Lög

um öryggi net- og upplýsingakerfa mikilvægra innviða.

_____

I. KAFLI
Almenn ákvæði.

1. gr.
Markmið.

Markmið laga þessara er að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða eins og þeir eru skilgreindir í lögum þessum.

2. gr.
Gildissvið.

Lög þessi gilda um net- og upplýsingakerfi rekstraraðila nauðsynlegrar þjónustu hér á landi á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja, að uppfylltum skilyrðum 3. gr.

Lög þessi gilda jafnframt um net- og upplýsingakerfi veitenda stafrænnar þjónustu sem starfrækja netmarkað, leitarvél á netinu eða skýjavinnsluþjónustu, þó ekki veitendur stafrænnar þjónustu sem teljast örfélög í skilningi laga um ársreikninga.

3. gr.
Rekstraraðilar nauðsynlegrar þjónustu.

Þjónusta rekstraraðila skv. 1. mgr. 2. gr. telst nauðsynleg í skilningi laga þessara að uppfylltum eftirtöldum skilyrðum:

a. Þjónusta er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi,
b. veiting þjónustu er háð net- og upplýsingakerfum og
c. atvik hefðu verulega skerðandi áhrif á veitingu þjónustu.

Ráðherra skal í reglugerð mæla nánar fyrir um þjónustu sem telst nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi í skilningi a-liðar 1. mgr.

Við mat á því hvort atvik hefðu verulega skerðandi áhrif í skilningi c-liðar 1. mgr. skal a.m.k. horft til fjölda notenda sem reiða sig á umrædda þjónustu, hvort rekstraraðilar nauðsynlegrar þjónustu á öðrum sviðum reiði sig á umrædda þjónustu, mögulegra áhrifa atvika á efnahagslega og samfélagslega starfsemi eða almannaöryggi, mögulegrar landfræðilegrar útbreiðslu áhrifa af atvikum, markaðshlutdeildar og mikilvægis samfellu í þjónustustigi, að teknu tilliti til varaleiða. Enn fremur skal tekið tillit til sjónarmiða sem sértæk kunna að vera fyrir ólík svið.

Ráðherra skal halda opinbera skrá yfir rekstraraðila nauðsynlegrar þjónustu hér á landi samkvæmt ákvæði þessu með auglýsingu í B-deild Stjórnartíðinda, að fenginni tillögu Póst- og fjarskiptastofnunar. Skráin skal uppfærð eftir því sem tilefni er til og á a.m.k. tveggja ára fresti.

4. gr.

Stefna um net- og upplýsingaöryggi. Netöryggisráð.

Ráðherra skal marka stefnu um net- og upplýsingaöryggi, sem endurskoðuð skal reglubundið. Í stefnu skal m.a. greina frá markmiðum og ráðstöfunum stjórnvalda í því skyni að stuðla að öryggi og viðnámsþrótti net- og upplýsingakerfa mikilvægra innviða.

Ráðherra skipar netöryggisráð. Fulltrúar sem skipaðir eru í ráðið skulu hafa viðeigandi menntun og/eða reynslu. Hlutverk ráðsins er einkum að fylgja eftir framkvæmd stefnu stjórnvalda á sviði net- og upplýsingaöryggis. Ráðið leggur mat á stöðu netöryggis á Íslandi á hverjum tíma og er vettvangur upplýsingamiðlunar og samhæfingar. Netöryggisráð skal setja sér starfsreglur. Fundir netöryggisráðs skulu haldnir fyrir luktum dyrum og getur ráðið ákveðið að trúnaður ríki um fundi þess eða einstök mál á dagskrá fundar, svo og gögn og afrakstur vinnu í smærri hópum fyrir ráðið. Ráðherra er heimilt að setja nánari ákvæði um netöryggisráð í reglugerð.

5. gr.

Tengsl við önnur lög.

Um eftirlit með framkvæmd laga þessara fer samkvæmt ákvæðum III. kafla og þeim sérlögum sem um mikilvæga innviði gilda.

Ef hætta steðjar að net- og upplýsingaöryggi með þeim hætti að teljist neyðarástand sem kann að ógna lífi og heilsu almennings, umhverfi og/eða eignum í skilningi laga um almannavarnir fer um viðbrögð stjórnvalda á grundvelli þeirra laga.

6. gr.

Orðskýringar.

Í lögum þessum merkir:

1. *Atvik:* Hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa.
2. *Áhætta:* Aðstæður eða atburðir sem geta haft skaðleg áhrif á öryggi net- og upplýsingakerfa.
3. *Bankastarfsemi:* Lánastofnun í skilningi laga um fjármálafyrirtæki.
4. *Eftirlitsstjórnvald:* Stjórnvald sem falið er eftirlit með framkvæmd laga þessara um öryggi net- og upplýsingakerfa á sínu sviði.
5. *Flutningastarfsemi:* Flutningar á lofti; flugrekendur eins og skilgreint er í 10. tölul. 2. gr. reglugerðar (EB) nr. 1008/2008, framkvæmdastjórnir flugvalla eins og skilgreint er í 2. tölul. 2. gr. tilskipunar 2009/12/EB, flugvellir eins og skilgreint er í 1. tölul. 2. gr. tilskipunar 2009/12/EB, þ.m.t. flugvellir í grunnneti sem skráðir eru í 2. þætti II. viðauka reglugerðar (ESB) nr. 1315/2013 og einingar sem starfrækja viðbúnað sem staðsettur er innan flugvalla, kerfisstjórar umferðarstjórnunar sem veita flugstjórnarþjónustu (ATC) eins og skilgreint er í 1. tölul. 2. gr. reglugerðar (EB) nr. 549/2004. Flutningar á sjó og vatnaleiðum; fyrirtæki sem sjá um vatna-, millilanda- og strandsiglingar með farþega og vöruflutninga á sjó og vatnaleiðum eins og skilgreint er fyrir flutninga á sjó í I. viðauka reglugerðar (EB) nr. 725/2004 að frátöldum einstökum skipum sem þau fyrirtæki gera út, stjórnir hafna eins og hafnir eru skilgreindar í 1. tölul. 3. gr. tilskipunar 2005/65/EB,

þ.m.t. hafnaraðstöður þeirra eins og skilgreint er í 11. tölul. 2. gr. reglugerðar (EB) nr. 725/2004 og einingar sem annast mannvirki og búnað sem staðsett eru innan hafna og rekstraraðilar skipaumferðarþjónustu eins og skilgreint er í o-lið 3. gr. reglugerðar nr. 80/2013, um vaktstöð siglinga og eftirlit með umferð skipa, sem innleiðir tilskipun 2002/59/EB. Flutningar á vegum; þ.e. vegamálayfirvöld sem bera ábyrgð á skipulagningu, eftirliti með eða rekstri vega sem falla undir lögsögu þeirra samkvæmt vegalögum og rekstraraðilar skynvæddra flutningakerfa, þ.e. rekstraraðilar kerfa þar sem upplýsinga- og fjarskiptatækni er beitt á sviði flutninga á vegum, þ.m.t. grunnvirki, ökutæki og notendur, og á sviði umferðarstjórnunar og hreyfanleikastjórnunar og á sviði tenginga við aðra flutningsmáta.

6. *Forskrift:* Tækniforskrift í skilningi 4. tölul. 2. gr. reglugerðar (ESB) nr. 1025/2012.
7. *Heilbrigðisþjónusta:* Veitendur heilbrigðisþjónustu samkvæmt skilgreiningu í lögum um heilbrigðisþjónustu og g-lið 3. gr. tilskipunar 2011/24/ESB.
8. *Hitaveitur:* Hitaveitur samkvæmt orkulögum.
9. *Innviðir fjármálamarkaða:* Rekstraraðilar skipulegra verðbréfamarkaða og markaðstorgs fjármálagerninga samkvæmt skilgreiningu laga um verðbréfaviðskipti og miðlægir mótaðilar samkvæmt skilgreiningu reglugerðar (ESB) nr. 648/2012, sem lögfest er með lögum um afleiðuviðskipti, miðlæga mótaðila og afleiðuviðskiptaskrár.
10. *Leitarvél á netinu:* Stafræn þjónusta sem leyfir notendum að framkvæma leit, að meginreglu til, að öllum vefjum eða vefjum á tilteknu tungumáli á grundvelli fyrirspurnar um viðfangsefni í formi leitarorðs, orðasambands eða annars konar gagna sem færð eru inn í tölvu. Þjónustan skilar tenglum þar sem finna má upplýsingar um efnið sem óskað er eftir.
11. *Lénsheitakerfi:* Stigskipt dreift gagnasafn í netkerfi sem annast fyrirspurnir um lénsheiti.
12. *Meðhöndlun atvika:* Allt það verklag sem styður við að koma upp um, greina og afmarka atvik og viðbrögð við þeim.
13. *Mikilvægir innviðir:* Rekstraraðilar nauðsynlegrar þjónustu og veitendur stafrænnar þjónustu eins og þeir eru skilgreindir í lögum þessum.
14. *Netmarkaður:* Stafræn þjónusta sem leyfir neytendum og/eða seljendum, eins og þeir eru skilgreindir í a- og b-lið 1. mgr. 4. gr. tilskipunar 2013/11/ESB, að gera sölu- og þjónustusamninga á netinu við seljendur, annaðhvort á vef netmarkaðar eða á vef seljanda sem notar þjónustu á sviði gagnaumferðar í gegnum netmarkaðinn.
15. *Net- og upplýsingakerfi:* Fjarskiptanet í skilningi laga um fjarskipti; tæki eða samsafn innbyrðis tengdra eða skyldra tækja þar sem í einu þeirra eða fleiri fer fram sjálfvirk stafræn gagnavinnsla eftir forriti; eða stafræn gögn sem eru geymd, unnin, sótt eða send fyrir tilstilli þátta sem falla undir framangreint að því er varðar starfrækslu þeirra, notkun, verndun og viðhald.
16. *Orkuveitur:* Rafmagn; raforkufyrirtæki eins og skilgreint er í 35. tölul. 2. gr. tilskipunar 2009/72/EB sem sinna hlutverki afhendingar eins og skilgreint er í 19. tölul. 2. gr. tilskipunarinnar, dreifikerfisstjórar eins og skilgreint er í 6. tölul. 2. gr. tilskipunar 2009/72/EB og flutningakerfisstjórar eins og skilgreint er í 4. tölul. 2. gr. tilskipunar 2009/72/EB. Olía; rekstraraðilar flutningsleiðslna fyrir olíu og rekstraraðilar olíuframleiðslu, olíuhreinsunar- og meðhöndlunarstöðva, olíugeymslu og olíuflutnings. Gas; afhendingarfyrirtæki eins og skilgreint er í 8. tölul. 2. gr. tilskipunar 2009/73/EB, dreifikerfisstjórar eins og skilgreint er í 6. tölul. 2. gr. tilskipunar 2009/73/EB, flutningakerfisstjórar eins og skilgreint er í 4. tölul. 2. gr. tilskipunar 2009/73/EB, geymslukerfisstjórar eins og skilgreint er í 10. tölul. 2. gr. tilskipunar 2009/73/EB, kerfisstjórar með fljótandi

jarðgas eins og skilgreint er í 12. tölul. 2. gr. tilskipunar 2009/73/EB, jarðgasfyrirtæki eins og skilgreint er í 1. tölul. 2. gr. tilskipunar 2009/73/EB og kerfisstjórar hreinsunar- og meðhöndlunarstöðva fyrir jarðgas.

17. *Rekstraraðili nauðsynlegrar þjónustu:* Opinber aðili eða einkaaðili sem veitir þjónustu sem telst nauðsynleg skv. 3. gr. á sviði bankastarfsemi, innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.
18. *Samhæfingarstjórnvald:* Stjórnvald sem gegnir samhæfingarhlutverki við eftirlit með framkvæmd laga þessara, sbr. 13. gr.
19. *Skráningarstofa höfuðléna:* Aðili sem annast og vinnur að skráningu lénsheita á netinu undir sérstöku höfuðléni.
20. *Skýjavinnsluþjónusta:* Stafræn þjónusta sem veitir aðgang að skalanlegum og sveigjanlegum brunni tölvunargetu sem hægt er að deila.
21. *Spillikóði:* Sérhver kóði, þ.e. runa skipana og/eða gagna, sem er ætlaður til að leiða til óæskilegra áhrifa, öryggisrofs eða skemmda á net- og upplýsingakerfum.
22. *Staðall:* Staðall í skilningi 1. tölul. 2. gr. reglugerðar (ESB) nr. 1025/2012.
23. *Stafræn grunnvirki:* Tengi- og skiptipunktar, þjónustuveitendur lénsheitakerfis og skráningarstofur höfuðléna.
24. *Stafræn þjónusta:* Þjónusta í skilningi b-liðar 1. mgr. 1. gr. tilskipunar 2015/1535/ESB sem fellur undir skilgreiningu laga þessara á hugtökunum netmarkaður, leitarvél á netinu eða skýjavinnsluþjónusta.
25. *Tengi- og skiptipunktur:* Netvirki sem gerir kleift að samtengja fleiri en tvö sjálfstæð og sjálfstýrð kerfi, fyrst og fremst í þeim tilgangi að greiða fyrir miðlun netumferðar. Tengi- og skiptipunkturinn veitir einungis samtengingu fyrir sjálfstýrð kerfi og gerir ekki kröfu um að netumferð sem fer á milli tveggja hlutaðeigandi sjálfstýrðra kerfa fari í gegnum þriðja sjálfstýrða kerfið, né breytir hún eða truflar slíka umferð.
26. *Vatnsveitur:* Birgjar og dreifingaraðilar neysluvatns, eins og skilgreint er í a-lið 1. tölul. 2. gr. tilskipunar 98/83/EB um gæði neysluvatns. Á ekki við þegar dreifing neysluvatns er einungis hluti af almennri starfsemi þeirra sem felur í sér dreifingu annarra verslunarvara og varnings sem telst ekki vera nauðsynleg þjónusta.
27. *Veitandi stafrænnar þjónustu:* Sérhver lögaðili með höfuðstöðvar, þ.e. aðalskrifstofu eða staðfestu, hérlendis sem veitir stafræna þjónustu í skilningi laga þessara eða fulltrúi hans með staðfestu hérlendis.
28. *Þjónustuveitandi lénsheitakerfis:* Aðili sem veitir þjónustu fyrir lénsheitakerfi á netinu.
29. *Öryggi net- og upplýsingakerfa:* Geta net- og upplýsingakerfis til að standast, með tilteknu öryggisstigi, hvers konar aðgerðir sem stofna í hættu aðgengi að sannvottuðum uppruna, réttleika eða trúnaði um vistuð, send eða unnin gögn eða tengda þjónustu sem boðin er eða er aðgengileg um þessi net- og upplýsingakerfi.

II. KAFLI
Öryggiskröfur og tilkynningarskylda.

7. gr.
Lágmarkskröfur um áhættustýringu og viðbúnað.

Mikilvægir innviðir skulu hafa skjalfesta stefnu og ferla til að meta, stýra og lágmarka áhættu sem steðjað getur að öryggi net- og upplýsingakerfa þeirra, þ.m.t. vegna fátíðra atburða sem geta haft alvarlegar afleiðingar. Þeir skulu setja sér öryggisstefnu, framkvæma áhættumat reglubundið og ákvarða og endurmeta öryggisráðstafanir á grundvelli þess. Með öryggisráðstöfunum er átt við bæði tæknilegar og skipulagslegar ráðstafanir, eftir því sem

við kann að eiga. 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 á hverjum tíma.

Mikilvægir innviðir skulu hafa skjalfesta viðbragðsáætlun og áætlun um samfelldan og órofinn rekstur og þjónustu til að tryggja takmörkun á tjóni ef alvarleg röskun verður á starfsemi þeirra. Verkferlum og viðbrögðum við atvikum í eða tengdum rekstri net- og upplýsingakerfa mikilvægra innviða skulu gerð skil í áætlunum, þar á meðal skráningu atvika. Meðhöndlun atvika skal m.a. fela í sér að finna orsakir þeirra, koma aftur á eðlilegu rekstrarástandi og koma í veg fyrir að atvik endurtaki sig.

Í starfsemi mikilvægra innviða skal vera til staðar virkt kerfi innra eftirlits sem samræmist lögum þessum og sérlögum sem um starfsemi þeirra kunna að gilda.

Ráðherra getur sett nánari fyrirmæli í reglugerð um lágmarkskröfur samkvæmt ákvæði þessu að fenginni umsögn eftirlitsstjórnvalda og Póst- og fjarskiptastofnunar, m.a. um lágmarksöryggisráðstafanir, innra eftirlit, raunlæga vernd net- og upplýsingakerfa og framfylgni alþjóðlega viðurkenndra forskrifta, staðla eða viðmiða um bestu framkvæmd. Heimilt er að gera greinarmun á kröfum til rekstraraðila nauðsynlegrar þjónustu og veitenda stafrænnar þjónustu í reglugerð samkvæmt ákvæði þessu.

8. gr.

Tilkynning til netöryggissveitar.

Mikilvægir innviðir skulu tilkynna netöryggissveit Póst- og fjarskiptastofnunar skv. IV. kafla svo fljótt sem verða má um alvarleg atvik eða áhættu sem ógnar öryggi net- og upplýsingakerfa þeirra.

Við mat á alvarleika atviks eða áhættu skv. 1. mgr. skal einkum horft til:

a. fjölda notenda þjónustunnar sem atvik hefur áhrif á,
b. hversu lengi atvik stendur yfir,
c. landfræðilegrar útbreiðslu og umfangs áhrifa atviks og
d. mögulegra áhrifa atviks á aðra mikilvæga innviði eða efnahagslega og samfélagslega starfsemi eða stafræna þjónustu.

Í tilkynningu skal m.a. upplýst um mögulegt útvistunarfyrirkomulag, svo sem ef mikilvægir innviðir reiða sig á þjónustu veitanda stafrænnar þjónustu í rekstri sínum, og hugsanleg smitáhrif, jafnvel yfir landamæri. Umfang tilkynningar ræðst að öðru leyti af efni og aðstæðum.

Ráðherra getur sett nánari fyrirmæli í reglugerð um tilkynningar atvika til netöryggissveitar, þar á meðal um form, efni og meðferð þeirra.

9. gr.

Miðlun upplýsinga um atvik til eftirlitsstjórnvalds og lögreglu.

Netöryggissveit skal tryggja að upplýsingar um atvik skv. 8. gr. séu aðgengilegar eftirlitsstjórnvöldum án tafar.

Netöryggissveit skal án tafar hvetja mikilvæga innviði til að tilkynna um atvik til lögreglu leiki grunur á um refsiverða háttsemi.

10. gr.

Upplýsingar veittar almenningi.

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 mikilvæga innviði í aðdraganda upplýsingagjafar skv. 1. málsl., enda verði því við komið.

Póst- og fjarskiptastofnun er heimilt að tilkynna almenningi um veikleika og almennar hættur ef það er nauðsynlegt í þágu almannahagsmuna. Samráð skal viðhaft um slíkar tilkynningar við lögreglu og eftirlitsstjórnvöld ef við verður komið.

Þrátt fyrir 1. og 2. mgr. fer um meðferð trúnaðarupplýsinga samkvæmt ákvæðum laga þessara og annarra laga, eftir því sem við á.

III. KAFLI
Eftirlit með mikilvægum innviðum.

11. gr.
Eftirlitsstjórnvöld.

Eftirlit með framkvæmd ákvæða laga þessara um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu er í höndum eftirfarandi eftirlitsstjórnvalda:

a. Orkustofnunar vegna orku- og hitaveitna,
b. Samgöngustofu vegna flutninga,
c. Fjármálaeftirlitsins vegna bankastarfsemi og innviða fjármálamarkaða,
d. embættis landlæknis vegna heilbrigðisþjónustu,
e. Umhverfisstofnunar vegna vatnsveitna og
f. Póst- og fjarskiptastofnunar vegna stafrænna grunnvirkja.

Eftirlitsstjórnvald ákveður hvaða aðilar teljast til rekstraraðila nauðsynlegrar þjónustu á sínu sviði skv. 3. gr. og miðlar tilkynningu þar um til Póst- og fjarskiptastofnunar eftir því sem tilefni er til og a.m.k. á tveggja ára fresti. Ef aðili veitir jafnframt þjónustu í öðru ríki á Evrópska efnahagssvæðinu skal eftirlitsstjórnvald, við ákvörðun skv. 1. málsl., viðhafa samráð við þarlend stjórnvöld. Áður en ákvörðun er tekin skv. 1. málsl. skal eftirlitsstjórnvald gefa aðila kost á að tjá sig um málið.

Póst- og fjarskiptastofnun hefur eftirlit með framkvæmd laga þessara um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu.

12. gr.
Eftirlitsheimildir.

Rekstraraðili nauðsynlegrar þjónustu skal að beiðni eftirlitsstjórnvalds skv. 11. gr. afhenda allar upplýsingar og gögn um skipulag net- og upplýsingaöryggis sem að mati eftirlitsstjórnvaldsins eru nauðsynleg vegna framkvæmdar eftirlits, til að mynda öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum, viðbragðsáætlun, skýrslur um innra eftirlit og niðurstöður öryggisúttekta og prófana. Eftirlitsstjórnvald getur kallað til skýrslugjafar einstaklinga sem það telur búa yfir upplýsingum um tiltekið mál.

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.

Ákvæði 1. mgr. gildir um veitendur stafrænnar þjónustu, að fenginni beiðni frá Póst- og fjarskiptastofnun, þegar stofnunin telur á grundvelli rökstuddra grunsemda að hlutaðeigandi uppfylli ekki kröfur skv. 7. og 8. gr.

Eftirlitsstjórnvaldi skv. 11. gr. er heimilt að óska eftir reglubundinni skýrslugjöf af hálfu mikilvægra innviða um meðhöndlun atvika, í því skyni að leggja mat á umgjörð áhættustýringar og viðbúnað andspænis kröfum laga þessara.

Komi í ljós að mikilvægir innviðir fylgi ekki lögum þessum eða öðrum reglum sem um net- og upplýsingakerfi þeirra gilda skal eftirlitsstjórnvald krefjast þess að úr sé bætt innan hæfilegs frests, svo sem um tilteknar lágmarksöryggisráðstafanir. Vanræki mikilvægir innviðir að fara að fyrirmælum eftirlitsstjórnvalds um úrbætur getur eftirlitsstjórnvald látið vinna verkið á kostnað hlutaðeigandi. Krafa um kostnað vegna þessa er aðfararhæf skv. 5. tölul. 1. mgr. 1. gr. laga um aðför, nr. 90/1989.

13. gr.

Samhæfingarstjórnvald.

Póst- og fjarskiptastofnun skal gegna ráðgefandi samhæfingarhlutverki gagnvart eftirlitsstjórnvöldum í því skyni að stuðla að samræmdri framkvæmd laga þessara.

Póst- og fjarskiptastofnun er jafnframt tengiliður stjórnvalda hér á landi vegna eftirlits með net- og upplýsingaöryggi mikilvægra innviða og framkvæmd tilskipunar (ESB) 2016/1148 um ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan Evrópska efnahagssvæðisins.

Ráðherra getur sett nánari fyrirmæli í reglugerð um hlutverk samhæfingarstjórnvalds samkvæmt ákvæði þessu, að viðhöfðu samráði við eftirlitsstjórnvöld.

IV. KAFLI
Þjónusta og samstarf við netöryggissveit.

14. gr.

Netöryggissveit.

Póst- og fjarskiptastofnun starfrækir lögum samkvæmt netöryggissveit sem gegnir hlutverki landsbundins öryggis- og viðbragðsteymis vegna atvika og áhættu er varðar net- og upplýsingaöryggi hér á landi, CSIRT-teymi fyrir Ísland.

Netöryggissveit skal bregðast við tilkynningum um atvik skv. 8. og 15. gr. með því að veita viðeigandi upplýsingar eða ráðgjöf um viðbrögð og aðgerðir, eftir því sem tilefni og nauðsyn ber til, í því skyni að styðja við skilvirka meðhöndlun atviks.

Netöryggissveit er heimilt að tilkynna ríkislögreglustjóra um alvarleg eða útbreidd atvik og áhættu sem ógnar net- og upplýsingaöryggi og skal, eftir því sem við kann að eiga, viðhafa samstarf við embættið um varnir og viðbrögð.

Í meðhöndlun atvika skal netöryggissveit leitast við að fyrirbyggja að atvik breiðist út og valdi tjóni, eftir atvikum í samstarfi við ríkislögreglustjóra. Ef tilefni er til gefur netöryggissveit Póst- og fjarskiptastofnunar út tilmæli til mikilvægra innviða um aðgerðir vegna atviks eða gegn bráðri aðsteðjandi netógn, hvort sem það atvik eða sú ógn steðjar að einum eða fleiri mikilvægum innviðum eða mikilvægum innviðum á einu eða fleiri sviðum. Verði mikilvægir innviðir ekki við tilmælum netöryggissveitar Póst- og fjarskiptastofnunar um viðbrögð eða aðgerðir við atviki eða áhættu, á þeim forsendum að mat hlutaðeigandi sé að aðrar ráðstafanir eigi betur við í því skyni að tryggja vernd net- og upplýsingakerfa þeirra, skal netöryggissveit og hlutaðeigandi eftirlitsstjórnvald upplýst um ástæður þeirrar afstöðu. Í öllum tilvikum skal tilmælum netöryggissveitarinnar svarað eins fljótt og kostur er. Um upplýsingagjöf til almennings fer skv. 10. gr.

Ef áhrifa atviks sem netöryggissveit berst tilkynning um gætir yfir landamæri skal netöryggissveitin miðla tilkynningu þar um til útnefndra tengiliða í viðkomandi ríki.

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.

15. gr.

Tilkynningar um atvik og viðbrögð við þeim.

Netöryggissveit skal gera öðrum en mikilvægum innviðum kleift að miðla til sín tilkynningum um atvik í net- og upplýsingakerfum sem hafa umtalsverð áhrif á starfsemi þeirra.

Um tilkynningar skv. 1. mgr. og viðbrögð við þeim fer skv. 8. og 14. gr. eftir því sem við á.

Ef þörf krefur er netöryggissveit heimilt að forgangsraða í starfsemi sinni þannig að brugðist sé við tilkynningum um atvik frá mikilvægum innviðum og opinberum stofnunum áður en tilkynningum frá öðrum er sinnt.

Ráðherra getur sett nánari fyrirmæli í reglugerð um tilkynningar til netöryggissveitar samkvæmt ákvæði þessu.

16. gr.

Þjónusta við mikilvæga innviði og opinberar stofnanir.

Mikilvægir innviðir geta leitað til netöryggissveitar um aðstoð og leiðbeiningar um sérhæfðar forvarnir í tengslum við öryggi net- og upplýsingakerfa sinna, en hlutverk sveitarinnar er einkum að styðja við skjót viðbrögð gegn aðsteðjandi hættu.

Netöryggissveit er heimilt að bjóða mikilvægum innviðum og opinberum stofnunum tæknilega vöktunarþjónustu, á nánar skilgreindum og skjalfestum forsendum, í því skyni að greina ummerki um árásir, spillikóða og aðrar hættulegar aðstæður. Vöktunarþjónustan getur verið hluti af tæknilegum öryggisráðstöfunum og áhættustýringu mikilvægra innviða og opinberra stofnana. Endurgjald vegna vöktunarþjónustu skal taka mið af útlögðum kostnaði netöryggissveitar vegna búnaðar sem staðsettur verður við eigin net- og upplýsingakerfi hlutaðeigandi rekstraraðila.

Stjórnarráð Íslands skal njóta þjónustu Póst- og fjarskiptastofnunar á sviði netöryggismála skv. 1. og 2. mgr., án sérstaks endurgjalds. Aðrar opinberar stofnanir geta gert samninga við Póst- og fjarskiptastofnun um aðstoð og ráðgjöf skv. 1. mgr. gegn endurgjaldi. Póst- og fjarskiptastofnun skal vekja athygli opinberra stofnana á ákvæðum þessara laga um tilkynningar um atvik og viðbrögð við þeim.

Ráðherra getur sett nánari fyrirmæli í reglugerð um starfsemi netöryggissveitar samkvæmt ákvæði þessu, þar á meðal gjaldtöku.

17. gr.

Aðgangur netöryggissveitar að upplýsingum.

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, þ.m.t. umferðarskrám 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 að 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.

Netöryggissveit skal fylgja skjalfestum vinnureglum um öflun upplýsinga og gera viðeigandi ráðstafanir til að tryggja öryggi og eyðingu gagna, svo og aðrar ráðstafanir sem nauðsynlegar eru til að tryggja friðhelgi einkalífs og öryggis- og viðskiptahagsmuni aðila.

18. gr.

Samstarf.

Netöryggissveit er heimilt að setja á fót þverfaglegan samráðshóp í þeim tilgangi að efla tengsl og samstarf á milli mikilvægra innviða og sveitarinnar.

Netöryggissveit er jafnframt heimilt að setja á fót sviðshópa til samráðs fyrir hvert svið nauðsynlegrar þjónustu skv. 1. mgr. 2. gr., fyrir hverja tegund veitenda stafrænnar þjónustu og opinberar stofnanir. Sviðshópar skulu vera vettvangur tæknilegs samráðs og upplýsingaskipta á sviði net- og upplýsingaöryggis er hefur það að meginmarkmiði að greina ógnir og áhættu, stuðla að auknu net- og upplýsingaöryggi og takmarka tjón af völdum netárása.

Samráðs- og sviðshópar skv. 1. og 2. mgr. skulu setja sér starfsreglur og er aðilum að samstarfinu einungis heimilt að skiptast á upplýsingum sem skipta máli fyrir net- og upplýsingaöryggi. Í starfsreglum skal m.a. gætt að reglum samkeppnislaga um upplýsingaskipti.

Trúnaður skal ríkja um upplýsingar sem ræddar eru á fundum samráðs- og sviðshópa og gögn sem þeir kunna að vinna með eða afhent eru á vettvangi þeirra skulu teljast til vinnugagna í skilningi 2. og 3. tölul. 2. mgr. 8. gr. upplýsingalaga, nr. 140/2012, og vera undanþegin aðgangsrétti almennings, sbr. 5. tölul. 6. gr. sömu laga.

Netöryggissveit getur, í því skyni að stuðla að efldum viðnámsþrótti net- og upplýsingakerfa og eftir atvikum í samstarfi við ríkislögreglustjóra og eftirlitsstjórnvöld, skipulagt viðbúnaðaræfingar með þátttöku fulltrúa mikilvægra innviða og opinberra stofnana.

V. KAFLI
Þagnarskylda.

19. gr.

Sérstök þagnarskylda.

Starfslið eftirlitsstjórnvalda, hvert á sínu sviði, samhæfingarstjórnvalds, netöryggissveitar og netöryggisráðs er bundið sérstakri þagnarskyldu umfram þá sem greinir í lögum um réttindi og skyldur starfsmanna ríkisins. Starfsliðið má ekki, að viðlagðri ábyrgð, skýra óviðkomandi frá því sem það kemst að í starfi sínu og leynt á að fara. Þagnarskyldan helst þótt látið sé af starfi.

Starfsmenn netöryggissveitar Póst- og fjarskiptastofnunar eru bundnir þagnarskyldu um þau gögn og upplýsingar sem netöryggissveitin hefur undir höndum, hefur aðgang að eða vinnur með og sem þeir fá vitneskju um í starfi.

20. gr.

Undanþágur frá þagnarskyldu.

Ákvæði laga þessara um þagnarskyldu standa ekki í vegi fyrir að eftirlitsstjórnvöld, hvert á sínu sviði, samhæfingarstjórnvald, netöryggissveit og netöryggisráð veiti upplýsingar eða

taki við upplýsingum hver frá öðrum eða frá lögreglu- eða persónuverndaryfirvöldum, ef þær upplýsingar varða framkvæmd þessara laga, almannavarnir eða persónuvernd.

Ákvæði laga þessara um þagnarskyldu hindra ekki að eftirlitsstjórnvöld hvert á sínu sviði, samhæfingarstjórnvald, netöryggissveit eða netöryggisráð veiti upplýsingar eða taki við upplýsingum frá erlendum stjórnvöldum, eftirlitsaðilum eða öðrum aðilum eða sérfræðingum sem sinna net- og upplýsingaöryggi þegar slíkt er nauðsynlegt vegna skipulagðrar alþjóðasamvinnu sem hefur það markmið að stuðla að eða framkvæma aðgerðir til að tryggja öryggi net- og upplýsingakerfa.

Við upplýsingaskipti skv. 1. og 2. mgr. skal gæta trúnaðar um öryggis- og viðskiptahagsmuni mikilvægra innviða og sérstök þagnarskylda skv. 19. gr. skal ríkja um þær upplýsingar sem veittar eru eða tekið er á móti skv. 1. og 2. mgr.

Um trúnað upplýsinga frá Atlantshafsbandalaginu, öryggisdeild aðalskrifstofu ráðs Evrópusambandsins (GSCSO) og sambærilegum erlendum öryggisstofnunum fer skv. 2. mgr. 24. gr. varnarmálalaga, nr. 34/2008.

21. gr.

Vinnsla persónuupplýsinga.

Netöryggissveit er heimil vinnsla persónuupplýsinga að því marki sem nauðsynlegt er til að hún geti sinnt hlutverki sínu samkvæmt lögum þessum. Í því felst m.a. móttaka persónuupplýsinga frá aðilum sem ákvæði laga þessara gilda um og frá innlendum og erlendum samstarfsaðilum, sem og miðlun þeirra til viðeigandi þriðju aðila, án samþykkis hins skráða, ef netöryggissveit metur það nauðsynlegt í þágu þjóðaröryggis eða almannahagsmuna og vinnslan er til þess fallin að upplýsa um aðsteðjandi ógnir, koma í veg fyrir netárás eða önnur alvarleg atvik eða til að takmarka útbreiðslu eða draga úr tjóni vegna slíkra tilvika. Ef rökstuddur grunur er um að einstakar sendingar innihaldi spillikóða er netöryggissveit heimilt, með samþykki mikilvægra innviða og án samþykkis hins skráða, að greina efni einstakra fjarskiptasendinga til og frá neti mikilvægra innviða.

Netöryggissveit er heimil vinnsla persónuupplýsinga og viðkvæmra persónuupplýsinga sem henni berast, til að mynda vegna atvika. Sveitinni er einnig heimilt að miðla þeim upplýsingum til viðeigandi þriðju aðila, án samþykkis hins skráða, ef hún metur það nauðsynlegt í þágu almannahagsmuna eða í þágu hagsmuna hins skráða til að koma í veg fyrir eða takmarka mögulegt tjón sem viðkomandi getur orðið fyrir.

Öll vinnsla persónuupplýsinga á grundvelli laga þessara skal vera í samræmi við ákvæði laga um persónuvernd og vinnslu persónuupplýsinga, nr. 90/2018, og reglna settra á grundvelli þeirra. Ákvæði 17. og 20.–22. gr. laga nr. 90/2018, sbr. 12.–22. og 34. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB, gilda þó ekki um starfsemi netöryggissveitar samkvæmt lögum þessum.

Ráðherra skal í reglugerð, að viðhöfðu samráði við Póst- og fjarskiptastofnun og að fengnu áliti Persónuverndar, kveða á um forsendur vinnslu persónuupplýsinga hjá netöryggissveit, meðferð þeirra og eyðingu, rétt skráðra einstaklinga og takmörkun á rétti þeirra. Í reglugerðinni skal a.m.k. fjalla um tilgang vinnslu, tegundir persónuupplýsinga, meðferð, geymslu og eyðingu persónuupplýsinga og verndarráðstafanir til að koma í veg fyrir misnotkun eða ólögmætan aðgang eða miðlun og, eftir því sem við á, mat á áhrifum á persónuvernd.

VI. KAFLI
Viðurlög og önnur ákvæði.

22. gr.
Dagsektir.

Ef ekki er farið að fyrirmælum eftirlitsstjórnvalds eða orðið við ósk um afhendingu upplýsinga og gagna skv. 12. gr. er heimilt að leggja dagsektir á þá mikilvægu innviði sem fyrirmæli eða ósk beinist að og þar til úr verður bætt að mati eftirlitsstjórnvaldsins. Sektir geta numið allt að 500.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælunum sé fylgt eða gögn afhent.

Ef ákvörðun um dagsektir skv. 1. mgr. er skotið til dómstóla byrja dagsektir ekki að falla á fyrr en dómur er endanlegur. Dagsektir renna í ríkissjóð og má gera aðför til fullnustu þeirra án undangengins dóms eða sáttar.

23. gr.
Stjórnvaldssektir.

Eftirlitsstjórnvald skv. 11. gr. getur lagt stjórnvaldssektir á einstakling eða lögaðila sem brýtur gegn eftirtöldum ákvæðum laga þessara og reglum settum á grundvelli þeirra:

1. 7. gr. um lágmarkskröfur um áhættustýringu og viðbúnað.
2. 8. gr. um tilkynningu til netöryggissveitar.
3. 19. gr. um sérstaka þagnarskyldu.

Stjórnvaldssektir geta numið frá 10.000 kr. til 10.000.000 kr. Sektin skal þó ekki vera hærri en sem nemur 3% af veltu síðasta almanaksárs ef um lögaðila er að ræða.

Við ákvörðun um fjárhæð stjórnvaldssektar samkvæmt ákvæði þessu skal eftirlitsstjórnvald taka tillit til allra atvika sem máli skipta, þ.m.t. hafa hliðsjón af alvarleika brots, hversu lengi það hefur staðið og hvort um ítrekað brot sé að ræða. Líta skal til þess hvort ætla megi að brotið hafi verið framið í þágu hagsmuna hlutaðeigandi og hvort brot hafi leitt til tjóns eða áhættu fyrir þriðja aðila.

Ákvarðaðar stjórnvaldssektir eru aðfararhæfar og renna í ríkissjóð að frádregnum kostnaði við innheimtuna. Sé stjórnvaldssekt ekki greidd innan mánaðar frá ákvörðun eftirlitsstjórnvalds skv. 11. gr. skal greiða dráttarvexti af fjárhæð sektarinnar. Um ákvörðun og útreikning dráttarvaxta fer eftir lögum um vexti og verðtryggingu.

Stjórnvaldssektum verður beitt óháð því hvort lögbrot eru framin af ásetningi eða gáleysi.

Ákvörðun eftirlitsstjórnvalds skv. 11. gr. er endanleg á stjórnsýslustigi. Aðili máls getur skotið ákvörðun um stjórnvaldssekt til dómstóla og er málshöfðunarfrestur þrír mánuðir frá því að ákvörðun var tekin. Málskot frestar aðför.

24. gr.
Réttur manna til að fella ekki á sig sök.

Í máli sem beinist að einstaklingi og lokið getur með álagningu stjórnvaldssekta eða kæru til lögreglu hefur sá sem rökstuddur grunur leikur á að hafi gerst sekur um lögbrot rétt til að neita að svara spurningum eða afhenda gögn eða muni nema hægt sé að útiloka að það geti haft þýðingu fyrir ákvörðun um brot hans. Eftirlitsstjórnvald skv. 11. gr. skal leiðbeina hinum grunaða um þennan rétt.

25. gr.

Kæra til lögreglu.

Eftirlitsstofnun er heimilt að kæra brot á lögum þessum og reglugerðum sem settar eru á grundvelli þeirra til lögreglu.

Varði meint brot á lögum þessum bæði stjórnvaldssektum og refsingu metur eftirlitsstjórnvald hvort mál skuli kært til lögreglu eða því lokið með stjórnvaldsákvörðun hjá stofnuninni. Ef brot eru meiri háttar ber eftirlitsstjórnvaldi að vísa þeim til lögreglu. Brot telst meiri háttar ef það lýtur að verulegum fjárhæðum, ef verknaður er framinn með sérstaklega vítaverðum hætti eða við aðstæður sem auka mjög á saknæmi brotsins. Jafnframt getur eftirlitsstjórnvald á hvaða stigi rannsóknar sem er vísað máli vegna brota á lögum þessum til rannsóknar lögreglu. Gæta skal samræmis við úrlausn sambærilegra mála.

Með kæru eftirlitsstjórnvalds skulu fylgja afrit þeirra gagna sem grunur um brot er studdur við. Ákvæði IV.–VII. kafla stjórnsýslulaga gilda ekki um ákvörðun eftirlitsstjórnvalds um að kæra mál til lögreglu.

Eftirlitsstjórnvaldi er heimilt að láta lögreglu og ákæruvaldi í té upplýsingar og gögn sem stofnunin hefur aflað og tengjast þeim brotum sem tilgreind eru í 2. mgr. Eftirlitsstjórnvaldi er heimilt að taka þátt í aðgerðum lögreglu sem varða rannsókn þeirra brota sem tilgreind eru í 2. mgr.

Lögreglu og ákæruvaldi er heimilt að láta eftirlitsstjórnvaldi í té upplýsingar og gögn sem hún hefur aflað og tengjast þeim brotum sem tilgreind eru í 2. mgr. Lögreglu er heimilt að taka þátt í aðgerðum eftirlitsstjórnvalds sem varða rannsókn þeirra brota sem tilgreind eru í 2. mgr.

Telji ákærandi að ekki séu efni til málshöfðunar vegna ætlaðrar refsiverðrar háttsemi sem jafnframt varðar stjórnsýsluviðurlögum getur hann sent eða endursent málið til eftirlitsstjórnvalds til meðferðar og ákvörðunar.

26. gr.

Refsingar.

Brot sem framið er af ásetningi á ákvæðum 7., 8. og 19. gr. og reglugerða settra samkvæmt þeim varðar fangelsi allt að tveimur árum nema þyngri refsing liggi við samkvæmt öðrum lögum.

Nú er brot skv. 1. mgr. framið í starfsemi lögaðila og má þá gera lögaðilanum fésekt skv. II. kafla A almennra hegningarlaga, nr. 19/1940.

Tilraun og hlutdeild í brotum skv. 1. mgr. eru refsiverð skv. III. kafla almennra hegningarlaga.

Hver sá sem uppvís er að því að gefa af ásetningi eða stórkostlegu gáleysi ranga tilkynningu til netöryggissveitar skv. 8. eða 15. gr. skal sæta refsingu skv. 120. gr. og 120. gr. a almennra hegningarlaga.

27. gr.

Bótaábyrgð.

Tilkynning um atvik til netöryggissveitar samkvæmt lögum þessum skal ekki hafa áhrif á eða auka mögulega bótaskyldu vegna atviksins.

VII. KAFLI
Gildistaka o.fl.

28. gr.
Reglugerðarheimild.

Ráðherra er heimilt að setja reglugerð um nánari framkvæmd laga þessara.

29. gr.
Gildistaka.

Lög þessi öðlast gildi 1. september 2020.

30. gr.
Breytingar á öðrum lögum.

Við gildistöku laga þessara verða eftirfarandi breytingar á öðrum lögum:

1. *Lög um Póst- og fjarskiptastofnun, nr. 69/2003, með síðari breytingum:*
   a. 2. mgr. 1. gr. laganna orðast svo:
      Póst- og fjarskiptastofnun er sjálfstæð stofnun sem heyrir stjórnarfarslega undir ráðherra.
   b. Eftirfarandi breytingar verða á 3. gr. laganna:
      1. Í stað orðanna „fjarskiptum og póstþjónustu“ í 1. tölul. 1. mgr. kemur: fjarskiptum, póstþjónustu og öryggi net- og upplýsingakerfa.
      2. 1. málsl. 5. tölul. 1. mgr. orðast svo: Að vera ráðgefandi fyrir stjórnvöld og ráðuneyti um málefni er varða fjarskipti, póstþjónustu og öryggi net- og upplýsingakerfa og hafa eftirlit með því að Ísland uppfylli á hverjum tíma þær skuldbindingar sem mælt er fyrir um í alþjóðlegum samningum á umræddum sviðum.
      3. Við 6. tölul. 1. mgr. bætist: svo og hvað varðar öryggi net- og upplýsingakerfa.
      4. Í stað orðanna „fjarskipta- og póstmála“ í 7. tölul. 1. mgr. kemur: laga um fjarskipti, laga um póstþjónustu og laga um öryggi net- og upplýsingakerfa mikilvægra innviða.
      5. Við 1. mgr. bætist nýr töluliður, svohljóðandi: Að starfrækja netöryggissveit sem gegnir hlutverki öryggis- og viðbragðsteymis, svo sem nánar er kveðið á um í lögum þessum og öðrum lögum.
      6. Við bætist ný málsgrein, 3. mgr., svohljóðandi:
         Póst- og fjarskiptastofnun og ríkislögreglustjóri skulu hafa gagnkvæmt og virkt samstarf um net- og upplýsingaöryggi.
   c. Á eftir 4. gr. laganna kemur ný grein, 4. gr. a, ásamt fyrirsögn, svohljóðandi:
      Netöryggissveit.
      Netöryggissveit Póst- og fjarskiptastofnunar gegnir hlutverki landsbundins öryggis- og viðbragðsteymis vegna atvika og áhættu er varðar net- og upplýsingaöryggi, ógnir, hættur og atvik á netinu hér á landi, CSIRT-teymis fyrir Ísland. Netöryggissveitin gegnir hlutverki tengiliðar íslenskra stjórnvalda í alþjóðlegu samstarfi CSIRT-teyma.
      Netöryggissveit er ætlað að fyrirbyggja og draga úr hættu á netárásum og öðrum öryggisatvikum í netumdæmi Íslands eins og kostur er og sporna við og lágmarka tjón á fjarskiptamarkaði og mikilvægum innviðum í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða. Netöryggissveitin leitast við að greina ógnir og atvik á frumstigi í netumdæmi Íslands, fyrirbyggja og takmarka útbreiðslu þeirra og

tjón sem af þeim kann að hljótast. Netöryggissveit samhæfir aðgerðir aðila varðandi viðbrögð við ógnum og atvikum, í samstarfi við ríkislögreglustjóra þegar við á.

Starfslið netöryggissveitar skal uppfylla skilyrði öryggisvottunar skv. 24. gr. varnarmálalaga, nr. 34/2008. Hið sama gildir um annað starfslið sem kemur að netöryggismálum hjá Póst- og fjarskiptastofnun og því ráðuneyti sem fer með mál er varða netöryggi.

Forstjóri Póst- og fjarskiptastofnunar veitir aðgangsheimildir að starfssvæði netöryggissveitar. Takmarka má, synja um eða afturkalla aðgangsheimild af öryggisástæðum eða ef allsherjarregla krefst þess.

Þeim einum er heimill aðgangur að starfssvæði netöryggissveitar sem þangað á lögmætt erindi og hefur gilda aðgangsheimild.

Ráðherra setur, að viðhöfðu samráði við Póst- og fjarskiptastofnun og að fenginni umsögn frá Persónuvernd og ríkislögreglustjóra, eftir því sem við á, nánari fyrirmæli um starfsemi netöryggissveitar í reglugerð. Í henni skal m.a. mælt fyrir um:

a. hlutverk, skipulag og verkefni netöryggissveitar,
b. skipun og hæfi starfsmanna netöryggissveitar, þ.m.t. um öryggisvottun,
c. meðferð upplýsinga og viðeigandi öryggisráðstafanir, þar á meðal gagnvart erlendum samstarfsaðilum,
d. ráðstafanir til að tryggja öryggi og eyðingu gagna og aðrar ráðstafanir til að tryggja friðhelgi einkalífs,
e. viðbúnaðaræfingar,
f. samstarf við önnur stjórnvöld og stofnanir, og
g. skýrslugjöf um starfsemi netöryggissveitar.

d. Eftirfarandi breytingar verða á 5. gr. laganna:
   1. Við 1. mgr. bætist nýr málsliður, svohljóðandi: Um aðgang að og vinnslu upplýsinga vegna starfrækslu netöryggissveitar og um eftirlit með starfsemi stafrænna grunnvirkja og veitenda stafrænnar þjónustu fer samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða.
   2. Við 8. mgr. bætist nýr málsliður, svohljóðandi: Um kröfur Póst- og fjarskiptastofnunar um úrbætur gagnvart stafrænum grunnvirkjum og veitendum stafrænnar þjónustu fer samkvæmt lögum um öryggi net- og upplýsingakerfa mikilvægra innviða.

e. Eftirfarandi breytingar verða á 8. gr. laganna:
   1. Við 1. málsl. 4. mgr. bætist: eða verkefnum.
   2. Við bætist ný málsgrein, 5. mgr., svohljóðandi:

      Um meðferð upplýsinga og þagnarskyldu vegna hlutverks Póst- og fjarskiptastofnunar sem eftirlitsstjórnvalds og samhæfingarstjórnvalds, svo og starfrækslu netöryggissveitar, gilda jafnframt lög um öryggi net- og upplýsingakerfa mikilvægra innviða.

f. Við 15. gr. laganna bætist nýr málsliður, svohljóðandi: Enn fremur skal fjallað almennt um stöðu og þróun net- og upplýsingaöryggismála á Íslandi.

2. *Lög um fjarskipti, nr. 81/2003, með síðari breytingum:*
   a. Eftirfarandi breytingar verða á 3. gr. laganna:
      1. 20. tölul. orðast svo: *Mikilvægir innviðir:* Mikilvægir innviðir samkvæmt skilgreiningu laga um öryggi net- og upplýsingakerfa mikilvægra innviða.

2. 21. tölul. orðast svo: *Net- og upplýsingakerfi:* Net- og upplýsingakerfi samkvæmt skilgreiningu laga um öryggi net- og upplýsingakerfa mikilvægra innviða.
3. 24. tölul. fellur brott.
4. 25. tölul. orðast svo: *Netöryggissveit Póst- og fjarskiptastofnunar* eða *netöryggissveitin:* Öryggis- og viðbragðsteymi samkvæmt lögum um Póst- og fjarskiptastofnun.
5. 39. tölul. fellur brott.
6. Á eftir 41. tölul. kemur nýr töluliður, svohljóðandi: *Öryggi net- og upplýsingakerfa:* Öryggi net- og upplýsingakerfa samkvæmt skilgreiningu laga um öryggi net- og upplýsingakerfa mikilvægra innviða.
7. Við 43. tölul. bætist: og atvik í skilningi laga um öryggi net- og upplýsingakerfa mikilvægra innviða.

b. Í stað 47. gr. a laganna koma fjórar nýjar greinar, 47. gr. a – 47. gr. d, ásamt fyrirsögnum, svohljóðandi:

a. (47. gr. a.)

Öryggisatvik, viðbúnaður og hlutverk netöryggissveitar.

Fjarskiptafyrirtæki skulu tilkynna netöryggissveit án tafar um öryggisatvik eða áhættu sem ógnar net- og upplýsingakerfum þeirra. Um tilkynningar til netöryggissveitar samkvæmt ákvæði þessu fer skv. 8. og 14. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða. Netöryggissveit skal án tafar hvetja fjarskiptafyrirtæki til að tilkynna lögreglu um öryggisatvik leiki grunur á um refsiverða háttsemi.

Netöryggissveit er heimilt að tilkynna ríkislögreglustjóra um alvarleg eða útbreidd atvik og áhættu sem ógnar öryggi net- og upplýsingakerfa og skal, eftir því sem við kann að eiga, hafa samstarf við embættið um varnir og viðbrögð.

Netöryggissveit skal aðstoða fjarskiptafyrirtæki við forvarnir, leiðbeina þeim og styðja við skjót viðbrögð gegn aðsteðjandi hættu. Við útbreitt öryggisatvik samhæfir netöryggissveit aðgerðir viðeigandi aðila gegn aðsteðjandi hættu til að lágmarka tjón og reisa við óvirk kerfi.

Netöryggissveit skal greina og meðhöndla ógnir, hættur og atvik í net- og upplýsingakerfum fjarskiptafyrirtækja og fyrirbyggja og draga úr hættu á öryggisatvikum eins og kostur er og sporna við og lágmarka tjón aðila sem af slíku kann að hljótast.

Fjarskiptafyrirtækjum er skylt að bregðast án tafar við tilmælum Póst- og fjarskiptastofnunar um aðgerðir gegn bráðri aðsteðjandi netógn, hvort sem sú ógn steðjar að net- og upplýsingakerfum eins eða fleiri fjarskiptafyrirtækja. Hið sama á við í tilviki mjög alvarlegrar hættu sem steðjar að net- og upplýsingakerfum mikilvægra innviða eða opinberra stofnana, almannahagsmunum eða þjóðaröryggi, enda yfirgnæfandi líkur á að fjarskiptafyrirtæki geti átt hlutdeild í að sporna við ógn, áhættu eða atviki eða lágmarka mögulegt tjón af völdum þess.

Netöryggissveit skal leitast við að greina netógnir, áhættu og öryggisatvik á sviði fjarskipta á frumstigi og skal hún senda út snemmviðvaranir í þeim tilgangi að styðja við skjót viðbrögð gegn aðsteðjandi hættu. Skal netöryggissveit tilkynna og miðla upplýsingum til viðeigandi hagsmunaaðila um ógnir, áhættu og öryggisatvik. Netöryggissveit veitir ráðgjöf um varnir og viðbúnað og kemur upplýs-

ingum á framfæri við almenning ef þurfa þykir, eftir atvikum í samráði við önnur stjórnvöld.

Netöryggissveit skal setja á laggirnar samstarfshóp með fjarskiptafyrirtækjum fyrir tæknilegt samráð og upplýsingaskipti á sviði net- og upplýsingaöryggis, m.a. til að greina ógnir og samræma viðbrögð.

b. (47. gr. b.)

Samningar netöryggissveitar og fjarskiptafyrirtækja.

Ef Póst- og fjarskiptastofnun metur það nauðsynlegt skulu fjarskiptafyrirtæki og netöryggissveit gera með sér samning um uppsetningu og rekstur tæknilegrar vöktunarþjónustu fyrir net- og upplýsingakerfi fjarskiptafyrirtækisins í þeim tilgangi að greina hættur og ummerki um árásir, spillikóða og aðrar vísbendingar um aðstæður sem gætu skapað hættu fyrir öryggi net- og upplýsingakerfa fjarskiptafyrirtækja.

Samningar skv. 1. mgr. skulu a.m.k. innihalda ákvæði er varða:

a. búnað og netkerfi sem tengist vöktun netöryggissveitar,
b. tæknilegar lausnir sem beitt er við vöktun,
c. tegund og vinnslu þeirra gagna, þ.m.t. persónuupplýsinga, sem safnað er, meðferð þeirra, vistun og eyðingu.

Fjarskiptafyrirtækjum er skylt að hýsa og samtengjast þeim búnaði netöryggissveitar sem Póst- og fjarskiptastofnun metur nauðsynlegan skv. 1. mgr. vegna tæknilegrar vöktunarþjónustu endurgjaldslaust. Netöryggissveit er heimilt að móttaka upplýsingar á grundvelli samnings um vöktunarþjónustu án dómsúrskurðar.

Hvorki er heimilt að persónugreina netumferð né skima einstaka netpakka eða flæði sem netöryggissveitin kann að nema í almennum netkerfum fjarskiptafyrirtækja. Netöryggissveit er þó heimilt að móttaka upplýsingar um almenna netumferð án dómsúrskurðar, þ.m.t. á samtengipunktum og í útlandagáttum, enda séu þær upplýsingar ópersónugreinanlegar.

c. (47. gr. c.)

Aðgangur að upplýsingum, þagnarskylda og vinnsla persónuupplýsinga.

Um aðgang netöryggissveitar að gögnum og upplýsingum, um sértæka þagnarskyldu og undanþágur frá slíkri skyldu og um meðferð persónuupplýsinga skal, að breyttu breytanda, fara eftir ákvæðum 17. og 19.–21. gr. laga um öryggi net- og upplýsingakerfa mikilvægra innviða.

d. (47. gr. d.)

Reglugerðarheimild.

Ráðherra setur, að fenginni umsögn frá Persónuvernd og ríkislögreglustjóra, nánari fyrirmæli í reglugerð um starfsemi netöryggissveitar samkvæmt lögum þessum. Í henni skal m.a. fjalla um meðferð tilkynninga og flokkunarkerfi fyrir atvik, áhættu, upplýsingar og framsetningu tilmæla, svo og samstarf við lögreglu.

Ákvæði til bráðabirgða.

I.

Þrátt fyrir ákvæði 29. gr. skal ráðherra tímanlega fyrir 1. september 2020 birta skrá yfir rekstraraðila nauðsynlegrar þjónustu í samræmi við 3. gr.

II.

Þrátt fyrir ákvæði 29. gr. skal ráðherra þegar hefja vinnu við gerð stefnu um net- og upplýsingaöryggi skv. 1. mgr. 4. gr. og skipa netöryggisráð í samræmi við 2. mgr. 4. gr.

_____

Samþykkt á Alþingi 11. júní 2019.