

Samgöngu- og sveitarstjórnarráðuneytið
Sölvhóls götu 7
101 Reykjavík

Reykjavík, 11. janúar 2021

Efni: Umsögn um drög að reglugerð um netöryggissveit (CERT-ÍS)

I. Inngangur

Síminn hf. (hér eftir „Síminn“) vísar til draga samgöngu- og sveitarstjórnarráðuneytisins til reglugerðar um netöryggissveit (CERT-ÍS), sem birt var í Samráðsgáttinni þann 14. desember sl.

Síminn hefur rýnt drögin og vill góðfúslega koma á framfæri eftirfarandi athugasemdum til ráðuneytisins.

II. Umsögn Símans

Þótt ákvæði reglugerðarinnar séu að mörgu leyti nánari útfærslu á atriðum sem þegar koma fram í lögum, einkum lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, leggur Síminn engu að síður áherslu á að það sé tryggt að orðalag reglugerðarinnar sé í samræmi við lagatextann. Þess ber að gæta að ósamræmi í texta sé ekki fyrir hendi, ella er hætt við að reglugerðin verði haldslaus ef fyllsta samræmis sé ekki gætt.

Þá verður að telja varasamt að fyrirhugað sé að veita opinberri stofnun hlutverk sem felur í sér þjónustu sem einkaaðilar eru þegar að selja, í þessu tilviki sérstaklega upplýsingatæknifyrirtæki, sbr. nánari umfjöllun neðar um V. kafla draganna.

Einnig vakna spurningar um samspil þessara reglna við ákvæði laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér eftir „persónuverndarlaga“). Þótt ákveðin atriði séu skýr varðandi vinnsluheimildir netöryggissveitarinnar sjálfrar, bæði á grundvelli laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða og þessara draga, þá eru engu að síður ákveðin atriði sem eru óljós gagnvart þeim aðilum sem munu þurfa afhenda netöryggissveitinni persónugreinanleg gögn, m.a. varðandi heimildir þessa aðila fyrir miðlun persónugreinanlegra gagna til netöryggissveitarinnar.

Eftirfarandi athugasemdir félagsins við einstök ákvæði draganna taka mið af framangreindu.

II. kafli: Skipulag og starfsumhverfi

Til að tryggja aðgreiningu milli starfa netöryggissveitarinnar og eftirlitsstarfsemi Póst- og fjarskiptastofnunar, í samræmi við 2. mgr. 4. gr. draganna, verður að mati Símans að tilgreina í reglugerðinni að starfsmönnum PFS sé óheimilt að sinna eftirlitshlutverki hjá PFS samhliða því að sinna öðrum störfum fyrir netöryggissveitina. Telur félagið það ella skjóta skökku við ef starfsmaður eftirlitsaðila fjarskiptageirans eigi jafnframt að sinna hlutverki á vettvangi netöryggissveitarinnar sem hefur svo víðtækt samstarf við fjarskiptafélögin. A.m.k. ætti að taka tillit til þess hvaða hlutverki viðkomandi starfsmaður PFS gegnir ef til skoðunar kemur að bæta viðkomandi starfsmanni við í starfslið netöryggissveitarinnar.

IV. kafli: Samstarf og upplýsingagjöf netöryggissveitar

➤ Um 13. gr.

Í 4. mgr. 13. gr. draganna er fjallað um trúnað sem skuli ríkja um allar upplýsingar sem ræddar eru á fundum netöryggissveitarinnar og þjónustuhópa hennar, og teljast þar að auki til *vinnugagna* í skilningi upplýsingalaga nr. 140/2012.

Sé um að ræða persónugreinanleg gögn, sem hafi verið afhent eða útbúin af aðila innan þessa þjónustuhóps netöryggissveitarinnar (t.d. fjarskiptafélagi), þá vakna spurningar um hvernig *aðgangsrétti einstaklinga* að sama skjali skuli háttað hjá aðilanum sem afhendir netöryggissveitinni skjalið, ef einstaklingurinn óskar eftir aðgangi að upplýsingum um sig hjá þeim aðila, sbr. 17. gr. persónuverndarlaga nr. 90/2018. Síminn minnir á að heimilt er skv. 3. mgr. 17. gr. persónuverndarlaga að takmarka aðgangsrétt einstaklinga með lögum, en af ákvæðum laga nr. 78/2019 eða drögunum sem hér eru til umfjöllunar fæst ekki séð að slíkur aðgangsréttur einstaklinga hafi verið takmarkaður ef þeir fara fram á aðgang að gögnunum hjá *afhendingsaðilanum* (ekki netöryggissveitinni), þ.e. aðilanum sem afhent hefur netöryggissveitinni gögn. Hann hefur einungis verið takmarkaður ef einstaklingurinn óskar eftir aðgangi hjá netöryggissveitinni sjálfri, að því er virðist.

Sé ætlunin að takmarka rétt einstaklinga til aðgangs að gögnunum hjá aðilum innan þessa þjónustuhóps netöryggissveitarinnar, á grundvelli sjónarmiða sem tilgreind eru í 4. mgr. 17. gr. persónuverndarlaga, verður að tilgreina það sérstaklega í reglugerðinni, svo hún taki ekki bara á trúnaðinum sem ríkir á fundum netöryggissveitarinnar og gögnum sem *netöryggissveitin* meðhöndlar á slíkum vettvangi.

V. kafli: Samningar við netöryggissveit

➤ Um 20. gr.

Samkvæmt 20. gr. draganna er netöryggissveitinni heimilt að óska eftir að mikilvægir innviðir eða fjarskiptafyrirtæki geri samninga við sveitina um sjálfvirka upplýsingamiðlun í því skyni að greina og meta áhættu, atvik og aðrar ógnir í net- og upplýsingakerfum þeirra. Ákvæði 20. gr. í drögunum byggir á ákvæði 17. gr. laga nr. 78/2019.

Af skilgreiningum laga nr. 78/2019 og reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu virðist liggja fyrir að

fjarskiptafélag starfi á sviði stafrænna grunnvirkja og teljist því rekstraraðili mikilvægrar þjónustu. Með orðalaginu hér í 20. gr. reglugerðarinnar, um „mikilvægir innviðir eða fjarskiptafyrirtæki“ (áherslubr. undirr.) virðist það opna fyrir túlkun á því að fjarskiptafélag teljist *ekki* meðal mikilvægra innviða. Slíkt gæti valdið misskilningi. Hér að tryggja betur samræmi í orðalagi með hliðsjón af áðurnefndum lögum og reglugerð.

Jafnframt er bent á að í áðurnefndu ákvæði 17. gr. laga nr. 78/2019 segir að *Póst- og fjarskiptastofnun* geti óskað eftir að komið skuli upp sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi mikilvægra innviða og netöryggissveitar. Hins vegar er hér *netöryggissveitinni* falin slík heimild skv. 20. gr. draganna. Í ljósi þess að netöryggissveitin skuli vera skipulagslega aðgreind frá eftirlitshlutverki Póst- og fjarskiptastofnunar, skv. 4. gr. draganna, þykir sérstakt að heimild verði því fyrir tvo aðila á grundvelli annars vegar lagaheimildar og hins vegar heimildar í reglugerð, jafnvel þótt netöryggissveitin sé starfrækt innan Póst- og fjarskiptastofnunar. Þykir Símanum því orðalag 17. gr. laga nr. 78/2019 frekar sæta furðu í þessu samhengi en heimild 20. gr. til handa netöryggissveitinni, m.t.t. hlutverks og verkefna sveitarinnar skv. lögnum og reglugerðinni.

Loks bendir Síminn á að ákvæði 20. gr. gefur ekki skýrlega til kynna hvaða heimild afhendingaraðili gagnanna geti byggt á við miðlun þeirra til netöryggissveitarinnar, í skilningi 9. gr. persónuverndarlaga. Þótt ekki sé víst að hin umrædda sjálvvirka upplýsingamiðlun taki alltaf til persónugreinanlegra gagna virðist þó gert ráð fyrir því samkvæmt orðalagi e)-liðar 1. mgr. 20. gr. Með hliðsjón af framangreindu vill Síminn því góðfúslega koma á framfæri nokkrum athugasemdum vegna ákvæðisins eins og það lítur út núna:

- Almennt þegar um ræðir miðlun til opinbers aðila er venjan sú að miðlun persónugreinanlegra gagna frá einkaaðila til hins opinbera byggir á því að miðlunin sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila (hér afhendingaraðilanum), sbr. orðalag 3. tölul. 9. gr. persónuverndarlaga. Byggir framangreint líka á lögmætisreglu stjórnarsýsluréttar. Hins vegar er orðalagið í 20. gr. draganna mun vægara, þ.e. að þar er talað um *heimild* til handa netöryggissveitinni *til samningagerðar* um miðlun gagna. Ákvæðið minnst ekki á að heimildin stafi af því að það sé í tilvikum þegar netöryggissveitin telur *nauðsynlegt* að afla gagnanna, sbr. 21. gr. laga nr. 78/2019. Að minnsta kosti gefur orðalag 20. gr. það ekki til kynna, þó það sé með almennum hætti vísað til þess í 30. gr. draganna. Er því núverandi orðalag 20. gr. ekki fullnægjandi til þess að afhendingaraðili geti byggt miðlunina á 3. tölul. 9. gr. persónuverndarlaga sem heimild fyrir sjálfvirkri miðlun persónuupplýsinga til netöryggissveitarinnar.
- Enn fremur er óljóst fyrir viðsemjanda netöryggissveitarinnar (eða Póst- og fjarskiptastofnunar, sbr. vangaveltur ofar) hvort honum sé yfir höfuð skylt að ganga til samninga við netöryggissveitina, þar sem orðalagið ákvæðisins virðist einungis mæla fyrir um samningsheimild til handa netöryggissveitinni án þess að nein skylda sé tilgreind í ákvæðinu á hendur afhendingaraðilanum um að verða við slíkri beiðni, sbr. aftur á móti orðalag í 1. mgr. 22. gr. draganna.

- Þótt unnt sé að byggja miðlun persónugreinanlegra upplýsinga skv. 3. tölul. 9. gr. persónuverndarlaga á heimild í stjórnvaldsfyrirmælum settum á grundvelli laga, þá virðist ekki vera ekki um slíkt tilvik að ræða hér þar sem um ræðir samningsheimild til handa netöryggissveit án þess að tilgreint sé að slík miðlun sé nauðsynleg eða afhendingaraðilanum sé skylt að verða við slíkri beiðni um gerð samnings um miðlun gagna. Í þessu samhengi bendir Síminn á að í athugasemdum sem fylgdu með frumvarpi laga nr. 90/2018 segir um 3. tölul. 9. gr. að samningsskyldur falli ekki undir þetta ákvæði. Af framangreindu má ráða, miðað við núverandi orðalag í drögunum, að afhendingaraðili gagnanna geti ekki byggt á 3. tölul. 9. gr. sem heimild fyrir miðlun gagnanna, ef netöryggissveitin óskar eftir að ganga til samninga við „mikilvæga innviði eða fjarskiptafyrirtæki“. Þá tilgreina aðrar heimildir 9. gr. (að undanskildum 1. tölul.) að vinnslan þurfi að vera „nauðsynleg“, en orðalag 20. gr. hefur ekki að geyma slíkt skilyrði, eins og áður segir.
- Þá þykir Símanum það varhugaverð þróun að ekki skuli gerðar strangari kröfur til svo umfangsmikillar upplýsingaöflunar eins og hér um ræðir, sér í lagi þar sem hér er um að ræða sjálfvirka upplýsingamiðlun, sem er a.m.k. fordæmalaus upplýsingamiðlun fyrir fjarskiptafélag hér á landi til opinbers aðila svo vitað sé. Svo umfangsmikil og stöðug gagnaöflun ætti að mati Símans að byggja á afdráttarlausu ákvæði, sem tryggir um leið lögmæti miðlunarinnar frá afhendingaraðilanum, hvort sem er í lögum eða reglugerð. Í þessu samhengi telur Síminn það nauðsynlegt að gerð sé krafa um það í 20. gr. að netöryggissveitin framkvæmi mat á á áhrifum á persónuvernd áður en gengið er frá samningi við mikilvægan innvið eða fjarskiptafélag um sjálfvirka upplýsingamiðlun skv. ákvæðinu, sbr. 29. gr. persónuverndarlaga og auglýsingu nr. 828/2019 um skrá yfir vinnsluaðgerðir sem krefjast ávallt mats á áhrifum á persónuvernd.

Með vísun til framangreindra athugasemda og þeirrar umfangsmiklu og sjálfvirkvinnslu sem hér um ræðir, telur Síminn að gera þurfi ríkari kröfur til ákvæðisins. Til að mynda mætti að mati Símans tryggja að ákvæðið hafi að geyma afdráttarlausu gagnamiðlunarheimild umræddra aðila til netöryggissveitarinnar, n.t.t. í þeim tilvikum sem netöryggissveitin telur slíka gagnaöflun vera *nauðsynlega í þágu þjóðaröryggis eða almannahagsmuna*, eins og skilyrði 21. gr. laga nr. 78/2019 gefa til kynna. Að minnsta kosti þarf umræddum afhendingaraðilum að vera ljóst hvaða heimild miðlunin geti byggt á: 3., 5. eða 6. tölul. 9. gr. persónuverndarlaga. Slíkt ætti um leið að tryggja samræmi milli aðila sem koma til með að þurfa miðla gögnum með þessum hætti til netöryggissveitarinnar.

Berist ráðuneytinu ekki umsögn frá Persónuvernd vegna þessara draga bindur Síminn vonir við að ráðuneytið kalli eftir sjónarmiðum stofnunarinnar við a.m.k. þessu ákvæði í drögunum, til að tryggja að miðlun afhendingaraðilanna verði lögmæt, ella gæti verið um óheimila vinnslu að ræða sem gæti kostað mögulega bæði netöryggissveitina og afhendingaraðilunum háar stjórnvaldssektar skv. persónuverndarlögum.

Í ljósi þeirrar öryggis-, orðspors- og setkaráhættu sem fylgir því fyrir afhendingaraðilana að afhenda umfangsmikil gögn til netöryggissveitar með

sjálfvirkum hætti eins og hér um ræðir, ætti jafnframt að tilgreina í reglugerðinni að netöryggissveitin skuli bera ábyrgð á vinnslu gagna sem verður til vegna beiðna og/eða tilmæla hennar og að netöryggissveitin skuli halda fjarskiptafélag skaðlausu af kvörtunum eða skaðabótakröfum sem kunna að berast vegna þess að fjarskiptafélag fylgdi tilmælum eða varð við beiðni netöryggissveitar.

➤ *Um 21. gr.*

Síminn áréttar að það sé varasamt að ætla opinberri stofnun, sem fjármögnuð er með ríkisframlögum eða skattlagningu, hlutverk sem á köflum felur í sér þjónustu sem einkaaðilar hafa fulla burði til að sinna og eru jafnvel þegar að selja í dag. Þar af leiðandi skapast sú áhætta að netöryggissveitin fari inn á svið þjónustu sem er ekki á grundvelli almannahagsmuna og eðlilegt sé að ríkið fjármagni. Mörkin á milli þess sem er á grundvelli ríkisstuðnings og þjónustu í samkeppni við einkaaðila þurfa að vera afdráttarlaus.

➤ *Um 22. gr.*

Ákvæðið felur í sér heimild til handa netöryggissveitinni að skylda fjarskiptafélög til að gera samning við sig um „tæknilega vöktun“.

Hér mætti fyrst skýra betur hvað falli undir „tæknilega vöktun“ í skilningi ákvæðisins.

Bent er á að einkaaðilar (upplýsingatæknifyrirtæki) eru nú þegar að veita slíka þjónustu gegn endurgjaldi. Vafalaust eru flest fjarskiptafélög hérlandis þegar að nýta sér slíka þjónustu. Í ljósi þessa er óljóst hvers vegna fjarskiptafélög þurfi að gera slíka samninga við netöryggissveitina, sér í lagi þar sem skyldan virðist ganga lengra en ákvæði 2. mgr. 16. gr. laga nr. 78/2019 og eru því engin rök fyrirbyggjandi um ákvæðið. Þá liggur ekki fyrir hvernig sveitin muni tryggja viðeigandi og fullnægjandi öryggi í tengslum við slíka vöktun, þótt reglugerðin hafi að geyma almenn fyrirmæli til handa sveitinni um öryggisráðstafanir (sbr. 29. gr. og 32. gr.). Ekki er því fyrirséð í fljótu bragði að þau fjarskiptafélög sem nú þegar kaupa slíka þjónustu hjá einkaaðila muni segja henni upp og stóla einvörðungu á vöktunarþjónustu netöryggissveitarinnar þegar að því kemur ef minnsti vafi leikur á að öryggisráðstafanir sveitarinnar séu ekki eins ríkar og hjá núverandi þjónustuveitanda.

Telur Síminn jafnframt í þessu samhengi eðlilegt að netöryggissveitin eða PFS taki á sig ábyrgð vegna mögulegs tjóns sem fjarskiptafélag eða viðskiptavinir þess kunna að verða fyrir vegna vöktunarþjónustu netöryggissveitarinnar, svo sem ef netöryggissveitin getur af einhverjum ekki veitt þjónustuna eða tryggt öryggi hennar.

Einnig vísar Síminn til athugasemda ofar um ákvæði 20. gr. draganna, varðandi þá óvissu sem ríkir um hvaða heimild fjarskiptafélag geti byggt miðlun persónuupplýsinga á skv. 9. gr. persónuverndarlaga, ef gert er ráð fyrir að vinnslan taki til persónugreinanlegra gagna. Þótt orðalag 22. gr. sé afdráttarlausara í orðalagi (sbr. „farið fram á“ og „skal fjarskiptafyrirtæki verða við slíkri beiðni“), er einnig talað hér um samningsheimild til handa netöryggissveitinni. Hér mætti skerpa betur á að heimild netöryggissveitarinnar til vöktunarinnar sé *nauðsynleg* á grundvelli þessa reglugerðarheimildar, sbr. einnig 21. gr. laga nr. 78/2019, svo

það sé afdráttarlaust fyrir fjarskiptafélög að miðlun eða jafnvel aðgengi að persónuupplýsingum sín megin sé heimil á grundvelli 9. gr. persónuverndarlaga.

Að öðru leyti vísar Síminn einnig til athugasemda ofar um ákvæði 20. gr. um að reglugerðin eigi að tilgreina sérstaklega að netöryggissveitin skuli halda fjarskiptafélagi skaðlausu af hvers kyns kröfum eða kvörtunum sem kunna verða eða berast þegar fjarskiptafélag fylgir tilmælum eða verðum við beiðnum netöryggissveitar.

Loks verður að tryggja að fjarskiptafélaginu sé þó veitt svigrúm til að semja um ákveðna þætti í samningi sínum við netöryggissveitina, svo sem um tegund búnaðar sem tengja skal við búnað netöryggissveitarinnar, með hliðsjón af þeim kostnaði sem fjarskiptafélagið gæti ella þurft að bera ef íþyngjandi skilyrði af slíkum toga eru sett einhliða af hálfu netöryggissveitarinnar.

VII. kafli: Vinnsla persónuupplýsinga

➤ 30. gr.

Eins og ofar greinir þarf að tryggja rökrétt samhengi milli ákvæða 20., 22. og 30. gr. reglugerðarinnar, svo það sé ekki misvísandi hvort um sé að ræða valkvæða heimild netöryggissveitarinnar til gagnaöflunar eða hvort um sé að ræða afdráttarlausa heimild til nauðsynlegrar gagnaöflunar. Með skýru og samræmdu orðalagi verður afhendingaraðilum ljóst hvort unnt sé að byggja gagnamiðlun til netöryggissveitarinnar á 9. gr. persónuverndarlaga og þá hvaða heimild í ákvæðinu.

Til viðbótar framangreindu þykir afar sérstakt að netöryggissveitinni sé veitt svigrúm að meta sjálf varðveislutíma gagna sem sveitin vinnur með eins og henni þykir nauðsynlegt, án neinna viðmiða eða frekari fyrirmæla. Slíkt fyrirkomulag hlýtur að teljast hæpið í ljósi ákvæðis um varðveisluskyldu gagna skv. 1. mgr. 24. gr. laga nr. 77/2014 um opinber skjalasöfn nema fyrir liggi samþykkt þjóðskjalavarðar eða *sérstakt lagaákvæði*. Þá hafa önnur lög og stjórnvaldsfyrirmæli almennt vísað til „varðveislutíma“ gagna, fremur en „geymslutíma“.

➤ Um 31. gr.

Komi til þess að framkvæma þurfi mat á áhrifum á persónuvernd vegna gagna sem netöryggissveitin aflar frá þriðja aðila ætti einnig að tilgreina í ákvæði 31. gr. að að matið eigi jafnframt taka til gagnaöflunarinnar, sér í ljósi þar sem umrætt mat getur tekið til margra vinnsluaðgerða. Í þeim tilvikum sem matið tekur jafnframt til gagnaöflunarinnar skal jafnframt, eftir því sem frekast er unnt, framkvæma það með aðstoð og aðkomu viðkomandi afhendingaraðila.

Virðingarfyllt,
f.h. Símans hf.

Helga Grethe Kjartansdóttir,
lögfræðingur og persónuverndarfulltrúi