Samgöngu- og sveitarstjórnarráðuneytið
srn@srn.is

Reykjavík, 20. júlí 2018

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

Samtök atvinnulífsins og Samtök iðnaðarins hafa tekið til umsagnar nýtt frumvarp til laga um öryggi net- og upplýsingakerfa mikilvægra innviða sem birt var á samráðsgátt stjórnarráðsins hinn 21. júní 2018.

Frumvarpið felur í sér innleiðingu á tilskipun Evrópuþingsins og ráðsins nr. 1148/2016/ESB um net- og upplýsingaöryggi (NIS-tilskipunin). Samtökin fagna því 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. **Rekstraraðilar nauðsynlegrar þjónustu**

Samkvæmt tilskipuninni er það undir aðildarríkjunum komið að skilgreina með nákvæmum hætti hverjir falli undir skilgreininguna *rekstraraðilar nauðsynlegrar þjónustu*. Í 5. gr. frumvarpsins eru sett fram þau viðmið sem tilskipunin mælir fyrir um og vísað til 5. gr., 6. gr. og II. viðauka tilskipunarinnar um það hverjir teljist vera rekstraraðilar nauðsynlegrar þjónustu og hvaða þjónusta fallir þar undir. Viðmiðin eru að þjónusta skuli vera nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi, að veiting þjónustu sé háð net- og upplýsingakerfum og að atvik myndu hafa veruleg skerðandi áhrif á veitingu þjónustu. Samkvæmt 3. mgr. 5. gr. frumvarpsins er það undir ráðherra komið að mæla nánar fyrir um þessar viðmiðanir til auðkenningar rekstraraðila nauðsynlegrar þjónustu og útbúa skrá yfir þá þjónustu sem telst nauðsynleg.

Viðmiðin eru matskennd og því mikilvægt að gætt sé að því að öll þau atriði sem geti haft áhrif á túlkun þeirra séu höfð til hliðsjónar og séu lögfest. Vísa samtökin hér sérstaklega til þess hvaða atvik myndu teljast hafa *veruleg skerðandi áhrif* á veitingu þjónustu. Í 6. gr. tilskipunarinnar og 27. lið formálsorða tilskipunarinnar er sérstaklega tekið fram til hvaða atriði eigi að líta til þegar metið er hvort atvik teljist hafa veruleg skerðandi áhrif á veitingu nauðsynlegrar þjónustu. Þessi atriði geta haft áhrif á hverjir falli undir skilgreininguna og þar af leiðandi undir lögin. Til að auka skýrleika er mikilvægt að þau viðmið sem fram komi í 6. gr. tilskipunarinnar séu færð inn í lagatextann eða að minnsta kosti inn í greinargerðina.

Samtökin vilja benda á að mögulegt er að aðilar sem starfi í þeim geirum og undirgeirum sem 5. gr. tilgreinir geti bæði veitt nauðsynlega þjónustu og þjónustu sem ekki telst vera nauðsynleg. Vísa samtökin hér til 22.- 23. liða formálsorða tilskipunarinnar en þar er tekið dæmi um að flugvellir veiti bæði nauðsynlega þjónustu s.s rekstur flugbrauta og einnig þjónustu sem ekki myndi teljast nauðsynleg t.d. verslunarrekstur.

Mikilvægt er að skýrt komi fram, í texta laganna eða í greinargerð, að einungis eigi sú þjónusta sem telst vera nauðsynleg að falla undir sérstakar öryggiskröfur laganna.

2. Eftirlitsstjórnvöld öryggis net- og upplýsingakerfamála

Í frumvarpinu er gert ráð fyrir að eftirlitið með ákvæðum laganna verði í höndum hvers og eins eftirlitsstjórnvalds, hvert 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 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.

3. Öryggiskröfur og tilkynningar um atvik

Tilskipunin tekur til aðila sem teljast vera rekstraraðilar nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu, sbr. 5. gr. og 6. gr. frumvarpsins, 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 eftirliti, 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.

4. Eftirlit og afhending gagna

Hið sama gildir um 15. gr. frumvarpsins sem fjallar um eftirlit og afhendingu gagna. Í tilskipunni er skýrt tekið fram að veitendur stafrænnar þjónustu eigi að sæta *vægu eftirliti* sem byggi á viðbragði eftir á vegna eðlis þjónustu þeirra og starfsemi.

Er þar tekið fram að einungis megi grípa til aðgerða þegar sönnunargögn eru lögð fram sem sýna að veitandi stafrænnar þjónustu uppfylli ekki kröfur einkum eftir að atvik hefur átt sér stað. Af þessu er ljóst að stjórnvöldum ber ekki nein almenn skylda til að hafa yfirumsjón með veitendum stafrænnar þjónustu. Þetta er nánar útfært í 17. gr. tilskipunarinnar.

Í 15. gr. tilskipunarinnar er fjallað um hvernig eftirlitinu eigi að vera háttað með rekstraraðilum nauðsynlegrar þjónustu. Samkvæmt ákvæðinu getur eftirlitsstjórnvald krafist allra nauðsynlegra upplýsinga til að meta öryggi net- og upplýsingakerfa og sannana fyrir skilvirki framkvæmd öryggisreglna. Ekki þarf því að hafa orðið atvik til að eftirlitsskyldan verði virk.

Þessi greinarmunur sem gerður er í tilskipunninni á eftirliti með annars rekstraraðilum nauðsynlegrar þjónustu og stafrænum þjónustuveitendum þarf að koma skýrt fram í lögunum. Ekki nægir að taka slíkt einungis fram í greinargerð með frumvarpinu. Til að tryggja skýrleika telja samtökin að endurskoða verði 15. gr. frumvarpsins, til samræmis við 15. gr. og 17. gr. tilskipunarinnar.

5. Dagsektir

Í 27. 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.

6. Refsiákvæðið

Í 28. gr. frumvarpsins er mælt fyrir um að brot gegn ákvæðum 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. 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. 161/200 um fjármálafyrirtæki sem fyrirmyndar.

Virðingarfyllst,

Unnur Elfa Hallsteinsdóttir, f.h. Samtaka atvinnulífsins

Björg Ásta Þórðardóttir f.h. Samtaka iðnaðarins