Síminn

Samgöngu- og sveitarstjórnarráðuneytið
Sölvhólsgötu 7
101 Reykjavík

Reykjavík, 23. júní 2020

Efni: Umsögn um drög að reglugerð um öryggi net- og upplýsingakerfi mikilvægra innviða

I. Inngangur

Síminn hf. vísar til draga samgöngu- og sveitarstjórnarráðuneytisins til reglugerðar um öryggi net- og upplýsingakerfa mikilvægra innviða. Markmið reglugerðarinnar er að innleiða nánari útfærslur á tilteknum ákvæðum laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða sem munu öðlast gildi þann 1. september nk.

Síminn hefur yfirfarið drögin og vill góðfúslega koma á framfæri eftirfarandi athugasemdum til ráðuneytisins fyrir hönd félagsins, þ.m.t. dótturfélags þess Sensa ehf.

II. Umsögn Símans

Áður en lengra er haldið vill Síminn vekja athygli á því að NIS tilskipunin gildir ekki um fjarskiptafyrirtæki og virðist þannig útvíkkun reglugerðarinnar í þá veru fela í sér ólögmæta innleiðingu sem væri í andstöðu við EES rétt. Þannig segir eftirfarandi með berum orðum í inngangi tilskipunarinnar (7. liður):

> „To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. **However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council (3), which are subject to the specific security and integrity requirements laid down in that Directive**, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council (4), which are subject to the security requirements laid down in that Regulation."

Er þetta síðan sérstaklega tekið fram í gildissviði tilskipunarinnar í 3. Mgr. 1. Gr. hennar, en þar segir:

> „The security and notification requirements provided for in this Directive **shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC,** or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014."

Ennfremur er áréttað að í frumvarpi til laganna sem innleiddi NIS tilskipunina segir m.a. eftirfarandi:

> „Því skal haldið til haga að **fjarskiptafyrirtæki falla ekki undir gildissvið tilskipunar (ESB) 2016/1148**, enda er nú þegar í fjarskiptalögum og evrópsku regluverki á sviði fjarskipta að finna sambærilegar skyldur varðandi skipulag upplýsingaöryggis."

Framangreint virðist einnig vera ljóst af orðalagi skýrslu[1] framkvæmdastjórnar ESB frá október 2019, sbr. eftirfarandi umfjöllun í skýrslunni:

> „Article 1(3) stipulates that the NIS Directive **does not apply to undertakings subject to the requirements of the Telecom Framework Directive**. However, some Member States appear to have identified OES providing services that should actually be regulated under the Telecom Framework Directive, such as internet access and telephony services.
>
> In addition, according to Article 1(7) the provisions of the NIS Directive on security requirements and incident notification **do not apply to operators that are already regulated by sector-specific Union legal acts laying down obligations of at least equivalent effect."**

Í ljósi framangreinds og þess að sérlög og -reglur eiga við um starfsemi fjarskiptafélaga hér á landi (þ.m.t. í tengslum við öryggi), eiga fjarskiptafyrirtæki og fjarskiptaþjónusta þar af leiðandi að vera undanskilin með skýrum hætti í reglugerðinni sem hér er til umfjöllunar og að um leið verði skýrlega afmarkað hvaða þjónusta í reglugerðinni falli undir tilskipunina, en telst ekki til fjarskiptaþjónustu. Ef mörkin milli laganna eru ekki skýr blasir við ágreiningur um efnislegt inntak laganna. Síminn hefur lagt áherslu á að það verði að vera skýrt hvaða þjónusta falli undir hvaða lög.

Sé ætlunin að láta fjarskiptafélög falla undir gildissvið reglugerðarinnar telur Síminn það brýnt og nauðsynlegt að ráðuneytið afli viðbragða sérstaklega frá fjarskiptafélögum þar að lútandi.

Þrátt fyrir framangreint vill Síminn engu að síður koma á framfæri eftirfarandi athugasemdum um drögin, þótt félagið telji sig ekki falla undir gildissvið reglugerðarinnar.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN, bls. 20.

I. og II. Kafli: Almenn ákvæði og þjónusta sem skilgreind er nauðsynleg

- *1. gr.*

Samkvæmt 3. mgr. 1. gr. reglugerðarinnar gildir hún einnig um „net- og upplýsingakerfi stafrænnar þjónustu sem starfrækja netmarkað, leitarvél á netinu og skýjavinnsluþjónustu og teljast ekki til örfélaga í skilningi laga um ársreikninga".

Síminn bendir á að það er afar erfitt að greina hvaða aðilar falli undir hér, og þar með líka gildissvið samnefndra laga nr. 78/2019, sérstaklega í ljósi þess að ekki er fyrirhugað að birta nein sérstök viðmið í reglugerðinni um þessa aðila. Þá virðist ekki heldur fyrirhugað að birta sambærilega skrá yfir þessa aðila, líkt og gert verður um rekstraraðila nauðsynlegrar þjónustu fyrir 1. september nk. Nauðsynlegt er því að rýna ekki bara reglugerðina sjálfa, heldur skilgreiningar á alls þremur hugtökum í 6. gr. áðurnefndra laga (20., 24., og 27. tölul.), sem og skýringar um 20. tölul. 6. gr. í athugasemdum með frumvarpi þeirra laga, til þess eins að átta sig á hvort viðkomandi falli undir gildissvið regluverksins.

Framsetningin er því, eins og gefur að skilja, afar þjál og erfið yfirferðar. Þótt lögin sjálf byggi að mestu leyti á tilskipun Evrópusambandsins, þá telur Síminn engu að síður tilefni til að ráðuneytið skoði hvort unnt sé að haga framsetningu reglugerðarinnar m.t.t. veitenda stafrænnar þjónustu með öðrum hætti til að tryggja að regluverkið nái markmiði sínu, t.d. með því að bæta við skilgreiningu á því hverjir falli undir þetta hugtak.

Með hliðsjón af framangreindu telur Síminn það einnig vera nokkuð erfitt að lesa reglugerðina m.t.t. stöðu þessara aðila, þar sem þessir aðilar verða um leið að vera meðvitaðir um að þeir teljast einnig til „mikilvægra innviða" í skilningi laganna, þótt reglugerðin tilgreini á vissum stöðum undantekningar fyrir einungis veitendur stafrænnar þjónustu (13., 15., 17. og 22. gr.).

- *a-liður 1. mgr. 10. gr.*

Samkvæmt drögunum er skilgreind „þjónusta á sviði stafrænna grunnvirkja" í 10. gr. reglugerðarinnar. Að mati félaganna er orðalag bæði a- og b-liðar 1. mgr. ekki nógu skýrt og þarf að skilgreina mun betur hvað sé átt við með „stafrænu grunnvirki".

Að því er varðar skilyrði a-liðar um markaðshlutdeild viðkomandi rekstraraðila vill Síminn benda á að núverandi orðalag ákvæðisins miðar við markaðshlutdeild á landsvísu, að því er virðist. Sé það ætlun ráðuneytisins að viðhalda slíku skilyrði í reglugerðinni vill Síminn vekja athygli á að það geti eftir atvikum leitt til þess að ákvæðið nái ekki til þeirra rekstraraðila sem ráðuneytið hefur ætlað að láta reglugerðina ná til svo að hún nái markmiði sínu skv. 2. gr. Eins og kunnugt er getur markaðshlutdeild fjarskiptafélaga til að mynda verið afar mismunandi eftir því hvort miðað sé við landið í heild sinni eða afmörkuð landssvæði eða jafnvel hverfi (þegar um ræðir höfuðborgarsvæðið).

Jafnframt þarf að vera skýrt hvaða markað sé þarna verið að vísa til. Er verið að vísa til þess að „tengi- og skiptipunktar" sé sérstakur markaður þar sem rekstraraðili er með umfangsmikla markaðshlutdeild? Síminn telur brýnt að

ráðuneytið taki framangreind áhyggjuefni til nánari skoðunar og uppfæri drögin til að eyða þeirri óvissu sem ákvæðið ber með sér í óbreyttri mynd. Einnig er alls kostar óljóst, ef ekki ómögulegt, fyrir aðila að þekkja hver hlutdeild þeirra sé á viðkomandi markaði og hvaða aðrir aðilar kunni að vera á þeim markaði.

- *b-liður 1. mgr. 10. gr.*

Síminn gerir ekki sérstakar athugasemdir við þau viðmið sem tilgreind eru í b-lið 1. mgr., en vekur þó athygli á umfjöllun ofar um afmörkun viðmiða m.t.t. reksturs fjarskiptafélaga, einkum í ljósi skýrslu framkvæmdastjórnar ESB. Hins vegar dregur Síminn þá ályktun af þessum viðmiðum að huga þurfi sérstaklega að því í samningagerð og samskiptum við birgja sem félagið kaupir þjónustu sína frá og reglugerðin nær *ekki* til. Sem dæmi virðist liggja ljóst fyrir að félög á borð við Mílu ehf., Gagnaveitu Reykjavíkur ehf. og Tengir ehf. falla ekki undir reglugerðina. Í tilviki Símans er afar mikilvæg þjónusta aðkeypt frá þessum aðilum. Í ljósi þess að fjarskiptaþjónusta fellur ekki undir NIS-tilskipunina, sbr. umfjöllun ofar, þarf að vera ljóst að samningar og samskipti þessara aðila falli ekki undir reglugerðina.

III. kafli: Lágmarkskröfur um áhættustýringu og ráðstafanir

Af orðalagi reglugerðarinnar virðist vera ljóst að ekki sé gerð skýlaus krafa um að þeir aðilar sem falla undir gildissvið reglugerðarinnar séu með formlega vottað stjórnkerfi upplýsingaöryggis, heldur fremur að stjórnkerfi þess (eða a.m.k. framkvæmd áhættustýringar og viðbúnaðar skv. 11. gr. reglugerðarinnar) „byggi á" viðurkenndum stöðlum. Þótt skiljanlegt sé að torsótt sé að gera formlega kröfu um það í reglugerð að allir umræddir aðilar skuli votta stjórnkerfi sín, þá vill Síminn engu að síður vekja athygli á að þeir aðilar sem hafa þegar lagt mikla vinnu og kostnað í að öðlast *formlega* vottun af slíkum toga hljóta að standa betur að vígi þegar kemur að eftirliti eftirlisstjórnvaldsins. Með hliðsjón af framangreindu telur Síminn því tilefni til þess að ráðuneytið taki til vandlegrar skoðunar hvort unnt sé að taka tillit til stöðu slíkra aðila í reglugerðinni þegar um ræðir eftirlitsheimildir .

Til að mynda mætti í reglugerðinni tilgreina á ákveðnum stöðum að *sérstakt tilefni* eða *sérstök ástæða* þurfi að standa að baki beiðni eða úrræðum eftirlitsstjórnvaldsins, sem í framkvæmd myndi þá almennt þýða að eftirlitsstjórnvaldið telji ekki vottun eina og sér nægilega fullnægjandi heldur sé tilefni til að greina nánar tiltekin atriði hjá viðkomandi aðila. Einnig mætti hugsa sér aðra leið þar sem reglugerðin gerir ráð fyrir að eftirlitsstjórnvaldið hafi þau úrræði sem reglugerðin kveður á um hjá vottuðum aðila þegar t.d. þjóðar- eða almannaöryggi er stefnt í hættu.

Að minnsta kosti hlýtur vottun á stjórnkerfi aðila sem falla undir reglugerðina að draga að einhverju leyti úr umfangi eftirlitsins af hálfu eftirlitsstjórnvaldsins, miðað við þá aðila sem einungis „byggja á" eða taka með einhverjum hætti mið af viðurkenndum stöðlum í rekstri sinna upplýsingakerfa.

- *11. gr.*

Að mati Símans er orðið „áhrifagreining" í 1. mgr. 11. gr. óþarft, þar sem áhættumatsgerð felur alltaf í sér mat á áhættu, áhrifum og líkindum þess.

IV. og V. kafli: Skipulagslegar og tæknilegar ráðstafanir

- *13. gr.*

Síminn telur orðalag ákvæðisins, einkum 1. mgr., of afdráttarlaust. Það að mikilvægur innviður *skuli ávallt* endurskoða áhættumat í kjölfar atviks eða áhættu virðist vera óþarfi í *öllum* tilvikum. Það hlýtur að vera matskennt hvort atvikið eða áhættan sem um ræðir sé þess eðlis að það/hún kalli á slíka endurskoðun.

- *a-liður 1. mgr. 15. gr.*

Í staðinn fyrir orðalagið „[m]eta hvort *tilefni* sé til að afla sakavottorðs[...]", mætti að mati Símans breyta orðalaginu í „[m]eta hvort *nauðsynlegt* sé að afla sakavottorðs[...]", í ljósi orðalags 8. gr. og 12. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga. (sbr. einnig orðalag í 28. gr. þessarar reglugerðar um „nauðsyn").

- *tölul. a-liðar 1. mgr. 18. gr.*

Að mati Símans ætti ákvæðið fremur að vísa til *„viðeigandi aðgangsstýringarkerfis* til auðkenningar á notendum og kerfum" fremur en „[...]*sannvottunar* á notendum og kerfum".

- *4. tölul. a-liðar 1. mgr. 18. gr.*

Að mati Símans ætti að bæta við orðinu „viðeigandi" í ákvæðið, svo það hljóði svona:

> „4. Viðhafa *viðeigandi* ráðstafanir sem tryggja rekjanleika uppflettinga og vinnsluaðgerða"

- *c-liður 1. mgr. 18. gr.*

Í ljósi meðalhófssjónarmiða ætti einnig að mati Símans að bæta við orðinu „viðeigandi" í ákvæðið, svo það hljóði svona:

> „a. Setja *viðeigandi* umferðartakmarkanir í net- og upplýsingakerfum."

- *g-liður 1. mgr. 18. gr.*

Í ákvæðinu er vísað til „mikilvægra atburða". Skilningur Símans á ákvæðinu er að það hljóti að vera undir hverjum og einum aðila að meta fyrir sitt leyti hvað teljist vera „mikilvægur atburður" sem ákvæðið tekur til, miðað við rekstur aðilans og þær áhættur sem skilgreindar hafa verið í tengslum við þann rekstur.

VI. kafli: Viðhald, viðbragðsáætlun, innra eftirlit og atvikatilkynningar

- 25. gr.

Í 1. mgr. er minniháttar innsláttarvilla („net- og upplýsingaskerfumskerfum").

Varðandi leiðbeiningar Netöryggissveitarinnar kallar Síminn eftir því að þær verði birtar fyrir gildistöku laganna (og þar með reglugerðarinnar) þann 1. september nk., í ljósi þeirra hagsmuna sem hér um ræðir.

Síminn bendir einnig á innsláttarvillu í 5. mgr. ákvæðisins („eigi síðar en eigi síðar en"), en burtséð frá því telur Síminn að ekki sé unnt að tilgreina sérstaklega 6 klukkustundir í þessu samhengi, þar sem lögin og NIS-tilskipunin tilgreinir orðalagið „svo fljótt sem verða má" (e. „without undue delay"). Hvergi er minnst á fjölda klukkkustunda í þessum efnum í lögunum. Að mati Símans ætti því að taka út tilvísun um 6 klukkustundir í 5. mgr. 25. gr., til samræmis við orðalag laganna, sbr. 1. mgr. 8. gr. laga nr. 78/2019. Þar að auki er slíkur 6 klukkustunda tímafrestur of skammur að mati Símans. Til samanburðar má t.d. benda á að sambærilegar tilkynningar um öryggisbresti við meðferð persónuupplýsinga, skv. lögum nr. 90/2018, eiga að berast Persónuvernd eigi síðar en 72 klst. frá því að ábyrgðaraðili varð var við öryggisbrestinn. Afar ósennilegt þykir a.m.k. að mikilvægur innviður geti veitt Netöryggissveitinni allar þær upplýsingar sem tíundaðar eru í ákvæðinu, ef einhverjar, innan þessa skamma tímafrests. Þá gæti orðið erfitt í framkvæmd að láta mikilvæga innviði starfrækja nokkurs konar bakvakt sem sinni eftirliti með atvikum af þessum toga undir allan sólarhringinn, alla daga vikunnar, svo unnt sé að uppfylla þessar ströngu tímakröfur.

- *26. gr.*

Samkvæmt ákvæði 26. gr. skal „[á] heimasíðu mikilvægs innviðar, eða með öðrum sambærilegum leiðum, [...] *tilgreina þjónustuviðmið, svo sem um þjónustustig og reglubundið viðhald*". Að mati Símans ætti framangreind krafa að vera háð ákveðnum fyrirvara í lokin, n.t.t. með eftirfarandi orðalagi „[]*ef slíkar lýsingar eru til staðar*". Sé það afdráttarlaus krafa að birta slík þjónustuviðmið á heimasíðu aðilans mun það kalla á umfangsmikla og tímafrekar vinnu af hálfu þeirra aðila sem búa ekki nú þegar yfir slíkum lýsingum í starfsemi sinni. Að minnsta kosti ætti þetta ákvæði reglugerðarinnar ekki að eiga við um slíka aðila fyrr en að a.m.k. einu ári liðnu frá gildistöku reglugerðarinnar að mati Símans.

III. Lokaorð

Að mati Símans er ljóst að starfsemi fjarskiptafélaga eigi ekki að falla undir gildissvið reglugerðarinnar. Telji ráðuneytið engu að síður að regluverkið eigi að taka til slíkrar starfsemi telur félagið brýnt að nánara samráð verði haft við fulltrúa fjarskiptafélaga hérlendis áður en drög reglugerðarinnar verða samþykkt.

Til viðbótar framangreindum athugasemdum telur Síminn það nauðsynlegt að ráðherra birti skrá yfir rekstraraðila nauðsynlegrar þjónustu í við fyrsta tækifæri, þar sem afar skammur tími er fram að gildistöku laganna og þar með reglugerðarinnar sm hér um ræðir.

f.h. Símans,

Helga Grethe Kjartansdóttir, lögfræðingur