Nefndasvið Alþingis,
b.t. umhverfis- og samgöngunefndar
Austurstræti 8-10
150 Reykjavík

nefndasvid@althingi.is

Reykjavík, 14. janúar 2019

Efni: Frumvarp til laga um öryggi net- og upplýsingakerfa mikilvægra innviða

Samtök atvinnulífsins og Samtök iðnaðarins vísa til tölvupósts umhverfis – og samgöngunefndar Alþingis, dags. 13. desember 2018, þar sem óskað er umsagnar samtakanna um frumvarp til laga um öryggi net- og upplýsingakerfa mikilvægra innviða, 416. mál. Um er að ræða innleiðingu á tilskipun Evrópuþingsins og ráðsins nr. 1148/2016/ESB um net- og upplýsingaöryggi (NIS tilskipunin).

Samtökin fagna því að auka eigi vernd net- og upplýsingakerfa og að bæta eigi viðbrögð við öryggisatvikum. Þar sem frumvarpið felur þó í sér auknar kröfur og strangara eftirlit á þá aðila sem teljast vera rekstraraðilar mikilvægra innviða leggja samtökin áherslu á að við innleiðingu NIS tilskipunarinnar sé gætt fyllsta samræmis og að ekki sé gengið lengra í setningu íþyngjandi reglna en nauðsynlegt er. Að því sögðu vilja samtökin koma eftirfarandi sjónarmiðum á framfæri.

1. Eftirlitsstjórnvöld öryggis net- og upplýsingakerfamála

Samtökin árétta það sem fram kom í umsögn þeirra um frumvarpið frá 13. júlí 2018. Í frumvarpinu er gert ráð fyrir að eftirlitið með ákvæðum laganna verði í höndum hvers og eins eftirlitsstjórnvalds, hvers á sínu sviði. Samtökin mótmæla því ekki en benda að sama skapi á mikilvægi þess að tryggt sé að eftirlit umræddra stjórnvalda sé samræmt. Telja samtökin að samhæfingarstjórnvald verði að hafa heimildir til að knýja fram samræmingu bæði í eftirliti og túlkun reglnanna.

Nægir að mati samtakanna ekki að ráðherra sé falið með reglugerð að mæla nánar fyrir um hlutverk samhæfingarstjórnvaldsins, sbr. 3. mgr. 13. gr. frumvarpsins, heldur þurfi að mæla með skýrum hætti fyrir um í lögum hvert sé umfang og eðli þeirra heimilda sem stjórnvaldið hefur til að rækja hlutverk sitt.

2. Öryggiskröfur og tilkynningar um atvik

Tilskipunin tekur til aðila sem teljast vera rekstraraðilar nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu, en til þeirra beggja er vísað til sem rekstraraðila mikilvægra innviða í frumvarpinu. Af lestri tilskipunarinnar er ljóst að grundvallarmunur er á milli rekstraraðila nauðsynlegrar þjónustu og veitenda stafrænnar þjónustu og er fjallað um þessa tvo aðila, bæði hvað varðar skyldur og eftirlit, með aðgreindum hætti.

Ákvæði tilskipunarinnar er lúta að öryggiskröfum og tilkynningum um atvik eru mismunandi eftir því hvort um rekstraraðila nauðsynlegrar þjónustu er að ræða, sbr. 14. gr., eða veitendur stafrænnar þjónustu, sbr. 16. gr. Í frumvarpinu er þessum ákvæðum hins vegar slegið saman, og því settar saman í eitt ákvæði skyldur beggja þessara aðila, sem gerir ákvæðið óskýrt og ruglingslegt. Sér í lagi í ljósi þess að skyldur aðilanna eru ólíkar skv. áðurnefndri tilskipun. Þessu til stuðnings vísa samtökin sérstaklega til 49. liðar formálsorða tilskipunarinnar þar sem fram kemur:

> Veitendur stafrænnar þjónustu ættu að tryggja öryggisstig í réttu hlutfalli við áhættuna fyrir öryggi stafrænu þjónustunnar sem þeir veita, að gefnu mikilvægi þeirra þjónustu fyrir rekstur annarra fyrirtækja innan Sambandsins. Í raun er áhættustigið hærra fyrir rekstraraðila nauðsynlegrar þjónustu, sem oft er nauðsynleg til að halda uppi mikilvægri samfélagslegri og efnahagslegri starfsemi, en það er fyrir veitendur stafrænnar þjónustu. Því ættu öryggiskröfur til veitenda stafrænnar þjónustu að vera minni.

Af lestri tilskipunarinnar er ljóst að það er beinlínis rangt að hafa sömu efnisákvæði fyrir báða þessa aðila. Það eykur ennfremur skýrleika að skyldur aðilanna séu útlistaðar í sitt hvoru ákvæðinu. Leggja samtökin því fremur til að sett sé eitt ákvæði sem innleiði 14. gr. tilskipunarinnar og fjalli um öryggiskröfur og tilkynningar um atvik í tilviki rekstaraðila mikilvægra þjónustu. Þá sé sett annað ákvæði sem fjalli um öryggiskröfur og tilkynningar um atvik í tilviki veitenda stafrænnar þjónustu og 16. gr. tilskipunarinnar innleidd í heild sinni.

Í 4. mgr. 7. gr. frumvarpsins er nú kveðið á um heimild fyrir ráðherra að setja nánari fyrirmæli um lágmarkskröfur samkvæmt ákvæðinu í reglugerð. Í reglugerðinni hefur ráðherrann heimild til þess til þess að gera greinarmun á kröfum til rekstraraðila nauðsynlegrar þjónustu og stafrænna þjónustuveitenda. Líkt og áður segir eru Samtökin þeirrar skoðunar að öryggiskröfur er varða rekstraraðila nauðsynlegrar þjónustu annars vegar og veitendur stafrænnar þjónustu hins vegar eigi heima í tveimur aðskildum lagaákvæðum. Verði niðurstaðan sú að útfæra mismunandi öryggiskröfur með reglugerð er lágmarkskrafan sú að skylda verði lögð á ráðherra að setja reglugerð um efnið og jafnframt að sú reglugerð verði sett samhliða gildistöku laganna. Að öðrum kosti skapast ósamræmi við efni áðurnefndrar tilskipunar og óvissa ríkir um beitingu laganna gagnvart stafrænum þjónustuveitendum.

3. Eftirlit og afhending gagna.

Í 12. gr. frumvarpsins er fjallað um eftirlitsheimildir. Í 1. mgr. er fjallað um skyldu rekstraraðila nauðsynlegrar þjónustu til að afhenda allar upplýsingar og gögn um skipulag net- og upplýsingaöryggis að beiðni eftirlitsstjórnvalds. Í 3. mgr. 12. gr. segir að ákvæði 1. mgr. gildi um stafræna þjónustuveitendur, að fenginni beiðni frá Póst- og fjarskiptastofnun, þegar stofnunin telur á grundvelli rökstuddra grunsemda að hlutaðeigandi uppfylli ekki kröfur um tilkynninga- og öryggiskröfur. Ákvæðið er breytt frá fyrra frumvarpi og er í þessari mynd í betra samræmi við tilskipunina.

Tilskipunin gerir ráð fyrir því að veitendur stafrænnar þjónustu eigi að sæta vægu eftirliti og að einungis megi grípa til aðgerða þegar sönnunargögn eru lögð fram sem sýna að veitandi stafrænnar þjónustu uppfylli ekki kröfur og einkum eftir að meint brot hefur átt sér stað. Í frumvarpinu er hinsvegar notast við annað orðalag og er gert ráð fyrir heimild Póst- og fjarskiptastofnunar til aðgerða gagnvart stafrænum þjónustuveitendum þegar fyrir liggur rökstuddur grunur. Í greinargerð er þó ekki útskýrt hvað sé átt við með orðunum „rökstuddur grunur“ og hvort hér séu þá sömu skilyrði til aðgerða gagnvart veitendum stafrænnar þjónustu og tilskipunin gerir ráð fyrir. Eðlilegra væri að orðalag væri í samræmi við tilskipunina, svo fyllsta samræmis sé gætt.

4. Dagsektir

Vísað er til fyrri umsagnar samtakanna frá 13. júlí 2018. Í 22. gr. frumvarpsins er mælt fyrir um heimildir eftirlitstjórnvalda til að leggja á dagsektir sem geta numið allt að 500.000 krónum á dag. Í greinargerð er vísað til sambærilegs ákvæðis í lögum um Póst- og fjarskiptastofnun og fjárhæðin rökstudd með þeim hætti. Samtökin gera athugasemd við umrætt ákvæði enda er dagsektarheimildin umtalsvert hærri en almennt tíðkast í stjórnsýslunni. Ennfremur telja samtökin skorta greiningu á nauðsyn umræddrar dagsektarfjárhæðar og rökstuðning. Það er að mati samtakanna ekki nægjanlegt að vísa með almennum hætti til annarra lagabálka. Hvetja samtökin því til þess að hámarkið verði endurskoðað með tilliti til markmiða ákvæðisins.

5. Refsiákvæðið

Í 23. gr. frumvarpsins er mælt fyrir um að brot gegn ákvæðum II. kafla og 19. gr. laganna og reglugerða geti varðað fésektum eða fangelsi allt að 2 árum. Í 2. mgr. er tekið fram að ef brot sé framið í starfsemi lögaðila eigi að fylgja II. kafla A almennra hegningarlaga. Samtökin telja ekki nægilega skýrt koma fram í hvaða tilvikum einstaklingar myndu eiga á að hættu á að sæta refsingu sem og í hvaða tilvikum lögaðilar myndu eiga á því hættu. Sem dæmi má nefna að skyldur laganna taka almennt til starfsemi lögaðila og því óljóst hvort að einstaklingur, og þá hvaða einstaklingur, sem starfar hjá lögaðilanum myndi þurfa að sæta refsingu. Þá er í II. kafla laganna að finna ákvæði er varða netöryggissveit og skyldur er á henni hvíla. Óljóst er hvort að refsiákvæði eiga jafnframt við um hana. Á grundvelli skýrleika refsiheimilda væri einnig hentugra að fram kæmi með skýrum hætti hvaða ákvæði laganna varði refsingu. Vísa samtökin hér til 145. gr. laga nr. 108/2007 um verðbréfaviðskipti og til 112. gr. b. laga nr. 161/2002 um fjármálafyrirtæki sem fyrirmyndar en þar er skýrlega listuð upp sú háttsemi sem brot liggur við.

Virðingarfyllst,

Heiðrún Björk Gísladóttir, f.h. SA

Björg Ásta Þórðardóttir, f.h. SI