Stjórnarráð Íslands
Samgöngu- og sveitarstjórnarráðuneytið

Skýrsla um samráð

Efni samráðs

Drög að reglugerð um netöryggissveit Póst- og fjarskiptastofnunar (CERT-ÍS).

Samráðstímabil:

Mál nr. 266/2020 – drög að reglugerð um netöryggissveit (CERT-ÍS) – samráð hófst 14.12.2020 og lauk 11.1.2021.

Fjöldi umsagna:

Alls bárust sjö umsagnir um mál nr. 266/2020.

Umsagnaraðilar:

Sýn hf., Síminn hf., Isavia ohf., Advania, Persónuvernd, embætti ríkislögreglustjóra og einn einstaklingur.

Samantekt um umsagnir og viðbrögð:

Megintilefni heildarendurskoðunar á gildandi reglugerð var nýleg útvíkkun á þjónustuhópi netöryggissveitar Póst- og fjarskiptastofnunar (CERT-ÍS) með lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, sem jafnframt breyttu ákvæðum um CERT-ÍS í gildandi lögum nr. 81/2003 um fjarskipti og nr. 69/2003 um Póst- og fjarskiptastofnun ,hér eftir nefnt PFS. Aðilar sem lögum samkvæmt njóta þjónustu netöryggissveitar eru einkum mikilvægir innviðir, fjarskiptafyrirtæki, Stjórnarráð Íslands og eftir atvikum aðrir aðilar. CERT-ÍS ber að taka við tilkynningum um öryggisbresti og getur hún gefið út tilmæli um aðgerðir eða ráðstafanir af hálfu mikilvægra innviða og fjarskiptafyrirtækja, í því skyni að bregðast við og samhæfa viðbrögð við alvarlegri ógn, atviki eða áhættu. Þá skal CERT-ÍS leitast við að skapa viðeigandi almenna ástandsvitund um ógnir, áhættu og atvik innan netumdæmis Íslands, auk þess að móta stöðumynd vegna netógna sem miðlað skal til netöryggisráðs og eftirlitsstjórnvalda. CERT-ÍS gegnir hlutverki tengiliðar íslenskra stjórnvalda í alþjóðlegu og evrópsku samstarfi sambærilegra sveita og er ætlað samhæfandi hlutverk, sem er nauðsynlegt til að takast á við fjölþættar netógnir er beinst geta að mismunandi geirum samfélagsins.

Drög að reglugerðinni voru birt til umsagnar í samráðsgátt stjórnvalda 14.12.2020-11.1.2021. Alls bárust sjö umsagnir um drögin, þar á meðal frá Persónuvernd og ríkislögreglustjóra eins og lög áskilja og var við endanlegan frágang reglugerðarinnar tekið mið af efni þeirra, eins og

kostur var. Í reglugerðinni er m.a. kveðið á um eftirtalið, í samræmi við 6. mgr. 4. gr. a í lögum nr. 69/2003: Hlutverk, skipulag og verkefni netöryggisveitar, skipun og hæfi starfsmanna, meðferð upplýsinga og viðeigandi öryggisráðstafanir, ráðstafanir til að tryggja öryggi og eyðingu gagna, viðbúnaðaræfingar, samstarf við önnur stjórnvöld og stofnanir og skýrslugjöf um starfsemi netöryggissveitar.

Ákvæðum 13. gr. og 30. gr. var breytt lítillega í því skyni að auka skýrleika (gögn sem unnin eru af hálfu þátttakenda í samstarfshópum teljast til vinnugagna, heimild þjónustu- og samstarfsaðila til miðlunar persónuupplýsinga til hennar og ljóst má vera að gögnum má ekki eyða ef nauðsynlegt er að geyma þau, s.s. skv. lögum nr. 77/2014 um opinber skjalasöfn eins og bent var á í umsögn). Ekki þótti tilefni til breytinga á 31. gr., enda skýrt í persónuverndarlöggjöfinni að öflun upplýsinga fellur undir hugtakið vinnsla. Ekki var talin þörf á að víkja frekar að sólarhringsvöktunarskyldu CERT-ÍS, enda verða ákvæði laga nr. 78/2019 og reglugerðarinnar ekki uppfyllt öðruvísi en með bakvöktun.

Athugasemdir voru gerðar við þann greinarmun sem endurspeglast í 21. og 22. gr. reglugerðarinnar en gildandi lög kveða þegar á um hann (samningar um tæknilega vöktun). Ekki þótti tilefni til að bregðast við ábendingu um þörf fyrir nánari skilgreiningu á tæknilegri vöktunarþjónustu, með vísan til 47. gr. b í lögum nr. 81/2003, 16. gr. laga nr. 78/2019 og umfjöllunar í greinargerð um síðastnefnt ákvæði. Tryggja ber sveitinni tæki og heimildir sem sambærileg öryggis- og viðbragðsteymi hafa erlendis, til nota við mótun stöðumyndar m.t.t. ógna á hverjum tíma. Að því er kostnað varðar vísast til 1. málsl. 3. mgr. 47. gr. b í lögum nr. 81/2003, en samkvæmt ákvæðinu skal fjarskiptafyrirtæki hýsa og tengjast við búnað netöryggissveitar sem metinn er nauðsynlegur endurgjaldslaust. Í 22. gr. reglugerðarinnar segir að netöryggissveit beri ábyrgð á öðrum kostnaði vegna framkvæmdar vöktunar. Sambærileg athugasemd kom fram við 23. gr. að því er varðar kostnað vegna öflunar tölfræðilegra upplýsinga um heildarmagn umferðar í almennum netkerfum, en umferðarmælingar verða að teljast hluti tæknilegrar vöktunarþjónustu í skilningi 47. gr. b. og þótti því ekki tilefni til breytinga.

Í tengslum við athugasemdir um öryggi og meðferð gagna í starfsemi sveitarinnar áréttast að PFS leggur ríka áherslu á að tryggja trúnað og öryggi þeirra persónuupplýsinga sem stofnunin vinnur með. PFS starfar eftir öryggisstefnu og aðgangsstefnu sem styðst við alþjóðlegan staðal um upplýsingaöryggi ISO/IEC 27001. Þann 19. maí 2020 hlaut stofnunin öryggisvottunina ISO/IEC 27001 (stjórnkerfi upplýsingaöryggis). Vísast einkum til 29. gr. reglugerðarinnar í þessu samhengi og þykir ekki tilefni til frekari breytinga. Aðrar athugasemdir voru metnar en höfðu lítil áhrif til breytinga.

Ný reglugerð leysir af hólmi gildandi reglugerð, nr. 475/2013, um málefni CERT-ÍS netöryggissveitar.

Skjal að loknu samráði:

Reglugerð nr. 480/2021, um netöryggissveit Póst- og fjarskiptastofnunar (CERT-ÍS).