Fjarskiptastofa

Suðurlandsbraut 4, 2. hæð• 108 Reykjavík
Sími: 510 1500 • fjarskiptastofa@fjarskiptastofa.is
www.fjarskiptastofa.is

Reykjavík, 18. ágúst 2023

Tilvísun: 2023080020/08.0

Háskóla-, iðnaðar- og nýsköpunarráðuneytið
Arnarhvoli við Lindargötu
101 Reykjavík

Efni: Umsögn um drög að reglugerð um netöryggisráð

Fjarskiptastofa vísar til máls nr. 122/2023 í samráðsgátt stjórnvalda sem birt var þann 29. júní sl. og varðar drög að reglugerð um netöryggisráð.

Fjarskiptastofa og netöryggissveit stofnunarinnar, CERT-IS, hefur haft fulltrúa í netöryggisráði frá stofnun ráðsins árið 2015 og hefur tekið virkan þátt í starfi þess. Fagnar stofnunin áformum ráðuneytisins að nýta sér reglugerðarheimild í 2. mgr. 4. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða sem samþykkt voru á Alþingi í júní 2019 og tóku gildi þann 1. september 2020.

Í framangreindu ákvæði kemur fram að ráðherra skipi netöryggisráð sem hafi einkum það hlutverk "... að *fylgja eftir framkvæmd stefnu* stjórnvalda á sviði net- og upplýsingaöryggis. Ráðið *leggur mat á stöðu netöryggis á Íslandi* á hverjum tíma og er *vettvangur upplýsingamiðlunar* og *samhæfingar*." Þá er vissulega sett fram í ákvæðinu krafa um að fulltrúar sem skipaðir séu í ráðið hafi viðeigandi menntun og/eða reynslu, ráðið skuli setja sér starfsreglur sem og að trúnaður geti ríkt um fundi ráðsins, einstök mál og gögn þess og vinnuhópa. Reglugerðardrögin hafa að geyma ákvæði sem taka á öllum þessum þáttum að undanskildu því hlutverki þess að vera *vettvangur samhæfingar*.

Fjarskipta bendir ráðuneytinu á að það er lögbundið hlutverk netöryggissveitar stofnunarinnar að bregðast við áhættum og atvikum er varðar net- og upplýsingaöryggi hér á landi og veita ráðgjöf um viðbrögð og aðgerðir. Þá er sveitin samhæfingaraðili, og eftir atvikum Almannavarnir, vegna ógna, áhættu og atvika sem upp koma hjá þjónustuhópum sveitarinnar og, ef við á, innan netumdæmis Íslands. Að mati Fjarskiptastofu er því mikilvægt að fjallað væri um í sérstöku ákvæði í reglugerðinni hvað felst í því hlutverki ráðsins að vera *vettvangur samhæfingar*.

Skipan netöryggisráðs (2. gr.)
Hvað varðar skipan ráðsins, skv. 2. gr. reglugerðardraganna, er ljóst að um fækkun fulltrúa er að ræða frá núverandi netöryggisráði. Sjö aðilar skulu tilnefndir af tilgreindum ráðuneytum eða, ef ráðuneyti ákveður svo, stofnunum sem heyra stjórnarfarslega undir viðkomandi ráðuneyti.

Þá kemur fram í ákvæðinu að ráðherra skipi formann (og varaformann) sem skal koma fram fyrir hönd ráðsins gagnvart ráðherra. Í ljósi þessa orðalags, sem og að ráðið skuli einungis skila inn skriflegum álitum, má lesa að ekki er gert sérstaklega ráð fyrir því að ráðherra komi fyrir ráðið, jafnvel þótt að kveðið sé á um að það sé faglegt ráðgjafaráð fyrir ráðherra og starfi í umboði hans, sbr. lokamálsliður 2. mgr. 1. gr. Telur Fjarskiptastofa mikilvægt að ráðið geti fylgt eftir álitum sínum til ráðherra.

Mat á netöryggisstefnu stjórnvalda (3. gr.)

Í 3. gr. reglugerðardraganna er kveðið á um að ráðið skuli leggja mat á framkvæmd netöryggisstefnu stjórnvalda útfrá upplýsingum ráðuneytis þess sem fer með netöryggismál og öðrum þeim upplýsingum sem ráðið aflar. Skal ráðið gefa ráðherra álit sitt skriflega.

Í skýringum við áðurnefnt ákvæði 2. mgr. 4. gr. netöryggislaganna segir m.a. að „[l]*agt er til að ráðinu verði með lögum falið það hlutverk að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis og að leggja mat á stöðu netöryggis á Íslandi á hverjum tíma.*" Að mati Fjarskiptastofu er þetta í samræmi við a.m.k. hluta 3. gr. reglugerðardraganna. En samkvæmt ákvæðinu skal ráðuneytið einnig veita ráðinu upplýsingar um stöðu aðgerðaráætlunar sem að ráðið skal leggja mat á og gefa skriflega skýrslu til ráðherra um. Þannig er mjög takmarkað hlutverk sem ráðið sjálft hefur þegar kemur að gerð aðgerðaráætlunar, áætlun sem í raun er sett til að fylgja eftir framkvæmd stefnunnar. Þannig skilur Fjarskiptastofa reglugerðardrögin með þeim hætti að það er ekki netöryggisráð sem að fylgir beint eftir stefnu stjórnvalda heldur sé það ráðuneytið sem setur aðgerðaráætlun, veitir ráðinu upplýsingar um framkvæmd aðgerðaráætlunar sem ráðið gerir þá skýrslu um til ráðherra.

Vissulega er tilgreint í 3. gr. reglugerðardraganna að ráðið skuli afla gagna með sjálfstæðum hætti til að geta lagt mat á *„framkvæmd stefnunnar og aðgerða hennar"*. Að mati Fjarskiptastofu er óljóst á grundvelli hvaða heimilda ráðið getur aflað sjálfstæðra upplýsinga frá aðilum sem mögulega hafa hlutverki að gegna við framkvæmd stefnunnar og aðgerða hennar. Fjarskiptastofa telur að um ákveðna tvítekningu geti verið að ræða og að eðlilegra sé að netöryggisráð komi að gerð aðgerðaráætlunar, annað hvort sjálfstætt eða í náinni samvinnu við ráðuneytið, enda felst í því eftirfylgni á framkvæmd á stefnu stjórnvalda. Þá á ráðið jafnframt að leggja mat á stöðu netöryggis, sbr. 4. gr., hér á landi og er það, að mati Fjarskiptastofu, nauðsynlegt inn í gerð slíkrar áætlunar, þ.e. hvar aðgerða er helst þörf.

Stöðumat á netöryggi. (4. gr.)

Í 4. gr. reglugerðardraganna segir að netöryggisráð skuli leggja sjálfstætt mat á stöðu netöryggis hér á landi á hverjum tíma og m.a. byggja á stöðumati netöryggissveitar Fjarskiptastofu ásamt upplýsingum sem ráðið aflar sjálfstætt. Ekki er nánar fjallað um gagnaöflunarheimildir ráðsins heldur vísað til þess sem lög heimila. Þá skal ráðið gefa álit sitt með skriflegum hætti til ráðherra að lágmarki árlega.

Að mati Fjarskiptastofu er hér um nokkuð þrönga nálgun að ræða. Núverandi stefna stjórnvalda nær til samfélagsins alls og er mun umfangsmeiri en einungis stöðumat netöryggissveitar. Um stöðumat netöryggissveitar er fjallað í 7. gr. reglugerðar um sveitina, nr. 480/2021. Þar kemur fram að sveitin móti stöðumynd vegna netógna sem að hún skal miðla

til netöryggisráðs. Þótt vissulega séu netógnir mikilvægur þáttur í stöðu netöryggis hér á landi þá er það einungis hluti þess sem að stefna stjórnvalda og aðgerðaráætlun á sviði netöryggis nær til. Að mati Fjarskiptastofu er því æskilegt að ná betur utan um þessa heildstæðu mynd netöryggis hér á landi sem nær t.a.m. til menntunnar, öryggi almennings á netinu, upplýsingaóreiðu, áhættumats margs konar, áfallaþols og þroskastigs net- og upplýsingaöryggis hjá t.a.m. mikilvægustu innviðum landsins. Með aðkomu þeirra aðila sem hafa með netöryggismál að gera í víðum skilningi, t.d. að gerð og eftirfylgni aðgerðaráætlunar á sviði netöryggis myndi nást mun breiðari yfirsýn yfir stöðu netöryggis hér á landi.

Tilgreint er að auk almennrar öflunar upplýsinga frá opinberum aðilum þá geti ráðið jafnframt framkvæmt kannanir og úttektir. Ljóst er að hér getur verið um nokkuð umfangsmikla vinnu að ræða fyrir fulltrúa ráðsins en ekki er fjallað um að ráðið hafi yfir að ráð sérstökum starfsmanni til að til að vinna úr slíkum gögnum, sé þeirra aflað, eða vinna að skýrslugerð.

Upplýsingamiðlun (5. gr.)
Að mati Fjarskiptastofu virðist sem svo að ráðið eigi að þjóna þeim tilgangi að miðla upplýsingum milli fulltrúa ráðsins um netöryggisógnir og netöryggisatvik. Gert er ráð fyrir að viðkomandi fulltrúar skuli afla upplýsinga um slíkt á sínum ábyrgðarsviðum. Fjarskiptastofa vill sérstaklega benda ráðuneytinu á 15. gr. reglugerðar um netöryggissveit stofnunarinnar þar sem m.a. fjallað er um að sveitin upplýsi netöryggisráðs um alvarleg og/eða útbreidd atvik eða áhættu sem ógna öryggi net- og upplýsingakerfa og tengjast þjónustuhópum sveitarinnar eða, ef við á, netumdæmi Íslands.

Starfsreglur ráðsins (6. gr.)
Fjarskiptastofa fagnar því að ráðið setji sér starfsreglur. Að mati stofnunarinnar mætti þó telja upp fleiri atriði sem að reglurnar skulu fjalla um, t.a.m. ritun og samþykkt fundargerða ráðsins, trúnaðarmerkingar og öryggi gagna ráðsins sem og mögulega vinnuhópa þess o.fl.

Trúnaður og þagnarskylda (7. gr.)
Í 7. gr. reglugerðardraganna er kveðið með almennum hætti á um þagnarskyldu fulltrúa ráðsins. Fjarskiptastofa bendir ráðuneytinu á að sérstök þagnarskylda hvílir á öllum fulltrúm netöryggisráðs á grundvelli 19. gr. laga nr. 78/2019. Horfa þarf til þess m.t.t. lokamálsliðs 5. gr. Fjarskiptastofa áréttar mikilvægi þess að tryggja viðeigandi öryggisstig þeirra gagna sem netöryggisráð hefur með höndum sem byggir á niðurstöðu áhættumats. Að mati stofnunarinnar er nauðsynlegt að kveða á um slíkt í reglugerðinni sem og starfsreglum ráðsins.

Lokaorð
Fjarskiptastofa áréttar að stofnunin er áfram um að setning reglugerðar um starfsemi netöryggisráðs nái fram að ganga. Telur stofnunin að hér sé gott tækifæri til að meta núverandi starfsemi ráðsins og gera breytingar á starfsemi þessi, markmiði og tilgangi til að tryggja með sem allra bestum hætti virkan vettvang um þróun netöryggis og stafrænnar umbreytingar hér á landi.

Aftur á móti er ljóst að mikil þróun á sér stað hvað varðar stafræna tækni, nýtingu upplýsingakerfa og gervigreindar. Þá er einnig fyrirséð að innleiða verði fjölmargar lagagerðir Evrópusambandsins á sviði netöryggis og stafrænnar þróunar. Má þar fremst í flokki nefna

nýja netöryggistilskipun nr. 2022/2555 (NIS-2) en þar eru settar fram kröfur til netöryggisstefnu aðildarríkja. Að mati Fjarskiptastofu má því líta á umrædd reglugerðardrög sem milliskref þar til endurskoðunar kemur á starfsemi og hlutverki netöryggisráðs við endurskoðun laga nr. 78/2019.

Þá er Fjarskiptastofa reiðubúin að taka virkan þátt í áframhaldandi vinnu við gerð reglugerðarinnar.

Virðingarfyllst,

f.h. Fjarskiptastofu

Hrafnkell V. Gíslason

Hrafnkell V. Gíslason, forstjóri