Samgöngu- og sveitarstjórnarráðuneytið
Sölvhólsgötu 7
101 Reykjavík

Reykjavíkurflugvelli, 23. júní 2020
2006002KSM

Efni: Drög að reglugerð um öryggi net- og upplýsingakerfa mikilvægra innviða

Vísað er til Samráðsgáttar þar sem til umsagnar eru drög að reglugerð um öryggi net- og upplýsingakerfa mikilvægra innviða. Reglugerðin kveður nánar á um lágmarkskröfur til umgjarðar og rekstrar net- og upplýsingakerfa sem falla undir lög nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða.

Isavia ohf. og dótturfélög (hér eftir „félagið“) telst vera rekstraraðili nauðsynlegrar þjónustu á sviði flutninga og gerir meðfylgjandi athugasemdir við drögin.

Við samningu frumvarps til laganna voru gerðar talsverðar breytingar. Fyrir vikið virðist sem svo að í staðinn hafi ítarlegum kröfum verið komið fyrir í reglugerð. Stjórnvöld hyggjast því innleiða NIS tilskipunina með meiri íþyngjandi hætti en nauðsynlegt er.

Félagið gerir athugasemd við hversu seint reglugerðin fram kemur en heilt ár er síðan að lögin voru samþykkt á Alþingi. Drögin birtast rétt fyrir sumarleyfi og er aðstaða rekstraraðila um margt sérstök vegna ástands síðustu mánaða sem getur leitt til ómöguleika við að verða við öllum kröfunum í tæka tíð. Félagið leggur því til að gildistöku reglugerðarinnar verði frestað til ársins 2021. Þannig væri hægt að vanda betur til verka við innleiðingu. Verði ekki fallist á frestun leggur félagið til að gildistöku ákvæða sem fela í sér heimildir til að beita rekstraraðilum viðurlögum vegna brota á reglugerðinni verði frestað til ársins 2021.

Sérsniðnar reglur um netöryggi þjónustu sem fellur undir lögin eru í undirbúningi hjá Flugöryggisstofnun Evrópu og sé ósamræmi milli þeirra reglna og reglugerðarinnar verður lagaramminn að vera skýr hvort gildir. Félagið vill að brugðist verði við með almennari hætti í reglugerðinni með undanþágu frá lágmarkskröfum m.a. vegna annarra reglna sem kunna að gilda um starfsemina.

Lagt er til að tilvísanir til númers laga sé fjarlægt úr ákvæðum reglugerðarinnar í samræmi við venjubundna lagaritunarhefð.

2. gr.
Þar sem lögin gilda aðeins um þau kerfi sem eru nauðsynleg við veitingu þjónustu leggur félagið til að skírskotað sé til þess að í tilfelli alvarlegra atvika er markmiðið að viðhalda lágmarksþjónustu.

3. gr.
Í 1. tölul. er hugtakið *atburður* skilgreint. Gerð er athugasemd við að um nýja skilgreiningu sé að ræða sem er ekki notuð víðar í lögunum. Gæta þarf samræmis til að einfalda rekstraraðilum innleiðingu á kröfunum. Þá er jafnframt gerð athugasemd við að *óþekkt staða* gæti komið upp án þess að tengjast net – og upplýsingaöryggi og er því lagt til að hnekkt verði á því að staðan verði að tengjast net – og upplýsingaöryggi, verði valið að halda skilgreiningunni inni.

Þá er 2., 3. og 5., tölul. endurtekning úr lögunum sem verður að telja óþarft.

Varðandi 2. tölul. þá er bent á að gæta þurfi samræmis við önnur lög og helstu staðla sem taka á upplýsingaöryggi t.d. ISO27001 til að einfalda rekstraraðilum innleiðingu á kröfum. Fjallað er um *atvik og öryggisbresti* í persónuverndarlögum en ekki atburð og atvik. Þá er talað um upplýsingaöryggisatvik og upplýsingaöryggisveikleika í ISO27001 staðlinum.

6. gr.
Starfsemi og þjónusta alþjóðaflugvalla er mjög víðtæk og verður að telja að b-liður 6. gr. sé talsvert víðtækari en aðrir liðir 6. gr. Þannig mætti þrengja skilgreiningu b-liðar í: *„starfsemi og þjónustu vöru- og fólksflutninga á alþjóðaflugvöllum“.*

11. gr.
Tekið er fram *skipuleg áhrifagreining* ásamt áhættumati. Ekki er útskýrt hvað átt sé við með áhrifagreiningu né eru leiðbeiningar um framkvæmd þess og verður að telja að framkvæmd áhættumats sé nægjanlegt til að greina áhættu og lagt til að *„skipuleg áhrifagreining“* sé tekin út.

Tekið er fram að mikilvægir innviðir skulu byggja á *nýjustu útgáfu* alþjóðlegra viðurkenndra staðla um bestu framkvæmd á sviði net – og upplýsingaöryggis. Krafan er erfið í framkvæmd, sérstaklega ef staðlarnir eru uppfærðir ört. Um leið og nýjustu staðlar eru útgefnir uppfyllir mikilvægur innviður um leið ekki reglugerðina. Staðlar fara ekki í gegnum sambærilegt ferli og þegar lög eru samþykkt, er því sérstakt að lögfesta slíka framfylgni við staðla án svigrúms. Skyldi rekstraraðili vera í miðri innleiðingu á stöðlum eða kjósa að taka upp staðla með frávikum vegna eðli starfseminnar, ætti það ekki að teljast brot á reglugerðinni, sé net – og upplýsingaöryggi uppfyllt að öðru leyti.

Lagt er því til að hugtakið *nýjustu útgáfu* sé tekið út. Sé ekki fallist á það, verði bætt við fyrir aftan setninguna, *eftir því sem við er komið og á við* eða *nema öryggi er talið ásættanlegt.*

13. gr.
Fram kemur að áhættumat skuli vera skriflegt, framkvæmt reglubundið og aðferðarfræði þess endurmetin, hvort tveggja á a.m.k. tveggja ára fresti**.** Gerð er athugasemd við að aðferðarfræðin skuli vera endurmetin á tveggja ára fresti. Mjög óljóst er hverju eigi að ná fram með því að byrja áhættumöt frá grunni á tveggja ára fresti. Þá er til dæmis ekki hægt að bera saman fyrri áhættumöt séu þau ekki sambærileg. Ekki er að finna sambærileg ákvæði í öðrum reglugerðum. Hér hlýtur meiningin að vera að „viðhalda áhættumatinu með reglubundnum hætti á a.m.k. tveggja ára fresti“. Það tryggir betur fullnægjandi öryggi net- og upplýsingakerfa heldur en að mögulega núllstilla áhættumatsaðferð á tveggja ára fresti eða færa rök fyrir því af hverju haldið er áfram með sömu aðferð.

Í 3. mgr. 13. gr. er heimild fyrir eftirlitsstjórnvald að krefjast þess að rekstraraðili framkvæmi sértækt áhættumat á einstökum hlutum net – og upplýsingakerfa. Félagið gerir athugasemd við að lagastoð skortir fyrir beitingu úrræðisins ásamt því að hvorki kemur fram umfang áhættumatsins né í hvaða tilfellum beiting heimildarinnar kemur til greina. Heimildin er því bæði of víðtæk og fær ekki stoð í lögunum. Jafnframt er óljóst hvað felist í hinu sértæka áhættumati, þ.e. hvaða tilgang það hefur fram yfir hið reglubunda áhættumat og hvernig það er frábrugðið. Krafan getur ekki rúmast innan eftirlitsheimilda sem fela í sér fyrirmæli um úrbætur þar sem úrbætur koma til greina vegna frávika og eru tæmandi taldar í lögunum. Félagið leggur til að ákvæðið sé tekið út.

14. gr.
Í 1. mgr. 4. gr. kemur fram að öryggisráðstafanir rekstraraðila nauðsynlegrar þjónustu skulu vera að lágmarki í samræmi við kröfur III.-V. kafla. Í þeim köflum eru öryggisráðstafanir ítarlega taldar upp án þess að veittur sé sveigjanleiki fyrir beitingu öryggisráðstafana þegar þær geti ekki eða þurfi ekki að eiga við.

Markmið félagsins er ávallt að tryggja öryggi til hins ítrasta en kröfur verða að vera raunhæfar og bæta í reynd öryggi. Þannig geta þær ekki átt við vegna krafna í regluverki sem gildir um þjónustuna, eðli kerfa eða gagna bjóða ekki upp á að ráðstöfun sé notuð eða haft í för með sér að gögn týna gildi sínu. Öryggisráðstafanir eru í sífelldri þróun og kemur fram í greinargerð með lögunum að ljóst er að umgjörð og leikreglur tengdar net – og upplýsingaöryggi munu þróast áfram eins og ógnirnar. Reglugerðin gerir ekki ráð fyrir þessu þar sem sveigjanleika skortir.

Öryggisráðstafanir skulu byggja á áhættumati samanber 7. gr. laganna og 1. mgr. 14. gr. reglugerðarinnar. Reglugerðin gengur lengra en lögin án lagastoðar þar sem skv. 1. mgr. 7. gr. laganna er með öryggisráðstöfunum átt við tæknilegar og skipulagslegar ráðstafanir *„eftir því sem við kann að eiga“.* Að eðli málsins samkvæmt geta allar öryggisráðstafanir ekki átt við í öllum tilvikum því er framkvæmt áhættumat til að meta hverjar koma að gagni. Virka kröfurnar frekar sem hámark heldur en lágmark og taka ekki til smæðar samfélagsins og hagkvæmnissjónarmiða.

Komi sú staða upp hjá rekstraraðila að allar lágmarkskröfur séu ekki til staðar í kerfum sem nauðsynleg eru samkvæmt reglugerðinni getur þurft að grípa til þess að innleiða ný kerfi og er afar ólíklegt að svo sé mögulegt fyrir 1. september. Jafnframt kann að vera nægjanlegt að lágmarkskröfur séu til staðar við ytri varnir en félagið telur að kröfurnar geti verið íþyngjandi án nauðsynjar varðandi innri kerfi.

Lagt er til að í lok 3. málsliðar 1. mgr. 14. gr. er bætt við, *„eftir því sem við á“.* Jafnframt að nýjum málslið verði bætt við, svohljóðandi: *„Heimilt er rekstraraðila að víkja frá lágmarkskröfu geti rekstraraðili sýnt fram á, á grundvelli áhættumats, að öryggisráðstafanir séu nægjanlegar eða ef aðrar reglur takmarki beitingu ráðstafana“.*

Í 2. mgr. kemur fram að setja skuli fram skriflega lýsingu á þeim öryggisráðstöfunum sem gripið er til samkvæmt 1. mgr. þar á meðal við hönnun o.fl. Mögulegt er að verða við kröfunni um skriflegar lýsingar í hönnunarferli nýrra kerfa og ætti krafan því að taka til kerfa sem eru tekin í notkun eftir gildistöku laganna en undanþiggja ætti skriflegar lýsingar um hönnun í kerfum sem eru nú þegar fullhönnuð séu þær ekki fyrirliggjandi.

15. gr.
Varðandi a-lið þá verður að telja að öflun sakavottorðs eða öryggisvottunar umsækjenda í starf og hjá þriðja aðila áður en gengið er til samninga þyrfti að hafa skýra stoð í settum lögum vegna persónuverndarlaga. Jafnframt getur krafan verið mjög íþyngjandi í framkvæmd þegar gengið er til samninga við þriðja aðila. Getur það verið vegna þess að þriðji aðili er staddur erlendis og ekki er ávallt hægt að fá aðgang að sakavottorði á stuttum tíma. Jafnframt er óljóst í framkvæmd hvort afla þurfi sakavottorðs sé aðili að þjónusta fyrirtæki á útstöð. Frekari leiðbeiningar er þörf fyrir virkni kröfunnar.

Varðandi b- lið þá þarf að láta starfsmenn og þriðja aðila undirrita trúnaðaryfirlýsingar. Horfa verður til þess að hluti þeirra starfsmanna sem falla undir lögin bera nú þegar trúnaðarskyldu á grundvelli laga eða reglna. Er því lagt til að bætt sé við eftir b- liðinn *„séu starfsmenn ekki bundnir trúnaði samkvæmt lögum“.* Varðandi þriðja aðila, ætti að vera nægjanlegt að fá staðfestingu á að þriðji aðili hafi gert

trúnaðaryfirlýsingu við starfsmenn sína og að þjónustusamningur endurspegli slíkt. Varðandi c - og e- lið má bæta við til skýringar að aðeins sé átt við þá starfsmenn sem með beinum hætti koma að rekstri þeirra kerfa sem falla undir lögin.

16. gr.
Í 1. mgr. kemur fram að sé samið við þriðja aðila um rekstur net – og upplýsingakerfa skuli tryggja að þjónustuveitandi starfi í samræmi við lög um öryggi net – og upplýsingakerfa mikilvægra innviða og uppfylli kröfur um öryggi net – og upplýsingakerfa í samræmi við reglugerðina. Í tilfelli erlendra aðila er erfiðleikum bundið að tryggja að þriðji aðili fari eftir íslenskum lögum.

Hafa þarf í huga eðli þess rekstrar sem þriðji aðili sinnir og umfangi veittrar þjónustu. Félagið leggur því til að 1. mgr. 16. gr. sé breytt á þá leið að þriðji aðili skuli uppfylla sambærilegar kröfur og lögin gera ráð fyrir, t.d. með því að vera bundinn af net – og upplýsingalögum í heimalandi sínu, uppfylli alþjóðlega staðla sbr. 2. mgr. 11. gr. reglugerðarinnar eða kröfur sem mikilvægur innviður setur út frá nauðsyn vegna veittrar þjónustu.

17. gr.
Vísað er til athugasemda við 14. gr. reglugerðarinnar og ítrekar félagið þá afstöðu sína að lagastoð skorti fyrir því að rekstraraðilum nauðsynlegrar þjónustu/mikilvægir innviðir sé gert að viðhafa strangari öryggiskröfur en áhættumat kveður á um.

18. gr.
Varðandi b-lið 1. mgr. 18. gr. leggur félagið til að í stað „og“ komi „eða“ þannig notast verði við dulritun eða aðrar viðeigandi ráðstafanir. Dulritun er of íþyngjandi krafa ef hún eykur ekki öryggi, dulritun kemur ekki alltaf til greina sem öryggisráðstöfun, getur leitt til þess að gögn missa gildi sitt og getur verið óhentug m.a. í lokuðum kerfum. Þau kerfi sem notuð eru í starfsemi félagsins eru mörg hver sérsniðin og hluti þeirra eru í svokölluðum lokuðum kerfum og myndi endurnýjun þeirra kosta ómælt fé. Í lokuðum kerfum er ekki verið að senda í kerfi sem eru opin almenningi. Reglur um net – og upplýsingaöryggi frá Flugöryggisstofnun Evrópu eiga að taka á samræmdri lausn fyrir dulritun svo tryggt sé að aðilar geti deilt gögnum með dulritun sem henti aðilum.

Varðandi 4. tölul. a-liðar 1. mgr. þá er lágmarkskrafa að viðhafa ráðstafanir sem tryggja rekjanleika uppflettinga og vinnsluaðgerða, krafan er of íþyngjandi því það getur verið erfitt í framkvæmd í ákveðnum kerfum. Óskýrt er hvað er átt við með vinnsluaðgerðum, lagt er til að bætt sé við vinnsluaðgerðum *„vegna viðhalds kerfanna“.*

G-liður er óskýr hvað sé átt við, leiðbeiningar skortir og getur oft verið erfitt í framkvæmd og því íþyngjandi sem lágmarkskrafa.

H-liður sem lágmarkskrafa getur ekki verið uppfyllt af félaginu vegna annarra laga og reglna sem félaginu er gert að uppfylla og geta komið í veg fyrir að uppfærslur séu innleiddar án tafar, þar sem gerðar eru kröfur um sannprófun og í raun biðtíma með uppfærslur. Allar breytingar á kerfum hjá veitendum flugleiðsöguþjónustu þurfa að gangast undir fastmótað breytingarferli. Ganga þarf úr skugga um að breytingin sé örugg, þjónustan sé áfram örugg (skilvirk, samfelld, nákvæm, varanleg). Því er ekki hægt að innleiða án tafar allar uppfærslur frá þriðja aðila því það getur beinlínis skert öryggi. Lagt er því til að setningin sé tekin út eða bætt sé við, „*sé svo mögulegt*“.

19. gr.
Gerðar eru athugasemdir við þær kröfur sem fram koma í b-lið 1. mgr. 19. gr. Í þeim tilfellum þar sem raunlægar varnir eru ekki til staðar núna þá er útilokað að hægt sé að uppfylla þær fyrir 1. september.

Einnig ætti krafa 1. tölul. b- liðar 1. mgr. 19. gr. að gilda um rými sem útbúin eru eftir gildistöku laganna en eftir því sem við getur átt í rýmum sem til staðar eru nú. Að öðru leyti getur krafan verið of íþyngjandi sem lágmarkskrafa.

22. gr.
Aftur er áhrifagreining tekin fram, vísað er til athugasemda við 11. gr. reglugerðarinnar.

25. gr.
Í 1. mgr. 25. gr. leggur félagið til að eftir *alvarleg atvik* komi „er varði net – og upplýsingaöryggi“ til að taka allan vafa um að atvikin verði að tengjast því. Í 2. ml. 1. mgr. er talað um öryggisatvik, en í gegnum lögin og reglugerðina er ávallt talað um atvik eða áhættur, öryggisatvik er ekki skilgreint sérstaklega og er því um ósamræmi að ræða og lagt til að stuðst sé við „atvik“ en ekki „öryggisatvik“.

Lagt er til að horft sé til tilkynningarferlis í persónuverndarlögum þannig að heimilt er að veita upplýsingar í pörtum, séu þær ekki allar fyrirliggjandi.

Samkvæmt 4. mgr. 8. gr. laganna er heimild fyrir ráðherra að setja nánari fyrirmæli í reglugerð um tilkynningu atviks til netöryggissveitar, þar á meðal um form, efni og meðferð þeirra. Í 3. mgr. 25. gr. reglugerðarinnar er að finna viðmið við mat á því hvort atvik eða áhætta teljist alvarleg. Samkvæmt 4. mgr. sama ákvæðis er síðan heimild fyrir netöryggissveit að gefa út nánari leiðbeiningar um hvaða atvik og áhætta teljist alvarleg á grundvelli ákvæðisins. Lagt er til að með tæmandi hætti sé tekið á því í reglugerðinni hvað teljist alvarlegt á grundvelli ákvæðisins í stað þess að ferlið við skilgreiningu sé framlengt. Verði ekki fallist á það er mikilvægt að rekstraraðilar fái að koma að þeirri vinnu.

27. gr.
Félagið leggur til að bætt verði við að áður en eftirlitsstjórnvald sinnir úttektum og eftirliti skal það hafa sett sér stefnuna.

28. gr.
Samkvæmt 4. mgr. 28. gr. ber mikilvægum innviði að verða við beiðni eftirlitsstjórnvalds „innan þeirra tímamarka sem eftirlitsstjórnvald setur“. Óljóst er hvað eftirlitsstjórnvald á að miða við og lagt til að skilgreint sé betur við hvaða tímamörk eigi að miða og tekið sé tillit til umfangs og áhættu.

29. gr.
Í 1. mgr. er eftirlitsstjórnvöldum heimilt að prófa öryggi net – og upplýsingakerfa rekstraraðila og gera úttektir. Mikilvægt er til að tryggja veitingu þjónustu að eftirlitsstjórnvald láti vita fyrirfram hvenær úttekt muni eiga sér stað svo rekstraraðili geti gert ráðstafanir. Lagt er til að bætt sé við *„eftirlitsstjórnvald skal tilkynna rekstraraðila með fyrirvara hvenær úttekt er fyrirhuguð og að lágmarki með 30 daga fyrirvara“.*

Félagið þakkar fyrir tækifærið að koma að umsögn um málið og lýsir við yfir vilja til að fjalla nánar um einstakar athugasemdir og útfærslur sé eftir því óskað.

Virðingarfyllst, f.h. Isavia ohf.

_____
Kolbrún Sara Másdóttir
Lögfræðingur