



Fjarskiptastofa
bt. skrifstofu stafræns öryggis
Suðurlandsbraut 4
108 Reykjavík

Reykjavík, 20. mars 2025

Efni: Athugasemdir við drög Fjarskiptastofu að stefnu um fyrirkomulag og framkvæmd eftirlits með net- og upplýsingaöryggi

I. Inngangur

Síminn hf. (hér eftir „Síminn“ eða „félagið“) vísar til fréttar Fjarskiptastofu (hér eftir „FST“ eða „stofnunarinn“) á vef stofnunarinnar frá 20. febrúar sl. þar sem birt voru drög að stefnu hennar um fyrirkomulag og framkvæmd eftirlits með rekstraraðilum stafrænna grunnvirkja, veitenda stafrænnar þjónustu og fjarskiptafyrirtækja.

Bauð stofnunarinn hlutaðeigandi aðilum að koma á framfæri sjónarmiðum og athugasemdum við drögin til og með 20. mars 2025.

Síminn þakkar fyrir veitt tækifæri til að koma á framfæri athugasemdum vegna draganna. Félagið fagnar því einnig að stofnunarinn beiti sér fyrir því að auka gagnsæi milli hennar og hlutaðeigandi aðila þegar kemur að framkvæmd eftirlits af þessum toga. Þá tekur félagið undir að hér sé um afar mikilvægan rekstur að ræða sem gegnir mikilvægu hlutverki í samfélaginu, ekki síst þegar kemur að öruggum tengingum landsins við umheiminn á umrótatímum.

Að mati félagsins er þó vert að benda á nokkur álítaefni sem vakna við lestur draganna, einkum hvað varðar tímasetningu stefnunnar og tíðni og umfang *ex ante* eftirlitsúrræða stofnunarinnar, eins og hér verður nánar lýst í umfjöllun neðar.

II. Sýn Fjarskiptastofu

Líkt og drögin bera með sér, er fyrirhugað að viðhafa ýmiss konar eftirlit með hlutaðeigandi aðilum, svo unnt sé m.a. að draga úr áhættu á þjónusturofi eða annars konar atvikum í rekstri umræddra aðila. Byggir stofnunarinn eftirlitsaðgerðir sínar á heimildum í fjarskiptalögum nr. 70/2022 og netöryggislögum nr. 78/2019 og mögulega 3. mgr. 24. gr. draga reglugerðar um öryggi fjarskiptaneta og fjarskiptaþjónustu.

Í stefnudrögunum eru ýmsar aðgerðir eftirlitsaðgerðir tilgreindar, einkum áhættumat á fjarskiptainnviðum, framkvæmd sjálfsmata hjá fjarskiptafyrirtækjum og rekstraraðilum stafrænna grunnvirkja. Þá hyggst stofnunarinn einnig ráðast í úttektir og prófanir, svo sem í formi skrifborðsúttekta, tæknilegra prófana eða vettvangsúttekta. Jafnframt fjallar stofnunarinn um að hún gæti eftir atvikum þurft að veita aðila bindandi fyrirmæli ef niðurstöður úr áðurnefndum aðgerðum kalla á úrbætur að mati stofnunarinnar og sinna í kjölfarið að þeim sé fylgt eftir af hálfu hlutaðeigandi félags.



Þá fjallar stofnunin einnig um sértæk áhættumöt á fjarskiptanetum og -þjónustu sem stofnunin gæti gripið til með stuttum fyrirvara, svo sem ef veruleg ógn steðjar að framangreindum þáttum. Þá nefnir stofnunin einnig að hún hafi á árinu 2024 tekið að sér að áhættumeta sérstaklega öryggi útvistunar og birgðakeðju 5G neta. Bendir stofnunin á að framangreindar aðgerðir séu allar hluti af *ex ante* eftirliti stofnunarinnar.

Til viðbótar framangreindum aðgerðum og úrræðum gegnir stofnunin einnig lögbundnu rannsóknar- og eftirlitshlutverki þegar upp koma tilkynningarskyld atvik, þá einkum alvarleg öryggisatvik, þ.e. *ex post* eftirliti.

III. Athugasemdir og sjónarmið Símans

a) Almenn

Áður en lengra er haldið skal tekið fram að Síminn er ekki í eftirfarandi umfjöllun að gera athugasemdir við eftirlitshlutverk stofnunarinnar eða markmið þess. Þvert á móti er skilningur fyrir hendi um mikilvægi þess og þá skyldu sem hvílir á stofnuninni lögum samkvæmt að sinna slíku eftirliti. Þó er einnig mikilvægt að eftirlitsstarfsemi stofnunarinnar gangi ekki lengra en lög og reglur gera ráð fyrir, ef það er ekki nauðsynlegt í ljósi aðstæðna hverju sinni og fyrirbyggjandi upplýsinga.

Það sem félagið telur þó vert að benda á í eftirfarandi umfjöllun er að það verði að vanda vel til verka þegar kemur að tímasetningu á útgáfu stefnu af þessum toga, útfærslu og framkvæmd eftirlitsaðgerða hverju sinni og að tekið verði tillit til vottana sem félag kann að búa yfir til að staðfesta að ákveðnu leyti sömu atriði og eftirlitsaðgerðir stofnunarinnar lúta að. Ella er hætt á að rekin verði umfangsmikil og íþyngjandi eftirlitsaðgerð án forsvaranlegra ástæðna, með tilheyrandi kostnaði og álagi fyrir hlutaðeigandi félög. Þar með er einnig hætt á að málarekstur stofnunarinnar stangist á við meðalhófssjónarmið og að eftirlitið verði óskilvirkt, t.d. ef mörg mál eru rekin hjá eftirlitinu á hverjum tíma gagnvart sama félaginu og/eða að þau gætu skarast innbyrðis.

b) Áhrif NIS-2

Óljóst er hvort náist að innleiða NIS2-regluverkið hér á landi á þessu ári, en afar líklegt er að það verði fremur innleitt á næsta ári, eða árið 2026. Með tilkomu þess regluverks munu bæði fleiri aðilar falla undir regluverkið auk þess sem það, eðli málsins samkvæmt, leiðir til umfangsmeiri eftirlitsstarfsemi af hálfu stofnunarinnar. Þar að auki hefur reglugerð um öryggi fjarskiptaneta og fjarskiptaþjónustu ekki enn tekið gildi heldur. Af þessum sökum telur félagið ótímabært að gefa út stefnu af þessum toga til rúmlega tveggja ára þegar það liggur fyrir að væntanlegar séu svo umfangsmiklar breytingar á regluverki á inna við næstu tólf mánuðum eða svo. Telur félagið því bæði skilvirkara og rökrétt að fresta útgáfu stefnunnar og útfæra hana nánar þegar framangreind regluverk hafa verið innleidd og tekið gildi hér á landi.

c) Tímabil stefnu

Samkvæmt drögunum gerir stofnunin ráð fyrir þriggja ára áætlun um framkvæmd *ex ante* eftirlits, þrátt fyrir að stefnan sjálf eigi bara að gilda út árið 2027. Vekur það strax upp spurningar um vægi stefnunnar þegar fram líða stundir, þar sem stofnunin nær að öllum líkindum ekki að beita þeim úrræðum sem þar eru til umfjöllunar fyrir lok tímabils stefnunnar.

Í ljósi þeirra umfangsmiklu og tímafreku *ex ante* eftirlitsaðgerða sem stefnan fjallar um ætti hún að hafa mun lengri gildistíma en til rúmlega tveggja ára, eins og stofnunin leggur hér til.



d) Áhrif tíðra og umfangsmikilla eftirlitsaðgerða

Hver og ein þeirra eftirlitsaðgerða sem eru til umfjöllunar í stefnunni er tímafrek og umfangsmikil og kallar á aðkomu margra sérfræðinga af hálfu hlutaðeigandi félags. Reynsla Símans er t.a.m. sú að framkvæmd sjálfsmats getur tekið nokkra mánuði. Þá þarf í slíkum málum að ráðstafa mikilvægum sérfræðingum úr daglegum skyldum og verkefnum til þess að svara ítarlegum gagnabeiðnum stofnunarinnar, jafnvel með stuttum fyrirvara, með tilheyrandi kostnaði. Í þessu samhengi skal bent á að jafnvel þótt stofnunin upplýsi um að það sé fyrirhuguð eftirlitsaðgerð á tilteknu ári eða jafnvel ársfjórðungi er nær ómögulegt fyrir félagið að undirbúa sig að nokkru leyti fyrir framkvæmdina fyrr en gagnabeiðnin sjálf berst og ljóst verður hvert umfangið og inntakið er í beiðninni. Þegar erindi berst frá stofnuninni um fyrirhugaða eftirlitsaðgerð, hverju nafni sem hún nefnist, þarf félagið að ráðstafa mikilvægum sérfræðingum innanhús í málið og um leið taka þau úr öðrum mikilvægum verkefnum sem þau eiga að sinna í þágu upplýsinga- og rekstraröryggis hjá félaginu. Má því leiða líkur að því að tímafrekar og tíðar *ex ante* eftirlitsaðgerðir gætu snúist upp í andhverfu sína og leitt til áhættu fyrir rekstur hlutaðeigandi félags.

Þá gæti einnig komið upp sú staða, þegar mál eru rekin hjá stofnuninni með stuttu millibili eða jafnvel samtímis að þau skarist innbyrðis. Gæti því komið upp sú staða að stofnunin óski umfangsmikilla gagna/upplýsinga frá félagi í einu máli þótt þau séu þegar til staðar í skjalasafni stofnunarinnar í tengslum við annað mál sem er þegar eða var nýlega til meðferðar, hvort sem það var í tengslum við *ex ante* eða *ex post* eftirlit stofnunarinnar. Því miður hefur Síminn þegar lent í aðstæðum af þessum toga, þar sem óskað var upplýsinga/gagna sem höfðu þegar verið afhent stofnuninni í tengslum við gagnabeiðni stuttu áður.

Einnig ber að hafa hugfast að hér á landi eru fjarskiptafélög ekki með sama starfsmannafjölda og annars staðar í Evrópu og því er sérstaklega brýnt að eftirlitsframkvæmd stofnunarinnar verði skilvirk, gagnsæ og standist meðalhófssjónarmið, eins og áður segir.

e) Tillögur Símans

Að teknu tilliti til þeirra markmiða sem drögin fjalla um, lögbundins hlutverks Fjarskiptastofu, og þeirra umfangsmiklu breytinga sem væntanlegar eru á netöryggisregluverki leggur Síminn í fyrsta lagi til að innleiðing og útfærsla stefnu af þessum toga verði frestað þar til NIS2-regluverkið hefur verið innleitt hér á landi.

Í öðru lagi leggur stofnunin til að stefna af þessum toga miði við lengri tímaramma en drögin miða við, sér í lagi í tengslum við reglubundnu *ex ante* eftirlitsaðgerðir. Að lágmarki ætti stefna af þessum toga að hafa u.þ.b. fimm til tíu ára gildistíma, í stað rúmlega tveggja ára eins og nú er lagt upp með. Að því sögðu væri þó vitanlega skiljanlegt ef slík stefna væri háð ákveðnum fyrirvörum, svo sem ef stofnunin myndi á tímabilinu telja þörf á að grípa til eftirlitsaðgerða oftar en stefnan kveður á um ef brýnar ástæður eru fyrir hendi, svo sem vegna alvarlegs öryggisatviks í starfsemi félagsins eða ef utanaðkomandi aðstæður stefna öryggi fjarskiptaneta/-þjónustu eða rekstrarumhverfi hlutaðeigandi félaga í hættu. Þannig þyrfti stofnunin að sýna fram á að nauðsyn og mikilvægi þess að ráðast í umfangsmeiri eftirlitsaðgerðir en stefnan gerir almennt ráð fyrir. Félagið getur ekki séð af hverju slík útfærsla ætti ekki að vera tæk af hálfu stofnunarinnar.

Í þriðja lagi telur félagið nauðsynlegt að stefna af þessum toga, og þar með eftirlit stofnunarinnar, taki í mun meira mæli mið af því hvort hlutaðeigandi félag sé með alþjóðlega viðurkennda vottun sem gefur til kynna ákveðnar forsendur í rekstri og upplýsingaöryggi hjá



félaginu. Hér er einkum átt við ISO-27001 vottun fyrir stjórnkerfi upplýsingaöryggis. Félag getur hæglega sýnt fram á útgáfu slíkrar vottunar og/eða gögn sem sýna fram á hvernig félagið rekur stjórnkerfi til að tryggja upplýsingaöryggi í sinni starfsemi. Sem dæmi hefur Síminn verið með vottað stjórnkerfi upplýsingaöryggis, ISO-27001, í rúmlega tíu ár og fór nýlega í gegnum ferli til að uppfæra vottun sína miðað við nýjustu útgáfu staðalsins (ISO-27001:2022). Mikill tími og kostnaður fer í að öðlast, viðhalda og fylgja slíkri vottun. Meðal annars fylgir þessu að fram fari reglubundið innra eftirlit hjá félaginu og að framkvæmdar séu reglulegar úttektir af hálfu innri endurskoðunar og jafnvel prófunaraðila. Þá kemur úttektaraðili á vegum BSI til félagsins til að framkvæma ISO-úttekt til að meta hvort unnt sé að gefa út/endurútgefa vottun fyrir félagið. Miðað við þau atriði sem stofnunin hyggst í megindráttum áhættumeta og hafa eftirlit með samkvæmt drögunum má álykta að þau séu að miklu leyti hin sömu og falla undir stjórnkerfi upplýsingaöryggis hjá félaginu, n.t.t. ISO-vottun félagsins. Félagið telur að vottun af þessum toga verði að hafa meira vægi hjá stofnuninni þegar kemur að því að viðhafa eftirlit með rekstri og öryggi hjá félaginu, a.m.k. þegar kemur að tíðni og/eða umfangi eftirlitsúrræða hverju sinni. Verði svo ekki gert með skýrum hætti gæti verið litið svo á að félög sem hafa ekki vottun af sambærilegum toga í sinni starfsemi séu lögð að jöfnu við félög með vottun, þegar kemur að tíðni og umfangi eftirlitsaðgerða stofnunarinnar. Slík stjórnsýsla myndi ekki að mati Símans standast meðalhófssjónarmið auk þess sem það myndi vekja spurningar um vægi vottunarinnar yfir höfuð ef hún hefur ekki þýðingu gagnvart stofnuninni ef enginn munur er gerður á aðilum með eða án vottunar.

Í fjórða lagi telur félagið mikilvægt að stofnunin geri ráð fyrir að félag þurfi að óska eftir undanþágu eða frestun *ex ante* eftirlitsaðgerða ef aðstæður og/eða verkefnaálag hjá félaginu er þess eðlis að það væri talið áhættusamt og/eða illframkvæmanlegt að verða við gagnabeiðni, úttektum eða prófunum af hálfu stofnunarinnar á því tímamarki.

IV. Lokaorð

Í megindráttum er það mat Símans að stefna af þessum toga sé ótímabær þar sem það liggur fyrir að NIS2-regluverkið er á döfinni og fastlega má reikna með að það muni hafa áhrif á eftirlitsframkvæmd stofnunarinnar, eflaust strax á næsta ári, 2026. Sérstaklega í ljósi þess að tímabil stefnunnar er afar stutt, eða til rúmlega tveggja ára, þá væri að mati félagsins skynsamlegra og skilvirkara að útfæra stefnu af þessum toga þegar búið er að innleiða NIS2-regluverkið hér á landi og hafa hana þá með mun lengri gildistíma, eða a.m.k. til fimm til tíu ára.

Með drögunum leggur stofnunin til fyrirkomulag um margvíslegar, reglubundnar *ex ante* eftirlitsaðgerðir á þriggja ára fresti telur Síminn enn mikilvægara að meðalhófs verði gætt við beitingu umræddra rannsóknar- og eftirlitsúrræða. Aðgerðirnar eru tímafrekar og kostnaðarsamar fyrir það félag sem á í hlut og er jafnvel þegar með vottaða starfsemi skv. viðurkenndum, alþjóðlegum stöðlum. Ætti því að hvíla enn meiri skylda á stofnuninni að beita einungis slíkum aðgerðum þegar nauðsynlega er þörf á, að teknu tilliti til þeirra upplýsinga sem þegar liggja fyrir hjá stofnuninni og þeim aðstæðum sem eru uppi hverju sinni. Þá ætti einnig vottun fyrir stjórnkerfi upplýsingaöryggis í rekstri félags að vega þyngra í mati stofnunarinnar, sérstaklega þegar kemur að því að ákveða tíðni og umfang eftirlitsúrræða. Loks þarf stofnunin að gæta þess að mörg mál verði ekki rekin á sama tíma gagnvart sama aðila og að stofnunin kalli ekki eftir upplýsingum/gögnum sem þegar hafa verið útveguð stofnuninni í tengslum við annað nýlegt mál.



Síminn bindur vonir við að stofnunin taki tillit til þeirra sjónarmiða sem rakin hafa verið í erindi þessu. Áskilur félagið sér rétt til að koma á framfæri frekari sjónarmiðum á síðari stigum ef frekari breytingar verða gerðar á drögunum.

Helga Grethe Kjartansdóttir,
lögfræðingur og persónuverndarfulltrúi

