Embætti landlæknis

Alþingi
Kirkjustræti
101 Reykjavík

Reykjavík, 18. ágúst 2023
2306210/0.4.1

Efni: Umsögn embættis landlæknis um drög að reglugerð um netöryggisráð og tillaga um formgerð samstarfs stjórnvalda og atvinnulífs á sviði netöryggis.

Embætti landlæknis vísar til draga að reglugerð um netöryggisráð og tillögu um formgerð samstarfs stjórnvalda og atvinnulífs á sviði netöryggis sem birt voru í samráðsgátt stjórnvalda 29. júní 2023. Embættið þakkar veitt tækifæri til að veita umsögn um umrædd mál.

Markmið fyrrnefndrar reglugerðar um netöryggisráð er, samkvæmt ráðuneyti háskóla-, iðnaðar- og nýsköpunar, að skýra skipan, hlutverk og ábyrgð netöryggisráðs. Embætti landlæknis fagnar því að vilji sé til að efla starf og hlutverk ráðsins með því að skilgreina hlutverk þess betur. Hins vegar telur embættið að fyrirhugaðar breytingar, eins og þær birtast í drögum ráðuneytisins, séu ekki til þess fallnar að ná þeim markmiðum.

Embættið gerir eftirfarandi athugasemdir við reglugerðardrögin:

1.

Í 1. gr. draganna (Tilgangur og markmið) kemur fram að netöryggisráð starfi á grundvelli 2. mgr. 4. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða, nr. 78/2019 (NIS-lögin) og sinni „ákveðnu ráðgjafahlutverki með því að fylgja eftir framkvæmda stefnu stjórnvalda á sviði net- og upplýsingaöryggis.“

Í umræddri grein laga nr. 78/2019 segir eftirfarandi: „Hlutverk ráðsins er einkum 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.“ Ekki er minnst á ráðgjafahlutverk í tengslum við netöryggisráð í umræddum lögum, né í frumvarpi til laganna. Að mati embættisins þarf að skýra hvernig ráðgjafahlutverk netöryggisráðs fellst í því að fylgja eftir stefnu stjórnvalda.

Í sömu grein reglugerðardraganna kemur jafnframt fram að netöryggisráð sé „þannig faglegt ráðgjafahlutverk ráðherra sem fer með málefni netöryggis.“ Embættið sér ekki hvernig þessi

Katrínartún 2
105 Reykjavík
mottaka@landlaeknir.is
Sími: 510 1900

fullyrðing á sér stoð í lögum og verður það að teljast vafasamt að ætla netöryggisráði að vera sérstakt faglegt ráðgjafahlutverk þegar það hlutverk er ekki stutt með ákvæði í lögum.

2.

Um skipan netöryggisráðs er fjallað í 2. gr. reglugerðarinnar. Embættið vill undirstrika mikilvægi þess að tryggð sé aðkoma sérfræðinga á vegum haghafa sem hafa lykilhlutverki að gegna þegar net- og upplýsingaöryggi er annars vegar. Með þessu móti er tryggt að ráðið hafi faglega sýn á málaflokkinn.

Í 2. gr. er jafnframt tilgreint á hvaða forsendum ráðuneytin skuli tilnefna fulltrúa í ráðið: „Forsætisráðuneytið vegna þjóðaröryggisráðs, dómsmálaráðuneyti vegna lögreglu- almannavarna- og persónuverndarmála, fjármálaráðuneyti vegna fjármálamarkaðar og ríkisreksturs, og utanríkisráðuneyti vegna varnamála.“

Án efa má færa sannfærandi rök fyrir því að varnarmál séu mikilvægur þáttur í hlutverki netöryggisráðs, og þá ásamt lögreglu- og almannavarnamála. Sömuleiðis má segja að persónuverndarmál séu miðlægt atriði í öryggi landsmanna og eiga þau því erindi hér. Hins vegar er sérkennilegt að málefni fjármálamarkaða séu sérstaklega nefnd í þessu samhengi en ekki aðrir mikilvægir innviðir sem þó eru tilgreindir í lögum nr. 78/2019 á borð við heilbrigðisþjónustu, orkumál, hitaveitur, vatnsveitur, flutningar og fjarskiptamál.

Þessu tengt bendir embættið á að í 5. gr. um upplýsingamiðlun segir að „fulltrúar ráðsins afla upplýsingar er varða netöryggi á sínum ábyrgðasviðum […].“ Miðað við ábyrgðasviðin eins og þau eru nefnd í drögunum verður ekki annað séð en að ekki verði sérstaklega vaktað þær netöryggisógnir og netöryggisatvik sem varða heilbrigðisþjónustu, fjarskiptaþjónustu, orku- og hitaveitumál og samgöngumál.

Þá er málaflokkurinn „ríkisrekstur“ ekki skilgreindur í drögunum og auk þess er ekki að finna stuðning við það sjónarmið að ríkisrekstur í almennri merkingu teljist til mikilvægra innviða í lögum nr. 78/2019. Ýmsar ríkisstofnanir og opinberir aðilar bera ábyrgð á innviðum, eins og t.d. heilbrigðisþjónustu, orku og hitaveitum, en rekstur ríkisins getur varla talist án frekari skýringa til mikilvægra innviða.

Í 2. gr. er einnig fjallað um þær kröfur sem gerðar eru til fulltrúa í ráðinu. Þeir skulu búa yfir sérfræðimenntun og starfsreynslu sem „telst fullnægjandi að mati ráðherra.“ Embættið vekur athygli á því að til eru viðurkenndar matsaðferðir til að staðfesta styrk og hæfni í neytöryggi.

3.

Embættið vill undirstrika að öryggi rafrænna heilbrigðisinnviða er ákaflega mikilvægur málaflokkur. Brestir í þessum innviðum geta valdið meiriháttar skaða, auk þess sem heilbrigðisþjónusta getur skipt sköpum í viðbrögðum við heilsutengdri vá. Þar að auki eru þær upplýsingar sem verndaðar eru í heilbrigðisþjónustu með allra mikilvægustu og viðkvæmustu upplýsingum sem til eru. Brestur á öryggi í þessum málaflokki getur valdið óbætanlegum skaða.

Í frumvarpi til NIS-laganna segir: "Með frumvarpinu er meðal annars lagt til að komið verði á fót umgjörð sem gera mun stjórnvöldum betur kleift en hingað til að samhæfa aðgerðir og lágmarksöryggiskröfur, en ýmsar stjórnsýslustofnanir hafa snertifleti við málefni tengd net- og upplýsingaöryggi."

Í inngangskafla skýringa með frumvarpi til NIS-laganna er ljóst að tilgangur laganna er að efla öryggi, viðnámsþrótt og áreiðanleika net- og upplýsingakerfi mikilvægra innviða. Í lögunum er skýrt að hlutverk netöryggisráðs er meðal annars að vera vettvangur upplýsingamiðlunar og samhæfingar, enda er slíkt lykil atriði til að unnt sé að vinna samstillt að eflingu öruggra innviða og grunngerða fyrir nauðsynlega þjónustu.

Það er því mjög mikilvægt að tryggja að þeir aðilar sem hafa skíran snertiflöt við öryggi net- og upplýsingakerfa mikilvægra innviða taki þátt í starfsemi netöryggisráðs og hafi þar áhrif í samræmi við sitt ábyrgðasvið.

4.

Sem áður segir þakkar embætti landlæknis veitt tækifæri til að veita umsögn þessa. Um leið er bent á að sérfræðingar embættisins eru ávallt reiðubúnir til að veita ráðuneytinu aðstoð og ráðgjöf.

Virðingarfyllst,

Kjartan Njálsson

Kjartan Hreinn Njálsson
aðstoðarmaður landlæknis

Háskóla-, iðnaðar- og nýsköpunarráðuneytið
Bt: Birgir Rafn Þráinsson, skrifstofustjóri
Arnarhvoli við Lindargötu
101 Reykjavík

Reykjavík, 7. mars 2023
xxxxxxxx/0.0/adm

Efni: Endurskoðun netöryggisráðs

Forsaga

Formaður netöryggisráðs sendi drög að reglugerð um netöryggisráð á fulltrúa ráðsins þann 6. febrúar 2023. Á fundi netöryggisráðs þann 22. febrúar 2023 var endurskoðun netöryggisráðs tekin fyrir sem dagskrárliður.

Endurskoðun netöryggisráðs hefur ekki verið formlega á vettvangi netöryggisráðs. Formaður netöryggisráðs hefur kynnt framgang málsins hjá háskóla-, iðnaðar- og nýsköpunarráðuneytinu á fyrri fundum ráðsins en efnisleg meðferð málsins hefur ekki farið fram innan netöryggisráðs.

Embætti landlæknis telur mikilvægt að koma á framfæri eftirfarandi athugasemdum við bæði framgang endurskoðunar netöryggisráðs og þær tillögur sem felast í fyrrnefndum drögum að reglugerð um netöryggisráð.

Inngangur

Í lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða (hér eftir kallað NIS-lögin) segir í 2. mgr 4. gr. að hlutverk netöryggisráðs sé að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis. Þar segir einnig að ráðið leggi mat á stöðu netöryggis á Íslandi á hverjum tíma og sé vettvangur upplýsingamiðlunar og samhæfingar.

Í 1. mgr. 4. gr. segir varðandi stefnu stjórnvalda um net- og upplýsingaöryggi að í henni skuli m.a. greina frá markmiðum og ráðstöfunum stjórnvalda í því skyni að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða. Þetta er í samræmi við meginmarkmið NIS-laganna sem tilgreint er í 1. gr.

Orðskýring á hugtakinu „öryggi net- og upplýsingakerfa“ í 6. gr. NIS-laganna er þannig: „Geta net- og upplýsingakerfis til að standast, með tilteknu öryggisstigi, hvers

konar aðgerðir sem stofna í hættu aðgengi að sannvottuðum uppruna, réttleika eða trúnaði um vistuð, send eða unnin gögn og tengda þjónustu sem boðin er eða er aðgengileg um net- og upplýsingakerfi.“

Í umfjöllun um 4. gr. í frumvarpi NIS-laganna segir að ákvæði um stefnu stjórnvalda sé ætlað að innleiða 7. gr. NIS-tilskipunar (ESB) 2016/1148 sem vísar til þess að stefnumörkun skuli meðal annars skilgreina markmið, forgangsraða þeim og fjalla um ráðstafanir til að stuðla að öryggi og viðmótsþrótti net- og upplýsingakerfa. Þar er einnig vísað til útlistunar á hlutverkum og ábyrgðum ólíkra stjórnsýslustofnana með snertiflöt við málaflokkinn og að aðferðafræði við áhættumat í því skyni að stöðumynd liggi fyrir á hverjum tíma. Að lokum er vísað sérstaklega til menntunar, þjálfunar og það hvernig standa beri að vitundarvakningu í samfélaginu gagnvart netógnum.

Framgangur málsins

Netöryggisráð hefur starfað frá árinu 2015 og í því sitja fulltrúar lykil ráðuneyta og mikilvægra stofnana sem hafa afgerandi snertiflöt við öryggi net- og upplýsingakerfa. Embætti landlæknis hefur átt fulltrúa í netöryggiráði frá upphafi.

Netöryggisráð hefur haft það hlutverk að fylgja eftir stefnu íslenskra stjórnvalda um net- og upplýsingaöryggi frá árinu 2015. Netöryggisráð vann einnig að tillögu að Netöryggisstefnu Íslands 2022-2037 sem var gefin út af háskóla-, iðnaðar- og nýsköpunarráðneyti í febrúar 2022.

Þegar drög að reglugerð um netöryggisráð voru send til fulltrúa í netöryggisráði var búið að kynna drögin fyrir ráðherra háskóla-, iðnaðar og nýsköpunar auk nokkurra annarra ráðuneyta. Fulltrúar í netöryggisráði komu ekki að mótun þeirrar endurskoðunar sem sett er fram í drögunum.

Embætti landlæknis telur eðlilegt að starfandi netöryggisráð standi á bak við tillögur sem sendar eru til ráðherra um endurskoðun á starfsemi ráðsins.

Embætti landlæknis gerir því athugasemd við það að fulltrúar embættisins og annarra lykil stofnana og ráðuneyta sem eiga fulltrúa í netöryggisráði hafi ekki haft tækifæri til þess að koma sjónarmiðum sínum á framfæri áður en tillögur um endurskoðun voru mótaðar og kynntar innan stjórnarráðsins.

Endurskoðun netöryggisráðs

Að mati embættis landlæknis er ljóst að tilgangur netöryggisráðs samkvæmt NIS-lögunum er að vera vettvangur til að stuðla að öryggi og viðmótsþrótti net- og upplýsingakerfa mikilvægra innviða með því að fylgja eftir stefnu stjórnvalda um net- og upplýsingaöryggi. Netöryggisráði er gert að leggja mat á stöðu netöryggis á Íslandi á hverjum tíma og vera vettvangur upplýsingamiðlunar og samhæfingar.

Því teljum við að netöryggisráð þurfi að vera samsett af þeim lykil stjórnsýslustofnunum sem hafa afgerandi snertiflöt við net- og upplýsingaöryggi mikilvægra innviða – þar sem mikilvæg samfélagsleg og efnahagsleg starfsemi er í húfi ef öryggi brestur.

Embætti landlæknis telur að netöryggisráð þurfi að vera vettvangur slíkra stjórnsýslustofnana sem koma saman með mismunandi hagsmuni og áherslur til að byggja upp sameiginlega grunngerð fyrir öryggi net- og upplýsingakerfa og nauðsynlega innviði sem eru sameiginlegir fyrir samfélagið, og styðji hverja aðra í uppbyggingu á sértækum innviðum fyrir tiltekin svið samfélagsins þar sem þess er þörf.

Nauðsynlegar áherslur netöryggisráðs

Sviðsmyndir netöryggis eru í raun tvær – dags-daglega sviðsmyndin og sú sviðsmynd sem tekur við ef alvarlegt áfall verður. Megin markmið í stjórnun öryggis er að lágmarka líkur á því að lenda í áfallasviðsmyndinni, þó ávallt verði að gera ráð fyrir því að svo geti farið.

Öryggi net- og upplýsingakerfa snýst um að efla getu kerfanna til að standast hvers konar aðgerðir sem stofna öryggi upplýsinga í hættu, með áherslu á aðgengi að sannvottuðum uppruna, réttleika eða trúnaði gagna og tengdri þjónustu sem eru boðin eða aðgengileg um net- og upplýsingakerfi. Markmið öryggisráðstafana er að lágmarka hættu á áföllum með því að efla viðnámsþrótt net- og upplýsingakerfa í dags-daglegri starfsemi. Það einkennir dags-daglegu sviðsmyndina og er megin áhersla í skilgreiningu í lögum á hlutverki netöryggisráðs.

Hin sviðsmyndin varðar viðbrögð við alvarlegum áföllum. Ef þær ráðstafanir sem gerðar eru í hinni dags-daglegu sviðsmynd reynast ekki nægjanlegar þá þarf að grípa

til aðgerða til að lágmarka skaða og endurreisa gögn og þjónustu hið fyrsta.
Netöryggissveitin gegnir mikilvægu hlutverki í þeirri sviðsmynd.
Við teljum áherslur fyrrnefndra lagaákvæða, um stefnu stjórnvalda á sviði net- og upplýsingakerfa og um hlutverk netöryggisráðs, séu á getu kerfa til að standast ógnir. Netöryggisráð þarf því að vera vettvangur upplýsingamiðlunar og samhæfingar með ásýnd á stöðu netöryggis á Íslandi á hverjum tíma, vettvangur sem vinnur markvisst að því að efla viðnámsþrótt net- og upplýsingakerfa mikilvægra innviða.
Það er jafnframt ljóst að netöryggisráð þarf, í samstarfi við netöryggissveitina og aðra lykilaðila, að hafa það hlutverk að samhæfa viðbrögð við alvarlegum áföllum. Þar er jafnframt mikilvægt að netöryggisráð sé skipað fulltrúum þeirra stjórnsýslustofnana sem sem hafa afgerandi snertiflöt við net- og upplýsingaöryggi mikilvægra innviða.
Sú tillaga sem nú liggur fyrir í drögum að reglugerð gerir ráð fyrir því að netöryggisráð sé skipað fimm fulltrúum ráðuneyta eða opinberra stofnana sem fara með málefni netöryggis, löggæslu og almannavarna, og varnarmála, þar sem ráðherra netöryggis skipar þrjá af þessum fimm fulltrúum (og þrjá til vara). Ráðuneyti sem fara með málefni löggæslu og almannavarna annars vegar og með málefni varnarmála hins vegar skipa hvort einn fulltrúa (og einn til vara).
Áherslan í þessari tillögu er á varnarmál, löggæslu og almannavarnir, auk almennrar áherslu á netöryggi. Þessir málaflokkar snúa því meira að áfallasviðsmyndinni en dags-daglegu sviðsmyndinni.
Það er því að okkar mati ljóst að netöryggisráðið mun ekki hafa forsendur til að vera sá vettvangur upplýsingamiðlunar og samhæfingar sem nauðsynlegur er til að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða á Íslandi.
Slíkur vettvangur fimm fulltrúa mun eiga erfitt með að leggja mat á stöðu netöryggis á Íslandi og tryggja getu net- og upplýsingakerfa til að standast þær ógnir sem steðja að mikilvægum innviðum dags-daglega.
Embætti landlæknis telur að þessi skipan netöryggisráðs sé ekki í samræmi við ákvæði laganna.

Lokaorð

Embætti landlæknis gegnir mjög mikilvægu hlutverki í öryggi heilbrigðisþjónustu á Íslandi. Heilbrigðisþjónusta telst til mikilvægra innviða og veiting heilbrigðisþjónustu

er mjög háð net- og upplýsingakerfum. Embættið ber mikla ábyrgð á sjúkraskrá á landsvísu, varðveislu heilbrigðisskráa og öryggi upplýsinga í heilbrigðisþjónustu almennt. Það er að mati embættisins orðið mjög brýnt að auka skilning á áhættum í heilbrigðisþjónustu og efla viðnámsþrótt heilbrigðiskerfa og undirliggjandi tæknilegum innviðum.

Embætti landlæknis leggur því ríka áherslu á formlega aðkomu að netöryggisráði og fulla þátttöku í starfsemi þess og verkefnum. Embættið telur einnig mikilvægt að Persónuvernd og Fjarskiptastofa eigi fulltrúa í netöryggisráði þar sem þær stofnanir hafa afgerandi snertiflöt við öryggi net- og upplýsingakerfa og bera mjög ríka ábyrgð á verndun upplýsinga í innviðum og þjónustu á Íslandi. Miðlun upplýsinga á milli þessara stofnana og samhæfing á netöryggi á þeirra vettvangi er mjög mikilvæg forsenda þess að tryggja viðunandi öryggi net- og upplýsingakerfa fyrir heilbrigðisþjónustu.

Alma Möller

Alma Möller

Landlæknir