SAMTÖK FJÁRMÁLAFYRIRTÆKJA
Icelandic Financial Services Association

Nefndasvið Alþingis
Austurstræti 8-10
Bt. Umhverfis-og samgöngunefndar
150 REYKJAVÍK

Reykjavík 15. febrúar 2019

Efni: Frumvarp til laga um öryggi net og upplýsingakerfa mikilvægra innviða, 416. mál

Samtök fjármálafyrirtækja (SFF) vísa til frumvarps til laga um öryggi net og upplýsingakerfa mikilvægra innviða sem umhverfis- og samgöngunefnd hefur til umfjöllunar. Eftirfarandi eru athugasemdir samtakanna.

Fjármálafyrirtæki eru í fremstu víglínu þegar kemur að baráttunni gegn netglæpum. Aðildarfélög SFF hafa um árabil átt í nánu samstarfi við löggæsluyfirvöld vegna slíkra glæpa og leggja ríka áherslu á að halda uppi öflugum vörnum gegn þeim og á forvarnarfræðslu til viðskiptavina sinna.

Samtökin styðja markmið frumvarpsins að auka vernd net- og upplýsingakerfa og efla viðbrögð við öryggisfrávikum. Frumvarpið felur í sér auknar kröfur til þeirra fyrirtækja sem eru rekstraraðilar mikilvægra innviða og eftirlit með þeim. Af þeim sökum brýna SFF að við innleiðingu NIS tilskipunarinnar sé gætt fyllsta samræmis og að ekki sé gengið lengra í setningu íþyngjandi reglna en nauðsynlegt er.

Áður en að komið er að athugasemdum um einstaka efnisgreinar frumvarpsins vilja samtökin halda á lofti eftirfarandi athugasemdum.

- Það má velta þeirri spurningu upp hvort að það sé heppilegt að netöryggissveitin heyri undir Póst- og fjarskiptastofnun. (PF) Í því samhengi má rifja upp að til stóð fyrir nokkrum árum að láta sveitina heyra undir ríkislögreglustjóra. Rekstur mikilvægra innviða á borð við fjármálakerfi kallar á sérhæfða þekkingu. Í frumvarpinu kemur ekki fram hvers vegna netöryggissveitin sé staðsett hjá PF, né heldur hvaða kröfur eru gerðar til Netöryggissveitarinnar og starfsmanna hennar varðandi þekkingu og reynslu til að sinna skyldum sínum á trúverðugan hátt fyrir svo mikilvægan málaflokk.
- Stefnt er að því að lögin taki gildi við upphaf næsta árs. Tryggja þarf að allir hlutaðeigandi aðilar geti undirbúið sig á faglegan og fullnægjandi hátt áður en löggjöfin tekur gildi. Margt er óljóst hvað löggjöfina varðar og annað virðist þarfnast nánari útfærslu. SFF veltir því upp hvort gildistaka ætti ekki að vera um mitt ár 2020.
- Fram kemur í greinargerð frumvarpsins að gert er ráð fyrir að kostnaðurinn við innleiðingu tilskipunarinnar á næstu árum eða frá 2020–2024 verði samtals um 2.745 milljarðar króna. NIS-tilskipunin leggur ákveðnar kvaðir á stjórnvöld annars vegar og fyrirtæki sem koma að rekstri mikilvægra innviða. SFF leggja mikla áherslu á að þessum kostnaði verði ekki mætt af hálfu stjórnvalda með álögum á þau fyrirtæki sem heyra undir lögin. Aðildarfélög SFF greiða nú þegar tæpa 40 milljarða í opinber gjöld á ári hverju og þar af nema eftirlitsgjöld á annan milljarð.

Athugasemdir við einstakar greinar frumvarpsins

4. gr. Stefna um net- og upplýsingaöryggi. Netöryggisráð

Samkvæmt 4. gr. skipar ráðherra netöryggisráð. Hlutverk þess er að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis. Ljóst er af umfjöllun í greinagerð að netöryggisráði er ætlað mikilvægt hlutverk.

Ekkert er hins vegar fjallað um hvaða kröfur eru gerðar til hæfni þeirra aðila sem skipaðir eru í ráðið. SFF telja mikilvægt að ákveðnar kröfur um þekkingu og hæfni þeirra komi fram í lögunum t.d. viðeigandi menntun og reynslu.

6. gr. Orðskýringar

Samkvæmt 3. tl. 1. mgr. 6. gr. er bankastarfsemi skilgreind sem lánastofnun í skilningi laga um fjármálafyrirtæki. Þetta verður að taka til athugunar með hliðsjón af því hvort að ætlunin sé að lögin nái um starfsemi fyrirtækja sem sinna greiðslumiðlun og öðrum tegundum af fjármálaþjónustu.

7. gr. Lágmarkskröfur um áhættustýringu og viðbúnað

Í greininni, sem fjallar um áhættustýringu og viðbúnað, segir:

> *„Aðgangsstýring skal viðhöfð í rekstri net- og upplýsingakerfa mikilvægra innviða eftir því sem við á og viðeigandi prófanir framkvæmdar reglubundið og í samræmi við alþjóðleg viðmið um bestu framkvæmd.“*

Nauðsynlegt er að skýra hvað er átt við með „alþjóðlegum viðmiðum“ en skýringar á slíku er ekki að finna í greinargerð frumvarpsins.

Í umfjöllun um 7. gr. í greinargerðinni er vísað til ISO27001:2005 staðals en sá staðall er að úreldast. Í dag fara flestir ISO27001:2013 og ISO27001:2017. Varhugavert getur verið að vísa í ákveðinn staðal þar sem þeir úreldast með tímanum,. Lagt er til að orðalag ákvæðisins verði víkkað út þannig að það vísi einnig til staðla sem munu koma í stað núgildandi staðla á þessu sviði.

8. gr. Tilkynning til netöryggissveitar

Greinin fjallar um tilkynningar til netöryggissveitar. Í 1. mgr. 8. gr. segir:

> *„Mikilvægir innviðir skulu tilkynna netöryggissveit Póst- og fjarskiptastofnunar skv. IV. kafla án tafar um alvarleg atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa þeirra.“*

Samkvæmt NIS-tilskipuninni er mikilvægum innviðum eingöngu gert að tilkynna netöryggissveitinni um atvik sem ógna öryggi net- og upplýsingakerfum. SFF telja að lögin eigi að vera samhljóða tilskipuninni. Áhættur geta verið margvíslegum toga. Að mati SFF er of mikið í lagt ef tilkynna skal öryggissveitinni um allar þá áhættur sem netöryggissérfræðingar mikilvægra innviða verða áskynja í störfum sínum. Hætt er við því að slíkt fyrirkomulag leiði til óskilvirkni.

Þá telja SFF að orðalagið „án tafar“ vera of íþyngjandi og leggja til að í staðinn komi orðalagið „svo fljótt sem verða má“.

Samkvæmt framansögðu leggja SFF til að 1. mgr. 8. gr. orðist svo:

> *„Mikilvægir innviðir skulu tilkynna netöryggissveit Póst- og fjarskiptastofnunar skv. IV. kafla svo fljótt sem verða má um alvarleg atvik sem ógna öryggi net- og upplýsingakerfa þeirra.“*

Einnig er rétt að benda á að eftirlitskyldum fjármálafyrirtækjum er nú þegar gert að tilkynna „alvarleg atvik“ til FME og Persónuverndar. Flækjustigið eykst enn frekar þegar þeim verður gert að tilkynna slík atvik til þriðju stofnunarinnar. Nauðsynlegt er að straumlínulaga þetta ferli og telja SFF að skilvirkast væri að FME kæmi slíkum tilkynningum til netöryggissveitar.

á segir í 3. mgr. 8. gr. :

> *„Í tilkynningu skal meðal annars upplýst um mögulegt útvistunarfyrirkomulag, svo sem ef mikilvægir innviðir reiða sig á þjónustu stafræns þjónustuveitanda í rekstri sínum, og hugsanleg smitáhrif, jafnvel yfir landamæri. Umfang tilkynningar ræðst að öðru leyti af efni og aðstæðum.“*

Ekkert er fjallað um útvistun í NIS-tilskipuninni. FME hefur nú þegar gefið út tilmæli sem varða slíka útvistun. Rétt væri að skoða málið til að koma í veg fyrir hugsanlega skörun.

10. gr. Upplýsingar veittar almenningi.

Greinin fjallar um upplýsingagjöf til almennings. Í 1. mgr. 10. gr. segir :

> *„Ef almenningsvitundar er þörf til að koma í veg fyrir eða takast á við atvik og þegar upplýsingagjöf um atvik er af öðrum ástæðum nauðsynleg í þágu almannahagsmuna er Póst- og fjarskiptastofnun heimilt að upplýsa almenning um atvikið. Samráð skal viðhaft við lögreglu og eftirlitsstjórnvöld sem í hlut kunna að eiga og, eftir atvikum, mikilvæga innviði, í aðdraganda upplýsingagjafar skv. 1. málsl., enda verði því við komið.* "

Hér er brýnt að breyta orðalagi þannig að Póst- og fjarskiptastofnun verði gert að eiga samráð við mikilvæga innviði áður en að almenningur er upplýstur um atvik. Mikilvægt er að mikilvægur innviður fái ráðrúm til þess að gera viðeigandi ráðstafanir til þess að útiloka frekari misnotkun á galla sem uppgötvast áður en tilkynnt er opinberlega um atvik.

Samkvæmt framangreindu leggja SFF til eftirfarandi breytingu á 1. mgr. 10. gr.

> *„Ef almenningsvitundar er þörf til að koma í veg fyrir eða takast á við atvik og þegar upplýsingagjöf um atvik er af öðrum ástæðum nauðsynleg í þágu almannahagsmuna er Póst- og fjarskiptastofnun heimilt að upplýsa almenning um atvikið. Samráð skal viðhaft við lögreglu og eftirlitsstjórnvöld sem í hlut kunna að eiga og~~, eftir atvikum,~~ mikilvæga innviði, í aðdraganda upplýsingagjafar skv. 1. málsl.~~, enda verði því við komið~~.* "

11. gr. Eftirlitsstjórnvöld

Greinin fjallar um eftirlit með mikilvægum innviðum. Þar kemur að FME er ætlað að hafa eftirlit með öryggi net- og upplýsingakerfa banka og innviða fjármálamarkaða. Þetta felur í sér að fjármálafyrirtækin eru með allt undir hjá FME fyrir utan samskipti við netöryggissveitina. Þetta styrkir röksemdafærslu athugasemdar SFF við 8. gr. frumvarpsins um að nauðsynlegt sé að straumlínulaga skipulagið þannig að FME sjái um samskipti við netöryggissveitina í stað þess að mikilvægir innviðir á fjármálamarkaði geri það beint.

Hér þarf að hafa í huga að í frumvarpinu er ekki fjallað um hvernig skuli fara með tilvik þegar gildandi lög og reglur leggja samsvarandi skyldur á fjármálafyrirtæki og ákvæði frumvarpsins. Tilskipunin er skýr um að núgildandi réttargerðir skuli gilda og er bankastarfsemi tekin sem dæmi um þess konar réttargerðir í inngangsorðum tilskipunarinnar sbr. 7. mgr. 1. gr.hennar. Að mati SFF er mikilvægt inn í frumvarpið verði bætt sambærilegu ákvæði til að taka af tvímæli um gildi sambærilegra ákvæði laga og reglna sem gilda um fjármálafyrirtæki sérstaklega.

12. gr. Eftirlitsheimildir

Í greininni er fjallað um eftirlitsheimildir. Í 2. mgr. 12. gr. segir:

> *„Eftirlitsstjórnvaldi skv. 11. gr. er heimilt að gera úttektir og prófanir á því hvort rekstraraðilar nauðsynlegrar þjónustu uppfylli kröfur laga þessara og reglugerða sem settar eru á grundvelli þeirra. Eftirlitsstjórnvald getur jafnframt gert kröfu um að til þess bær utanaðkomandi aðili geri úttektir og prófanir og kveðið á um framvísun skjalfestra niðurstaðna hlutaðeigandi.*"

Hér er ákaflega mikilvægt að lögin kveði skýrar á um skilyrði fyrir hæfi úttektaraðila.

Í 3. mgr. segir: *„Ákvæði 1. mgr. gildir um stafræna þjónustuveitendur... ".*

Ekki er ljóst hvers vegna ákvæðið nær eingöngu til veitendur stafrænnar þjónustu en ekki annarra rekstraraðila mikilvægra innviða á borð við veitufyrirtæki svo dæmi sé tekið.

14. gr. Netöryggissveit

Í þessari grein er fjallað um netöryggissveitina. Til þess að netöryggissveitin geti sinnt hlutverki sínu þarf að tryggja að þeir sem hana skipa búi yfir viðeigandi þekkingu og reynslu. Vakin er athygli á því að í hæfiskröfum starfsmanna netöryggissveitar í reglugerð er einungis gerð krafa um hæfi þeirra til að vinna með viðkvæmar upplýsingar. Ljóst er að gera þarf mun ríkari kröfur til hæfis starfsmanna netöryggissveitar.

Í 6. mgr. 14. gr.segir:

> *„Netöryggissveit vaktar og greinir atvik og áhættu tengda öryggi net- og upplýsingakerfa og mótar stöðumynd vegna netógna á hverjum tíma eftir því sem við kann að eiga. Stöðumati skal reglubundið miðlað til netöryggisráðs í samræmi við óskir þess.“*

Hér þarf að kveða á um að stöðumatinu sé einnig miðlað reglulega til mikilvægra innviða til að þeir geti brugðist við. Í tilfelli fjármálafyrirtækja færi best að sú miðlun færi í gegnum FME.

17. gr. Aðgangur netöryggissveitar að upplýsingum

Greinin fjallar um aðgengi netöryggissveitar að upplýsingum. Þar segir í 1. – 4. mgr. :

> *„Í því skyni að tryggja netöryggissveit bestu faglegu forsendur til viðbragða við atvikum og áhættu í net- og upplýsingakerfum skal henni, eins skjótt og við verður komið, heimilaður aðgangur að viðeigandi upplýsingum og gögnum sem hún metur nauðsynleg, þar með töldum umferðaskrám netbúnaðar og -þjóna, eftir atvikum í samráði við eftirlitsstjórnvöld.*
>
> *Til að greina og meta ógnir og áhættu við net- og upplýsingakerfi mikilvægra innviða getur Póst- og fjarskiptastofnun óskað eftir að komið skuli upp sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi mikilvægra innviða og netöryggissveitar.*
>
> *Netöryggissveit, eftir atvikum í samráði við eftirlitsstjórnvöld, getur óskað skriflegra upplýsinga eða gagna og kallað einstaklinga til skýrslugjafar ef þörf krefur svo sveitin geti gegnt hlutverki sínu samkvæmt lögum þessum.*
>
> *Réttur netöryggissveitarinnar til aðgangs að upplýsingum samkvæmt ákvæði þessu verður ekki takmarkaður með vísan til reglna um þagnarskyldu er kunna að gilda um mikilvæga innviði.“*

Ekki er ljóst af heimild 1. mgr. hvort að hún eigi við þau tilfelli þegar um öryggisatvik er að ræða eða hvort að sveitin geti nýtt þessa heimild hvenær sem er. Nauðsynlegt er að skýra betur í lögunum eða greinagerð með þeim að heimildin eigi einungis við þegar um er að ræða öryggisatvik.

Í 2. mgr. er kveðið á um heimild PF til að óska eftir að komið skuli upp sjálfvirkri upplýsingamiðlun á milli kerfa hlutaðeigandi mikilvægra innviða og netöryggissveitar til að greina og meta ógnir og áhættu við net- og upplýsingakerfi mikilvægra innviða. Sambærilegt ákvæði er ekki að finna í tilskipun þeirri sem frumvarp þetta byggir á. Um mjög íþyngjandi inngrip er að ræða sem býður upp á vöktun á hegðun fjölda skráðra einstaklinga í almennum og óskilgreindum tilgangi. Enga umfjöllun um úrræðið er að finna í athugasemdum við ákvæðið sem gæti skýrt nánar í hvaða tilfellum og með hvaða hætti unnt er að fara fram á slíkt eftirlit og hvaða viðurlög séu við því ef ekki er orðið við ósk stofnunarinnar. Full ástæða er til að gera ákvæðinu frekari skil í frumvarpinu. Það skiptir jafnframt máli með hvaða hætti slík sjálfvirk upplýsingamiðlun er sett upp, en allar viðbætur við kerfi mikilvægra innviða sem senda upplýsingar beint úr kerfum þeirra til þriðja aðila eru til þess fallin að skerða varnir hans og opna á frekari tækifæri fyrir óviðkomandi aðila til að brjótast í gegnum varnir hans. kallar enn fremur á útskýringar á hvaða þörf er fyrir sjálfvirka miðlun slíkra upplýsinga og hvers konar upplýsingar er um að ræða. Að óbreyttu felur þessi málsgrein í sér mjög umfangsmiklar heimildir til eftirlits með þegnum ríkisins.

Ákvæði 3. og 4. mgr. felur í sér afar víðtæka heimild netöryggissveitar til að afla gagna af hvaða tagi sem er og sérstaklega er tekið fram að réttur til gagnaöflunar verði ekki takmarkaður með vísan til reglna um þagnarskyldu sem kunna að gilda um mikilvæga innviði. Í tilfelli fjármálafyrirtækja gildir 58. gr. laga nr. 161/2002, um fjármálafyrirtæki, um þagnarskyldu (bankaleynd) til þess að vernda fjárhagsupplýsingar manna. SFF telja mikilvægt að lögin séu ekki víðtækari en nauðsyn ber til og gæta þarf meðalhófs að því leyti. Því telja SFF mikilvægt að taka fram í ákvæðinu að heimildin taki eingöngu til upplýsinga sem varða netöryggi en ekki til persónuupplýsinga svo sem fjárhagsupplýsinga viðskiptavina fjármálafyrirtækja. Sama kann að eiga við um aðrar

viðkvæmar persónuupplýsingar á öðrum sviðum. Hafa þarf í huga að þetta ákvæði getur verið notað á íþyngjandi hátt og skiptir virkilegu máli að varlega sé farið og að því sé beitt á faglegan hátt og á réttum forsendum.

19. og 20. gr. Þagnarskylda og sérstök þagnarskylda

Í 19. og 20. gr. frumvarpsins er fjallað um þagnarskyldu og undanþágu frá henni. SFF ítreka ábendinguna sem sett er fram við 17. gr. um samspil við 58. gr. laga nr. 161/2002, um fjármálafyrirtæki um þagnarskyldu (bankaleynd).

23. gr. Refsingar og kæruleið

Samkvæmt 23. gr. þá varða brot á lögunum fésektum eða fangelsi allt að tveimur árum, nema þyngri refsing liggi við samkvæmt öðrum lögum. Samkvæmt ákvæðinu liggur sama refsing til grundvallar ef ekki er farið að fyrirmælum eftirlitsstjórnvalda, og skulu gáleysisbrot eingöngu varða sektum. SFF taka undir athugasemdir í umsögn Samtaka atvinnulífsins og Samtaka iðnaðarins um óskýrleika ákvæðisins.

Þá er einnig mikilvægt að löggjafinn hugi að því hvort ekki sé rétt að mæla fyrir um kæruleið til æðra stjórnvalds fyrir aðila sem lögin taka til.

Virðingarfyllst,
f.h. Samtaka fjármálafyrirtækja

Örn Arnarson