og a. liðar 2. mgr. 17. gr. tilskipunarinnar hvað varðar stafræna þjónustuveitendur. Þótt fyrirbyggjandi (ex-ante)eftirlit með rekstraraðilum nauðsynlegrar þjónustu geti falist í framkvæmdum úttekta eða sönnunum fyrir hlítni við öryggisskipulag, sbr. b. lið 2. mgr. 15. gr. tilskipunarinnar, er nauðsynlegt fyrir eftirlitsyfirvald með stafrænum þjónustuveitendum að geta krafist slíkra upplýsinga við rannsókn á því hvort þeir farið að kröfum frumvarpsins og tilskipunarinnar. Þannig yrði ekki kallað eftir slíkum upplýsingum um sannanir á framkvæmd öryggisreglna nema að það væri rökstuddur grunur um að öryggisatvik hafi átt sér stað, þ.e. í kjölfar atburðar (ex-post). Telst það því til upplýsingaöflunar á grundvelli a. liðar 2. mgr. 17. gr. tilskipunarinnar. Þá er eins kveðið á um það að eftirlitsstjórnvald geti kallað aðila á fund til að óska skýringa eða fá upplýsingar um einstök atriði.

Í 3. mgr. ákvæðisins er svo innleidd heimild eftirlitsstjórnvalda skv. b. lið 2. mgr. 15. gr. tilskipunarinnar þess efnis að þau geti krafist þess að rekstraraðilar nauðsynlegrar þjónustu veiti sannanir fyrir skilvirkri framkvæmd á öryggisreglum, eins og niðurstöður úr öryggisúttekt sem eftirlitsstjórnvaldið eða hæfur úttektarmaður framkvæmir. Hér er um að ræða mikilvægan þátt í ex-ante eftirliti stjórnvalds með framkvæmd rekstraraðilans á öryggisskipulagi sínu. Ákvæðið felur því í sér heimild fyrir eftirlitsstjórnvald til að framkvæma úttekt eða standa fyrir slíkri úttekt á öryggisskipulagi rekstraraðilans. Hér getur ýmist verið um að ræða úttektir er varða afmarkaðan hluta öryggisskipulags eða stærri

heildstæðari úttekt. Er það í höndum eftirlitsstjórnvalds, m.t.t. og á grundvelli þeirrar samræmingar sem átt hefur sér stað á vegum samhæfingarstjórnvalds, að framkvæma úttekt og heimfæra niðurstöður á kröfur frumvarpsins. Úttektir sem þessar geta verið af mismunandi toga, misyfirgripsmiklar og mannaflafrekar. Geta þær verið allt frá skrifborðsúttektum á skjalfestingu skipulags, viðtalsúttektum, úttekt á grundvelli sjálfsmats og til hefðbundinna vettvangsskoðana. Mikilvægt er að við framkvæmd úttekta sem þessara sé jafnframt stuðst við úttektaraðferðir ISO-27001 staðalsins enda ljóst að krafa er um að öryggisskipulag aðila byggi á þeirri hugmyndafræði. Eins er mikilvægt að líta til leiðbeininga frá ENISA hvað þetta varðar. Það er nauðsynlegt að úttektir sem þessar séu unnar í sem bestri samvinnu við viðkomandi rekstraraðila nauðsynlegrar þjónustu með það að markmiði að auka öryggi net- og upplýsingakerfa hans.

Í 4. mgr. ákvæðisins er svo kveðið á um heimild ráðherra til að setja reglugerð hvað þetta varðar. Getur slíkt reynst nauðsynlegt t.a.m. þegar ákveðin samræmingarvinna af hálfu samhæfingarstjórnvalds hefur átt sér stað til þess að binda með lögformlegum hætti hvernig framkvæmd eftirlits eftirlitsstjórnvalda með rekstraraðilum nauðsynlegrar þjónustu skuli háttað. Getur slíkt verið nauðsynlegt til að tryggja með sem bestum hætti jafnræði rekstraraðila þegar kemur að framfylgni á ákvæðum frumvarpsins. Eins er ljóst að nauðsynlegt getur reynst að fjalla með ítarlegri hætti um framkvæmd eftirlits gagnvart stafrænum þjónustuveitendum.

Um 16. gr.

Í 14. gr. tilskipunar 2016/1148/ESB er kveðið á um öryggiskröfur og tilkynningar um atvik hvað varðar rekstraraðila nauðsynlegrar þjónustu og í 16. gr. tilskipunarinnar er kveðið á um öryggiskröfur og tilkynningar um atvik hvað varðar veitendur stafrænnar þjónustu. Ákvæðið mælir fyrir um tilkynningar um atvik og er ætlað að innleiða framangreind ákvæði tilskipunarinnar hvað varðar tilkynningar um atvik.

Í 1. mgr. ákvæðisins er kveðið á skyldu hvort tveggja rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda að tilkynna, án ástæðulausrar tafar, til hlutaðeigandi eftirlitsstjórnvalds og netöryggissveitar, um atvik sem hafa umtalsverð áhrif á samfellu þjónustunnar. Þá er talið upp í ákvæðinu það sem m.a. skal hafa til viðmiðunar þegar metið er hvort atvik hafi veruleg áhrif á þjónustu. Þannig er það ekki ætlunin með ákvæðinu að öll minniháttar atvik sem átt geta sér stað verði tilkynnt heldur fyrst og fremst þau sem að hafa veruleg áhrif á veitingu þjónustunnar. Í ákvæðum tilskipunarinnar eru sett fram eilítið mismunandi viðmið fyrir rekstraraðila nauðsynlegrar þjónustu og stafræna þjónustuveitendur en hinir síðarnefndu skulu, auk þeirra þátta sem taldir eru upp í 1.-3. tölul. málsgreinarinnar, jafnframt líta til umfangs atvik á virkni þjónustunnar og umfang áhrifa atviks á efnahagslega og samfélagslega starfsemi, þ.e. nauðsynlega þjónustu. Ljóst er að hér þarf að fara fram ákveðið mat á aðstæðum og atviki í hverju tilviki fyrir sig áður en að tilkynningarskyldan verður virk en í 3. mgr. ákvæðisins er kveðið á um skyldu ráðherra um að setja reglugerð sem mælir frekar fyrir um tilkynningarskyldu ákvæðisins. Við setningu slíkrar reglugerðar er afar mikilvægt að líta til leiðbeininga frá t.a.m. Evrópusambandinu og ENISA sem hefur t.d. gefið út leiðbeiningar hvað varðar tilkynningarskyld atvik hjá stafrænum þjónustuveitendum. Þá er vert að árétta ákvæði 29. gr. frumvarpsins um að tilkynning um atvik skuli ekki hafa áhrif eða auka mögulega bótaskyldu vegna atviksins. Þrátt fyrir að í ákvæðinu sé settur ákveðinn lágmarksþröskuldur um skyldu aðila til að tilkynna atvik er hvatt til þess að aðilar tilkynni, a.m.k. til netöryggissveitar, um önnur smærri atvik eða netógnir sem þeir kunna að verða varir við í og við net- og upplýsingakerfi sín. Með slíku er verið að stuðla að betri og aukinni upplýsingagjöf til netöryggissveitar sem getur aðstoðað við viðbrögð við slíkum ógnum eða

atvikum. Eins hefur netöryggissveitin ákveðna yfirsýn og upplýsingar sem að viðkomandi rekstraraðili hefur ekki, um ógnir og smærri atvik sem aðrir rekstraraðilar mikilvægra innviða hafa orðið fyrir eða verða varir við. Með þessari auknu upplýsingagjöf til netöryggissveitar fær sveitin mikilvægar upplýsingar með beinum hætti frá rekstraraðila sem fyrst og fremst stuðlar að auknu öryggi net- og upplýsingakerfa allra aðila.

Í 2. mgr. ákvæðisins er að finna skyldu rekstraraðila nauðsynlegrar þjónustu til að tilkynna stafrænum þjónustuveitenda, sem rekstraraðilinn reiðir sig á við veitingu þjónustu sinnar, um öll veruleg áhrif á þjónustuna sem hefur í raun áhrif á stafræna þjónustuveitandann. Hér er verið að tryggja það að stafrænn þjónustuveitandi fái nauðsynlegar upplýsingar um áhrif atvika sem haft gætu áhrif á starfsemi hans. Slíkar upplýsingar eru nauðsynlegar fyrir viðkomandi stafræna þjónustuveitenda til að geta sjálfur brugðist við þeim áhrifum sem að atvik eða truflun í þjónustu rekstraraðilans getur haft á stafrænu þjónustuna.

Í 3. mgr. ákvæðisins er, líkt og áður segir, fjallað um skyldu ráðherra til að setja reglugerð um tilkynningar skv. 1. mgr. ákvæðisins. Í reglugerðinni er nauðsynlegt að tekið sé mið að útgefnum leiðbeiningum Evrópusambandsins og ENISA hvað þetta varðar. Þá er mikilvægt að útlistað sé með ítarlegri hætti mismunandi þættir sem rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur skuli líta til við mat á því hvort áhrif atviks séu veruleg. Eins er nauðsynlegt að í reglugerð sé tiltekið hvaða upplýsingar skulu koma fram í tilkynningu rekstraraðila mikilvægra innviða en samræming hvað þetta varðar er til bóta og getur auðveldað hvort tveggja netöryggissveit og eftirlitsstjórnvaldi að bregðast við. Þá er mikilvægt að fram komi í reglugerðinni ákvæði er varða upplýsingagjöf eftirlitsstjórnvalda til samhæfingarstjórnvalds um atvik á grundvelli greinarinnar. Slík upplýsingagjöf getur verið nauðsynleg svo samhæfingarstjórnvald geti tekið þátt í alþjóðasamstarfi sem og þeim samstarfshópi sem komið er á fót í 11. gr. tilskipunarinnar. Árétta ber að séu upplýsingar veittar í slíku samstarfi skulu þær vera nafnlausar og ekki tengdar tilteknum rekstraraðila mikilvægs innviðar.

Í 4. mgr. ákvæðisins er kveðið á um að Stjórnarráð Íslands skuli, með sama hætti og um getur í 1. og 2. mgr. tilkynna til netöryggissveitar um atvik sem hafa veruleg áhrif á þjónustu þess. Með ákvæðinu er verið að tryggja að netöryggissveit fái upplýsingar um þau atvik sem hefur áhrif á þjónustu stjórnarráðsins með sambærilegum hætti og ef um rekstraraðila mikilvægs innviðar væri að ræða. Er hér fyrst og fremst um að ræða upplýsingagjöf til netöryggissveitar en frumvarpið gerir ekki ráð fyrir eftirlitsstjórnvaldi hvað varðar þjónustu stjórnarráðsins. Líkt og með tilkynningar rekstraraðila mikilvægra innviða þá er sett fram það viðmið að áhrifin þurfi að vera veruleg og er eðlilegt að litið sé til þeirra þátta sem fram koma í 1.-3. tölul. málsgreinarinnar og varða rekstraraðila nauðsynlegrar þjónustu. Þá er áfram hvatt til þess að smærri atvik eða netógnir séu tilkynntar til netöryggissveitarinnar svo sveitin hafi sem mestar upplýsingar um þær ógnir og atvik sem eiga sér stað í og við net- og upplýsingakerfi þeirra aðila sem hún sinnir vöktunarþjónustu fyrir og hefur lögbundnu hlutverki að gegna samkvæmt ákvæðum frumvarpsins.

Um 17. gr.

Í ákvæðinu er fjallað um þá stöðu er atvika gætir yfir landamæri. Meðal þess sem þarf að koma fram í tilkynningu um atvik, sbr. 3. tölul. 1. mgr. 7. gr. frumvarpsins, er stærð þess svæðis sem atvikið hefur áhrif á. Í 5. mgr. 14. gr. tilskipunar 2016/1148/ESB kemur fram að á grundvelli upplýsinga sem eru í tilkynningu rekstraraðila nauðsynlegrar þjónustu skal lögbært yfirvald eða viðbragðsteymi vegna atvika er varða netöryggi, hér eftirlitsstjórnvald eða netöryggissveit, upplýsa önnur ríki, þar sem áhrifa gætir, um hvort atvikið hafi veruleg

áhrif á samfellu nauðsynlegrar þjónustu í því ríki. Þá kemur einnig fram að þar sem aðstæður leyfa, skal lögbæra yfirvaldið eða viðbragðsteymið vegna atvika er varða netöryggi veita þeim rekstraraðila nauðsynlegrar þjónustu sem sendir tilkynninguna viðeigandi upplýsingar varðandi eftirfylgni við tilkynningu hans, eins og upplýsingar sem gætu stutt við skilvirka meðhöndlun atviks. Einnig skal sameiginlegi tengiliðurinn, að beiðni lögbærs yfirvalds eða viðbragðsteymis vegna atvika er varða netöryggi, áframsenda tilkynningar til sameiginlegra tengiliða í öðrum aðildarríkjum þar sem áhrifa gætir. Í 6. mgr. 16. gr. er ákvæði er varðar tilkynningar vegna atvika sem gætir yfir landamæri í tilviki stafrænna þjónustuveitenda en þar kemur fram að eftir því sem við á, sérstaklega þegar atvik snertir tvö eða fleiri ríki, skulu lögbært yfirvald og viðbragðsteymi vegna atvika er varða netöryggi, hér eftirlitsstjórnvald og netöryggissveit, tilkynna þeim ríkjum þar sem áhrifa gætir um atvikið.

Ákvæðinu er ætlað að innleiða framangreindar reglur tilskipunarinnar og er farin sú leið, til einföldunar, að láta sömu reglur gilda í tilviki rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda. Vísast til framangreindrar umfjöllunar hvað varðar skýringar við 1.-3. mgr. ákvæðisins. Hvað 1. mgr. varðar sérstaklega skal tekið fram að þegar atvika gætir yfir landamæri á ákvæðið eftir atvikum einnig við um tilkynningar til alþjóðastofnana.

Í 4. mgr. er kveðið á um heimildir ráðherra til að mæla nánar fyrir í reglugerð um tilkynningar um atvik sem gætir yfir landamæri m.a. um tilkynningar til alþjóðastofnana. Við mat á nauðsyn á setningu slíkra reglugerðar þykir rétt að horfa t.a.m. til ákvæða 7. mgr. 14. gr. og 8.-10. mgr. 16. gr. tilskipunarinnar.

Um 18. gr.

Í ákvæðinu er kveðið á um valfrjálsar tilkynningar þ.e. tilkynningar umfram skyldu. Ákvæðinu er ætlað að innleiða 20. gr. tilskipunar 2016/1148/ESB þar sem kveðið er á um valfrjálsa tilkynningu aðila sem hvorki eru rekstraraðilar nauðsynlegrar þjónustu né veitendur stafrænnar þjónustu. Ljóst er skv. 2. mgr. 20. gr. tilskipunarinnar að heimilt að veita skyldubundnum tilkynningum forgang umfram valfrjálsar tilkynningar. Þá kemur þar jafnframt fram að vinnsla valfrjálsra tilkynninga skuli einungis fara fram þegar slík vinnsla er ekki umfram það sem eðlilegt má teljast eða of íþyngjandi fyrir hlutaðeigandi ríki.

Í 1. mgr. kemur fram að aðilum sem falla utan gildissviðs laganna sé heimilt að tilkynna netöryggissveit um atvik sem hafa umtalsverð áhrif á samfellu þeirrar þjónustu sem þeir veita. Frumkvæði tilkynningar kemur frá þessum aðilum.

Í 2. mgr. kemur fram að um meðferð þeirra tilkynninga sem mælt er fyrir um í 1. mgr. skal fara eftir lögunum og reglugerðum settum á grundvelli þeirra en netöryggissveit er heimilt að veita skyldubundnum tilkynningum forgang umfram valfrjálsar tilkynningar.

Ráðherra er skv. 3. mgr. heimilt að mæla nánar fyrir um meðferð valfrjálsra tilkynninga. Þessi málsgrein á nokkra samleið með 2. mgr. 14. gr. þar sem ráðherra er heimilt að setja reglugerð um töku þjónustugjalda vegna valfrjálsra tilkynninga.

Um 19. gr.

Í greininni eru mælt fyrir um þær heimildir sem að netöryggissveit Póst- og fjarskiptastofnun þarf til að starfrækja þau verkefni sem henni eru sett samkvæmt tilskipuninni m.t.t. rekstraraðila mikilvægra innviða. Þær heimildir felast fyrst og fremst í aðgengi sveitarinnar að upplýsingum um netumferð við net- og upplýsingakerfi umræddra rekstraraðila og heimild til greiningar á óeðlilegri umferð sem og framsetningu tilmæla um viðbrögð rekstraraðila telji netöryggissveitin að hættu eða ógn um netárás sé að ræða.

Í 1. mgr. greinarinnar er kveðið á um skyldu rekstraraðila nauðsynlegra innviða og netöryggissveitarinnar um gerð samnings um vöktunarþjónustu. Slík vöktunarþjónusta getur verið mismunandi og t.a.m. falist í upplýsingagjöf t.d. með afhendingu logskráa, og í uppsetningu vöktunarbúnaðar sem þá yrði settur upp og rekinn í samvinnu milli aðila. En stefnt að því að almennt verði settur upp slíkur vöktunarbúnaður við net- og upplýsingakerfi mikilvægra innviða. Er hér um gríðarlega mikilvæga heimild að ræða sem gerir netöryggissveitinni, á grundvelli samnings við viðkomandi rekstraraðila mikilvægs innviðar, kleift að greina ummerki um árásir, spillikóða og fá upplýsingar sem geta falið í sér vísbendingar um aðstæður sem gætu skapað hættu fyrir viðkomandi aðila. Slíkur vöktunarbúnaður nær eingöngu til net- og upplýsingakerfis hlutaðeigandi rekstraraðila en ekki með neinum hætti til skimunar á almennri netumferð á Internetinu. Búnaður sem þessi getur m.a. verið með þeim hætti að sérstakir umferðarskynjarar væru settir upp fyrir utan eldvegg viðkomandi aðila þótt að jafnframt væri heimilt að afla gagna frá öðrum búnaði rekstraraðilans, svo sem aðgerðaskrám þjóna og eldveggja sem og öðrum endapunktavörnum á einmenningstölvum rekstraraðilans sé kveðið á um slíkt í vöktunarsamningi aðila. Ákvæðinu er ætla að tryggja netöryggissveitinni aðgang að upplýsingum svo hún geti sinnt því hlutverki sem krafist er samkvæmt 2. lið viðauka I við tilskipunina. En með búnaði sem þessum er netöryggissveitinni gert kleift að vakta mögulega atvik, greina mögulegar ógnir og áhættur sem og atvik ásamt því að geta gert og viðhaldið ógnarmati fyrir þjónustuhópinn og landið. Með þessum hætti er netöryggissveitinni jafnframt veitt nauðsynlegt verkfæri til að geta gert hlutaðeigandi rekstraraðila viðvart um mögulega ógn eða yfirvofandi árás, virkjað flokkunarkerfi sitt og samhæft varnarviðbrögð eða dregið úr skaðsemi árásar með samræmdum hætti. Rétt er að geta þess að netöryggissveitin hefur ekki yfir að ráða búnaði sem þessum í dag. Hefur það leitt til þess að sveitin hefur þurft að treysta á erlendar upplýsingaveitur, systursveitir sínar og almennar tilkynningar til að greina mat á ógnum, áhættum og mögulegum eða yfirstandandi árásum.

Til eru mismunandi gerðir vöktunarbúnaði og tekur slíkur búnaður jafnframt breytingum í samræmi við tækniþróun á þessu sviði. Ekki er gerð krafa í ákvæðinu um uppsetningu og rekstur tiltekinnar tegundar eða fyrirkomulags vöktunarbúnaðar og er slíkt gert svo að aðilar geti valið þann búnað sem hentar best fyrir hvern aðila og á hverjum tíma með tilliti til þarfa og tækniþróunar. Hins vegar verður að telja líklegast að a.m.k. í upphafi verði settur upp vöktunarbúnaður fyrir utan eldveggi net- og upplýsingakerfis viðkomandi rekstraraðila sem, undir stjórn netöryggissveitarinnar, vaktar þá umferð inn og út úr netkerfið rekstraraðilans. Þótt búnaðurinn vakti umferð þá er það einungis ef óeðlileg umferð eða sending á sér stað sem að búnaðurinn lætur vita um mögulega hættu eða ógn. Þannig fer greining fram með algjörlega sjálfvirkum hætti í umræddum búnaði.

Ef upp kemur óeðlileg umferð eða grunur um ógn við slíka sjálfvirka greiningu yrði frekari skoðun á viðkomandi umferð eða sendingu framkvæmd. Einungis þeim hluta gagnanna yrði þá beint inn á miðlæga þjóna netöryggissveitarinnar til frekari greiningar. Þannig er í vöktunarsamningi almennt miðað við að vinnslan fari fram á búnaði sem settur er upp hjá viðkomandi rekstraraðila og vistun gagna hjá netöryggissveitinni takmarkist þannig við stýrigögn fjarskiptapakka og vísa (*e. IoC – Indicators of Compromise*) sem geta gefið til kynna ógn og hættu. Til vísa teljast t.a.m. IP-tölur og port sendanda og viðtakanda, tölvupóstföng utanaðkomandi aðila og URL sem kerfi rekstraraðilans tengist.

Sú greining sem netöryggissveitin framkvæmdir getur verið hvort tveggja sjálfvirk og handvirk. Mun netöryggissveitin þá geta greint vísa sem fram koma í umferð til og frá rekstraraðilum þar sem eiginleikar stýrigagna fjarskiptapakka yrðu skoðaðir, svo sem

upprunaland, uppruni og áfangastaður. Greining fullra fjarskiptapakka myndi svo fara fram eftir atvikum og á grundvelli mats netöryggissveitarinnar á mögulegri ógn. Í slíkri greiningu gæti falist skoðun á viðhengi og slóðum í tölvupóstum sem og öðru innihaldi netpakka og tölvupóstsendinga sem gæti gefið til kynna spillikóða eða aðgerðir sem gætu ógnað mikilvægum innviðum í skilningi þessara laga. Mikilvægt er að árétta að þegar slík greining á sér stað þá hefur hvort tveggja sjálfvirk greining í vöktunarbúnaði við eldveggi netkerfis rekstraraðilans greint óeðlilega umferð eða sendingar sem og að netöryggissveitin hefur greint stýrigögn umferðarinnar eða sendinganna sem einnig leiða til þess að frekari greining á t.d. innihaldi sendinga fer fram. Það er því ljóst að búið er að þrengja til muna þá umferð sem sætir skoðun og einskorða hana við sendingar sem talin hefur verið þörf á að skoða frekar eftir tvöfalda greiningu. Eins ber þess að geta í þessu samhengi að margur algengur varnarbúnaður, s.s. hefðbundin vírusvarnaforrit, framkvæma sambærilegar, eða jafnvel inngripsmeiri, greiningar á t.a.m. tölvupóstsendingu, þ.e. þar sem að innihald er skimað. Ekki er því í raun um meira íþyngjandi nálgun að ræða af hálfu netöryggissveitarinnar. Aftur á móti hefur sveitin yfir að ráða upplýsingum og gögnum frá erlendum gagnastraumum og samstarfsaðilum sem að sveitin getur borið hina óeðlilegu umferð saman við og þannig mögulega greint ógnir og hættur m.t.t. þess.

Í 2. mgr. greinarinnar er kveðið á um þau atriði sem skulu að lágmarki koma fram í vöktunarsamningi milli netöryggissveitarinnar og rekstraraðila mikilvægs innviðar. Hér er um lágmarksupptalningu að ræða og kemur ekki í veg fyrir að aðilar samnings kveði á um önnur atriði sem þeir telja eðlilegt að kveðið sé á um á grundvelli eðli þeirrar þjónustu sem viðkomandi rekstraraðili veitir.

Í 3. mgr. greinarinnar er kveðið á um skyldu ráðherra til að setja reglugerð um efni og gerð vöktunarsamninga. Í slíkri reglugerð er mikilvægt að fjallað sé með ítarlegum hætti um þau efnisatriði sem að lágmarki skal kveða á um í vöktunarsamningi milli aðila skv. 2. mgr. Hér þarf að tilgreina tegund þeirra gagna og upplýsinga sem eru vaktaðar, hvar vinnsla þeirra fram, tilgang hennar og ábyrgðaraðila sem og meðferð gagnanna að öðru leiti. Hvað þetta varðar er nauðsynlegt að taka tillit til umfjöllunar um 1. mgr. greinarinnar um vöktunarbúnað og greiningu gagna. Hvað varðar þær upplýsingar og þau gögn sem safnað er samkvæmt vöktunarsamningi er rétt að kveðið sé á um að einungis er heimilt að nýta þau til að meta og bregðast við hættu sem stafar að viðkomandi rekstraraðila, viðkomandi sviði eða rekstraraðilum mikilvægra innviða í heild. Hér er um mikilvæga afmörkun að ræða enda nær heimild ákvæðisins einungis til uppsetningar á vöktunarbúnaði fyrir rekstraraðila mikilvægra innviða en ekki til almennrar skimunar. Þá er rétt að í reglugerð komi fram að ekki sé heimilt að dreifa öðrum upplýsingum en vísum eins og metið er að sé nauðsynlegt til að greina hættu hjá öðrum rekstraraðilum mikilvægra innviða eða gera þeim kleift að bregðast við aðsteðjandi hættu. Til vísa teljast m.a. IP-tölur, tölvupóstföng sendanda grunaðs spillipósts og nöfn skráa sem geta innihaldið spillikóða. Þannig er hvorki veitt heimild til að miðla upplýsingum líkt og tölvupóstföngum starfsmanna rekstraraðila, nöfnum þeirra og vélanöfnum né fullum pakkagögnum sem geta innihaldið viðkvæmar upplýsingar utan netöryggissveitarinnar. Þá er mikilvægt að í reglugerð ráðherra séu ákvæði er lúta að eyðingu upplýsinga en eðlilegt er að t.a.m. stýrigögn fjarskiptapakka séu ekki vistuð lengur en í 12 mánuði en upplýsingar og gögn fullra fjarskiptapakka skuli ekki geyma lengur en þörf er á og að hámarki í sex mánuði. Eins er það er mikilvægt að í reglugerð sé kveðið á um heimildir netöryggissveitarinnar að vinna tölfræðilegar greiningar til opinberrar birtingar í greiningarskýrslum sem og til nánari greininga á ógnarmynd hverju sinni í samvinnu við innlenda aðila, s.s. ríkislögreglustjóra sem samkvæmt lögum ber ábyrgð á öryggi ríkisins. Slíkar greiningar eru gríðarlega mikilvægar

við mótun stefnu um aðgerðir og úrbætur til að stuðla að bættu öryggi mikilvægra innviða. Þá munu slíkar upplýsingar einnig nýtast stjórnvöldum við mótum netöryggisstefnu og vera mikilvægar til að varpa ljósi á þróun netógna, tíðni þeirra, eiginleika og alvarleika. Allar opinberar birtingar hvað þetta varðar verða að vera ópersónugreinanlegar tölfræðiupplýsingar.

Um 20. gr.

Í 1. mgr. greinarinnar er kveðið á um heimildir netöryggissveitarinnar til aðgangs að upplýsingum og gögnum rekstraraðila mikilvægra innviða. Ákvæðið er liður í því að tryggja að sveitin hafi þau úrræði sem þarf til að tryggja að skilvirk og samrýmanleg geta sé til staðar innan hennar til að fást við öryggisatvik, netógnir og -árásir fyrir net- og upplýsingakerfi allra mikilvægra innviða. Umfang, tíðni og áhrif netárása fara vaxandi og hafa í för með sér mikla hættu gagnvart starfsemi net- og upplýsingakerfa. Slíkar árásir geta hamlað atvinnustarfsemi hlutaðeigandi rekstraraðila, valdið verulegu fjárhagslegu tjóni og grafið undan trausti notenda á þeirri þjónustu sem þeir veita. En áreiðanleiki net- og upplýsingakerfanna skiptir orðið lykilmáli fyrir efnahagslega og samfélaglega starfsemi hvort tveggja innanlands sem og milli landa.

Með ákvæðinu er netöryggissveitinni því veitt nauðsynleg heimild til að kalla eftir þeim upplýsingum, skriflegum skýringum og gögnum frá rekstraraðilum mikilvægra innviða sem hún telur nauðsynleg til að sinna því lögbundnu hlutverki sínu að vernda með sem bestum hætti þessa mikilvægu innviði þjóðarinnar fyrir netógnum og -árásum. Getur hér verið um að ræða ógn eða árás á viðkomandi rekstraraðila mikilvægra innviða, viðkomandi geira innviða eða mikilvæga innviði landsins í heild. Með upplýsingum er hér m.a. átt við upplýsingar og gögn um árásir og atburði sem hafa átt sér stað í kerfi viðkomandi rekstraraðila, þ.m.t. umferðarskrár (logskrár), spillikóðaskrár og önnur ummerki árásar eða atviks sem nota má til að greina það, bæði til að verja viðkomandi aðila en einnig þjónustuhópinn í heild. Skriflegar skýringar sem netöryggissveitin getur kallað eftir geta falist í greinargerðum um atvik, lýsingu mótvægisaðgerða sem þegar hefur verið gripið til og þeirra endurbóta sem fyrirhugaðar eru til að fyrirbyggja sambærilega atburði. Gögn í skilningi ákvæðisins geta, auk umferðar og aðgerðaskráa netbúnaðar og netþjóna, t.a.m. verið tölvupóstar, s.s. vefveiðapóstar, spillikóði í viðhengjum og önnur ummerki um spillikóða. Auk þess að geta kallað eftir framangreindum gögnum getur verið nauðsynlegt að geta kallað aðila á fund til þess að fá nánari skýringar og upplýsingar um einstaka atriði er varða vernd net- og upplýsingakerfa þeirra, auk nánari skýringa á atburðum og mótvægisaðgerðum sem framkvæmdar hafa verið eða eru fyrirhugaðar.

Í 2. mgr. greinarinnar er kveðið á um að rekstraraðilar nauðsynlegra innviða skuli bregðast við upplýsingabeiðni netöryggissveitarinnar tafarlaust og eigi síðar en 12 klukkustundum eftir að beiðni berst. Hér er lagður til nokkuð þröngur tímarammi fyrir aðila að bregðast við beiðnum sem berast frá netöryggissveitinni. Er slíkt nauðsynlegt svo að sveitin geti rannsakað og metið á sem allra skemmstum tíma þá ógn sem hún telur að geti verið yfirvofandi. Hér er nauðsynlegt að hafa í huga að beiðni netöryggissveitarinnar um afhendingu upplýsinga og gagna á grundvelli 1. mgr., þ.e. frá rekstraraðilum nauðsynlegra innviða, þarf að vera rökstudd. Þannig þarf að liggja fyrir ákveðinn rökstuddur grunur um hættur eða að ógn eða árás geti verið yfirvofandi eða yfirstandandi. Skammur viðbragðstími er algjör forsenda þess að netöryggissveitin geti sjálf brugðist við með nægjanlega skjótum hætti við ógnum og mögulegum árásum, m.a. með því að gera ráðstafanir til að vara aðra rekstraraðila mikilvægra innviða við aðsteðjandi hættu eða gera aðrar mótvægisráðstafanir. Tímarammi almennt í þessum málaflokki er skammur þar sem að ógnir og árásir geta gerst á gríðarlega skömmum

tíma. Innbrotsaðili þarf einungis nokkrar mínútur frá því hann hefur brotið sér leið inn í net- og/eða upplýsingakerfi rekstraraðila þar til að hann getur orsakað gríðarlegt tjón fyrir viðkomandi rekstraraðila mikilvægs innviðar og jafnvel fjölmargra einstaklinga líka.

Um 21. gr.

Í greininni er kveðið á um skyldu rekstraraðila mikilvægra innviða að bregðast við tilmælum netöryggissveitarinnar vegna ógna sem stafa að innviðum þeirra, hvort sem er einstökum innviðum eða í heild. Hér um gríðarlega mikilvægt úrræði fyrir netöryggissveitina að ræða til að tryggt sé með sem bestum hætti samræmd viðbrögð aðila til að koma í veg fyrir eða draga úr netárásum sem haft geta áhrif á mikilvæga innviði þjóðarinnar og að slíkt sé gert án allra tafa. Ef ekki er fyrir að fara ákvæði sem þessu er ljóst að öll þau úrræði sem netöryggissveitinni eru fær og öll sú greiningarvinna sem fram fer af hálfu sveitarinnar getur ónýst ef ekki er brugðist við greindum ógnum tafarlaust. Net- og upplýsingakerfi rekstraraðila mikilvægra innviða eru ávallt á þeirra forræði og undir þeirra stjórn og er það alfarið undir þeim komið að gera viðeigandi ráðstafanir í sínum kerfum til að bregðast við bráðum og aðsteðjandi ógnum. Það er því nauðsynlegt að netöryggissveit geti farið fram á tafarlaus viðbrögð þeirra þegar hún hefur greint bráðar og aðsteðjandi ógnir sem raskað geta starfsemi mikilvægra innviða, skaðað starfsemi rekstraraðilanna sem og mögulega hagsmunum viðskiptavini þeirra, t.a.m. með birtingu persónulegra upplýsinga um þá.

Um 22. gr.

Í ákvæðinu er kveðið á um upplýsingar sem veita skal almenningi. Í 6 mgr. 14. gr. tilskipunar 2016/1148/ESB kemur fram í tilviki rekstraraðila nauðsynlegrar þjónustu geta lögbær yfirvöld eða viðbragðsteymi vegna atvika er varða netöryggi, þ.e. eftirlitsstjórnvöld eða netöryggissveit, upplýst almenning um einstök atvik þar sem almenningsvitundar er þörf til að koma í veg fyrir atvik eða takast á við yfirstandandi atvik. Þá er áþekkt ákvæði í 7. mgr. 16. gr. tilskipunarinnar sem tekur til stafrænna þjónustuveitenda en þar er einnig tekið fram að heimilt sé að upplýsa almenning þegar upplýsingagjöf um atvikið er af öðrum ástæðum en þeim sem fjallað hefur verið um en er nauðsynleg í þágu almannahagsmuna. Að auki er heimilt að gera stafrænum þjónustuveitendum að sinna þessari upplýsingagjöf. Er ákvæðinu ætlað að innleiða framangreindar reglur tilskipunarinnar.

Ákvæði 1. mgr. inniheldur efnislega áþekkar reglur þeim sem fram koma í 6. mgr. 14. gr. og 7. mgr. 16. gr. tilskipunar 2016/1148/ESB en að auki er netöryggissveit heimilt að tilkynna almenningi um veikleika og almennar hættur ef það er nauðsynlegt í þágu almannahagsmuna. Ljóst er að oft þarf að bregðast við netógnum og atvikum með mjög skjótum hætti. Það er því lagt til í frumvarpinu að það verði á höndum netöryggissveitar að sjá um slíkar tilkynningar. Er sú leið farin, í stað eftirlitsstjórnvalda, sökum þess að netöryggissveitin hefur mun ítarlegri upplýsingar þegar kemur að því að bregðast við atvikum og takmarka áhrif þess. Það er því eðlilegt að netöryggissveit hafi ákveðið forræði þegar kemur að þessum tilkynningum. Hins vegar er kveðið á um það að samráð skuli haft við viðkomandi rekstraraðila mikilvægra innviða þegar upplýsingar eru veittar almenningi. Slíkt samráð er mikilvægt fyrir hagsmuni viðkomandi rekstraraðila. Séu aðstæður aftur á móti mjög brýnar og ógnir mjög aðsteðjandi eða atvik yfirstandandi verður netöryggissveit að geta tekið af skarið um að upplýsa almenning án formlegs samráðs. Í slíkum tilvikum er nauðsynlegt að netöryggissveit gæti í hvívetna að hagsmunum viðkomandi rekstraraðila og takmarki upplýsingar einungis við það sem allra nauðsynlegt er til að bregðast við ógn eða takmarka tjón. Samráð skal svo haft eins fljótt og auðið er við hlutaðeigandi aðila og áður en frekari upplýsingar eru veittar almenningi. Hér er

einungis um neyðarúrræði netöryggissveitar að ræða sem takmarka skal beitingu á. Þá ber netöryggissveitinni að upplýsa hlutaðeigandi eftirlitsstjórnvald um tilkynningar til almennings hvað þetta varðar og veita stjórnvaldinu ítarlegri upplýsingar eftir því sem við á og að beiðni eftirlitsstjórnvalds.

Í 2. mgr. er kveðið á um að ráðherra sé heimilt að mæla nánar fyrir um tilkynningar um atvik, veikleika og almennar hættur skv. 1. mgr., framkvæmd samráðs við rekstraraðila mikilvægra innviða og samskipti við eftirlitsstjórnvöld. Eins er heimilt í reglugerð að kveða á um skyldu stafrænna þjónustuveitenda um að sinna upplýsingagjöf skv. 1. mgr. sjálfir, sbr. 7. mgr. 16. gr. tilskipunarinnar. Sé ekki kveðið á um slíkt í reglugerð er það á höndum netöryggissveitar að sinna umræddri upplýsingaskyldu.

Um 23. gr.

Í ákvæðinu er kveðið á um sérstaka þagnarskyldu umfram þá sem greinir í 18. gr. laga um réttindi og skyldur starfsmanna ríkisins nr. 70/1996 en í því ákvæði kemur fram að starfsmönnum sé skylt „að gæta þagmælsku um atriði er hann fær vitneskju um í starfi sínu og leynt skulu fara samkvæmt lögum, fyrirmælum yfirmanna eða eðli málsins. Þagnarskyldan helst þótt látið sé af starfi.“ Er hér um að ræða ákvæði sem tekur til starfsmanna eftirlitsstjórnvalda, fulltrúa eftirlitsstjórnvalda sem eru skv. orðskýringu 2. gr. sérfræðingur í net- og upplýsingaöryggi sem eftirlitsstjórnvald gerir samning við um afmarkaða þætti eftirlits með net- og upplýsingaöryggi mikilvægra innviða, starfsmanna samhæfingarstjórnvalds og netöryggissveitar. Um er að ræða rýmri hóp en fellur undir gildissvið laga nr. 70/1996 og er ákvæðið þ.a.l. nauðsynlegt. Ákvæðið tekur til þeirra upplýsinga sem aflað hefur verið, þ.e. afhentar hafa verið framangreindum aðilum eða þeir óskað eftir, frá mikilvægum innviðum í tengslum við eftirlit með öryggi net- og upplýsingakerfa eða vegna meðferðar atvika. Tiltekið er sérstaklega að þagnarskylda helst þótt látið sé af starfi. Ákvæðinu er ætlað að vera sérstakt þagnarskylduákvæði gagnvart ákvæðum upplýsingalaga nr. 140/2012.

Um 24. gr.

Ákvæðið felur í sér vissar undanþágur frá ákvæði 22. gr. frumvarpsins um sérstaka þagnarskyldu. Meginreglan um sérstaka þagnarskyldu kemur því fram í 22. gr. en á henni eru vissar mikilvægar undantekningar sem fjallað er um í ákvæðinu. Ákvæðið er nauðsynlegt m.a. til að tryggja virk samskipti stjórnvalda innanlands sem og alþjóðasamstarf. Stjórnvöld þurfa að geta miðlað upplýsingum í vissum tilvikum auk þess sem eitt af megin markmiðum 1. gr. tilskipunar 2016/1148/ESB, sbr. 1. gr. frumvarpsins, er að stuðla að miðlun upplýsinga milli ríkja svo unnt sé unnt sé að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan ríkja Evrópusambandsins í því skyni að bæta starfsemi innri markaðarins.

Í 1. mgr. kemur fram að ákvæði frumvarpsins um þagnarskyldu standa því ekki í vegi að eftirlitsstjórnvöld hvert á sínu sviði, samhæfingarstjórnvald og netöryggissveit veiti upplýsingar eða taki við upplýsingum frá lögreglu eða persónuverndaryfirvöldum ef þær upplýsingar varða net- og upplýsingaöryggi, almannavarnir eða persónuvernd. Ljóst er að þær upplýsingar sem um ræðir eru tilgreindar sérstaklega þ.e. þær þurfa að varða net- og upplýsingaröryggi, almannavarnir eða persónuvernd. Framangreind stjórnvöld vinna öll með net- og upplýsingaöryggi upp að vissu marki og er reglan nauðsynleg svo þau geti haft með sér samstarf svo unnt sé að tryggja öryggi í net- og upplýsingakerfum sem falla undir gildissvið frumvarpsins, vernd almennings og persónuvernd.

Í 2. mgr. kemur fram að ákvæði frumvarpsins um þagnarskyldu standa því ekki í vegi að eftirlitsstjórnvöld hvert á sínu sviði, samhæfingarstjórnvald og netöryggissveit veiti

upplýsingar eða taki við upplýsingum frá erlendum stjórnvöldum, eftirlitsaðilum eða öðrum aðilum eða sérfræðingum sem sinna net- og upplýsingaöryggi þegar slíkt er nauðsynlegt vegna skipulagðrar alþjóðasamvinnu sem hefur það markmið að stuðla að eða framkvæma aðgerðir til að tryggja öryggi net- og upplýsingakerfa. Eins og málsgreinin ber með sér taka upplýsingaskiptin ekki einungis til erlendra stjórnvalda eða eftirlitsaðila heldur einnig annarra aðila eða sérfræðinga sem sinna net- og upplýsingaöryggi. Er hér t.d. um að ræða gagnastrauma sem netöryggissveit hefur aðgang að og kemur í stað rauntímaskimunar við almennt eftirlit hennar. Eins og starfsemi netöryggissveitar er í dag þá treystir hún í mjög miklum mæli á upplýsingar sem koma erlendis frá til að sinna lögbundnu eftirlitshlutverki sínu. Tryggja þarf trúnað þessara upplýsinga. Upplýsingaskipti sem þessi eru gríðarlega stór þáttur í alþjóðlegu samstarfi um net- og upplýsingaöryggi. Netógnir, öryggisatvik og aðrir glæpir sem framdir eru á netum eiga sér ekki hefðbundin landamæri og því er samstarf ríkja, netöryggissveita sem og annarra sérhæfðra aðila nauðsynlegt til að hægt sé að stemma stigum við slíkum ógnum og verjast þeim með sem skilvirkustum hætti. Er þessu undanþáguákvæði frá sérstakri þagnarskyldu ætlað að tryggja að Ísland geti verið virkur þátttakandi í slíku samstarfi, hvort tveggja með því að fá aðgang að upplýsingum og veita upplýsingar um mögulega ógnir og hættur. Það ber að árétta að í samstarfi sem þessu eru þó einungis veittar nauðsynlegar upplýsingar svo að markmið með samstarfinu náist, þannig nær ákvæðið ekki til upplýsinga líkt og tölvupóstföng starfsmanna rekstraraðila mikilvægra innviða eða stjórnarráðsins, sbr. einnig athugasemdir við ákvæði 26. gr. Málsgreinin fellur vel að markmiðum tilskipunarinnar eins og að framan greinir.

Í 3. mgr. kemur fram að við upplýsingaskipti skv. 1. og 2. mgr. skal gæta trúnaðar um öryggis og viðskiptahagsmuni hlutaðeigandi rekstraraðila mikilvægra innviða og að þagnarskylda skv. 22. gr. skuli ríkja um þær upplýsingar sem veittar eru eða tekið er á móti skv. 1. og 2. mgr. Um er að ræða upplýsingar til eða frá lögreglu eða persónuverndaryfirvöldum er varða net- og upplýsingaöryggi, almannavarnir eða persónuvernd og upplýsingar til eða frá erlendum stjórnvöldum, eftirlitsaðilum eða öðrum aðilum eða sérfræðingum sem sinna net- og upplýsingaöryggi þegar slíkt er nauðsynlegt vegna skipulagðrar alþjóðasamvinnu sem hefur það markmið að stuðla að eða framkvæma aðgerðir til að tryggja öryggi net- og upplýsingakerfa. Er 4. mgr. ætlað að innleiða ákvæði 5. mgr. 14. gr. og 6. mgr. 16. gr. tilskipunar 2016/1148/ESB þar sem kveðið er á um trúnað um öryggis- og viðskiptahagsmuni rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda.

Um 25. gr.

Í 1. og 2. mgr. ákvæðisins er að finna sjálfstæðar vinnsluheimildir netöryggissveitarinnar vegna lögbundins hlutverks hennar samkvæmt lögunum. Netöryggissveitin þarf í grunninn almenna vinnsluheimild fyrir gögn sem hún sjálf aflar, sbr. 1. mgr. ákvæðisins. Auk þess getur komið til þess að netöryggissveitin fái upp í hendurnar aðrar persónuupplýsingar sem sveitin verður að bregðast við, sbr. 2. mgr. ákvæðisins. Í 3. mgr. ákvæðisins er áréttað að öll vinnsla persónuupplýsinga hjá netöryggissveit skuli vera í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga og ákvæði evrópsku persónuverndarreglugerðarinnar (GDPR). Í 4. mgr. ákvæðisins er jafnframt lagt til að nýtt verði heimild í 23. gr. GDPR til að takmarka skyldur og réttindi samkvæmt III. kafla reglugerðarinnar þegar kemur að starfsemi netöryggissveitarinnar á grundvelli þessara laga. Að lokum er í 5. mgr. ákvæðisins sett skylda á ráðherra að setja reglugerð um vinnslu persónuupplýsinga hjá netöryggissveitinni.

Mikilvægi net- og upplýsingaöryggis er áréttað í formálsorðum GDPR. Þá var fjallað um mikilvægi net- og upplýsingaöryggis og starfsemi netöryggissveitarinnar í nefndaráliti meiri

hluta allsherjar- og menntamálanefndar á frumvarpi til nýrra laga um persónuvernd og vinnslu persónuupplýsinga en þar segir:

> „Bent var á að takmörkunarheimildin sem innleidd væri í 17. gr. frumvarpsins næði aðeins til 13.–15. gr. reglugerðarinnar, þ.e. til 1. og 2. þáttar III. kafla reglugerðarinnar en ekki 3. og 4. þáttar líkt og reglugerðin kveður jafnframt á um að takmarka megi. Það geti hins vegar verið nauðsynlegt með tilliti til net- og upplýsingaöryggis að víkja frá þeim réttindum einstaklinga sem er að finna í 3. og 4. þætti III. kafla reglugerðarinnar, líkt og rétti til takmörkunar á vinnslu, tilkynningarskyldu ábyrgðaraðila varðandi leiðréttingu persónuupplýsinga og andmælarétti hins skráða. Skortur á takmörkunarheimildum að þessu leyti geti haft mikil áhrif á starfsemi netöryggissveitar Póst- og fjarskiptastofnunar við vernd upplýsinga, þar á meðal persónuupplýsinga, í net- og upplýsingakerfum mikilvægra innviða hér á landi. Nauðsynlegt sé að kveðið sé á um slíka takmörkun í lögum þar sem heimild 23. gr. til takmarkana sé bundin við að slíkt sé ákveðið með löggjafarráðstöfun. Meiri hlutinn áréttar að skv. 6. mgr. 4. gr. gilda lögin og reglugerðin ekki um vinnslu persónuupplýsinga af hálfu ríkisins í tengslum við rannsókn á refsiverðum brotum eða til að koma í veg fyrir ógnir við almannaöryggi. Í nýjum lögum sem nú er unnið að vegna innleiðingar á NIS-tilskipun, tilskipun Evrópuþingsins og ráðsins (ESB) 2016/1148, verði jafnframt hægt að veita Póst- og fjarskiptastofnun allar nauðsynlegar heimildir sem rúmast innan 23. gr. reglugerðarinnar og henni eru nauðsynlegar til að sinna sínu hlutverki. Þá verði lögin um NIS-tilskipunina sérlög sem gangi framar almennum lögum um persónuvernd. Bent er á að sérstaklega er fjallað um netöryggissveitir í formálsorðum reglugerðarinnar og að vinnsla persónuupplýsinga í tengslum við netöryggi teljist til lögmætra hagsmuna fyrirtækja. Að lokum fellur netöryggi undir þjóðaröryggi, landvarnir og almannaöryggi sem getið er í 17. gr. frumvarpsins og 23. gr. reglugerðarinnar sem lögmætar ástæður takmörkunar á rétti einstaklings til upplýsinga og aðgangs.“

Það er því ljóst að horfa verður til þessa þegar veittar eru vinnsluheimildir til netöryggissveitarinnar samkvæmt frumvarpi þessu sem og þeirra takmarkana sem lagðar eru til í frumvarpinu, sbr. umfjöllun hér.

Í 1. mgr. ákvæðisins er að finna almenna vinnsluheimild netöryggissveitarinnar. Er hér um að ræða nauðsynlega heimild fyrir netöryggissveitina til að sinna almennu hlutverki sínu sem viðbragðsteymis á grundvelli laganna. Heimildin byggir á 6. tölul. 1. mgr. 9. gr. laga um persónuvernd og vinnslu persónuupplýsinga, sbr. einnig f. lið 1. mgr. 6. gr. GDPR, sem kveða á um heimildir til vinnslu persónuupplýsinga þegar vinnslan er nauðsynleg vegna lögmætra hagsmuna ábyrgðaraðila. Í 49. lið formálsorða GDPR er sérstaklega vísað til þess að vinnsla sem þessi, að því marki sem hún er beinlínis nauðsynleg og hófleg til að tryggja net- og upplýsingaöryggi, teljist til lögmætra hagsmuna ábyrgðaraðila. Er sérstaklega tekið sem dæmi að þetta gæti t.d. falið í sér að komið sé í veg fyrir óheimilan aðgang að rafrænum fjarskiptanetum og dreifingu spilliforrita og til að stöðvaðar séu atlögur að þjónustumiðlun og skemmdir á tölvum og rafrænum fjarskiptakerfum. Með net- og upplýsingaöryggi er í þessu samhengi átt við getu nets eða upplýsingakerfis til að standast, á tilteknu öryggisstigi, atburði sem verða fyrir slysni eða aðgerðir sem eru ólögmætar eða skaðlegar og stofna í hættu aðgengileika, sannvottuðum uppruna, heilleika og leynd vistaðra eða sendra persónuupplýsinga, og öryggi tengdrar þjónustu sem er boðin eða er aðgengileg um þessi net

og kerfi, af hálfu opinberra yfirvalda, viðbragðsteymis vegna neyðartilvika er varðar tölvuöryggi (CERT), viðbragðsteymis vegna váatvika er varða tölvuöryggi (CSIRT), þeirra sem reka rafræn fjarskiptanet og - þjónustu og þeirra sem útvega öryggistækni og þjónustu.

Aðgangur netöryggissveitarinnar, viðbragðsteymis vegna váatvika er varðar net- og upplýsingaöryggi, að gögnum er grundvallarforsenda þess að sveitin geti sinnt lögbundnu hlutverki sínu samkvæmt lögunum og þeim verkefnum sem viðauki I við NIS-tilskipunina kveður á um. Í athugasemdum við 21. og 22. gr. frumvarpsins er að finna ítarlega lýsingu á því hvernig starfsemi sveitarinnar, þegar kemur að mikilvægum innviðum hér á landi, verður háttað. Er þar að finna kröfu um gerð samninga milli netöryggissveitar og rekstraraðila mikilvægra innviða um uppsetningu og rekstur vöktunarbúnaðar fyrir net- og upplýsingakerfi viðkomandi rekstraraðila í þeim tilgangi að greina hættur og ummerki um atvik, spillikóða og aðrar vísbendingar um aðstæður sem gætu skapað hættu fyrir viðkomandi rekstraraðila. Þá er enn fremur lýst því hvernig sjálfvirk skimun á umferð og innihaldi sendinga við kerfi rekstraraðilans á sér stað og um hvaða gögn er verið að ræða. Eins eru tilgreind þau gögn sem að netöryggissveitin mun með þessum hætti, og á grundvelli almennrar upplýsingagjafar rekstraraðila, fá aðgang að. Umrædd gögn, svo sem IP-tölur og önnur umferðargögn, teljast persónuupplýsingar enda eru þær persónugreinanlegar í skilningi laga um persónuvernd og vinnslu persónuupplýsinga og GDPR. Það er því nauðsynlegt að kveða á um vinnsluheimildir netöryggissveitarinnar til vinnslu þessara upplýsinga svo ákvæði persónuverndarlaga og GDPR séu uppfyllt.

Með vinnslu í skilningi GDPR og laga um persónuvernd og vinnslu persónuupplýsinga er átt við „aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, s.s. söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtengin eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging.“. Þannig er ljóst að ákvæði 1. mgr. nær yfir hvort tveggja móttöku upplýsinganna og mögulegrar miðlunar þeirra. Aftur á móti verður að skýra ákvæðið með hliðsjón af öðrum ákvæðum frumvarpsins. Má þar í fyrsta lagi nefna ákvæði um sérstaka þagnarskyldu og undanþágu frá henni, sbr. 24. og 25. gr. Við samtúlkun þessara ákvæða er miðlun persónuupplýsinga frá netöryggissveit því einungis heimil til lögreglu, persónuverndaryfirvalds, sbr. 1. mgr. 25. gr. frumvarpsins, til erlendra stjórnvalda, eftirlitsaðila og annarra aðila sem sinna net- og upplýsingaöryggi þegar slík miðlun er nauðsynleg vegna alþjóðasamvinnu sem hefur það markmið að stuðla að netöryggi. Í öðru lagi verður að lesa ákvæði 1. mgr. í samræmi við ákvæði 23. gr. þ.e. að netöryggissveit geti gefið tilmæli til annarra rekstraraðila mikilvægra innviða um að bregðast gegn bráðri aðsteðjandi netógn. En þannig verður netöryggissveitin að geta miðlað ákveðnum persónuupplýsingum vegna þess til annarra rekstraraðila. Mikilvægt er að árétta í þessu samhengi að miðlum persónuupplýsinga, líkt og IP-talna mögulegs tölvuþrjóts, einskorðast alla jafna við þær upplýsingar sem að lágmarki eru nauðsynlegar til að bregðast við ógn, verjast árás eða öryggisatviki og draga úr mögulegu tjóni. Þannig væri ekki verið að miðla út fyrir netöryggissveitina öðrum persónuupplýsingum líkt og tölvupóstföngum starfsmanna rekstraraðila mikilvægra innviða, starfsmanna stjórnarráðsins eða annarra sem gera samning við netöryggissveitina, nöfnum þeirra eða vélanöfnum.

Í 2. mgr. ákvæðisins er að finna mikilvæga heimild fyrir netöryggissveitina til vinnslu og miðlunar á upplýsingum sem henni berast til verndar almannahagsmunum og hagsmunum einstaklinga án samþykkis hlutaðeigandi einstaklings. Hér er um að ræða upplýsingar sem geta verið eins konar andlag atviks eða árásar sem netöryggissveitinni berast umfram það sem

fellur undir almennt hlutverk hennar. Erfitt getur verið að segja til um hvaða upplýsingar geta verið um að ræða í þessum tilfellum, fer það allt eftir því öryggisatviki eða árás sem um er að ræða. Geta þær verið allt frá lykilorðum og kortanúmerum einstaklinga yfir í mögulegar heilsufarsupplýsingar þeirra en um er að ræða upplýsingar sem óprúttnir aðilar hafa komist yfir með ólögmætum hætti t.d. með innbroti í kerfi rekstraraðila. Í tilvikum sem þessum er nauðsynlegt fyrir sveitina að geta gripið til aðgerða, án samþykkis hins skráða, t.a.m. með því að miðla umræddum upplýsingum, eða a.m.k. upplýsa um hagsmuni einstaklinganna, til annarra rekstraraðila mikilvægra innviða, svo sem banka, eða annarra, allt eftir tegund og eðli upplýsinganna. Þessar upplýsingar eru í raun ekki á forræði netöryggissveitarinnar með neinum hætti fyrr en til atviks kemur og er um neyðarúrræði að ræða til að vernda viðkomandi einstakling. Það getur skipt sköpum fyrir umræddan einstakling að netöryggissveitin hafi skýra heimild til þess að grípa til nauðsynlegrar miðlunar á upplýsingunum til verndar hans eigin hagsmunum eða á grundvelli almannahagsmuna. Tímarammi í tilfellum sem þessum er mjög þröngur og getur skipt mínútum hvort óprúttnir aðilar sem komist hafa yfir upplýsingarnar geti misnotað þær með einhverjum hætti á kostnað viðkomandi einstaklings. Það er því nauðsynlegt fyrir netöryggissveitina að geta brugðist hratt við og komið slíkum mikilvægum upplýsingum áfram til hlutaðeigandi aðila, sem þá getur takmarkað eða komið í veg fyrir mögulegt tjón, viðkomandi einstaklings. Miðlun upplýsinganna þarf því að fara fram án sérstaks upplýsts samþykkis hins skráða, þ.e. viðkomandi einstaklings, enda eru eðli aðstæðna í raun þannig að hann getur ekki gætt hagsmuna sinna sjálfur. En krafa um öflun samþykkis yrði til þess fallin að hagsmunum viðkomandi og yrði stefnt í mikla hættu þar sem gríðarlegur tími færi í að hafa uppá viðkomandi einstaklingum til að leita eftir samþykki þeirra.

Á tilvik sem þetta hefur reynt. Í innbroti á vefsvæði Vodafone í nóvember 2013 var gríðarlegu magni gagna stolið og þau birt á Internetinu. Auk fjarskiptagagna var um að ræða lykilorð og kortaupplýsingar einstaklinga. Netöryggissveitin fékk umræddar upplýsingar í sínar hendur enda bar Vodafone að tilkynna öryggisatvik til sveitarinnar, sbr. ákvæði fjarskiptalaga. Í þessu tilfelli vildi netöryggissveitin miðla umræddum upplýsingum til fjármálastofnanna svo þær gætu gripið til viðeigandi ráðstafana til verndar umræddum einstaklingum og takmarka eða koma í veg fyrir að tjón. Aftur á móti taldi netöryggissveitin sér ekki fært um að miðla umræddum upplýsingum enda skorti hana lagaheimild til slíks. Í frumvarpi þessu er því verið að kveða á um slíka heimild til vinnslu persónuupplýsinga og viðkvæmra persónuupplýsinga, þ.e. eins konar neyðarmiðlun þeirra án samþykkis viðkomandi einstaklings, til aðila sem geta takmarkað eða komið í veg fyrir að einstaklingur verði fyrir skaða.

Í 35. gr. GDPR er fjallað um mat á áhrifum á persónuvernd (MÁP) en framkvæma skal slíkt mat á áhrifum fyrirhugaðar vinnsluaðgerða á vernd persónaupplýsinga ef líklegt er að tiltekin tegund vinnslu geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Ljóst er að í tilviki neyðarmiðlunar sem þessara er verið að vinna persónuupplýsingar og mögulega viðkvæmar persónuupplýsingar án samþykkis þeirra og er því rétt að fram fari mat á áhrifum á réttindi umræddra einstaklinga. Í slíku mati er nauðsynlegt að skoða umfang, eðli og tilgang vinnslunnar, hvort hún sé nauðsynleg og hvernig hægt sé að tryggja að meðalhófs sé gætt við að ná þeim tilgangi sem stefnt er að með vinnslunni, hvernig best sé gætt að réttindum einstaklinga t.d. með tilteknum ráðstöfunum við vinnsluna o.fl. Nauðsynlegt er í þessu samhengi að líta til þess að miðlun upplýsinga á grundvelli þessa ákvæðis er eingöngu hugsuð til að vernda hagsmuni viðkomandi einstaklings. Miðlunin myndi einskorðast við nauðsynlega móttakendur sem geta gripið til ákveðinna úrræða, svo sem loka ákveðnum kortum og aðgangi á ákveðnum leyniorðum o.þ.h. Netöryggissveit mun með engum hætti

greina umræddar upplýsingar eða vinna þær með öðrum hætti enda ekki beinn liður í því lögbundna hlutverki hennar að gæta að netógnum og netárásum. Persónuupplýsingum á grundvelli þessarar málsgreinar yrði því eytt eftir að miðlun er lokið, þ.e. þegar sveitin hefur reynt að gæta að hagsmunum hins skráða.

Í 3. mgr. ákvæðisins er kveðið á um að öll vinnsla persónuupplýsinga á grundvelli laganna skulu vera í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga. Er hér um að ræða almennt ákvæði sem er ætlað að tryggja að sú vinnsla sem fram fer hjá netöryggissveit verði í samræmi við þær meginreglur sem gerðar eru til vinnslu persónuupplýsinga í nýjum lögum um persónuvernd og GDPR. Þannig verður sú vinnsla netöryggissveitarinnar að uppfylla þær meginreglur sem gilda um vinnslu persónuupplýsinga og byggja á lögmætum heimildum. Þá verður netöryggissveitin að uppfylla skyldur sínar sem ábyrgðaraðili og gæta að öryggi upplýsinganna í samræmi við persónuverndarlög og GDPR.

Í 4. mgr. ákvæðisins er fjallað um ákveðnar undanþágur netöryggissveitarinnar frá ákvæðum persónuverndarlaga og GDPR þegar kemur að skyldum og réttindum sem um getur í 12.-22. og 34. gr. GDPR. Umrædd undanþáguheimild byggir á 23. gr. GDPR sem í raun 5. þáttur III. kafla GDPR sem fjallar um réttindi einstaklinga. Í 1. þætti kaflans, sbr. 12. gr., er fjallað um gagnsæi upplýsinga, tilkynningar og nánari reglur til að skráður einstaklingur geti neytt réttar síns. Í 2. þætti kaflans, sbr. 13.-15. gr. er fjallað um upplýsingar og rétt til aðgangs að upplýsingum. Í 3. þætti kaflans, sbr. 16.-20. gr., er fjallað um rétt til leiðréttingar og eyðingar. Í 4. þætti kaflans, sbr. 21. og 22. gr., er fjallað um andmælarétt og sjálfvirka einstaklingsmiðaða ákvörðunartöku. Í 5. þætti kaflans, sbr. 23. gr., er svo að lokum fjallað um takmarkanir, þ.e. heimild til að takmarka gildissvið skyldna og réttinda sem um getur í framangreindum þáttum kaflans, sbr. 12-22, ásamt 34. gr. og einnig í 5. gr. GDPR. Þá segir í 73. lið formálaorða reglugerðarinnar er fjallað um heimildina en það segir að landslög geti kveðið „ ... á um að takmarka megi sértækar meginreglur og rétt á upplýsingum, aðgang að persónuupplýsingum og leiðréttingu á þeim eða eyðingu þeirra, rétt til að flytja eigin gögn, rétt til andmæla, ákvarðanir sem byggjast á gerð persónusniðs, ásamt tilkynningum til skráðs einstaklings um öryggisbrot við meðferð persónuupplýsinga og tilteknar tengdar skyldur ábyrgðaraðila, að því marki sem nauðsynlegt er og hóflegt í lýðræðisþjóðfélagi til að vernda almannaöryggi, ... “.

Í ákvæðum GDPR er því gert ráð fyrir að takmarka megi skyldur ábyrgðaraðila og réttindi einstaklinga á grundvelli ákveðinna sjónarmiða, enda séu takmörkunin byggð á meðalhófi og virði eðli grundvallarréttinda og mannfrelsis. Í 1. mgr. 23. gr. er að finna upptalningu á þeim sjónarmiðum sem takmörkun getur byggt á. Þau sjónmarmið sem m.a. eru talin upp eiga með beinum hætti við um starfsemi netöryggissveitarinnar, þ.e. sjónarmið er lúta að þjóðaröryggi og almannaöryggi, sbr. a. og c. liðir 1. mgr. greinarinnar. Hlutverk og markmið NIS-tilskipunarinnar, líkt og fram kemur í fyrstu liðum formála hennar er að verja net- og upplýsingakerfi mikilvægra innviða hvers lands enda skiptir áreinaleiki og öryggi þeirra sköpum fyrir efnahagslega og samfélagslega starfsemi landsins og Evrópusambandsins. Netógnir og árásir geta hamlað atvinnustarfsemi, valdið verulegu fjárhagslegu tjóni, grafið undan trausti notenda og valdið miklu tjóni á efnahagi Evrópusambandsins og því er öryggi net- og upplýsingakerfa þess nauðsynlegt fyrir snurðulausa starfsemi hvers aðildarríkis og hins innri markaðar. Í þessu samhengi er jafnframt nauðsynlegt að líta til þess að með frumvarpinu er jafnframt stefnt að lögfestingu þjónustusamnings netöryggissveitarinnar og stjórnarráðsins, sbr. núverandi GovCert-samning.

Takmörkunarákvæði sem þetta er í raun ekki nýtt af nálinni því í þágildandi persónuverndarlöggjöf nr. 77/2000 kemur fram í 1. málsl. 2. mgr. 3. gr. að „[á]kvæði 16., 18.–

21., 24., 26., 31. og 32. gr. laganna gilda ekki um vinnslu persónuupplýsinga sem varða almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu.“. Tilgreind ákvæði fjalla fyrst og fremst um upplýsingarétt hins skráða og upplýsingaskyldu til hins skráða og tilkynningarskyldu til Persónuverndar. Um er að ræða rétt til almennrar vitneskju um vinnslu persónuupplýsinga (16. gr.), upplýsingarétt hins skráða (18. gr.), takmarkanir á upplýsingarétti hins skráða (19. gr.), fræðsluskyldu þegar persónuupplýsinga er aflað hjá hinum skráða (20. gr.), skyldu til að láta hinn skráða vita um vinnslu persónuupplýsinga þegar þeirra er aflað hjá öðrum en honum sjálfum (21. gr.), viðvaranir um rafræna vöktun (24. gr.), eyðingu og bann við notkun persónuupplýsinga sem hvorki eru rangar né villandi (26. gr.), tilkynningarskyldu til Persónuverndar (31. gr.) og efni slíkrar tilkynningar (32. gr.). Þannig gerðu þágildandi persónuverndarlög ráð fyrir því að takmarka megi rétt hins skráða á grundvelli ákveðinna almannahagsmuna, þ.e. þegar um er að ræða almannaöryggi, landvarnir ríkisins, öryggi þess og starfsemi á sviði refsivörslu.

Hliðstæða undanþágur frá ákvæðum dönsku persónuverndarlaganna má finna í danskri löggjöf um net- og upplýsingaöryggi, sbr. Lov om Center for Cybersikkerhed nr. 713/2014. En í löggjöfinni má finna fordæmi fyrir því að takmörkunarákvæði persónuverndarreglna sé beitt. Þá er jafnframt kveðið á um það í löggjöfinni að ráðherra varnarmála geti ákveðið að undanskilja netöryggissveitina fleiri ákvæðum persónuverndarlöggjafarinnar. Er í 6. kafla löggjafarinnar, sbr. 10. gr., fjallað um vinnsluheimildir dönsku netöryggissveitarinnar en þar er t.a.m. tilgreint að heimildirnar séu í þágu almannahagsmuna, þjóðaröryggis sem og almannaþjónustu. Er það jafnframt m.a. að finna heimild til miðlunar upplýsinga hvort tveggja frá og til þriðja aðila, sbr. 5. og 6. tölul. greinarinnar. Einnig er kveðið á um bann við almennri vinnslu viðkvæmra persónuupplýsinga, sbr. 11. gr. laganna. Aftur á móti eru undanþágur frá slíku banni, t.a.m. ef að vinnslan er nauðsynleg vegna þjóðaröryggis og varnarmála, sbr. 4. tölul. greinarinnar. Í löggjöfinni er jafnframt kveðið á um ákveðnar kröfur er varðar vinnsluna, svo sem um réttleika upplýsinganna, eyðingu þeirra og skyldu um að gera þær ópersónugreinanlegar.

Í 5. mgr. ákvæðisins er kveðið á um skyldu ráðherra til að setja reglugerð um vinnslu persónuupplýsinga hjá netöryggissveitinni. Er þar einnig lagt til að afla skuli álits Persónuverndar þegar umrædd reglugerð er sett. Í þessu tilliti er mikilvægt að gætt sé að þeim kröfum sem ákvæði persónuverndarlaga og GDPR gera til vinnslu persónuupplýsinga, takmarkana á skyldum og réttindum, sbr. fyrri umfjöllun um 23. gr. GDPR, kröfu um varðveislu og eyðingu gagna o.fl. Þannig getur verið eðlilegt að líta til mismunandi eðlis gagnanna, svo sem stýrigagna eða fullra pakka, þegar geymslutími þeirra er ákvarðaður. Allt með tilliti til nauðsyn vinnslunnar á grundvelli þjóðaröryggis og almannahagsmuna.

Um 26. gr.

Í ákvæðinu er kveðið á um bindandi fyrirmæli. Í 15. gr. tilskipunar 2016/1148/ESB er kveðið á um framkvæmd og fullnustu þegar kemur að öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu og segir í ákvæði 1. mgr. að tryggja skuli að lögbær yfirvöld, hér eftirlitsstjórnvöld, hafi nauðsynlegar valdheimildir og úrræði til að meta hvort rekstraraðilar nauðsynlegrar þjónustu uppfylli skuldbindingar sínar skv. 14. gr., þ.e. um öryggiskröfur og tilkynningar um atvik, og áhrif þess á öryggi net- og upplýsingakerfa. Í 1. mgr. 17. gr. tilskipunarinnar er áþekkt ákvæði um framkvæmd og fullnustu hvað varðar stafræna þjónustuveitendur og tilvísun til 16. gr. tilskipunarinnar um öryggiskröfur og tilkynningar um atvik í tilviki þeirra. Ákvæðinu er ætlað að innleiða framangreind ákvæði tilskipunarinnar.

Í 1. mgr. er heimild eftirlitsstjórnvalda, á hverju sviði fyrir sig, að gefa bindandi fyrirmæli er varða skipulag net- og upplýsingaöryggis. Undir það fellur m.a. lágmarks öryggisráðstafanir rekstraraðila mikilvægra innviða. Skylt er að verða við fyrirmælum án tafar og ef það er vanrækt getur eftirlitsstjórnvald látið vinna verkið á kostnað viðkomandi rekstraraðila mikilvægra innviða. Sé verk unnið á kostnað rekstraraðila í framangreindum tilvikum verður krafan aðfararhæf skv. 5. tölul. 1. mgr. 1. gr. laga um aðför nr. 90/1989.

Í 2. mgr. kemur fram að ráðherra er heimilt með reglugerð að mæla nánar fyrir um málsmeðferð vegna bindandi fyrirmæla. Ljóst er að um er að ræða heimildarákvæði en ekki skyldu til reglusetningar. Þá er ljóst að um beiting bindandi fyrirmæla fer að öðru leyti eftir því sem við á eftir ákvæðum stjórnsýslulaga nr. 37/1993 enda umrædd ákvörðun stjórnvaldsákvörðun í skilningi 2. mgr. 1. gr. þeirra laga.

Um 27. gr.

Eins og fram kemur í athugasemdum við ákvæði 25. gr. þá er í ákvæðum 15. gr. og 17. gr. tilskipunar 2016/1148/ESB kveðið á um framkvæmd og fullnustu tilskipunarinnar. Ákvæði 26. gr. er ætlað að taka til þeirra þátta 15. og 17. gr. tilskipunarinnar sem 26. gr. tekur ekki til og er í ákvæðinu kveðið á um dagsektir en dagsektir eru meðal nauðsynlegra valdheimilda og úrræða sem grípa getur þurft til ef ekki er farið eftir fyrirmælum eða ósk um afhendingu gagna. Í 2. mgr. 15. gr. tilskipunarinnar kemur fram að aðildarríki skulu tryggja að lögbær yfirvöld, hér eftirlitsstjórnvöld, hafi valdheimildir og þau úrræði til að krefjast þess að rekstraraðilar nauðsynlegrar þjónustu veiti annars vegar nauðsynlegar upplýsingar til að meta öryggi net- og upplýsingakerfa þeirra, þ.m.t. skjalfestar öryggisreglur, og hins vegar sannanir fyrir skilvirkri framkvæmd á öryggisreglum, eins og niðurstöður úr öryggisúttekt sem lögbært yfirvald eða hæfur úttektarmaður framkvæmir og, gerir niðurstöður úr, þ.m.t. þau sönnunargögn sem lögð eru til grundvallar, aðgengilegar lögbæru yfirvaldi. Í 2. mgr. 17. gr. er áþekkt ákvæði hvað varðar stafræna þjónustuveitendur en þar kemur fram að lögbær yfirvöld skulu hafa nauðsynlegar valdheimildir og úrræði til að krefja veitendur stafrænnar þjónustu um annars vegar nauðsynlegar upplýsingar til að meta öryggi net- og upplýsingakerfa, þ.m.t. skjalfestar öryggisreglur og hins vegar bæta úr öllum tilvikum þar sem kröfur, sem mælt er fyrir um í 16. gr., eru ekki uppfylltar.

Í 1. mgr. kemur fram að ef ekki er farið að fyrirmælum eftirlitsstjórnvalds skv. 25. gr. eða ósk þess eða netöryggissveitar um afhendingu upplýsinga skv. 16.og 21. gr. getur hlutaðeigandi eftirlitsstjórnvald ákveðið að leggja dagsektir á þann sem fyrirmælin beinast að og þar til úr verður bætt að mati eftirlitsstjórnvaldsins og eftir atvikum að höfðu samráði við netöryggissveit. Sektir geta numið allt að 500.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælum sé fylgt. Fjárhæð sekta er áþekk sektarfjárhæð 8. mgr. 11. gr. laga um fjarskipti nr. 81/2003.

Í 2. mgr. kemur fram að í þeim tilvikum sem dagsektir eru lagðar á skv. 1. mgr. og þeim í kjölfarið skotið til dómstóla byrja þær ekki að falla á fyrr en dómur er endanlegur. Dagsektir renna í ríkissjóð og má án undangengins dóms gera aðför til fullnustu þeirra. Fer um það eftir almennum reglum laga um aðför nr. 90/1989.

Um 28. gr.

Í ákvæðinu er kveðið á um refsingar og er því ætlað að innleiða 21. gr. tilskipunar 2016/1148/ESB þar sem fram kemur að setja skuli reglur um viðurlögum við brotum á þeim lögum sem innleiða tilskipunina. Viðurlögin skulu vera skilvirk, í réttu hlutfalli við brotið og þurfa þau að hafa varnaðaráhrif.

Í 1. mgr. er kveðið á um að brot á ákvæðum frumvarpsins og reglugerðum settum samkvæmt þeim varða fésektum eða fangelsi allt að tveimur árum nema þyngri refsins liggi við samkvæmt öðrum lögum. Sama refsing liggur við ef ekki er farið að fyrirmælum eftirlitsstjórnvalds eða netöryggissveitar. Gáleysisbrot skulu eingöngu varða sektum.

Í 2. mgr. kemur fram að í þeim tilvikum sem brot skv. 1. mgr. eru framin í starfsemi lögaðila megi gera lögaðilanum fésekt skv. II. kafla A almennra hegningarlaga nr. 19/1940. Í þeim kafla er kveðið á um refsiábyrgðir lögaðila en lögaðili er skv. 19. gr. b. sérhver ópersónulegur aðili sem getur átt réttindi og borið skyldur að íslenskum rétti, þar með talin hlutafélög, einkahlutafélög, samlagshlutafélög, evrópsk fjárhagsleg hagsmunafélög, sameignarfélög, samvinnufélög, almenn félög, sjálfseignarstofnanir, stjórnvöld, stofnanir og sveitarfélög. Í 19. gr. c. er sett fram það skilyrði að um refsiábyrgð lögaðila, nema annað sé tekið fram í lögum, að fyrirsvarsmaður lögaðilans, starfsmaður hans eða annar á hans vegum hafi með saknæmum hætti unnið refsinæman og ólögmætan verknað í starfsemi lögaðilans. Verður lögaðila gerð refsing þó að ekki verði staðreynt hver þessara aðila hafi átt í hlut. Refsiábyrgð stjórnvalda er bundin því skilyrði að unninn hafi verið refsinæmur og ólögmætur verknaður í starfsemi sem telst vera sambærileg starfsemi einkaaðila.

Um 29. gr.

Ákvæðið á sér samsvörun í 3. mgr. 14. gr. og 3. mgr. 16. gr. tilskipunar 2016/1148/ESB og er ætlað að taka af skarið um að tilkynningar til netöryggissveitar eins og fjallað er um þær í frumvarpinu hafa ekki áhrif á mögulega bótaskyldu vegna atviks. Á það bæði við um áhrif bótaskyldu og aukningu bótaskyldu.

Um 30. gr.

Ákvæðið þarfnast ekki sérstakra skýringa en með því er tiltekið að með frumvarpinu og þeim reglum sem settar ferða á grundvelli þess, verði það að lögum, sé innleidd tilskipun 2016/114/ESB. Ljóst er að með samþykkt frumvarpsins eins og sér hefur tilskipunin ekki verið innleidd með fullnægjandi hætti heldur þarf frekari reglusetning að koma til eins og ákvæði frumvarpsins bera með sér.

Um 31. gr.

Ákvæðinu er ætlað að veita almenna heimild til ráðherra til reglusetningar umfram þau ákvæði sem kveða sérstaklega á um skyldu eða heimild til setningu reglugerða. Í greininni er tiltekið að ráðherra sé heimil reglusetning að öðru leyti eins og nánar greinir í frumvarpinu. Í þeim tilvikum sem ráðherra er skylt að mæla fyrir um frekari reglusetningu er í athugasemdum við ákvæðin fjallað sérstaklega um þau ákvæði tilskipunarinnar sem útfæra þarf nánar í reglugerðum.

Um 32. gr.

Ákvæðið þarfnast ekki sérstakrar skýringar.

Um 33. gr.

Í ákvæðinu er mælt fyrir um breytingar á öðrum lögum sem eru nauðsynlegar verði frumvarpið að lögum. En lagðar eru til breytingar er varðar ákvæði laga nr. 81/2003, um fjarskipti og laga nr. 69/2003, um Póst- og fjarskiptastofnun.

Með lögum nr. 62/2012, um breytingu á lögum um fjarskipti og lögum um Póst- og fjarskiptastofnun, var ákvæði 47. gr. a í fjarskiptalögum um hlutverk netöryggissveitarinnar,

lögleitt. Samkvæmt ákvæðinu er ráðherra gert að setja reglugerð þar sem nánar er fjallað um starfsemi netöryggissveitarinnar, sbr. reglugerð nr. 475/2013, um málefni CERT-ÍS netöryggissveitar. Samkvæmt lagaákvæðinu og reglugerðinni er netöryggissveitinni ætlað mikilvægt hlutverk þegar kemur að upplýsingaöryggi fjarskiptaneta og annarra ómissandi upplýsingainnviða hér á landi. Er sveitinni í fyrsta lagi ætlað ákveðið almannavarnarhlutverk, þ.e. að fylgjast með og vakta ógnir sem steðja að Íslandi í heild og að vera tengiliður íslenskra stjórnvalda á alþjóðlegum vettvangi þegar kemur að viðbragðsvörnum net- og upplýsingaöryggis. Í öðru lagi er markmið með starfi sveitarinnar að fyrirbyggja og draga úr hættu á netárásum og öðrum öryggisatvikum eins og kostur er í netumdæmi sínu en það nær til þjónustuhóps sveitarinnar, þ.e. fjarskiptafyrirtækja og þeirra rekstraraðila ómissandi upplýsingainnviða sem gert hafa þjónustusamning við netöryggissveitina. Á netöryggissveitin að aðstoða þjónustuhópinn við forvarnir, leiðbeina honum og styðja við skjót viðbrögð gegn aðsteðjandi hættu.

Helstu verkefni sveitarinnar eru talin upp í 6. gr. framangreindrar reglugerðar en þar kemur m.a. fram að sveitin skuli vakta upplýsingainnviði þjónustuhópsins gagnvart ógnum og meta hvort grípa þurfi til ákveðinna viðbúnaðaraðgerða. Skal sveitin, ef til útbreidds öryggisatviks kemur, samhæfa aðgerðir aðila þjónustuhópsins gegn aðsteðjandi hættu til að lágmarka tjón og reisa við óvirk kerfi. Eins veitir netöryggissveitin þjónustuhópnum ráðgjöf um varnir og viðbúnað og kemur upplýsingum á framfæri við almenning ef þurfa þykir. Getur sveitin enn fremur upplýst ríkislögreglustjóra um meiri háttar netárásir gegn netumdæminu og um alvarleg eða útbreidd öryggisatvik sem valdið hafa tjóni eða skapa hættu á tjóni á ómissandi upplýsingainnviðum, í þeim tilvikum þar sem þjóðaröryggi og almannaheill er í húfi. Þá getur ríkislögreglustjóri falið sveitinni það hlutverk að viðhafa samstarf um varnir og viðbrögð. Ef alvarleiki árásar fer yfir ákveðið hættustig er sveitinni skylt að upplýsa ríkislögreglustjóra þar um.

Netumdæmi netöryggissveitarinnar byggir á fjarskiptafyrirtækjum og rekstraraðilum ómissandi upplýsinga sem undirritað hafa þjónustusamning við sveitina. Þessi mismunandi nálgun á aðilum skýrist fyrst og fremst af því að Póst- og fjarskiptastofnun fer með eftirlitshlutverk gagnvart fjarskiptageiranum, sbr. 1. mgr. 3. gr. laga nr. 69/2003, um Póst- og fjarskiptastofnun og 2. mgr. 2. gr. laga nr. 81/2003, um fjarskipti. Svo að starfsemi og heimildir netöryggissveitarinnar nái til allra ómissandi upplýsingainnviða hér á landi þarf sveitin því, samkvæmt núgildandi lagaumhverfi, að gera sérstaka þjónustusamninga við rekstraraðila þeirra. Samningarnir marka þannig þjónustuhóp og netumdæmi sveitarinnar en það er á höndum ríkislögreglustjóra að skilgreina hvað teljist til ómissandi upplýsingainnviða en í 27. tölul. 3. gr. fjarskiptalaga eru þeir almennt skilgreindir sem „[u]pplýsingakerfi þeirra mikilvægu samfélagslegu innviða sem tryggja eiga þjóðaröryggi, almannaheill og margs konar öflun aðfanga í þróuðu og tæknivæddu þjóðfélagi. Um er að ræða þann tækja- og hugbúnað sem nauðsynlegur er til reksturs og virkni kerfisins og þær upplýsingar sem þar eru hýstar eða um kerfið fara.“ Fram til þessa hefur ekki verið undirritaður þjónustusamningur milli netöryggissveitarinnar og rekstraraðila ómissandi upplýsingainnviða. Aftur á móti var undirritaður samningur við Stjórnarráð Íslands í janúar 2018, svokallaður GovCERT samningur og má því segja að núverandi netumdæmi netöryggissveitarinnar markist af þeim samningi og fjarskiptafyrirtækjum.

Með innleiðingu NIS-tilskipunarinnar breytist framangreint umhverfi með þeim hætti að skilgreindir verða mikilvægir innviðir, þ.e. rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur. Þessi nýja nálgun kemur því í stað þeirrar nálgunar sem er í núgildandi 47. gr. a, sbr. 27. tölul. 3. gr., um skilgreiningu á ómissandi upplýsingainnviðum. Sökum þessa er

nauðsynlegt að gera breytingar á ákvæðum fjarskiptalaga með hliðsjón af þeirri hugmyndafræði sem birtist í NIS-tilskipuninni. Ekki er um raunverulegar efnisbreytingar að ræða á hlutverki og heimildum netöryggissveitarinnar heldur eru breytingarnar nauðsynlegar til að samhljóða ákvæði gildi í raun um allan aðila sem netöryggissveitin kemur til með að þjónusta.

Í 1. töluliðs ákvæðisins er því að finna breytingar á fjarskiptalögum. Greinast breytingarnar í tvennt. Í fyrsta lagi eru lagðar til breytingar á skilgreiningarákvæðum fjarskiptalaga þar sem felldar verða brott skilgreiningar sem varða nafnlaus rauntímagögn, netumdæmi, ómissandi upplýsingainnviði og þjónustuhóp netöryggissveitarinnar, sbr. i. lið a. liðar 1. tölul. Eins eru lagðar til breytingar á skilgreiningu fyrir netöryggissveitina sem og að lagt er til að bætt verði við einum tölulið þar sem hugtakið netógn, verður skilgreint, sbr. i. og ii. liðir a. liðar 1 tölul. ákvæðisins. Með framangreindum breytingum eru felldar brott úr fjarskiptalögum þær skilgreiningar sem að vísað er til í núgildandi 47. gr. a við fjarskiptalög og verða í raun úreltar með innleiðingu NIS-tilskipunarinnar og breyttu efnisákvæði fjarskiptalaga. Breyting á skilgreiningu fyrir netöryggissveit og nýju skilgreiningarákvæði fyrir netógn er ætlað að ná betur utan um það starf sem að netöryggissveitin sinnir og nær nú til tveggja laga, þ.e. fjarskiptalaga og laga um öryggi net- og upplýsingakerfa mikilvægra innviða. Ekki er um efnisbreytingar að ræða.

Í öðru lagi er um að ræða breytingar á 47. gr. a í fjarskiptalögum, sbr. b. liður 1. tölul. ákvæðisins. Lagt er til að í stað gildandi ákvæðis komi þrjú ný ákvæði, þ.e. 47. gr. a – 47. gr. c. Í nýrri 47. gr. a verður áfram fjallað um hlutverk netöryggissveitarinnar. En sveitin skal skv. 1. mgr. gegna hlutverki öryggis- og viðbragðshóps hér á landi þegar kemur að netöryggismálum. Um er að ræða þjóðar-CERT fyrir Ísland (*e. National CERT*) með það að markmiði að vernda netumdæmi landsins gegn aðsteðjandi hættum og efla almenna netheilsu landsins og viðnám gegn netógnum. Netógnir og árásir eru sívaxandi vá sem nauðsynlegt er að takast á við með heildstæðum hætti í samvinnu við önnur ríki enda lúta þær ekki hefðbundnum landamærum. Netógnir einskorðast ekki við net- og upplýsingakerfi mikilvægra innviða heldur er að finna víðar í netumdæmi Íslands og er mikilvægt að kveða á um markmið með starfsemi netöryggissveitarinnar í víðara samhengi, þ.e. að efla netheilsu og vernda netumdæmi Íslands. Í dag skortir almennt lagaumhverfi sem nánar útfærir slíkt verkefni með fastmótuðum hætti, veitir netöryggissveitinni nauðsynlegar heimildir og tryggir samstarf sveitarinnar t.a.m. við lögregluyfirvöld.

Í 2.-4. mgr. ákvæðisins er fjallað nánar um hlutverk netöryggissveitarinnar m.t.t. fjarskiptafyrirtækja. Kemur þar fram að sveitin skuli greina og meðhöndla ógnir, hættur og atvik í net- og upplýsingakerfum fjarskiptafyrirtækjanna. Hér kemur fram mikilvæg afmörkun á gildisviði ákvæðisins en um er að ræða net- og upplýsingakerfi fjarskiptafyrirtækja en ekki almenn fjarskiptanet þeirra sem slík. Til frekari skýringar á net- og upplýsingakerfum er átt við þau kjarnakerfi sem nauðsynleg eru svo almenn fjarskiptanet þeirra virki og þau geti veitt þjónustu sína. Netöryggissveitin hefur áfram það hlutverk að veita ráðgjöf um varnir og viðbúnað sem og að aðstoða fjarskiptafyrirtæki við forvarnir, leiðbeina þeim og styðja við skjót viðbrögð við netógnum. Hins vegar verður fjarskiptafyrirtækjum nú skylt að bregðast án tafa við tilmælum sveitarinnar um aðgerðir gegn bráðri aðsteðjandi netógn. Er þetta nýtt og í samræmi við 22. gr. frumvarpsins þar sem sama skylda er lögð á rekstraraðila nauðsynlegra innviða og stjórnarráðið. Vísast því til skýringa við það ákvæði frumvarpsins enda er um efnislega sömu skyldu að ræða.

Í 5. mgr. ákvæðisins er lögð sú skylda á netöryggissveitina að setja á laggirnar samstarfshóp með fjarskiptafyrirtækjum fyrir tæknilegt samráð og upplýsingaskipti á sviði

net- og upplýsingaöryggis, m.a. til að greina ógnir og samræma viðbrögð. Nú þegar er starfandi samráðshópur netöryggissveitarinnar og fjarskiptafyrirtækjanna. Hins vegar er talið nauðsynlegt að veita hópnum lögbundna stöðu til samræmis við ákvæði 2. mgr. 11. gr. frumvarpsins. Netöryggissveitin getur þá kallað þessa hópa saman eftir þörfum.

Í 6. mgr. er að finna skyldu á ráðherra til að mæla nánar fyrir um starfsemi sveitarinnar í reglugerð. Er ljóst að mörg reglugerðarákvæði er að nú þegar að finna í frumvarpinu og það er því eðlilegt að í reglugerð um netöryggissveitina sé jafnframt fjallað um hlutverk hennar samkvæmt fjarskiptalögum og getur slíkt verið í sömu reglugerð eða reglugerðum, enda er hlutverk netöryggissveitarinnar samræmt milli þessara aðila. Þá er nauðsynlegt að í reglugerðinni verði fjallað um samstarf við ríkislögreglustjóra. Í núgildandi lagaumhverfi skal sveitin að eiga samstarf við ríkislögreglustjóra og er nauðsynlegt að í reglugerð komi ákvæði um slíkt samstarf þ.e. um ógnir og atvik sem netöryggissveit telur að geti valdið, eða hafi valdið, tjóni í íslensku netumdæmi, þ.m.t. upplýsingainnviðum fjarskiptafyrirtækja, í þeim tilvikum þar sem þjóðaröryggi og almannaheill er í húfi. Að beiðni ríkislögreglustjóra skal netöryggissveitin viðhafa samstarf um varnir og viðbrögð í slíkum tilvikum.

Í nýrri 47. gr. b er kveðið á um skyldu fjarskiptafyrirtækja að gera, að beiðni netöryggissveitarinnar, samning við sveitina um uppsetningu og rekstur á vöktunarþjónustu. Hér er ekki um að ræða nýja skyldu enda segir í lokamálslið 3. mgr. núgildandi 47. gr. a að fjarskiptafyrirtækjum sé skylt að hýsa og samtengjast eftirlitsbúnaði netöryggissveitarinnar endurgjaldslaust. Með nýju ákvæði er þessi núgildandi skylda fjarskiptafyrirtækjanna samræmd nýju ákvæði 20. gr. frumvarpsins sem kveður á um sömu samningagerð mikilvægra innviða við netöryggissveitina. Með nýju ákvæði í fjarskiptalögum er því samræmt lagaumhverfi fyrir þá vöktun sem að netöryggissveitin skal sinna. Vísast til skýringa með 20. gr. frumvarpsins hvað þetta varðar. Aftur á móti er í 4. mgr. ákvæðisins að finna mikilvæga afmörkun þegar kemur að persónuvernd en nauðsynlegt er að árétta að netöryggissveitinni er óheimilt að persónugreina netumferð eða skima einstaka netpakka eða flæði sem að hún kann að nema í almennum fjarskiptakerfum fyrirtækjanna. Með þessu er tekið af skarið um að heimildir netöryggissveitarinnar ná ekki til almennra fjarskiptaneta fjarskiptafyrirtækjanna þar sem IP-umferð notenda fer í raun fram heldur ná heimildir sveitarinnar fyrst og fremst til IP-umferðar í og við net- og upplýsingakerfi fyrirtækjanna og þeirra kjarnakerfa sem nauðsynleg eru fyrir þau að veita almenna fjarskiptaþjónustu. Í ákvæðinu er sveitinni þó veitt heimild að fá upplýsingar um almenna netumferð enda séu þær upplýsingar ópersónugreindar.

Í nýrri 47. gr. c er að finna mjög veigamikið og nauðsynlegt ákvæði. Með ákvæðinu, sem er tilvísunarákvæði til 21., 24-26. gr. frumvarpsins. En tilgreind efnisákvæði skulu gilda, að breyttu breytanda, um starfsemi netöryggissveitarinnar samkvæmt fjarskiptalögum. Með þessum hætti er verið að innleiða í fjarskiptalög nauðsynleg ákvæði um upplýsingaöflun, vinnsluheimildir og þagnarskyldu netöryggissveitarinnar, þ.e. verið er að útvíkka þau til fjarskiptageirans. Þannig mun sama sértæka þagnarskylda, og undanþágur frá henni, eiga við um starfsemi sveitarinnar gagnvart fjarskiptageiranum. Sama má segja um vinnslu persónuupplýsinga. Er þetta nauðsynlegt til að tryggja að netöryggissveitin hafi viðeigandi heimildir til vinnslu persónuupplýsinga og miðlunar á þeim sem og að sömu takmörkunarákvæði nái til vinnslunnar samkvæmt fjarskiptalögum. Það er eðlilegt að þessi ákvæði séu samræmd yfir alla starfsemi netöryggissveitarinnar og vísast til skýringa með framangreindum ákvæðum.

Í 2. tölulið 34. gr. eru lagðar til breytingar á ákvæðum laga nr. 69/2003 um Póst- og fjarskiptastofnun. Er hér um að ræða nauðsynlega breytingu þar sem að frumvarpið kveður á um nýtt hlutverk stofnunarinnar. Er hér um að ræða eftirlitshlutverk með stafrænum

grunnvirkjum og stafrænum þjónustuveitendum samkvæmt ákvæðum frumvarpsins sem og hlutverk stofnunarinnar sem samhæfingarstjórnvald