SAMORKA

Samorka eru samtök orku- og veitufyrirtækja á Íslandi. Innan samtakanna starfa fráveitur, hitaveitur, vatnsveitur, raforku– framleiðendur, raforkusalar og flutnings- og dreifingaraðilar raforku

Reykjavík, 22. júní 2020

Samgöngu- og sveitarstjórnarráðuneytið
101 Reykjavík

Efni: Drög að reglugerð um öryggi net- og upplýsingakerfa mikilvægra innviða.
Samráðsgáttarmál nr. 111/2020.

Samorka tók virkan þátt í umsagnaferli við setningu laga nr. 78/2019 um öryggi net og upplýsingakerfa mikilvægra innviða og margar jákvæðar breytingar voru gerðar á frumvarpsdrögunum af því tilefni. Það er því ánægjulegt að almennt ríkir ánægja í okkar hópi með þau reglugerðardrög sem hér eru lögð fram, þótt nokkrar spurningar vakni og skýringa kunni að vera þörf á einstaka stöðum.

Rétt er að taka fram að Samorka hefur óskað eftir samstarfi við Orkustofnun sem eftirlitsstjórnvalds orku- og veitugeirans við innleiðingu nýrra laga og þá þeirrar reglugerðar sem hér er lagður grunnur að. Sama á við um Umhverfisstofnun vegna Vatnsveitna. Hafa aðilar komið sér saman um að skipa vinnuhópa í því skyni enda markmiðin algjörlega sameiginleg þ.e. að tryggja samfelldan og órofinn rekstur og áfallaþol orku- og veituinnviða.

Hér á eftir koma nokkrar hugleiðingar og ábendingar um einstakar greinar í reglugerðardrögunum.

Í lögunum og í reglugerðardrögunum er ekki fjallað um fráveitur en við höfum bent á að í raun eiga sömu grundvallar sjónarmið viðum rekstur þeirra kerfa eins og um önnur veitukerfi (sjá 2. mgr. 1. gr. reglugerðardraganna).

Á nokkrum stöðum í reglugerðinni eru félög að ákveðinni stærð eða þjónustu umfangi undanskilin ákvæðum væntanlegrar reglugerðar. Dæmi um þetta eru „örfélög í skilningi laga um ársreikning“ eins og segir í 3. mgr. 1. gr. reglugerðardraganna. Samorka bendir á að væntanlega þarf hér að skoða og meta sérstaklega áhættuna af tengingu slíkra aðila við sameiginleg netkerfi fremur en stærðina eina og sér. Sjá ennfremur frekari athugasemdir síðar.

Í 3. gr. reglugerðardraganna eru skilgreiningar á helstu hugtökum. **Atvik** eru þannig skilgreind að „hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa“, en **áhætt** skilgreind sem „aðstæður eða atburður sem geta haft skaðleg áhrif á öryggi net- og upplýsingakerfa. Í öryggisfræðum er lögð mikil áhersla á það hjá fyrirtækjum að skrá jafnt slys og næstum slys og spurning hvernig best væri að gera þetta í samhengi við öryggi net- og upplýsingakerfa en þá jafnframt að skilgreiningin verði heldur ekki allt of víð þannig að verið skrá allt of mikið.

Í 8. gr. reglugerðardraganna er fjallað um þjónustu á sviði orku- og hitaveitu og í 9. gr. er fjallað um þjónustu á sviði vatnsveitu. Hér erum við aftur komin að því atriði sem nefnt er hér að framan um hvort fremur verið að horfa til áhættu en stærðar þegar undanskilja á rekstraeiningar ákvæðum reglugerðarinnar. Hér má nefna að minni dreifiveitur eða orkuframleiðendur kunna að vera með alveg jafn virka tengingu við stjórnkerfi Landsnets og þar með tengingar milli dreifiveitna og framleiðenda og stærri fyrirtækin. Þar með getur áhættan af tengingu þeirra við samtengd net- og upplýsingakerfi verið jafn mikil. Því er ástæða til að skoða hvort viðmiðin og þar með orðalagið í 8. og 9. gr. nær nægjanlega vel utan um þessi öryggissjónarmið. Einnig er spurning um að samræma orðalagið milli 8. gr. og 9. gr. þegar fjallað er um veitustarfsemina.

Í 10. gr. er fjallað um þjónustu á sviði starfrænna grunnvirkja og spurning hvort þetta ákvæði er nægjanlega skýrt m.t.t. að ekki er fjallað um hugtakið í skilgreiningu hugtaka í 3. gr. reglugerðardraganna. Hér er þá spurningin sú til hverra nákvæmlega þetta ákvæði tekur.

Í 11. gr. er fjallað um skipulag net- og upplýsingaöryggis og áréttað að fyrirtækin skuli tryggja öryggið með ýtrasta hætti. Þetta orðalag er í raun mjög strangt því ævinlega fer fram mat á áhættu annars vegar og kostnaði hins vegar. Því væri eðlilegt að tengja þetta við skilvirkt og sívirkt áhættumat fyrirtækjanna.

Í umsögn Samorku um frumvarp til laga um öryggi net- og upplýsingakerfa var mikil áhersla lögð á að tengja saman skilvirkt og vottað innra og ytra eftirlit samkvæmt viðurkenndum stöðlum við framkvæmd ytra eftirlit eftirlitsstjórnvalds orku- og veitugeirans (Orkustofnun – Umhverfisstofnun í okkar tilviki). Með því væri hægt að draga úr reglu- og eftirlitsbyrði með jákvæðum formerkjum og þar með kostnaði allra hlutaðeigandi aðila. Teljum við mikilvægt þetta endurspeglist í þessari reglugerð þannig að tekið sé tillit til þess þegar fyrirtæki uppfylla staðla og eru með vottuð gæða- og eftirlitskerfi og þar með ytra eftirlit vottunaraðila. Væri eðlilegt að þetta endurspeglist t.d. í 2. mgr. 11. gr. og ýmsum ákvæðum V. kafla sbr. IV. kafla reglugerðardraganna.

Á ýmsum stöðum í reglugerðardrögunum er veitendum starfrænnar þjónustu veittar undanþágur sem vekur spurningar einmitt út frá sömu ástæðum og nefndar eru með stærðarmörk t.d. í orku- og veitustarfsemi. Hér vakna aftur spurningar um áhættumatið frekar en gerð eða stærð viðkomandi starfsemi (sjá t.d. niðurlag 15. gr., 18. gr. o.s.frv.).

Í 18. gr. er fjallað um kerfislægar ráðstafanir og ákveðnar lágmarkskröfur sem gerðar eru til mikilvægra innviðum í þeim efnum. Taldar eru upp í ellefu atriðum ýmsar kröfur sem fljótt á litið hljóma eðlilegar og sanngjarnar. Hér þarf þó að hafa í huga að hjá mörgum samfélagslega mikilvægum innviðum kunna enn að vera rekin stjórnkerfi sem eru hluti af búnaði sem styður ekki við allar umræddar kröfur. Margir af þessum innviðum, m.a. hjá aðildarfyrirtækjum Samorku, hafa starfað áratugum saman og tekur stjórnbúnaður eftir atvikum mið af því. Því er nauðsynlegt að taka mið af þessu við innleiðingu á lögunum um öryggi net- og upplýsingakerfa mikilvægra innviða

og tilheyrandi reglugerð. Hér er vísað til þess öryggislausnir geti verið margvíslegar og því mikilvægt að liðir a) til g) í 18. gr. taki mið af þessu. Hér má nefna dæmi um að nota orðalagið og/eða í stað og í b) liðnum. Skýra betur hvað er átt við með umferðartakmarkanir í lið c). Er verið að vísa til eldveggja eða eitthvað meira en það? Varðandi 18. gr. mætti meta hvort allir þættir eru þar skilyrðislausir eða hvort mikilvægir innviðir skuli líta til bestu lausna og þá þessi atriði nefnd í dæma skyni (e. should consider following).

Í 19. gr. b) lið er fjallað um öryggisrými en skilgreining á því er ekki í 3. gr. og því ekki með öllu ljóst til hvaða rýma er verið að vísa í þessu samhengi og þá þeirra krafna sem þarna á að gera, nema þessi skilgreining sé einfaldlega skilin eftir hjá viðkomandi innviði.

Varðandi 23. gr. viljum við árétta það sem áður var nefnt um mikilvægi þess að eftirlitsaðilar geti tekið mið af því við eftirlit sitt ef orku- og veituinnviðir hafa komið sér upp vottuðu innra eftirliti með kerfum sínum.

Í 24. gr. virðist vera um tvítekningu að ræða í málslið eitt og í tvö í 1. mgr.

Í 25. gr. eða öðrum góðum stað í reglugerðinni væri ástæða til að gera ráð fyrir samstarfi milli landa hjá orku- og veituinnviðum eins og þegar er í undirbúningi hjá Samorku. Í 1. mgr. 25. gr. er fjallað um tilkynningaskyldu um alvarleg atvik og áhættu sem koma upp í net- og upplýsingakerfum. Hér þarf að skýra betur hvað er átt við með að tilkynna áhættu. Væntanlega er átt við greinarmuninn á milli atviks og næstum atviks eða þess háttar sbr. fyrri umfjöllunar hér að ofan.

Í 28. gr. er fjallað um aðgengi að upplýsingum og þar með talið persónugreinanlegum upplýsingum „að því marki sem nauðsynlegt er“ eins og þar segir. Mikilvægt er að þetta ákvæði og framkvæmd þess sé skoðuð sérstaklega og þá í samráði Persónuvernd.

Loks er ástæða til að skoða matskennda þætti eins og hæfilegur frestur í 31. gr. og setja það í samhengi við umfang þess máls og áhættu sem til umfjöllunar er í hvert skipti.

Um leið og SAMORKA þakkar þetta tækifæri til þess að koma að umsögn um málið lýsum við yfir vilja til að fjalla nánar um einstakar athugasemdir og útfærslur sé eftir því óskað.

Að öðru leyti vísar SAMORKA til umsagna einstakra aðildarfyrirtækja.

Virðingarfyllst,

f.h. Samorku

Baldur Dýrfjörð lögfræðingur