PÓST- OG FJARSKIPTASTOFNUN
SUÐURLANDSBRAUT 4
108 REYKJAVÍK

SÍMI 510 1500 PÓSTUR PFS@PFS.IS
FAX 510 1509 VEFUR WWW.PFS.IS

Umhverfis- og samgöngunefnd Alþingis
b.t. Ingu Skarphéðinsdóttur, nefndarritara
Austurstræti 8-10
150 Reykjavík

Reykjavík, 18. janúar 2019

Málsnúmer: 2018120053
Skjalalykill: 15.3.4

Málefni: Umsögn Póst- og fjarskiptastofnunar um frumvarp til laga um öryggi net- og upplýsingakerfi mikilvægra innviða, þskj. 557 - 416. mál.

I.
Almennt

Póst- og fjarskiptastofnun vísar til tölvupósts nefndasviðs Alþingis, dags. 13. desember sl., þar sem óskað er umsagnar stofnunarinnar um frumvarp samgöngu- og sveitarstjórnarráðherra um öryggi net- og upplýsingakerfa mikilvægra innviða, sbr. þskj. 557 – 416. mál. Þakkar stofnunin fyrir að fá tækifæri til að koma á framfæri umsögn sinni um frumvarpið.

Póst- og fjarskiptastofnun fagnar því að fram sé komið frumvarp sem leggur í fyrsta lagi lágmarkskröfur um skipulag upplýsingaöryggis á mikilvæga innviða og í öðru lagi kveður á um skyldu þeirra til að tilkynna atvik til netöryggissveitar Póst- og fjarskiptastofnunar. Þá er í frumvarpinu kveðið á um starfsumhverfi netöryggissveitar, heimild hennar til upplýsingaöflunar, trúnað gagna og vinnsluheimildir m.t.t. persónuupplýsinga. Eins er netöryggisráði formaður lagalegur grundvöllur í frumvarpinu.

Með frumvarpinu eru Póst- og fjarskiptastofnun falin ný verkefni sem samhæfingarstjórnvaldi og sem eftirlitsstjórnvaldi með stafrænum grunnvirkjum og stafrænum þjónustuveitendum. Auk þess mun netumdæmi netöryggissveitar stofnunarinnar stóraukast enda eitt af yfirlýstum markmiðum með frumvarpinu að efla starfsemi hennar. Að mati Póst- og fjarskiptastofnunar felst í þessu mikil traustyfirlýsing til stofnunarinnar og þeirra starfa sem hún hefur unnið. Aftur á móti er ljóst að ef stofnunin á að geta sinnt þessum nýju lögbundnu verkefnum þarf hvort tveggja að tryggja henni fjármagn sem og viðeigandi heimildir sem **efla** netöryggissveitina í raun en leiða ekki einungis til stækkunar á netumdæmi hennar.
Verði frumvarpið að lögum er um að ræða ákveðið framfaraskref þegar kemur að netöryggismálum hér á landi. Enn er þó nokkuð langt í land þar til netöryggismálum hér á landi verði háttað með sambærilegum hætti og á hinum Norðurlöndunum.

Í ljósi vaxandi netógna á heimsvísu, þ.m.t. hér á landi, er að mati Póst- og fjarskiptastofnunar nauðsynlegt að búa svo um hnútana, hvað netöryggismál varðar, að viðnám gegn ógnum og viðbrögð hér á landi, á grundvelli þessa frumvarps, dugi í raun til að takast á við vandann. Okkar borgaralega stofnanaumhverfi er veikburða í þessu tilliti og vantar þætti sem gegna mikilvægu hlutverki erlendis. Því er það sérstaklega mikilvægt hérlendis að lagaumfrumvarp það sem hér

er til umfjöllunar sé þannig útfært að það geti nái utan um þau markmið sem að er stefnt. Að mati stofnunarinnar skortir nokkuð upp á frumvarpið svo að það náist.
Mikilvægt er að hafa í huga, í öllu samtali um þetta frumvarp, að þótt hin nauðsynlega þjónusta sem að frumvarpið nær til sé í mörgum tilvikum veitt af aðilum á markaði, er þjónustan nauðsynleg almannahagsmunum og almannaöryggi. Það eru því ríkir þjóðarhagsmunir, að stuðla að auknu öryggi þjónustunnar frá utanaðkomandi ógnum.

Í umsögn þessari mun Póst- og fjarskiptastofnun því leggja til tillögur að fimm **nauðsynlegum** breytingum á frumvarpinu. Telur stofnunin að í *fyrsta lagi* sé nauðsynlegt að gera ákveðnar breytingar á efni frumvarpsins er varðar starfsemi netöryggissveitarinnar svo sveitin verði fær um að sinna þeim verkefnum sem henni er ætlað samkvæmt frumvarpinu. Í *öðru lagi* þarf að lagfæra ákvæði er varða trúnað þeirra gagna sem að hún aflar eða fær afhent. Í *þriðja lagi* leggur stofnunin til smávægilegar breytingar á vinnsluheimildum sveitarinnar. Í *fjórða lagi* telur stofnunin nauðsynlegt að gera breytingar á ákvæði 7. gr. frumvarpsins er varðar öryggiskröfur sem gerðar eru til mikilvægra innviða. Í *fimmta lagi* er um að ræða breytingar á reglugerðarákvæðum er varða starfssemi netöryggissveitarinnar.

Að mati stofnunarinnar er um að ræða mikilvægar breytingar og verður gerð ítarleg grein fyrir tillögum stofnunarinnar í þessari umsögn og þær rökstuddar.

II.
Lágmarkssamræming NIS-tilskipunarinnar

Með frumvarpinu er ætlunin að innleiða ákvæði svokallaðar NIS-tilskipunar, þ.e tilskipunar Evrópuþingsins og ráðsins nr. 2016/1148 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í Sambandinu. Efni tilskipunarinnar kveður á um lágmarkssamræmingu innan Evrópusambandsins hvað varðar, í *fyrsta lagi* skipulag upplýsingaöryggis rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda sem og eftirlit með þeim og, í *öðru lagi* tiltekinna verkefna viðbragðsteyma vegna váatvika (netöryggissveita) í tengslum við framangreinda aðila.

Ljóst er að netöryggismál og starfsemi netöryggissveita eiga sér þó lengri sögu, hvort tveggja á vettvangi Evrópusambandsins sem og einstakra ríkja, þ.m.t. Norðurlandanna og Íslands. Staða netöryggismála innan ríkjanna er eðlilega mismunandi og byggir á ólíkum uppruna. Það er því, að mati Póst- og fjarskiptastofnunar, gríðarlega mikilvægt að túlka ekki efni NIS-tilskipunar sem almennan samnefnara fyrir skipulag og stöðu netöryggismála almennt meðal ríkja í Evrópu. Um er að ræða þær lágmarkskröfur sem Evrópusambandið hefur talið sér fært að gera til aðildarríkja sambandsins, til að tryggja skilvirka starfsemi innri markaðsins, án þess að stíga inn á viðkvæmari svið er varðar öryggismál þeirra. Það verður því að horfa til þeirrar reynslu sem þegar er til staðar, hvort tveggja hér á landi og í helstu nágrannaríkum okkar, t.a.m. á Norðurlögnunum,[1] sem og framtíðarsýnar og bestu framkvæmdar á sviði netöryggismála þegar unnið er að lagasetningu á sviði netöryggismála hér á landi.

Það frumvarp sem nú liggur fyrir Alþingi gengur ekki lengra en sem nemur ákvæðum tilskipunarinnar og, að mati stofnunarinnar, á tíðum með þrengri hætti en tilskipunin sjálf gerir ráð fyrir. Á það einkum við um starfsemi netöryggissveitarinnar og heimildir hennar til að afla nauðsynlegra upplýsinga svo hún geti sinnt því mikilvæga og lögbundna starfi að nema ógnir

[1] Sjá viðauka I við umsögn þessa. *Minnisblað - Stutt samantekt um stöðu netöryggissveita og innleiðingu NIS-tilskipunar á Norðurlöndum.*

og áhættur sem stafa að net- og upplýsingakerfum mikilvægra innviða. Frumvarpið er ekki afdráttarlaust þegar kemur það þessu hlutverki sveitarinnar. Leggur frumvarpið fyrst og fremst áherslu á starf sveitarinnar sem samhæfingaraðila og leiðbeinanda þegar kemur að viðbrögðum við atvikum í kerfum aðilanna en skortir heimildir til að geta eflt viðnám við ógnum og mögulega komið í veg fyrir atvik í net- og upplýsingakerfum mikilvægra innviða. Mun stofnunin gera nánar grein fyrir þessu síðar í umsögn þessari.

III.
Núverandi starfsumhverfi netöryggissveitar

3.1 Almennt

Áður en athugasemdir verða settar fram er nauðsynlegt að gera grein fyrir því umhverfi sem netöryggissveitin starfar nú í lögum samkvæmt og varpa ljósi á þá reynslu sem hefur skapast. En Póst- og fjarskiptastofnun hefur starfrækt netöryggissveit (CSIRT-teymi) Íslands frá árinu 2012, sbr. ákvæði 47. gr. a í fjarskiptalögum, sbr. einnig lög nr. 62/2012, um breytingu á fjarskiptalögum. Þá starfar sveitin á grundvelli reglugerðar nr. 475/2013, um málefni CERT-ÍS netöryggissveitar.

3.2 Lögbundið hlutverk netöryggissveitar

Samkvæmt núgildandi lögum 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 einungis til hins takmarkaða 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 tilkynnt til 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.

Þannig er netöryggissveitinni ætlað mikilvægt hlutverk þegar kemur að upplýsingaöryggi fjarskiptaneta og annarra ómissandi upplýsingainnviða[2] hér á landi. Almennt má segja að ómissandi upplýsingainnviðir nái til t.a.m. fjármálastofnananna, rafmagnsframleiðenda og -dreifiaðila, aðila er koma að dreifingu neysluvatns sem og hitaveitna, stærri heilbrigðisstofnana,

[2] Ómissandi upplýsingainnviðir eru skilgreindir í 27. tl. 3. gr. fjarskiptalaga nr. 81/2003: *„Upplýsingakerfi 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.“*

stærri aðila á sviði flutninga og samgangna o.fl. Í raun má segja að hér sé um sambærilega aðila að ræða og sem teljast nú mikilvægir innviðir í skilningi frumvarpsins og NIS-tilskipunarinnar.

Þannig byggir núgildandi ákvæði á því svokallað netumdæmi netöryggissveitarinnar nái til fjarskiptafyrirtækja og rekstraraðila ómissandi upplýsingainnviða að því tilskyldu þó að hinir síðarnefndu hafi undirritað þjónustusamning við sveitina. Í slíkum þjónustusamningi yrði því fjallað um samstarf, upplýsingaflæði milli aðila o.fl. Fram til þessa hefur ekki verið undirritaður þjónustusamningur milli netöryggissveitarinnar og rekstraraðila ómissandi upplýsingainnviða.[3] Hefur það reynst mikil hindrun í uppbyggingu öflugs og heildstæðs netöryggis hér á landi og leitt til skorts á yfirsýn sveitarinnar á raunverulegri ógnarmynd varðandi ómissandi upplýsingainnviði hér á landi sem og skorts á samstarfi og upplýsingaskiptum þessara aðila og sveitarinnar.

Að mati Póst- og fjarskiptastofnunar hefur núgildandi lagaumhverfi því ekki virkað sem skyldi. Því er nauðsynlegt nú að breytingarnar á lagaumhverfi netöryggissveitarinnar komi á þessu samstarfi sveitarinnar og mikilvægra innviða. Slíkt samstarf byggist að miklu leyti á veitingu upplýsinga. Því verður að tryggja lágmarks upplýsingaflæði milli aðila svo að raunverulegt markmið með starfsemi hennar náist, þ.e. að tryggja með sem bestum hætti virkni nauðsynlegrar þjónustu hér á landi, almannaöryggi og almannahagsmuni, fyrir einni aðgangshörðustu ógn okkar tíma, netógnum af ýmsu tagi.

Að mati Póst- og fjarskiptastofnunar er því nauðsynlegt að herða upp á frumvarpi því sem nú er til umfjöllunar í ljósi reynslu stofnunarinnar og netöryggissveitarinnar undanfarin ár og tryggja með afdráttarlausum hætti ákveðnar nauðsynlegar forsendur raunverulegri eflingu á starfi sveitarinnar.

3.3 Persónuupplýsingar hjá netöryggissveit

Ekki verður fjallað um starfsemi netöryggissveita og aðgengi þeirra að upplýsingum án þess að gera grein fyrir samspili þess við persónuverndarlög og meðferð persónuupplýsinga. Þær upplýsingar sem að netöryggissveitir vinna með, og eru grundvallarforsenda fyrir starfi þeirra, eru almennt séð persónugreinanlegar upplýsingar. Hér vegast því á ákveðnir hagsmunir varðandi almannaöryggi og friðhelgi einkalífs sem persónuvernd byggir á.

Ný persónuverndarlöggjöf í Evrópu tekur á þessu hagsmunamati að ákveðnu leyti þar sem að tilgreint er sérstaklega í 49. formálslið GDPR[4] að „[v]*innsla persónuupplýsinga, að því marki sem hún er beinlínis nauðsynleg og hófleg til að tryggja net- og upplýsingaöryggi,* [...] *telst til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna.*“

Að mati Póst- og fjarskiptastofnun er nauðsynlegt að finna rétt jafnvægi milli framangreindra hagsmuna. Verður það hvort tveggja gert með því að afmarka með réttum hætti heimildir netöryggissveitarinnar til aðgangs að upplýsingum og með því að setja ákveðna varnagla við vinnslu upplýsinganna og tryggja að hún sé í samræmi við persónuverndarlög. Er slíkt reynt í gildandi ákvæði 47. gr. a í fjarskiptalögum og í áðurnefndri reglugerð um málefni sveitarinnar

[3] Einungis hefur verið undirritaður samningur milli Póst- og fjarskiptastofnunar (netöryggissveitar) og fjármálaráðuneytis vegna Stjórnarráðs Íslands, svo kallaður GovCERT samningur. Hann var undirritaður í janúar 2018. Frumvarpið lögfestir í raun þann samning, sbr. 3. mgr. 16. gr. frumvarpsins.

[4] Reglugerð Evrópuþingsins og ráðsins 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin).

er mikið fjallað um heimildir og meðferð sveitarinnar á þessum upplýsingum, sbr. IV. kafli hennar.

Hins vegar er ljóst að endurskoða þarf lagaumhverfið með tilliti til nýrrar persónuverndarlöggjafar líkt og gert er í frumvarpinu.[5] Telur stofnunin að í ákvæði um vinnsluheimildir netöryggissveitarinnar í 21. gr. frumvarpsins sé að finna ákvæði sem tryggir með sem bestum hætti framangreint jafnvægi. Er það í nokkru samræmi við lagaumhverfi dönsku netöryggissveitarinnar.

Í 1. mgr. ákvæðisins er sú vinnsluheimild sem starf sveitarinnar byggir á.[6] Þar eru vinnsluheimildir sveitarinnar takmarkaðar við það hlutverk sem henni er ætlað á grundvelli frumvarpsins. Frumvarpið gildir um þau kerfi sem eru nauðsynleg mikilvægum innviðum við veitingu þjónustu sinnar. Því er einungis um að ræða upplýsingar, t.d. IP-tölur, sem varða þau kerfi en nær með engum hætti til almennrar umferðar á internetinu. Á það jafnframt við um fjarskiptafyrirtækin en ekki er heimild til að vakta almenna netumferð. Er að finna sérstakt ákvæði í frumvarpinu sem bannar slíkt, sbr. 4. mgr. nýrrar 47. gr. b, sbr. b. liður 2. tölul. 27. gr. frumvarpsins.[7]

Má einnig nefna að sveitinni er einungis heimilt að miðla upplýsingunum sé það í *þágu þjóðaröryggis eða almanna hagsmuna*. Sú miðlun verður einnig að vera til þess fallin að upplýsa um aðsteðjandi ógnir, til að koma í veg fyrir nátárás, til að takmarka umfang hennar eða tjón. Þá er sveitinni óheimilt að skoða einstaka sendingar án *rökstudds grunar* um að hún innihaldi spillikóða og *að fengnu samþykki* mikilvægs innviðar.

Þá kemur skýrt fram í 3. mgr. ákvæðisins að öll vinnsla skuli vera í samræmi við ákvæði nýrra laga um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018. Þannig verður öll meðferð, þ.m.t. geymsla, öryggi og eyðing, upplýsinganna að vera í samræmi við persónuverndarlög. Einungis eru gerð tillaga að undanþágu frá ákvæðum persónuverndarlögunum þegar kemur að 1.-4. þáttum III. kafla GDPR, en slíkar undanþágur eru heimilar á grundvelli 5. þáttar kaflans. Hefur meiri hluti allsherjarnefndar Alþingis nú þegar fjallað um möguleika netöryggissveitar Póst- og fjarskiptastofnunar til að vera undanþegin þessum þáttum persónuverndarlöggjafarinnar.[8]

Að mati Póst- og fjarskiptastofnunar hefur verið leitast við í frumvarpinu að tryggja rétt jafnvægi milli vinnslu persónuupplýsinga, meðferð þeirra, öryggi og eyðingu og friðhelgi einkalífs í samræmi við heimildir persónuverndarlöggjafarinnar sjálfrar.

---

[5] Í viðauka II er að finna umsögn Póst- og fjarskiptastofnunar til allsherjarnefndar, dags. 4. júní 2018, um frumvarp til laga um persónuvernd og vinnslu persónuupplýsinga þingskjal nr. 1026 — 619. mál á 148. löggjafarþingi. Umsögnin varpar nokkru ljósi á þær vinnslur sem að eiga sér stað hjá netöryggissveitinni.

[6] Í 2. mgr. 21. gr. frumvarpsins er að finna vinnsluheimild sem nær til atvika þar sem að netöryggissveitinni berast upplýsingar vegna atvika. Hér getur t.a.m. verið um að ræða kortaupplýsingar, lykilorð o.fl. sem að hafa verið andlag árásar. Var þetta raunin í innbroti sem gert var á vefsíðu Vodafone í desember 2013. Netöryggissveitin hafði ekki sérstaka lagaheimild til að miðla þessum upplýsingum, t.a.m. til fjármálastofnanna, án samþykkis hins skráða. Í 2. mgr. 21. gr. er því í raun verið að heimila netöryggissveit til að miðla slíkum upplýsingum til að vernda hagsmuni hins skráða.

[7] Einungis er gerð ein undantekning á því, þá er það umferðarupplýsingar á samtengipunktum og í útlandagáttum enda séu þær upplýsingar þá ópersónugreinanlegar.

[8] Vísar Póst- og fjarskiptastofnun til nefndarálits meirihluta allsherjarnefndar um frumvarp til laga um persónuvernd og vinnslu persónuupplýsinga þingskjal nr. 1026 — 619. mál á 148. Löggjafarþingi. Vísast sérstaklega til 5. mgr. í umfjöllun um meginreglur um gagnsæi upplýsinga, rétt hins skráða til upplýsinga og aðgangs og undantekningar frá honum (17. gr.) í álitinu.

IV.
Athugasemdir Póst- og fjarskiptastofnunar og breytingartillögur

4.1 Almennt

Líkt og áður segir leggur Póst- og fjarskiptastofnun til fimm breytingar á ákvæðum frumvarpsins. Varða þær breytingar að mestu leyti starfsemi netöryggissveitarinnar, þ.e. heimildir til öflunar upplýsinga og trúnað þeirra.[9] Þá leggur stofnunin einnig til smávægilega breytingu varðandi ákvæði 21. gr. frumvarpsins. Þá telur stofnunin jafnframt nauðsynlegt að gera breytingar á orðalagi 7. gr. frumvarpsins sem og reglugerðarákvæðum þess. Verða nú færð fram rök fyrir framangreindu og breytingartillögur settar fram.

4.2 Athugasemdir er varðar starfsemi netöryggissveitar

4.2.1 Aðgangur að nauðsynlegum upplýsingum er ekki tryggður

Að mati Póst- og fjarskiptastofnunar tryggir frumvarpið ekki aðgengi netöryggissveitar að upplýsingum sem henni eru nauðsynlegar til að geta uppfyllt hlutverk sitt samkvæmt frumvarpinu.

Með frumvarpinu verða rekstaraðilar mikilvægara innviða (aðrir en fjarskiptafyrirtæki) hluti af netumdæmi sveitarinnar í stað valkvæðs samnings þessara aðila við netöryggissveitina á grundvelli núgildandi laga. Hins vegar, þegar að er gáð, er óvíst að það breyti núverandi ástandi og starfsumhverfi netöryggissveitarinnar m.t.t. aðgengis að upplýsingum.

Ýmsar leiðir eru færar til að tryggja slíkt, t.a.m. með ákveðinni fyrirfram skilgreindri vöktun við kerfi mikilvægs innviðar, sbr. 2. mgr. 16. gr. eða með ákveðnu sjálfvirku upplýsingaflæði frá mikilvægum innviðum líkt og 2. mgr. 17. gr. kveður á um. Hér er áréttað að einungis er verið að ræða upplýsingaflæði í og við þau kerfi mikilvægs innviðar sem eru skilgreind sem nauðsynleg við veitingu þjónustu hans. Með engum hætti má leggja þann skilning í að hér sé um að ræða almenna netumferð á Internetinu.

Frumvarpið fjallar því um báðar þessar leiðir en tryggir þó ekki aðgengi sveitarinnar að nauðsynlegum upplýsingum með ótvíræðum hætti. Í 2. mgr. 16. gr. er netöryggissveitinni veitt heimild til að bjóða upp á vöktunarþjónustu á nánar skilgreindum og skjalfestum forsendum, þ.e. á grundvelli samnings. Það er í reynd óbreytt ástand miðað við núgildandi lög.

Þá er í 2. mgr. 17. gr. frumvarpsins kveðið á um að Póst- og fjarskiptastofnun geti „ ... *óskað eftir að komið skuli upp sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi mikilvægra innviða og netöryggissveitar.*“ Að mati Póst- og fjarskiptastofnunar er þetta ákvæði alltof óljóst. Hvað felst í því að sveitinni sé heimilt að *óska eftir*? Er rekstraraðila skylt að verða við slíkri ósk? Ekki er að finna neinar skýringar við ákvæðið í greinargerð frumvarpsins hvað þetta varðar.

Póst- og fjarskiptastofnun telur alltof óljóst hvernig túlka ber þetta ákvæði 2. mgr. 17. gr. Það að frumvarpið kveði einungis á um það að stofnunin geti óskað eftir upplýsingum, þ.e. í formi sjálfvirkrar upplýsingamiðlunar á milli kerfa, en er þögult um skyldu aðila til að verða við slíkri ósk og útfærslu á þessari upplýsingamiðlun er ekki tækt að mati stofnunarinnar. Býður þetta orðalag uppá þá túlkun að mikilvægum innviðum sé í raun ekki skylt að verða við þessari ósk sveitarinnar.

---

[9] Hér er verið að fjalla um trúnað upplýsinga, skv. sérstöku þagnarskylduákvæði 19. gr. en ekki vinnslu persónuupplýsinga skv. 21. gr. frumvarpsins.

Þannig er í raun engu breytt frá núgildandi lögum þar sem netöryggissveit er sett í þá stöðu að þurfa að biðla til aðila um upplýsingar til að geta sinnt því hlutverki sem stjórnvöld hafa skyldað hana að sinna samkvæmt lögum. Slíkt hefur ekki borið árangur til þessa og leiðir til þess að netöryggissveitin getur tæplega uppfyllt það hlutverk sem henni er sett samkvæmt lögum.

Upplýsingar eru nauðsynleg forsenda þess að netöryggissveitin geti sinnt hlutverki sínu. Því hlutverki sem Alþingi markaði sveitinni árið 2012 og samgöngu- og sveitarstjórnarráðherra hefur lagt til að verði áfram. Því verður að veita sveitinni viðhlítandi verkfæri til að sinna þessu mikilvæga verkefni. Að mati Póst- og fjarskiptastofnunar skortir verulega í þá verkfærakistu í frumvarpinu og er ekki tekið mið af reynslu síðastliðnu tæpra sjö ára. En sú reynsla sýnir með ótvíræðum hætti að þjónustusamningsleiðin hefur ekki reynst nægjanleg til að efla starfsemi sveitarinnar eða til að tryggja aðgengi að upplýsingum. Ef það er áframhaldandi vilji stjórnvalda og Alþingis að byggja upp netöryggi efnahagslegra og samfélagslegra grunnþátta íslensks samfélags þá verður að taka mið af þeirri reynslu og tryggja netöryggissveitinni aðgengi að upplýsingum.

Póst- og fjarskiptastofnun telur fullkomlega eðlilegt, og ætlast ekki til annars, en að útfærsla á því með hvaða hætti upplýsingar séu veittar byggist á samkomulagi við hlutaðeigandi mikilvægan innvið enda ljóst að samstarf og samkomulag er lykilatriði svo árangur náist. Aðalatriðið er hins vegar að netöryggissveitin fái þær nauðsynlegu upplýsingar sem hún þarf til að finna ógnir, áhættur og atvik svo hægt sé að bregðast við þeim eða koma í veg fyrir atvik eða takmarka tjón þeirra. Hér skiptir tímasetning á aðgengi sveitarinnar að upplýsingunum gríðarmiklu máli.

Skylda til að veita upplýsingar, sem yrði þá útfærð fyrir hvern og einn aðila, er ekki eingöngu forsenda þess að netöryggissveitin geti uppfyllt lagaskyldur sem á henni hvíla heldur jafnframt forsenda þess að byggja megi um öflugt netöryggisumhverfi hér á landi.

Eðlilegt er að upplýsingamiðlun sé sem sjálfvirkust og í samræmi skilgreindar viðmiðanir sveitarinnar þar um. Þannig er hér um að ræða sjálfvirkar tilkynningar frá mikilvægum innviðum, um þegar skilgreinda atburði sem byggja þá á umræddum viðmiðunum sveitarinnar t.d. helstu vísa sem sveitin hefur fengið tilkynningar um að séu óvinveittir. Upplýsingaflæði sem þetta yrði ávallt úrfært með tilliti til einstakra aðila og er val á aðferð til miðlunar upplýsinganna aðlöguð rekstri hans og uppbyggingu á kerfi.

Þá er eins mikilvægt að hafa í huga að upplýsingamiðlun sem þessi er í raun í formi ákveðnar tilkynningar rekstraraðila og innihalda almennt ekki frumgögn samskipta, upplýsingar um einstök kerfi innan veggja rekstraraðilans eða starfsmenn hans. Úrvinnsla af sjálfvirkri upplýsingamiðlun sem þessari felst í því að netöryggissveitin gerir viðkomandi aðila viðvart um mögulega ógn, áhættu eða að atvik hafi átt sér stað. Eins getur sveitin gefið út viðvaranir á grundvelli úrvinnslunnar, hvort heldur til tiltekinna aðila, svo sem annarra mikilvægra innviða eða almennings, svo þeir geti gripið til viðeigandi ráðstafana. Líkt og með alla vinnslu netöryggissveitarinnar á gögnum yrði farið að ákvæðum V. kafla frumvarpsins. Þannig gæti, ef að grunur leikur á um að ógn sé til staðar eða árás yfirvofandi, netöryggissveitin skoðað ítarlegir gögn svo sem ákveðna samskiptalogga og eftir atvikum innihald einstakra pakka, með samþykki rekstraraðilans.

4.2.2 Gagnrýnisraddir hagsmunaaðila

Líkt og fram kemur í almennum athugasemdum við frumvarpið sem og í niðurstöðuskjali samráðs þess sem viðhaft var í samráðsgátt Stjórnarráðsins komu fram gagnrýnisraddir frá

hagsmunaaðilum á frumvarpsdrögin en þar var kveðið á um skyldubundna samningsgerð um vöktunarþjónustu. Getur Póst- og fjarskiptastofnun tekið undir þær athugasemdir að nokkru leyti þar sem ákvæðið var ekki nægjanlega afdráttarlaust um að sú vöktunarþjónusta gæti t.a.m. falist í hvers kyns upplýsingamiðlun milli aðila. Það var í raun samningsatriði þó skylda til samnings (og þar með upplýsingagjafar) hafi verið skýr. Þannig gat upplýsingagjöf verið í formi sjálfvirkrar upplýsingagjafar frá mikilvægum innviði[10] eða með uppsetningu vöktunarbúnaðar við kerfi innviðarins eða öðrum búnaði í eigu aðilans[11], en ekki einungis í formi skynjarakerfis, eins og gagnrýnin virtist að mestu lúta að.

Þá kemur fram í athugasemdum frumvarpsins og framangreindu niðurstöðuskjali að komið hafi verið á móts við þessar athugasemdir hagsmunaaðila. Hins vegar var það skilningur Póst- og fjarskiptastofnunar að hagsmunaaðilar hafi ekki verið að andmæla upplýsingagjöf til netöryggissveitarinnar sem slíkri, heldur fyrst og fremst að vera skyldaðir eina leið upplýsingagjafar, þ.e. í uppsetningu skynjara. Slíkt var þó ekki ætlunin miðað við frumvarpsdrögin.

Áréttar stofnunin mikilvægi samstarfs og aðlögun form upplýsingagjafar m.t.t. þarfa hvers og eins mikilvægs innviðar.

4.2.3 Kröfur viðauka 1 við NIS-tilskipunina

Þá er einnig ljóst að 1. viðauki NIS-tilskipunarinnar sjálfrar kveður á um það lágmarkshlutverk viðbragðsteyma, líkt og netöryggissveitarinnar, að senda snemmviðvaranir, viðvörunarmerki og tilkynningar um áhættur og atvik, sbr. ii. liður a. liðar 2. tölul. viðaukans, og *„ ... að veita virka greiningu á áhættum og atvikum og næmni á aðstæðum (ógnarmynd[12])*.[13] Að sama skapi og áður hefur verið greint frá getur Póst- og fjarskiptastofnun ekki séð hvernig uppfylla skuli þessar skyldur tilskipunarinnar án afdráttarlauss aðgangs að nauðsynlegum lágmarksupplýsingum frá aðilum, með hvaða tæknilegu útfærslu þær yrðu svo veittar. Frumvarpið er því tæplega að ná að uppfylla þessi markmið NIS-tilskipunarinnar.

Í raun þarf frumvarpið að tryggja að virkri miðlun upplýsinga sé komið á frá rekstraraðilum mikilvægra innviða til sveitarinnar svo henni sér fært að greina ógnir, áhættur og atvik við kerfi þeirra. Sé það ekki vilji stjórnvalda, líkt og fram kemur í athugasemdum við frumvarpið, að feta þann veg að leggja skyldu á mikilvæga innviði um tæknilega vöktunarþjónustu, t.a.m. með skynjurum eða öðrum búnaði á kerfi aðilans, þá þarf a.m.k. að gera sjálfvirka upplýsingamiðlun, sbr. 2. mgr. 17. gr., að skýrri skyldu og ekki gefa svigrúm fyrir aðra túlkun á ákvæðinu.

Þá bendir Póst- og fjarskiptastofnun á ákveðið ósamræmi í frumvarpinu varðandi öflun upplýsinga frá fjarskiptafyrirtækjum annars vegar og frá mikilvægum innviðum hins vegar. Frumvarpið kveður á um ákveðnar breytingar á lögum um fjarskipti í stað núgildandi 47. gr. a. Í núgildandi lögum er kveðið á um skyldu fjarskiptafyrirtækja til að hýsa og samtengjast eftirlitsbúnaði netöryggissveitarinnar endurgjaldslaust. Í tillögu að nýju ákvæði 47. gr. b í

[10] Sambærilegt því sem 2. mgr. 17. gr. Frumvarpsins gerir nú ráð fyrir.
[11] Sambærilegt því sem 2. mgr. 16. gr. Frumvarpsins gerir nú ráð fyrir.
[12] Hugtakið „ógnarmynd" er viðbót PFS en það gefur betri mynd en „næmni á aðstæðum" sem er bein þýðing á enska hugtakinu „situational awareness".
[13] Mikilvægt er að gera grein fyrir því að í þessum hugtökum; *snemmviðvaranir, viðvörunarmerki* og *tilkynningar*, felast ákveðnar merkingar innan Evrópusambandsins og hjá ENISA. Fela þau í sér hvort tveggja "ractive" og "proactive" hlutverk til handa viðbragðsteymum vegna váatvika. ENISA hefur í fjölda skýrslna gert grein fyrir merkingu og tilgangi þessara hugtaka sem og hlutverki viðbragsteyma hvað það varðar. Má hér t.a.m. nefna skýrslu ENISA frá 2011 – *Proactive Detection of Network Security Incidents* og skýrslu ENISA frá 2013 – *Alerts, Warnings and Announcements.* Sjá einnig á heimasíðu ENISA: https://www.enisa.europa.eu/topics/csirt-cert-services?tab=details.

fjarskiptalögum, sbr. b. liður 2. tölul. 27. gr. frumvarpsins, veitir ákvæðið netöryggissveitinni heimild til að móttaka upplýsingar á grundvelli samnings um vöktunarþjónustu án dómsúrskurðar. Ekki er kveðið á um sambærilegt vegna mögulegra samninga netöryggissveitarinnar við mikilvæga innviði vegna tæknilegrar vöktunarþjónustu eða sjálfvirkrar upplýsingagjafar, sbr. 2. mgr. 16. gr. og 2. mgr. 17. gr. frumvarpsins. Gæti þetta leitt til ákveðins ómöguleika á framkvæmd þeirra ákvæða.

4.2.4 Tillaga að ákvæði 2. mgr. 17. gr.
Á grundvelli framangreinds leggur Póst- og fjarskiptastofnun til að gerðar verði breytingar á 2. mgr. 17. gr. þannig að tekinn yrði af allur vafi um rétt netöryggissveitar að nauðsynlegum upplýsingum og skyldu viðkomandi mikilvægs innviðar að veita aðgengi að þeim með sjálfvirkri upplýsingamiðlun líkt og að framan hefur verið líst. Leggur stofnunin til að 2. mgr. 17. gr. frumvarpsins orðist svo:

Til að greina og meta ógnir, áhættur og atvik við kerfi mikilvægs innviðar getur netöryggissveit ákveðið, eftir eðli mikilvægs innviðar, að komið skuli upp sjálfvirkri upplýsingamiðlun milli hlutaðeigandi innviðar og sveitarinnar. Tæknileg útfærsla slíkrar upplýsingaöflunar skal ákveðin í samráði við mikilvægan innvið, eftir því sem kostur er.

4.3 Þagnarskylduákvæði
Póst- og fjarskiptastofnun telur að sérstakt þagnarskylduákvæði 19. gr. frumvarpsins sé of þröngt og nái ekki til ákveðinna gagna hjá netöryggissveit sem nauðsynlegt er að sé undanskilin almennri meginreglu upplýsingalaga um aðgang. Þá er ákveðið ósamræmi milli 19. og 20. gr. frumvarpsins.

Ákvæðið kveður á um sérstaka þagnarskyldu umfram þá sem greinir í 18. gr. laga nr. 70/1996, um réttindi og skyldur starfsmanna ríkisins. Nær það til alls starfsfólks eftirlitsstjórnvalda, samhæfingarstjórnvalds, netöryggissveitar og netöryggisráðs. Þá segir í athugasemdum við ákvæðið að um sé að ræða sérstakt þagnarskylduákvæðið gagnvart ákvæðum upplýsingalaga nr. 140/2012, og að það taki „ *... 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.*“

Í 3. mgr. 4. gr. upplýsingalaga nr. 140/2012 segir að almenn ákvæði laga um þagnarskyldu takmarka ekki rétt til aðgangs að gögnum samkvæmt lögunum. Í framkvæmd hefur verið gagnályktað frá þessu ákvæði og sérstök þagnarskylduákvæði laga þar með talin takmarka rétt til aðgangs samkvæmt upplýsingalögum, sbr. t.d. nýlega úrskurði úrskurðarnefndar upplýsingamála nr. 769/2018, 607/2016 og 614/2016 og dóm Hæstaréttar í máli nr. 329/2014. Það er því eðlilegt að í frumvarpinu sé kveðið á um sérstaka þagnarskyldu.

Að mati Póst- og fjarskiptastofnunarinnar þarf að víkka gildissvið hins sérstaka þagnarskylduákvæði til að tyggja trúnað upplýsinga sem netöryggissveitin fær afhent sem CSIRT-teymi Íslands. Hér vísast til allra þeirra trúnaðargagna sem að sveitin fær í gegnum alþjóðlegt samstarf netöryggissveita, í gegnum erlenda gagnastrauma og á grundvelli ábendinga og tilkynninga t.d. frá almenningi. Alþjóðlegt samstarf á sviði netöryggismála byggir á gagnkvæmu trausti og trúnaði um gögn sem miðlað er. Slíkt, ásamt aðgengi að gagnastraumum og erlendum upplýsingaveitum, sem sveitin byggir nú starf sitt að miklu leyti á, yrði sjálfhætt ef minnsti vafi léki á um að trúnaður gagnanna væri ekki tryggður.

Eins og ákvæðið er orðað núna, ásamt skýringum við ákvæðið, nær það einungis til upplýsinga frá mikilvægum innviðum. Hins vegar er í 2. mgr. 20. gr. frumvarpsins er gert ráð fyrir ákveðnum undanþágum frá sérstöku þagnarskyldu 19. gr. sem varða alþjóðlegt samstarf og upplýsingaskipti t.a.m. við erlenda gagnastrauma, þ.e. aðilum eða sérfræðingum sem sinna net- og upplýsingaöryggi. Ákveðið ósamræmi er því milli ákvæðanna sem bregðast þarf við.

Póst- og fjarskiptastofnun leggur því til breytingar á ákvæðinu því til samræmis. Ákvæðið myndi því orðast svo (viðbót er undirstrikuð):

> ***Starfslið eftirlitsstjórnvalda, hvert á sínu sviði, samhæfingarstjórnvalds, netöryggissveitar og netöryggisráðs er bundið sérstakri þagnarskyldu umfram þá sem greinir í lögum um réttindi og skyldur starfsmanna ríkisins. Starfsliðið má ekki, að viðlagðri ábyrgð, skýra óviðkomandi frá því sem það kemst að í starfi sínu og leynt á að fara. Starfsmenn netöryggissveitar Póst- og fjarskiptastofnunar eru bundnir þagnarskyldu um þau gögn og upplýsingar sem netöryggissveitin hefur undir höndum, hefur aðgang að eða vinnur með og sem þeir fá vitneskju um í starfi. Þagnarskyldan helst þótt látið sé af starfi.***

4.4 Viðbót við ákvæði 21. gr. um vinnslu persónuupplýsinga

Póst- og fjarskiptastofnun leggur til smávægilegar breytingar á ákvæði 21. gr. frumvarpsins er varðar vinnsluheimildir sveitarinnar. Um er að ræða breytingu sem tryggir heimildir sveitarinnar til að vinna með persónuupplýsingar sem sveitin kann að fá aðgang að frá innlendum og erlendum samstarfsaðilum á sviði netöryggis. Slíkt ákvæði er nauðsynlegt vegna alþjóðasamstarfs, t.d. þegar hún fær upplýsingar um þekktar áraásar IP-tölur. Slíkar upplýsingar geta jafnframt komið frá erlendum gagnastraumum eða innlendum aðilum.

Leggur stofnunin til að 1. mgr. ákvæðisins orðist svo (viðbót er undirstrikuð):

> ***Netöryggissveit er heimil vinnsla persónuupplýsinga að því marki sem nauðsynlegt er til að hún geti sinnt hlutverki sínu samkvæmt lögum þessum. Í því felst meðal annars móttaka persónuupplýsinga frá aðilum sem ákvæði laga þessara gilda um og frá innlendum og erlendum samstarfsaðilum, sem og miðlun þeirra til viðeigandi þriðju aðila, án samþykkis hins skráða, ef netöryggissveit metur það nauðsynlegt í þágu þjóðaröryggis eða almannahagsmuna og vinnslan er til þess fallin að upplýsa um aðsteðjandi ógnir, koma í veg fyrir netárás eða önnur alvarleg atvik eða til að takmarka útbreiðslu eða draga úr tjóni vegna slíkra tilvika. Ef rökstuddur grunur er um að einstakar sendingar innihaldi spillikóða er netöryggissveit heimilt, með samþykki mikilvægra innviða og án samþykkis hins skráða, að greina efni einstakra fjarskiptasendinga til og frá neti mikilvægra innviða.***

4.5 Lágmarkskröfur á grundvelli 7. gr.

Í 7. gr. frumvarpsins er fjallað um þær lágmarkskröfur sem gerðar eru til net- og upplýsingaöryggis mikilvægra innviða. Ákvæðinu er ætlað að innleiða 14. og 16. gr. NIS-tilskipunarinnar. Í 1. mgr. 14. gr. segir orðrétt að „[a]*ðildarríki skulu tryggja að rekstraraðilar nauðsynlegrar þjónustu geri viðeigandi og hóflegar tæknilegar og skipulagslegar ráðstafanir til að stýra þeirri áhættu sem steðjar að öryggi þeirra net- og upplýsingakerfa sem þeir nota í starfsemi sinni. Þær ráðstafanir skulu vera með hliðsjón af nýjustu tækni á því sviði og tryggja hæfilegt öryggisstig í net- og upplýsingakerfum miðað við þá áhættu sem getur skapast.*“

Orðalag tilskipunarinnar á sér lengri sögu í löggjöf Evrópusambandsins sem almennt lágmarksákvæði um skipulag upplýsingaöryggis og lágmarkskrafna á aðila. Það er t.a.m. samhljóða orðalagi 13. gr. a í núgildandi Rammatilskipunar á sviði fjarskipta og 4. gr. persónuverndartilskipunar á sviði fjarskipta.[14] Þá er sama orðalag notað í eldri persónuverndartilskipun Evrópusambandsins frá 1995, nýrri GDPR og nýrri heildarlöggjöf á sviði fjarskipta sem taka á gildi á þessu ári innan ESB.[15]

Íslensk löggjöf á sviði fjarskipta og persónuverndar hefur verið nokkuð samhljóða framangreindum viðeigandi ákvæðum, sbr. 47. gr. fjarskiptalaga[16] og 23. gr. nýrra persónuverndarlaga. Póst- og fjarskiptastofnun hefur því sinnt eftirliti með ákvæði sem þessu í yfir áratug og hefur byggst upp framkvæmd á beitingu þessa orðalags og krafna hjá stofnuninni í gegnum árin hvort tveggja er varðar raunlægt öryggi sem og kerfislægt öryggi.[17]

Póst- og fjarskiptastofnun telur að núverandi orðalag 1. mgr. 7. gr. frumvarpsins skapi óþarfa rugling um til hvers sé ætlað í öryggisskipulagi mikilvægra innviða og feli í raun í sér tvenns konar kröfur. Málsgreining nú fjallar hvort tveggja um skjalfestingu stefnu og ferla til að meta, stýra og lágmarka áhættu sem steðjað getur að kerfum þeirra sem og að þeir skuli einnig setja sér öryggisstefnu, framkvæma áhættumat reglubundið og ákvarða og endurmeta öryggisráðstafanir á grundvelli þess.

Þannig eru í raun komnar inn í ákvæðið ákveðnar aukakröfur um skjalfestingu stefnu og ferla sem er með öllu óþarft að mati stofnunarinnar og felur í sér ákveðna tvöföldun á kröfum.

Það orðalag sem Póst- og fjarskiptastofnun leggur til er byggt á þeirri aðferðarfræði sem framfylgt hefur verið í Evrópu. Hefur það einnig beina skírskotun í leiðbeiningar um framkvæmd á NIS-tilskipuninni sem nú þegar eru farnar að koma frá Framkvæmdastjórninni, Net- og upplýsingaöryggisstofnun Evrópu (ENISA) og samstarfshópi[18] NIS-tilskipunarinnar sjálfrar.

Þá hefur ENISA gefið út leiðbeiningar um þessar greinar fjarskiptaregluverksins sem byggja á aðferðarfræði ISO 27001 staðalsins sem fjallar um skipulag upplýsingaöryggis í formi öryggisstefnu, gerð áhættumats og gerð öryggisráðstafana, líkt og orðalag 47. gr. fjarskiptalaga byggir á sem og afleiddar reglur nr. 1221/2007 og 1222/2007. Staðallinn tryggir í raun heildstætt og skriflegt skipulag upplýsingaöryggis. Þá hvetur NIS-tilskipunin sjálf til staðlanotkunar, sbr. 19. gr. hennar. Þá hefur ENISA gert könnun hjá aðildarríkjum vegna NIS

[14] Ákvæðið kom inn í rammatilskipunina með breytingu á fjarskiptaregluverkinu árið 2009.
[15] EECC stendur fyrir *European Electronic Communication Code* sem er nýsamþykkt heildarendurskoðun á fjarskiptaregluverki Evrópusambandsins, sbr. tilskipun nr. 2018/1972, frá 11. desember 2018.
[16] Settar hafa verið ítarlegar reglur um vernd upplýsinga á almennum fjarskiptanetum og virkni almennra fjarskiptaneta á grundvelli þessa ákvæðis, sbr. reglur nr. 1221-1223/2007.
[17] Sjá t.a.m. ákvarðanir um raunlægt öryggi nr. 36/2015, um raunlægt öryggi mikilvægra hýsingarrýma Mílu og nr. 24/2018, um úttekt á öryggisskipulagi Farice ehf. og raunlægu öryggi landtökustaða FARICE-1 og DANICE hér á landi. Hvað varðar kerfislægt öryggi vísast til ákvörðunar nr. 24/2016, um öryggisatvik á vefsíðu Vodafone. Þá er byggt á sömu aðferðarfræði í fimm ákvörðunum PFS er varða meðferð og eyðingu fjarskiptaumferðarupplýsinga, sbr. ákvarðanir nr. 35-39/2014 og ná til Símans, Nova, IP-fjarskipta, Vodafone og Hringdu.
[18] Með 11. gr. NIS-tilskipunarinnar er komið á fót samstarfshópi til að styðja og greiða fyrir stefnumótandi samstarfsverkefnum og upplýsingaskiptum milli aðildarríkja og að þróa traust og tiltrú þeirra á milli með það fyrir augum að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í Sambandinu.

og sýna niðurstöður að ISO 27001 staðallinn[19] er notaður í flestum tilfellum. Nær þetta jafnvel til mismunandi rekstraraðila þótt ýmsir staðlar séu einnig notaðar m.t.t. viðkomandi starfsemi.

Ef orðalag 1. mgr. 7. gr. verður óbreytt að lögum er ljóst að taka þarf mið af því við framfylgd ákvæðisins. Það klippir á beina tengingu við fordæmi í íslenskum rétti sem og, líkt og áður segir, þeim leiðbeiningum sem koma frá Evrópu um framfylgd ákvæðisins. Póst- og fjarskiptastofnun hefur í raun fylgt fyrirmyndum frá Evrópu varðandi kröfurnar sem er nú hliðrað yfir á þá aðila sem koma til með að falla undir NIS-tilskipunina. Rétt er að benda á að bæði í Danmörku og Svíþjóð er orðalag NIS-tilskipunar tekið beint inn, sbr. tillaga stofnunarinnar hér að neðan.[20]

Þá er jafnframt í 1. mgr. 7. gr. einnig tekin sérstaklega fyrir ein öryggisráðstöfun umfram aðrar, þ.e. aðgangsstýring. Segir að hún sé skylda, eftir því sem við á. Póst- og fjarskiptastofnun getur vissulega tekið undir það að aðgangsstýringar eru nauðsynlegur liður í að tryggja öryggi neta og upplýsingakerfa. Það er hins vegar alveg ljóst að aðrar öryggisráðstafanir eru ekki síður mikilvægar, svo sem afmörkun og takmörkun á nettengingu við kerfi, aðgreining kerfanna (e. segregation), „filtering" á umferð um kerfi, möguleg dulkóðun o.fl.[21] Það að taka út eina ráðstöfun er annkanalegt, sér í lagi þegar fjalla á um lágmarkskröfur í reglugerð ráðherra. Sama á við um innra eftirlit og prófanir.

Leggur Póst- og fjarskiptastofnun til að orðalagi 1. mgr. 7. gr. frumvarpsins verði breytt og orðist svo:

> ***Rekstraraðilar mikilvægra innviða skulu gera viðeigandi 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.***

Samhliða framangreindri breytingu er eðlilegt að reglugerðarákvæði 4. mgr. ákvæðisins verði aðlagað nýju orðalagi 1. mgr. þess. Leggur stofnunin til að 4. mgr. orðist svo:

> ***Ráðherra skal með reglugerð, mæla nánar fyrir um skipulag net- og upplýsingaöryggis og virkni net- og upplýsingakerfa rekstraraðila mikilvægra innviða að fenginni umsögn eftirlitsstjórnvalda og Póst- og fjarskiptastofnunar. Skal m.a. kveðið á um skjalfestingu net- og upplýsingaöryggis, gerð skriflegrar viðbragðsáætlunar og áætlana um samfelldan og órofinn rekstur, framkvæmd virks innra eftirlits, raunlæga vernd net- og upplýsingakerfa, stjórnunar rekstrarsamfellu, notkun alþjóðlegra staðla eða forskrifta og helstu lágmarks öryggisráðstafanir sem til greina koma. Heimilt er að gera greinarmun á kröfum til rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda í reglugerð samkvæmt ákvæði þessu.***

---

[19] Tveir staðlar úr 27000-staðlaröðinni hafa verið gerðir að íslenskum stöðlum og þýddir á íslensku. Annars vegar er um að ræða staðallinn ÍST ISO/IEC 27001 *Upplýsingatækni - Öryggistækni - Stjórnkerfi upplýsingaöryggis - Kröfur*. Hins vegar staðalinn ÍST ISO/IEC 27002 *Upplýsingatækni - Öryggistækni - Starfsvenjur fyrir stjórnun upplýsingaöryggis*.

[20] Einnig má benda á að í frumvarpi að innleiðingu tilskipunarinnar í Noregi (sem nú er í opnu samráði) er einnig byggt á orðalagi tilskipunarinnar.

[21] Umræddar kröfur, ásamt fleirum, hafa nú verið listaðar upp í leiðbeiningum frá samstarfshópi 11. gr. NIS-tilskipunarinnar.

4.6 Reglugerðarákvæði er varða netöryggissveit

Í frumvarpinu er að finna ítarleg ákvæði er varða netöryggissveitina, starfsemi hennar og hlutverk gagnvart fjarskiptafyrirtækjum sem og mikilvægum innviðum. Með samþykkt frumvarpsins verður þannig fjallað um sveitina í þremur lagabálkum. Í fyrsta lagi verður kveðið á um starfsrækslu og umgjörð sveitarinnar innan Póst- og í lögum nr. 69/2003, um Póst- og fjarskiptastofnun. Í öðru lagi verður kveðið á um hlutverk hennar gagnvart fjarskiptafyrirtækjum í lögum nr. 81/2003, um fjarskipti og, í þriðja lagi, verður kveðið á um hlutverk hennar gagnvart mikilvægum innviðum í hinum nýju lögum um net- og upplýsingaöryggi mikilvægra innviða.

Í tveimur tilvikum er í frumvarpinu gert ráð fyrir skyldu ráðherra að setja reglugerð *annars vegar* er varðar starfsemi sveitarinnar, sbr. c. liður 1. tölul. 27. gr. frumvarpsins, sem kveður á um nýja 4. gr. a. í lögum nr. 69/2003, og *hins vegar* um vinnslu persónuupplýsingar, sbr. 4. gr. 21. gr. í frumvarpinu.

Í fyrrnefnda tilvikinu er kveðið á um skyldu ráðherra um að setja reglugerð um starfsemi netöryggissveitarinnar, eftir því sem við á, að fenginni umsögn frá Persónuvernd og ríkislögreglustjóra. Ekki er minnst á að samráð skuli haft við Póst- og fjarskiptastofnun en í töluliðum málsgreinarinnar eru tilgreind þau atriði sem reglugerðin skal fjalla um. Þau atriði varða t.a.m. hlutverk, skipulag og verkefni sveitarinnar, skipun og hæfi starfsmanna hennar, skýrslugjöf um starfsemi hennar o.fl. Að mati Póst- og fjarskiptastofnunar er eðlilegt að gert sé að skyldu ráðherra að hafa samráð við stofnunina sjálfa þegar kemur að þessari reglugerðarsetningu enda lýtur hún m.a. að utanumhaldi og rekstri sveitarinnar sem að stofnunin ber ábyrgð á. Leggur stofnunin því til að 1. málsl. 6. mgr. nýrrar 4. gr. a í lögum nr. 69/2003, skv. c. lið 1. tölul. 27. gr. frumvarpsins orðist svo:

Ráðherra setur, að viðhöfðu samráði við Póst- og fjarskiptastofnun og, eftir því sem við á, að fenginni umsögn frá Persónuvernd og ríkislögreglustjóra, nánari fyrirmæli um starfsemi netöryggissveitar í reglugerð.

Þá er í síðarnefnda tilvikinu kveðið á um skyldu ráðherra um að setja reglugerð, að fengnu áliti Persónuverndar, þar sem kveðið er á um forsendur vinnslu persónuupplýsinga hjá netöryggissveitinni. Hér telur Póst- og fjarskiptastofnun eðlilegt að viðhaft sé samráð við stofnunina sjálfa enda ljóst að netöryggissveitin er best til þess fallin að gefa upplýsingar um og yfirlit yfir hvaða persónuupplýsingar hún vinnur með, nauðsyn þeirra og meðhöndlun. Leggur stofnunin því til að 1. málsl. 4. mgr. 21. gr. frumvarpsins orðist svo:

Ráðherra skal í reglugerð, að viðhöfðu samráði við Póst- og fjarskiptastofnun og að fengnu áliti Persónuverndar, kveða á um forsendur vinnslu persónuupplýsinga hjá netöryggissveit, meðferð þeirra og eyðingu, rétt skráðra einstaklinga og takmörkun á rétti þeirra.

V.
Niðurlag

Hér að framan hefur Póst- og fjarskiptastofnun bent á atriði og lagt til breytingar sem hún telur að séu nauðsynlegar svo markmið með frumvarpinu náist. Um er að ræða fimm mikilvægar breytingar er varða i) aðgengi netöryggissveitar að upplýsingum, ii) trúnað upplýsinga hjá netöryggissveit, iii) breytingar á ákvæði er varðar vinnsluheimildir netöryggissveitarinnar, iv)

lágmarkskröfur sem settar eru á mikilvæga innviði, og v) samráð við Póst- og fjarskiptastofnun við setningu reglugerða um starfsemi netöryggissveitarinnar.

Að lokum er áréttað að getu Póst- og fjarskiptastofnun til að stuðlað að auknu netöryggi efnahagslegrar og samfélagslegrar mikilvægrar þjónustu hér á landi, á grundvelli óbreytts frumvarps, eru settar afgerandi skorður. Frumvarpið tryggir einungis heimildir til handa netöryggissveitinni vegna viðbragða við þegar höfnum eða afloknum atvikum, þ.e. á grundvelli tilkynningarskyldu aðila, en skortir heimildir til öflunar nauðsynlegra upplýsinga, í samstarfi við aðila, hvort tveggja til að nema ógnir, fyrirbyggja atvik og árásir hjá mikilvægum innviðum og til að skapa heildarmynd af netógnum í netumdæmi sveitarinnar.

Er það von stofnunarinnar að umhverfis- og samgöngunefnd Alþingis telji það skynsamlegt að gera umbeðnar breytingar á frumvarpinu. Telur stofnunin að fagleg rök styðji slíkt.

Póst- og fjarskiptastofnun er að sjálfsögðu reiðubúin að koma á fund nefndarinnar og ræða efni þessarar umsagnar og svara spurningum varðandi hana. Að mati stofnunarinnar er um gríðarlega mikilvægt mál að ræða sem varðar mikla efnahagslega og samfélagslega hagsmuni hér á landi.

Virðingarfyllst,

Unnur Kristín Sveinbjarnardóttir

Viðauki I

Minnisblað - Stutt samantekt um stöðu netöryggissveita og innleiðingu NIS-tilskipunar á Norðurlöndum.

PÓST- OG FJARSKIPTASTOFNUN

Minnisblað

- Stutt samantekt um stöðu netöryggissveita og innleiðingu NIS-tilskipunar á Norðurlöndum -

Í minnisblaði þessu er að finna stutta samantekt um stöðu netöryggissveita á Norðurlöndunum. Verður gert grein fyrir bakgrunni þeirra, stöðu þeirra og hlutverki og lagaumhverfi sem gildir í dag. Ekki er ætlunin að gefa tæmandi lýsingu á starfsemi þeirra eða heimildum. Þá verður ein farið yfir stöðu innleiðingar NIS-tilskipunarinnar og sýn gefin á vali á innleiðingaraðferð.

Danmörk

Netöryggismál eiga sér nokkra sögu í Danmörku. En árið 2009 var komið á viðbragsteymi fyrir ríkisstjórn og stjórnsýslustofnanir Danmerkur, þ.e. GovCERT sem var ætlað að vera viðbragsteymi fyrir ógnir á internetinu sem ríkinu stafaði hætta af. Undir GovCERT féllu einnig upplýsingaöryggi fjarskiptafélaga. Þá var sett á stofn sérstakt viðbragðsteymi m.t.t. varnarmála árið 2010, þ.e. MILCERT sem var starfrækt innan varnarmálastofnunar Danmerkur. Árið 2012 voru framangreind viðbragsteymi svo sameinuð í sérstakri miðstöð fyrir netöryggi (d. Center for Cybersikkerhed) innan varnarmálaráðuneytis Danmerkur. Markmiðið með þessari sameiningu var að efla netöryggi danska ríkisins. Fyrsta heildarlöggjöf fyrir hina nýju sameinuðu netöryggissveit voru samþykkt árið 2014, þ.e. lög nr. 713 frá 25. júní 2014, til að styrkja stoðir og heimildir sveitarinnar þar sem að hvort tveggja dönsk yfirvöld sem og dönsk fyrirtæki voru í auknum mæli að verða fyrir netárásum. Áður var í gildi löggjöf fyrir starfsemi GovCERT. Í hinni nýju löggjöf var kveðið á um hlutverk sveitarinnar, henni veittar auknar heimildir til að nema, rannsaka og koma í veg fyrir netárásir ásamt því að rannsaka öryggisatvik. Í frumvarpi sem var að lögunum kemur fram að varnarmálastofnun Danmerkur hafi metið að alvarlegustu ógnir ríkisins hafi stafað frá öðrum ríkjum, til að mynda til njósna og ólögmætrar upplýsingaöflunar, t.a.m. að afla upplýsinga sem verndaðar eru á grundvelli einkaleyfis, rannsóknarniðurstaðna og viðskiptaleyndarmála. Eins var hætta talin stafa af hökkurum sem störfuðu á grundvelli pólitískra skoðana sinna. Árásir af hálfu þessara aðila gætu verið mjög tæknilega flóknar og gætu valdið skemmdum á dönskum vefsíðum og netþjónum. Eins var talið að hryðjuverkasamtök væru farin að sýna þá tilhneigingu að nota internetið til árása. Auk þessa var jafnframt talið að hættur gætu komið innan frá, þ.e. að starfsmenn gætu, jafnvel að grandlausu, valdið því að árás ætti sér stað og yrði jafnvel árangursrík, t.d. með því að árásaraðilinn kæmist yfir ákveðnar upplýsingar eða næði að dreifa óværu (e. malware) inn í kerfi viðkomandi stofnunar eða fyrirtækis.

Samkvæmt framangreindum lögum frá 2014 er netöryggissveit Danmerkur ábyrg fyrir að nema, greina og takast á við öryggisatvik með stjórnvöldum innan danska varnarmálaráðuneytisins og stjórnvöldum eða fyrirtækjum, sem eru tengd er kerfi netöryggissveitarinnar. Um er að ræða sérhannað skynjarakerfi til að nema ógnir og árásir. Er þessu ætlað tryggja að netöryggissveitin geti viðhaft, óværugreiningar (e. malware analyzes) sem og rannsóknir á ógnum, áhættum og atvikum. Þá geta geta æðstu stjórnvöld og stofnanir tengst þessu kerfi sveitarinnar kjósi þau að njóta þjónustu hennar. Eins geta sveitarfélög og fyrirtæki sem reka mikilvæga innviði óskað eftir að tengjast kerfi sveitarinnar. Slíkt er þó háð því mati sveitarinnar að slík tenging myndi styrkja hátt öryggisstig í dönsku samfélagi. Þá er það í höndum sveitarinnar að kveða á um

frekari reglur eða skilyrði fyrir tengingu við þjónustu hennar, þ.m.t. gjaldtöku. Eins geta aðilar sem almennt eru ekki tengdir kerfi netöryggissveitarinnar til að tengjast því enda sér rökstuddur grunur um netógn eða árás. Í greinargerð sem varð að dönsku lögunum má finna lýsingu á því hvernig gengið er frá tenginu aðila við kerfi sveitarinnar. Er slíkt á grundvelli samninga sem tilgreina skilyrði fyrir tengingunni, þ.m.t. um hvernig vöktun á tengingu viðkomandi aðila við internetið skuli háttað, svo sem með uppsetningu skynjara sem nemur og greinir atburði.

Töluvert er lagt upp ótvíræðum heimildum dönsku netöryggissveitarinnar til aðgangs að gögnum og upplýsingum. Þannig er sveitinni heimilt, sbr. 4., 5., og 7. gr. laganna að vinna gagnapakka og umferðarupplýsingar hjá þeim aðilum sem að hafa tengst kerfi þeirra án sérstaks dómsúrskurðar. Í skýringum við umrædd ákvæði kemur fram að ákvæðið er í raun óbreytt frá þágildandi ákvæði laga um GovCert Danmerkur og er ætlað að heimila netöryggissveitinni að vinna með gögn án dómsúrskurðar. Í lögum um dönsku netöryggissveitina er finna skýra vinnsluheimild fyrir vinnslu persónuupplýsinga ásamt því að tiltekið er að vinnslan sé undanþegin hluta dönsku persónuverndar-löggjafarinnar. 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 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. Einnig er kveðið á um bann við almennri vinnslu viðkvæmra persónuupplýsinga nema að vinnslan er nauðsynleg vegna þjóðaröryggis og varnarmála. Í löggjöfinni er jafnframt að kveðið á um ákveðnar kröfur er varðar vinnsluna, svo sem um réttleika upplýsinganna, eyðingu þeirra og skyldu um að gera þær ópersónugreinanlegar. Vert er þó að geta að ekki verður séð að umrædd ákvæði laganna hafi, enn sem komið er, verið uppfærð m.t.t. gildistöku nýrrar reglugerðar Evrópusambandsins um persónuvernd, GDPR.

Hvað varðar innleiðingu á NIS-tilskipuninni þá var farin sú leið við innleiðingu á NIS að gerðar voru breytingar á löggjöf hvers sviðs nauðsynlegrar þjónustu eins og hún er skilgreind í II. viðauka við tilskipunina. Það er því á höndum tiltekinna eftirlitsstjórnvalda að hafa eftirlit með að þeir aðilar sem undir lögin falla uppfylli þær kröfur sem tilskipunin kveður á um, þ.e. um skipulag upplýsingaöryggis, lágmarksöryggisráðstafanir, neyðaráætlun o.fl. Þá verða sett á stofn sviðsbundin netöryggisteymi sem einnig hafa ákveðinn aðgang að dönsku netöryggissveitinni. Þá hefur verið samþykkt breytingarfrumvarp við lögin frá 2014 sem heimilar mikilvægum innviðum að tengjast inn á skynjarakerfi sveitarinnar. Því er ekki um nýja heildarlöggjöf að ræða líkt og lagt er til í því frumvarpi sem nú liggur fyrir Alþingi.

Noregur

Töluverð hefð er fyrir netöryggismálum í Noregi en það var í ársbyrjun 2006 sem var sett á fót landsbundið viðbragðsteymi, NorCERT. Þjónusta sú sem NorCERT veitir á sér hins vegar lengri sögu eða allt til ársins 2000 þegar sérstöku skynjarakerfi (n. Varslingssystem for digital infrastruktur – VDI) var komið á fót í samstarfi milli aðila sem fara með löggæslu og varnarmál í Noregi, þ.m.t. hersins. Þetta viðbragðskerfi var flutt til norsku öryggsmálastofnunarinnar (n. National Sykkerhetsmyndighet – NSM)) árið 2003 og, frá 2006, var það hluti af NorCERT, sem er starfandi innan varnamálastofnunar landsins. Það er á þessum grunni sem að áhersla NorCERT hefur frá upphafi verið á vernd mikilvæga innviði landsins en kerfið var í upphafi ætlað að gæta gas- og olíuframleiðslu í Noregi.

Þjónusta NorCERT byggist hvort tveggja á viðbragsþjónustu sem og ákveðinni forvarnarþjónustu. Hvað varðar viðbragsþjónustu þá er netöryggissveitin ábyrg fyrir því að samhæfa viðbragð við alvarlegum netöryggisatvikum sem varða Noreg, þannig forgangsraðar sveitin og samhæfir ferla þegar brugðist er við atvikum. Ábyrgðin á meðhöndlun atvika er þó ávallt hjá eiganda net- og upplýsingakerfisins sem verður fyrir atviki. Hvað varar forvarnarþjónustu NorCERT þá ráðleggur sveitin þjónustuhóp sínum m.t.t. nýrra veikleika, gefur út skýrslur með reglulegum hætti og starfrækir áðurnefnd skynjarakerfi sem eru settir upp

hjá þjónustuhópi sveitarinnar. Það má því ætla að norska netöryggissveitin sé nú þegar að uppfylla flestallar kröfur sem að NIS-tilskipunin gerir kröfu um, sbr. 9. gr. hennar og viðauki I við hana. Þá má einnig nefna það að til staðar eru dæmi um samstarf innan sérstakra geira í Noregi. Má þar til dæmis nefna samstarf norska orkugeirans, öryggisfyrirtækisins Mnemonic og KraftCERT. Orkufyrirtæki sem eru aðilar að KraftCERT hafa í gegnum þann samning aðgang að þjónustu Mnemonic, sem innifelur m.a. skynjarabúnaði á netkerfi þeirra og virka vöktun. KraftCERT og viðkomandi rekstraraðili gera síðan sín á milli samning um þá atburði sem berast frá búnaði Mnemonic á þeirra netkerfum til KraftCERT. Umfang þess gagnastraums getur verið allt frá einungis mjög alvarlegum atburðum og til flæðis allra atburða sem eiga sér stað.

Hvað varðar stöðu innleiðingar á NIS-tilskipuninni í Noregi þá liggur fyrir frumvarp sem nú er í opnu samráði. Samráðinu lýkur 22. mars 2019. Frumvarpið er nokkuð einfalt og innleiðir lágmarkskröfur til skipulags net- og upplýsingaöryggis og tilkynningarskyldu. Töluvert er um reglugerðarheimildir þar sem m.a. verður tilgreint um eftirlitsstjórnvöld, settar ítarlegri reglur um öryggiskröfur o.fl. Ekki er að finna sérstök ákvæði er varðar netöryggissveitir.

Ný heildaröryggislöggjöf tók aftur á móti gildi þann 1. janúar sl. En áðurnefnd öryggismálastofnun (NSM) starfar á grundvelli hennar. Löggjöfin er nokkuð ítarleg og er ætlað að koma í veg fyrir, afhjúpa og vinna gegn starfsemi eða hættum sem geta ógnað öryggi Noregs. Þar koma fram skyldur á aðila er falla undir lögin um að viðhafa virkt netöryggi sem og skyldur Öryggismálastofnunarinnar, samstarf hennar við aðila sem falla undir lögin og heimildir hennar, t.a.m. um aðgang og vinnslu persónuupplýsinga.

Svíþjóð

Sænska netöryggissveitin CERT-SE er staðsett innan sænsku almannavarnastofnunarinnar. Markmið netöryggissveitarinnar kemur fram í reglum 2008:1002 sem varða stofnunina. Helsta hlutverk sveitarinnar er að bregðast við öryggisatvikum með því að miðla upplýsingum, og ef það er talið nauðsynlegt, að vinna að samhæfingu aðgerða og aðstoða við draga úr áhrifum atviksins. Sveitin hefur þó ekki heimildir til frekari inngripa. Hins vegar getur það sett fram tilmæli varðandi veikleika og aðgerðar til að draga úr atvikum. Tilmæli sem þessi geta til að mynda kveðið á um lokun á IP-tölu eða neti. Þótt netöryggissveitin gefi út tilmæli sem þessi þá er það ávallt á ábyrgði viðkomandi aðila hvernig hann framkvæmir slík tilmæli en ekki á ábyrgð sveitarinnar. Umdæmi sveitarinnar samanstendur af, en einskorðast ekki við, stjórnsýslustofnunum, svæðisbundnum stjórnvöldum, sveitarfélögum og fyrirtækjum. Þá er sveitin jafnframt GovCERT fyrir sænsk stjórnvöld og hefur ákveðnar viðbótarskyldur innan stjórnvalda. Sveitin er þjóðartengill Svíþjóðar við systurstofnanir sveitarinnar og kemur að þróun samstarfs og upplýsingaskipta hvað það varðar.

Svíþjóð hefur innleitt NIS-tilskipunina, sbr. lög frá 20. júní sl., nr. 2018:1174 og reglugerð frá sama degi nr. 2018:1175. Við innleiðinguna var farin sú leið að setja heildarlöggjöf sem kveður á um skyldur á hendur þeirra aðila sem sinna nauðsynlegri þjónustu og stafræna þjónustuveitendur. Þá er sama leið farin og í Danmörku, og sem lögð er til í frumvarpi þessu, að eftirlitsstjórnvöld, hvert á sínu sviði fari með eftirlit með þeim aðilum sem undir lögin falla. Það er hins almannavarnarstofnun Svíþjóðar sem hefur hlutverk samhæfingarstjórnvalds en þar er CERT-SE staðsett.

Finnland

Á Finnlandi er stofnun fyrir þjóðarnetöryggi (e. The National Cyber Security Center – NCSC-FI) staðsett innan finnska fjarskiptaeftirlitsins (FICORA). Stofnunin hefur starfað í núverandi mynd síðan 1. janúar 2014 og bæði þróar og vaktar rekstrarhæfni og öryggi fjarskiptaneta og fjarskiptaþjónustu í Finnlandi. Innan stofnunarinnar er hvort tveggja CERT-teymi, þ.e. netöryggissveit, sem og teymi sem ber ábyrgð á öryggisatvikum sem tengjast rafrænum færslum og vinnslu trúnaðarupplýsinga (e. National Communication Security Authority – NCSA). Netöryggi innan Finnlands á sér nokkuð langa sögu og var CERT-FI sett á stofn upp úr aldamótum. CERT-teymið byggir þannig á gömlum grunni en markmið með starfsemi þess er

að tryggja öryggi og virkni almennra fjarskiptaneta og fjarskiptaþjónustu sem og að vernda nauðsynlega þjónustu fyrir finnskt samfélag. Skyldur þess felast m.a. í því að nema ógnir, koma í veg fyrir öryggisatvik sem og að leysa úr þeim öryggisatvikum sem upp koma. Þá heldur teymið utan um upplýsingar um atvik og miðlar upplýsingum um öryggismál. CERT-teymið þjónustar hvort tveggja opinberan markað, þ.e. ríkisstjórn og stjórnsýslustofnanir sem og einkamarkaðinn. Þannig nær þjónusta þess til alls landsins þó að sérstök áhersla sé á fjarskiptafyrirtæki, þjónustuveitendur og mikilvæga innviði.

NCSC-FI er þjóðartengill Finnlands og CSIRT-teymi fyrir aðila sem ekki hafa sambærilega þjónustu innan annarra CSIRT-teyma. Stofnunin fer jafnframt með hlutverk GovCert í samræmi við samning við finnska fjármálaráðuneytið þar um. Þá hagnast rekstraraðilar mikilvægra innviða frá starfsemi CSIRT-þjónustu sem veitt er af stofnuninni í samræmi við samning milli stofnunarinnar og þjóðarstofnun Finna sem fer með neyðarmál (e. Nationnal Emergency Supply Agency). Sú þjónusta sem að NSCS-FI veitir byggist í fyrsta lagi á viðbrögðum við atvikum og í öðru lagi á fyrirbyggjandi aðgerðum. Hvað fyrri flokkinn varðar þá samhæfir stofnunin aðgerðir annarra CSIRT-teyma, eigenda umræddra kerfa og netrekenda með það að markmiði að halda kerfum öruggum. Stofnunin rekur sérstakt tilkynningarkerfi sem og viðvörunarkerfi sem safna upplýsingum um atvik sem varða Finnland. Þá getur stofnunin kveðið á um að fjarskipafyrirtæki grípi til ákveðinna aðgerða sem og haft frumkvæði að aðgerðum innan finnska stjórnarráðsins í samræmi við GovCERT samning. Hvað þetta varðar er vert að hafa í huga gildissvið ákvæða finnsku lagana sem fjalla um upplýsingaöryggi, lög 917/2014, en samkvæmt þeim eru lagðar skyldur á fjarskiptanetsrekendur eða eiganda eða umráðamann fjarskiptanets eða búnaðar að aftengja fjarskiptanet, þjónustu eða búnað ef að hann er að valda skaða á rekstrarsamfellu annarra fjarskiptaneta, þjónustu eða tengdrar þjónustu, búnaðar, notenda eða annarra aðila. Hefur FICORA (þar sem NCSC-FI er staðsett) jafnframt heimildir til að kveða á um slíka aftengingu fjarskiptanets, þjónustu eða búnaðar. Af þessu má sjá að inngripsheimildir eru nokkuð íþyngjandi og ná til fleiri aðila en fjarskiptafyrirtækja, svo sem hýsingaraðila og eigendur einstakra þjóna sem ógn stafar af fyrir aðra þjónustu á netinu. Þá hefur FICORA nokkuð viðamiklar heimildir til aðgangs að gögnum samkvæmt löggjöfinni. En stofnunin hefur, ásamt öðrum stofnunum sem hafa hlutverki að gegna samkvæmt lögunum, heimild til aðgangs að gögnum sem eru nauðsynlegt til að hún geti framfylgt þeim skyldum sem á hana eru lagðar samkvæmt lögunum. Nær þessi heimild til allra þeirra sem hafa réttindi og skyldur á grundvelli laganna, sem og fulltrúa þeirra.

Hvað varðar hinn flokkinn, þ.e. fyrirbyggjandi aðgerðir, þá er NCSC-FI virkur þáttakandi í upplýsingaskiptum og vitundaruppbyggingaraðgerðum. Gefur stofnunin út efni, svo sem greinar, ráðgefandi álit, viðvaranir og ýmsar leiðbeiningar varðandi netöryggi. Þá sinnir hún einnig hlutverki við samhæfingu aðgerða vegna veikleika. Í því hlutverki flest m.a. að stuðla að ábyrgri meðferð á upplýsingum um veikleika, allt frá því að hann finnst og þar til brugðist hefur verið við honum.

NIS-tilskipunin hefur nú þegar verið innleidd í Finnlandi með því að gera breytingar á löggjöf hvers sviðs rekstraraðila nauðsynlegrar þjónustu. Þannig eru það jafnframt mismunandi stjórnvöld sem hafa eftirlit með ákvæðum NIS-tilskipunarinnar og skulu öryggisatvik tilkynnt til hlutaðeigandi stjórnvalds. Þá hefur FICORA fengið það hlutverk að vera eftirlitsstjórnval með stafrænum þjónustuveitendum sem og að vera sameiginlegi tengiliður samkvæmt tilskipuninni. Hér er því að finna mjög sambærilega aðferðarfræði og lögð er til í frumvarpi sem nú liggur fyrir Alþingi.

Póst- og fjarskiptastofnun, *í janúar 2019*

Viðauki II

Umsögn Póst- og fjarskiptastofnunar til allsherjarnefndar, dags. 4. júní 2018, um frumvarp til laga um persónuvernd og vinnslu persónuupplýsinga þingskjal nr. 1026 — 619. mál á 148. löggj.þ.

PÓST- OG FJARSKIPTASTOFNUN
SUÐURLANDSBRAUT 4
108 REYKJAVÍK
SÍMI 510 1500 PÓSTUR PFS@PFS.IS
FAX 510 1509 VEFUR WWW.PFS.IS

Alþingi
Allsherjar- og menntamálanefnd
Elisabeth P. Kruger, nefndarritari
Kirkjustræti 1
101 Reykjavík

Reykjavík, 4. júní 2018

Málsnúmer: 2018060005
Skjalalykill: 15.0

Málefni: Umsögn um frumvarp til laga um persónuvernd og vinnslu persónuupplýsinga

I. Almennt

Vísað er til erindis allherjar- og menntamálanefndar Alþingis, dags. 30. maí 2018, þar sem Póst- og fjarskiptastofnun er gefinn kostur á því að veita umsögn um frumvarp til laga um persónuvernd og vinnslu persónuupplýisnga, sbr. þingskjal nr. 1026 — 619. mál.

Með fruvarpinu er ætlunin að innleiða í íslensk lög ákvæði persónuverndarreglugerðar Evrópuþingsins og Ráðsins nr. 2016/679 frá 27. apríl 2016 sem tók gildi innan sambandsins þann 25. maí sl.

Þar sem að um reglugerð frá Evrópusambandinu er að ræða er lítið svigrúm til aðlögunar eða breytinga þegar kemur að innleiðingu í landsrétt. Þá er reglugerðin ítarleg og umfangsmikil og mun Póst- og fjarskiptastofnun því ekki fjalla um ákvæði er varða almennar meginreglur um vinnslu persónuupplýsinga, vinnsluheimildir, flokkun persónuupplýsinga o.fl. sem munu gilda um vinnslu persónuupplýsinga hjá stofnuninni sjálfri heldur fyrst og fremst þann snertiflöt sem ákvæði reglugerðarinnar eiga við mjög *sértæka* vinnslu persónuupplýsinga sem fram fer innan netöryggissveitar Póst- og fjarskiptastofnunar og lýtur að vernd net- og upplýsingaöryggis hér á landi.

II. Vinnsluheimildir GDPR m.t.t. net- og upplýsingaöryggis

Í ákvæði 47. gr. a í fjarskiptalögum nr. 81/2003 og reglugerð nr. 475/2013, um málefni CERT-ÍS er fjallað um hlutverk netöryggissveitar Póst- og fjarskiptastofnunar. Í framangreindu lagaákvæði og reglugerð 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 í netumdæmi sínu en það nær til þjónustuhóps sveitarinnar, þ.e. fjarskiptafyrirtækja og þeirra rekstraraðila ómissandi upplýsingainnviða sem gert hafa þjónustusamning við netöryggissveitina.

Í farvatninu eru þó ákveðnar breytingar á umfangi starfsemi sveitarinnar en í samgöngu- og sveitarstjórnarráðuneytinu er nú unnið að gerð frumvarps til innleiðingar á svo kallaðri NIS-tilskipunu, þ.e. tilskipun Evrópuþingsins og ráðsins nr. 2016/1148 frá 6. júlí 206 varðandi

ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu.
Samkvæmt tilskipuninni skulu aðildarríki skilgreina rekstraraðila mikilvægrar þjónustu hvers lands sem að munu falla undir ákvæði tilskipunarinnar sem og stafræna þjónustuveitendur, svo kallaðir rekstraraðilar mikilvægra innviða. Settar eru kröfur á umrædda aðila til að viðhafa ákveðið skipulag upplýsingaöryggis á net- og upplýsingakerfum sínum sem lúta eftirliti hins opinbera. Þá gerir tilskipunin jafnframt kröfu til að starfrækt sé í hverju aðildarríki viðbragðsteymi vegna váatvika er varða netörggi, sbr. I. viðauka við tilskipunina, sem skal annast vöktun atvika á landsstigi, veita virka greiningu á áhættum og atvikum og veita stöðumynd af þeim netógnum sem uppi eru, bregðast við atvikum og tilkynna og miðla upplýsingum til hlutaðeigandi hagsmunaaðila um áhættur og atvik. Hér á landi er nú þegar starfandi tilgreint viðbragðsteymi, þ.e. framangreind netöryggissveit Póst- og fjarskiptastofnunar.

Innleiðing NIS-tilskipunarinnar kallar á mjög *sértæka* vinnslu persónuupplýsinga í ákveðnum *afmörkuðum* tilgangi. Er í *fyrsta lagi* um að ræða upplýsingar um netumferð í og við net- og upplýsingakerfi rekstraraðila mikilvægra innviða. Slíkar upplýsingar, svo sem IP-tölur, port sendanda og viðtakanda, tölvupóstföng og URL sem kerfi rekstraraðilans tengist eru persónugreinanlegar og því þarf vinnsla þeirra að byggjast á lögmætri vinnsluheimild skv. persónuverndarlögum. Slík heimild er einmitt veitt með GDPR en í 49. formálsorða hennar 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.

Í *öðru lagi* getur komið til annarrar tegundar vinnslu persónuupplýsinga hjá netöryggissveitinni, þ.e. eins konar *neyðarmiðlunar* á upplýsingum sem netöryggissveitinni berast þegar netárásir hafa átt sér stað. Hér getur verið erfitt að segja til um hvaða upplýsingar um ræðir enda fer það allt eftir því hvaða hvert er andlag árásarinnar. En tilgangur miðlunar sem þessarar er að koma í veg fyrir eða a.m.k. draga úr tjóni sem hinir skráðu, þ.e. einstaklingar sem upplýsingarnar varða, geta orðið fyrir. Vinnsluheimild fyrir miðlun sem þessari, án samþykkis hins skráða, byggist í raun á almannahagsmunum eða brýnum verndarhagsmunum viðkomandi einstaklings, skv. nýrri GDPR. Við innbrot í vefkerfi Vodafone í nóvember 2013 reyndi á atvik sem þetta þar sem leyninúmerum og kortanúmerum þúsunda einstaklinga var stolið og þau birt á internetinu. Í slíku tilviki hefði verið nauðsynlegt fyrir netöryggissveitina að geta miðlað umræddum upplýsingum til fjármálastofnanna svo þær gætu gripið til viðeigandi verndarúrræða fyrir viðkomandi einstakling. Vert er að nefna að öllum upplýsingum sem þessum er eytt hjá netöryggissveitinni eftir að miðlun til hlutaðeigandi aðila hefur átt sér stað. Hér er í raun um einskiptisaðgerð að ræða af hálfu netöryggissveitarinnar.

Í *þriðja lagi* er nauðsynlegt fyrir netöryggissveitina að geta tekið á móti og miðlað mjög afmörkuðum hluta upplýsinganna til erlendra yfirvalda, systursveita og annarra aðila er sinna

net- og upplýsingaöryggi. Er hér um að ræða upplýsingar sem varða þá einstaka netógnir og hættur sem greindar hafa verið af sveitinni. Hér er í raun um að ræða vinnslu persónuupplýsinga á grundvelli almannahagsmuna og þjóðaröryggis. Netógnir og -glæpir þekkja ekki hefðbundin landamæri og því er alþjóðasamstarf á þessu sviði gríðarlega mikilvægt til að hægt sé að vernda með sem bestum hætti þau net- og upplýsingakerfi sem teljast til mikilvægra innviða. Er í NIS-tilskipuninni jafnframt kveðið á um mikilvægi slíks samstarf og settir á stofn evrópskir samstarfshópar hvað þetta varðar og net viðbragsteyma til að stuðla að þraun trausts og tiltrúar milli aðildarríkja og til að stuðla að skjótvirkri og árangursríkri samvinnu.

Aðgangur netöryggissveitarinnar, viðbragðsteymis vegna váatvika er varðar net- og upplýsingaöryggi, að gögnum er grundvallarforsenda þess að sveitin geti sinnt lögbundnu hlutverki sínu samkvæmt núgildandi ákvæði fjarskiptalaga og komandi laga er innleiða NIS-tilskipunina og þeim verkefnum sem viðauki I við NIS-tilskipunina kveður á um. Póst- og fjarskiptastofnun leggur því ríka áherslu á að framangreind atriði verði áréttað í nefndaráliti allsherjar- og menntamálanefndar. Um er að ræða lágmarks- og grundvallarvinnsluheimilidir fyrir viðbragðsteymi líkt og netöryggissveitina til að tryggja með sem bestum hætti þær upplýsingar, þ.m.t. perónuupplýsingar, sem finnast í net- og upplýsingakerfum mikilvægra innviða hér á landi.

III. Takmörkunarákvæði GDPR m.t.t. net- og upplýsingaöryggis

Í III. kafla GDPR er fjallað um réttindi skráðs einstaklings og skiptist kaflinn upp í fimm þætti. 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.

Athygli vekur, að mati Póst- og fjarskiptastofnunar, að takmörkunarheimildir skv. 23. gr. GDPR virðast ekki nýttar að fullu í því frumvarpi sem hér er til umræðu til innleiðingar á reglugerðinni. Í 17. gr. frumvarpsins er framangreind takmörkunarheimild innleidd en samkvæmt 3. og 4. mgr. greinarinnar nær sú takmörkunarheimild einungis til 13.-15. gr. reglugerðarinnar, þ.e. til 1. og 2. þáttar III. kafla GDPR, en ekki 3. og 4. þáttar líkt og GDPR kveður jafnframt á um að takmarka megi gildisvið á.

Að mati Póst- og fjarskiptastofnunar þarf að bæta hér úr enda ljóst að um gríðarlega mikilvæga takmörkunarheimild getur verið að ræða. Áréttað er að 1. mgr. 23. gr. GDPR gerir kröfu um að takmörkun sé sett með löggjafarráðstöfun og því þarf ávallt að koma til kasta Alþingis til að takmörkun sem þessi sé heimil, annað hvort með setningu sérákvæða eða á grundvelli nákvæmra raglurgerðaheimilda. Ekki er því um sjálfkrafa takmörkun að ræða sem að ábyrgðaraðilar geta vísað til með einhverjum hætti í vinnslu sinni.

Í 73. lið formálsorða reglugerðarinnar er fjallað um framangreinda takmörkunarheimild 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 áðurnefndrar 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 Sambandsins. Geta netógnir og árásir hamlað atvinnustarfsemi, valdið verulegu fjárhagslegu tjóni, grafið undan trausti notenda og valdið miklu tjóni á efnahagi Sambandsins og því er öryggi net- og upplýsingakerfa þess nauðsynlegt fyrir snurðulausa starfsemi hvers aðildarríkis og hins innri markaðar. Auk þessa hafa dæmi hér á landi sýnt að einstaklingar geta orðið fyrir beinum skaða í slíkum árásum.

Takmörkunarákvæði sem þetta er í raun ekki nýtt af nálinni því í núgildandi 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. Þannig gera núgildandi 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.

Í starfsemi netöryggissveitarinnar er verið að vinna með nokkuð magn persónugreinanlegra upplýsinga. Upplýsingar eru ekki alltaf greindar niður á persónu en þegar að einstakar upplýsingar eru skoðaðr sérstaklega er ávallt um að ræða skoðun á upplýsingum sem byggir á ákveðnum grun um að eitthvað vafasamt sé að eiga sér stað, þ.e. einhver ógn geti verið uppi, t.a.m. í formi óeðlilegrar IP-umferðar, óeðliegrar tölvupóstsendingar o.þ.h. Það er því mikilvægt að starf sem þetta gangi sem skjótast fyrir sig enda getur tími sem gefst til að bregðast við netógnum verið mjög skammur. Það getur því verið nauðsynlegt og í samræmi við takmörkunarákvæði 23. gr. GDPR að vikið sé frá þeim réttinum einstaklinga sem einnig er að finna í 3 og 4. þætti III. kafla GDPR, líkt og rétt til takmörkunar á vinnslu, tilkynningarskyldu ábyrgðaraðila varðandi leiðréttingu persónuupplýsinga og andmæalaréttur hins skráða svo eitthvað sé nefnt, en ekki einungis 1. og 2. þætti kaflans.

Það er gríðarlega mikilvægt að við innleiðingu GDPR, með frumvarpi því sem liggur fyrir allsherjar- og menntamálanefnd, að öll þau ákvæði sem reglugerðin kveður á um að heimila megi takmörkun á verði nýtt og tilgreind í innlendum lögum um persónuvernd og vinnslu persónuupplýsinga, þ.e. ákvæði 16. – 22. gr. GDPR auk þeirra sem 17. gr. frumvarpsins kveður nú á um. Telur Póst- og fjarskiptastonfun nauðsynlegt að þessu verði breytt í meðferðum nefndarinnar á frumvarpinu.

IV. Lokaorð

Líkt og fram kom í upphafi þessarar umsagnar Póst- og fjarskiptastofnunar er fyrst og fremst fjallað um þá sértæku vinnslu persónuupplýsinga sem á sér stað hjá netöryggisveit stofnunarinnar í þágu net- og upplýsingaöryggis mikilvægra innviða hér á landi. Hefur verið lýst mikilvægi þess að í nefndaráliti allsherjar- og menntamálanefndar verði áréttaðar heimildir netöryggissveitarinnar, sbr. umfjöllun í II. Kafla hér að framan. Þá hefur verið bent á ákveðinn annmarka í því frumvarpi sem nú liggur til grundvallar innleiðingu GDPR, þ.e. varðar takmörkunarheimildir 23. gr. GDPR en þær hafa ekki verið nýttar að fullum hætti í 17. gr.

frumvarpsins að mati stofnunarinnar. Leggur Póst- og fjarskiptastofnun ríka áherslu á að nefndin breyti ákvæðinu með þeim hætti að takmörkunarástæður nái jafnframt til 3. og 4. þátta III. kafla GDPR. Skortur á takmörkunarheimildum þessum getur haft mikil áhrif á starfsemi netöryggissveitar við vernd upplýsinga, þ.á.m. persónuupplýsinga, í net- og upplýsingakerfum mikilvægra innviða hér á landi.

Það væri slæmt til þess að hugsa að almenn lög um persónuvernd og vinnslu persónuupplýsinga kæmu í veg fyrir að hægt væri að beita viðeigandi ráðstöfunum til verndar persónuupplýsingum þegar mest á reynir, þ.e. í netárásum sem beinast að viðkvæmum upplýsingum í mikilvæðum innviðum hér á landi.

Póst- og fjarskiptastofnun er reiðubúin að koma á fund nefndarinnar til að fylgja eftir umsögn þessari sé þess óskað af nefndinni. Að mati stofnunarinnar er um mikilvægt mál að ræða enda ljóst að netógnir og árásir á internetinu geta varðar hvort tveggja hagsmuni einstaklinga og þjóðfélagsins í heild. Mikilvægt er að möguleikar netöryggissveitar til að verjast slíkum ógnum verði ekki takmarkaður með innleiðingu GDPR enda ljóst að við samningu reglugerðarinnar var sérstaklega áréttað mikilvægi net- og upplýsingaöryggis innan Sambandsins.

Virðingarfyllst,

Unnur Kristín Sveinbjarnardóttir