REGLUGERÐ

um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu.

I. KAFLI

Almenn ákvæði.

1. gr.

Gildissvið.

Reglugerð þessi gildir um veitendur stafrænnar þjónustu, net- og upplýsingakerfi þeirra og eftirlitsstjórnvald í skilningi laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

Reglugerðin gildir þó ekki um veitendur stafrænnar þjónustu sem teljast örfélög í skilningi laga nr. 3/2006 um ársreikninga.

2. gr.

Markmið.

Markmið reglugerðarinnar er að tryggja með sem bestum hætti samfellda virkni og áfallaþol stafrænnar þjónustu með því að kveða nánar á um lágmarkskröfur til umgjarðar net- og upplýsingakerfa veitenda stafrænnar þjónustu, ekki síst í þágu almannahagsmuna. Enn fremur að tryggja samhæfð viðbrögð við ógnum og atvikum í net- og upplýsingakerfum sem eru undirstaða fyrir veitingu stafrænnar þjónustu.

Reglugerð þessari er einnig ætlað að stuðla að samræmi í eftirfylgni og framkvæmd eftirlits með net- og upplýsingakerfum mikilvægra innviða.

3. gr.

Skilgreiningar.

Í reglugerð þessari merkir:

1. *Atburður:* Óviðbúin staða, óþekkt eða þekkt, sem getur skipt máli fyrir öryggi net- og upplýsingakerfa eða skert þjónustu mikilvægs innviðar.
2. *Atvik:* Hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa.
3. *Áhætta:* Aðstæður eða atburðir sem gætu haft skaðleg áhrif á öryggi net- og upplýsingakerfa.
4. *Eftirlitsstjórnvald:* Eftirlitsstjórnvald skv. 11. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, þ.e. Póst- og fjarskiptastofnun í tilviki veitenda stafrænnar þjónustu.
5. *Eignir:* Hvaðeina, bæði efnislegt og óefnislegt, sem er einhvers virði fyrir starfsemi mikilvægra innviða.
6. *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.
7. *Mikilvægir innviðir:* Veitendur stafrænnar þjónustu og rekstraraðilar nauðsynlegrar þjónustu eins og þeir eru skilgreindir í lögum nr. 78/2019 og reglugerð þessari.
8. *Nauðsynleg þjónusta:* Þjónusta sem skilgreind er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi samkvæmt ákvæðum laga nr. 78/2019 og reglugerðar nr. 866/2020, um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegrar þjónustu, þ.e. á sviði bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.
9. *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.
10. *Notendaklukkustund:* Fjöldi notenda innan Evrópska efnahagssvæðisins sem verða fyrir afleiðingum atviks í 60 mínútur.
11. *Rekstraraðili nauðsynlegrar þjónustu:* Opinber aðili eða einkaaðili sem veitir þjónustu sem telst nauðsynleg á sviði bankastarfsemi, innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.

12. *Skýjavinnsluþjónusta:* Stafræn þjónusta sem veitir aðgang að skalanlegum og sveigjanlegum brunni tölvunargetu sem hægt er að deila.
13. *Stafræn þjónusta:* Þjónusta í skilningi b-liðar 1. mgr. 1. gr. tilskipunar 2015/1535/ESB sem fellur undir skilgreiningu laga nr. 78/2019 og reglugerðar þessarar á hugtökunum netmarkaður, leitarvél á netinu eða skýjavinnsluþjónusta.
14. *Stjórnunarkerfi:* Fyrirkomulag skipulagslegra og tæknilegra ráðstafana sem notast er við til að tryggja öryggi net- og upplýsingakerfa.
15. *Umferðartakmarkanir:* Stýringar á takmörkun á umferð í og úr kerfum til að tryggja öryggi gegn ógnum.
16. *Veitandi stafrænnar þjónustu:* Veitandi stafrænnar þjónustu í skilningi laga nr. 78/2019, sem starfrækir netmarkað, leitarvél á netinu eða skýjavinnsluþjónustu.

Að öðru leyti gilda orðskýringar í lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

II. KAFLI
Lágmarkskröfur um áhættustýringu og ráðstafanir.

4. gr.
Skipulag net- og upplýsingaöryggis.

Veitandi stafrænnar þjónustu skal eftir fremsta megni tryggja öryggi net- og upplýsingakerfa sinna, er liggja til grundvallar starfsemi hans. Honum ber að útbúa og viðhalda skjalfestri lýsingu á stjórnskipulagi og stjórnunarkerfi net- og upplýsingakerfa sinna og skal jafnframt, með skipulegu áhættumati, bera kennsl á nauðsynlegar ráðstafanir og viðhafa aðgerðir til að stýra og stjórna net- og upplýsingakerfum með tilliti til áhættu. Skilgreina skal með skýrum hætti hlutverk og ábyrgð stjórnenda og starfsmanna, svo og ytri aðila ef við á, sem bera ábyrgð á framkvæmd áhættumats og skipulagi net- og upplýsingaöryggis.

Við framkvæmd áhættustýringar og viðbúnaðar í starfsemi sem fellur undir gildissvið reglugerðar þessarar, skal veitandi stafrænnar þjónustu byggja á gildandi alþjóðlega viðurkenndum stöðlum um bestu framkvæmd á sviði net- og upplýsingaöryggis. Það á bæði við um almenna staðla á borð við ISO/IEC 27001 (Stjórnunarkerfi um upplýsingaöryggi), ISO/IEC 27002 (Starfsvenjur fyrir upplýsingaöryggisstýringar), ISO/IEC 27005 (Áhættustýring upplýsingaöryggis) og aðra sértæka staðla og reglur á hlutaðeigandi sviði.

III. KAFLI
Skipulagslegar ráðstafanir.

5. gr.
Öryggisstefna.

Veitandi stafrænnar þjónustu skal útbúa og viðhalda skriflegri öryggisstefnu. Í stefnunni skal tilgreina stefnuyfirlýsingu, markmið og meginreglur net- og upplýsingaöryggis og hvernig öryggi net- og upplýsingakerfa er best tryggt í starfsemi hans. Stefnan skal samþykkt með formlegum hætti af yfirstjórn og birt öllum starfsmönnum. Skal hún sérstaklega kynnt starfsmönnum sem vinna með beinum eða óbeinum hætti við net- og upplýsingakerfi. Þá skal vera skýrt í skipulagi veitanda stafrænnar þjónustu hver ber ábyrgð á framkvæmd öryggismála. Öryggisstefnu skal rýna og uppfæra eftir því sem tilefni er til og að lágmarki á tveggja ára fresti.

6. gr.
Áhættumat.

Veitandi stafrænnar þjónustu skal framkvæma áhættumat á net- og upplýsingakerfum sínum á grundvelli viðurkenndrar og þekktrar aðferðarfræði, með það að markmiði að skapa forsendur fyrir vali á öryggisráðstöfunum og draga úr áhættu sem steðjað getur að öryggi net- og upplýsingakerfa hans. Áhættumat skal vera skriflegt. Það skal framkvæmt reglubundið og aðferðarfræði þess endurmetin, hvort tveggja á a.m.k. tveggja ára fresti. Ávallt skal leggja mat á hvort atvik eða áhætta í net- og upplýsingakerfum gefi tilefni til endurskoðunar á áhættumati og bregðast strax við ef forsendur áhættumats eða aðstæður breytast sem kalla á slíkt endurmat.

Framkvæmd áhættumats samkvæmt 1. mgr. skal að lágmarki ná yfir eftirfarandi atriði:

a. Bera skal kennsl á áhættu, með því að greina umfang og áhrif ógna, sem og mat á líkindum þeirra. Áhættu skal forgangsraðað í ljósi skilgreindra og skriflegra viðmiða um ásættanlega áhættu og markmiða sem sett hafa verið í öryggisstefnu.

b. Eignir skulu skilgreindar og metnar, s.s. með tilliti til þess hverjir eru helstu veikleikar og/eða ógnir sem steðjað geta að eigninni, þar á meðal rýrnun trausts.
c. Ef við á, skal mat lagt á að hvaða marki veiting þjónustu er háð afhendingu á vöru eða þjónustu frá þriðja aðila (s.s. birgjum eða þjónustuveitendum), þ.m.t. öðrum mikilvægum innviðum, svo og möguleg áhrif ef rof verður á slíkri afhendingu.
d. Ef við á, skal mat lagt á það hvernig net- og upplýsingakerfi eða undirliggjandi búnaður eru háð kerfum þriðja aðila, þ.m.t. annarra mikilvægra innviða. Hér skal einnig líta til þess hvort, og þá hvernig, röskun á starfsemi kerfa þriðja aðila kann að hafa áhrif á starfsemi net- og upplýsingakerfa við veitingu stafrænnar þjónustu.

Heimilt er að víkja frá einstaka kröfum samkvæmt c- og d-liðum 2. mgr. ef veitandi stafrænnar þjónustu getur sýnt fram á að þær séu of íþyngjandi miðað við umfang og eðli starfsemi hans. Skylt er að skrásetja slík frávik sérstaklega.

7. gr.

Öryggisráðstafanir.

Veitandi stafrænnar þjónustu skal, á grundvelli niðurstöðu áhættumats, innleiða öryggisráðstafanir sem eru nauðsynlegar til að tryggja öryggi net- og upplýsingakerfa og koma til móts við greinda áhættu sem steðjað getur að hlutaðeigandi eignum og stafrænni þjónustu, takmarka líkur á henni og áhrifum sem hún getur haft. Öryggisráðstafanir skulu taka mið af alþjóðlegum viðmiðum um bestu framkvæmd sem og þeirri reynslu og lærdómi sem aflað hefur verið, til dæmis við beitingu fyrri öryggisráðstafana og meðhöndlun atvika og áhættu. Öryggisráðstafanir veitanda stafrænnar þjónustu skulu þó að lágmarki vera í samræmi við kröfur II.-IV. kafla, að teknu tilliti til 3. mgr. 6. gr., 2. mgr. 10. gr. og 4. mgr. 15. gr.

Setja skal fram skriflegar lýsingar á þeim öryggisráðstöfum sem gripið er til samkvæmt 1. mgr. sem og útfærslu þeirra og innleiðingu, þar á meðal við hönnun, þróun, rekstur, prófun og viðhald hvers kerfis sem og raunlæga vernd öryggisrýma, sbr. 12. gr. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir öryggi net- og upplýsingakerfa veitanda stafrænnar þjónustu.

Öryggisráðstafanir skulu endurskoðaðar reglubundið í samræmi við endurskoðun, framkvæmd og niðurstöður áhættumats og að minnsta kosti á tveggja ára fresti. Ávallt ber að endurskoða öryggisráðstafanir þegar atvik eða áhætta kemur upp eða aðstæður breytast sem kalla á endurmat.

8. gr.

Öryggisráðstafanir vegna starfsmanna.

Í þeim tilgangi að fyrirbyggja og takmarka tjón vegna mistaka, svika og annarrar misnotkunar starfsmanna og þriðju aðila, svo sem verktaka, sem vegna starfa sinna hafa aðgang að net- og upplýsingakerfum eða hýsingarrýmum kerfisbúnaðar (öryggisrýmum), skal veitandi stafrænnar þjónustur grípa til eftirfarandi öryggisráðstafana:

a. Leggja mat á hvort viðeigandi sé að afla sakavottorðs og, eftir því sem við getur átt, annarrar öryggisvottunar umsækjanda áður en starf er veitt eða gengið er til samninga við þriðju aðila. Við slíkt mat skal líta til ábyrgðar sem starfi eða verkefni fylgir.
b. Láta starfsmenn og þriðju aðila undirrita trúnaðaryfirlýsingar.
c. Skilgreina ábyrgð og skyldur starfsmanna og þriðju aðila í tengslum við öryggi net- og upplýsingakerfa og framkvæmd verkferla.
d. Skilgreina hvaða starfsmenn eða þriðju aðilar eru í lykilhlutverki við að tryggja öryggi net- og upplýsingakerfa og tryggja virkar boðleiðir, þannig að þess sé ávallt gætt að hægt sé að ná í þá eða varamenn þeirra í neyð.
e. Fræða og eftir atvikum prófa þekkingu starfsmanna og þriðju aðila á þeim lögum og reglum sem gilda um öryggi net- og upplýsingakerfa mikilvægra innviða. Einnig skal tryggja að starfsmönnum og þriðju aðilum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær.

9. gr.

Útvistun á rekstri net- og upplýsingakerfa.

Ef veitandi stafrænnar þjónustu semur við þriðja aðila um rekstur net- og upplýsingakerfa, í heild eða að hluta, skal hann tryggja að þjónustuveitandi þekki og starfi í samræmi við lög nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og uppfylli ákvæði reglugerðar þessarar.

Þjónustusamningur um rekstur net- og upplýsingakerfa skal vera skriflegur og afmarka á skýran hátt hlutverk og skyldur aðila. Þar skal tilgreina með skýrum hætti þá þjónustu sem veitanda stafrænnar þjónustu er veitt, svo og þau kerfi og búnað sem notaður er vegna veitingar stafrænnar þjónustu.

Veitanda stafrænnar þjónustu er heimilt, ef þörf þykir, að fela þjónustuveitanda á grundvelli þjónustusamnings að tilkynna um alvarleg atvik eða áhættu samkvæmt 18. gr. er varðar þann hluta reksturs net- og upplýsingakerfa sem hann sinnir.

Í þjónustusamningi skal tryggja að eftirlitsstjórnvald hafi aðgang að viðeigandi upplýsingum frá þjónustuveitanda og geti við framkvæmd eftirlits á grundvelli laga nr. 78/2019 og reglugerðar þessarar gert athuganir á starfsstöð þjónustuveitandans og prófanir á kerfum hans og búnaði sem tilgreind eru í þjónustusamningi.

Þrátt fyrir útvistun samkvæmt ákvæði þessu ber veitandi stafrænnar þjónustu sem í hlut á ábyrgð á að uppfylltar séu lágmarkskröfur laga nr. 78/2019 og reglugerðar þessarar um áhættustýringu og viðbúnað, þar með talið ábyrgð á því að tilkynningarskyldu sé fullnægt.

IV. KAFLI
Tæknilegar ráðstafanir.

10. gr.

Almennt.

Veitandi stafrænnar þjónustu skal, í samræmi við niðurstöður áhættumats, gera þær tæknilegu öryggisráðstafanir sem nauðsynlegar eru til að tryggja með sem bestum hætti öryggi net- og upplýsingakerfa sinna.

Veitandi stafrænnar þjónustu skal ávallt innleiða þær kerfislægu og raunlægu ráðstafanir sem nauðsynlegar teljast samkvæmt niðurstöðum áhættumats. Að öðru leyti er heimilt að víkja frá einstaka kröfum samkvæmt 11. og 12. gr. ef veitandi stafrænnar þjónustu getur sýnt fram á að þær séu of íþyngjandi miðað við umfang og eðli starfsemi hans. Skylt er að skrásetja slík frávik sérstaklega.

11. gr.

Kerfislægar ráðstafanir.

Veitandi stafrænnar þjónustu skal að lágmarki viðhafa eftirtaldar kerfislægar ráðstafanir fyrir net- og upplýsingakerfi sín:

a. Kerfislægar aðgangsstýringar:
    1. Innleiða viðeigandi aðgangsstýringarkerfi til sannvottunar á notendum og kerfum.
    2. Takmarka aðgangsréttindi starfsmanna og verktaka að upplýsingum og kerfum/kerfishlutum við það sem þeim er nauðsynlegt til að sinna starfi sínu og við þann tíma sem nauðsynlegur er.
    3. Skrá með formlegum hætti veitingu aðgangsheimilda og aðgangsréttinda og yfirfara aðgangsréttindi reglulega.
    4. Viðhafa ráðstafanir sem tryggja viðeigandi rekjanleika uppflettinga og vinnsluaðgerða.
b. Nota dulritun og/eða aðrar viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í net- og upplýsingakerfum.
c. Setja viðeigandi umferðartakmarkanir í net- og upplýsingakerfum.
d. Lágmarka virkni, tengingar og aðgang milli kerfishluta með því að skilgreina kröfur um samskipan kerfis (e. *system configuration*). Tilgangurinn er sá að uppsetning þjónustu eða annarrar virkni í net- og upplýsingakerfum, eða tenging slíks kerfis við búnað, takmarkist við þætti sem eru nauðsynlegir fyrir starfsemi og öryggi net- og upplýsingakerfa.

e. Aðgreina kerfishluta eins og kostur er til að takmarka dreifingu/útbreiðslu atvika innan og á milli net- og upplýsingakerfa.
f. Setja upp búnað sem vaktar umferð í net- og upplýsingakerfum og greinir t.a.m. ummerki um atvik eða áhættu, s.s. óeðlilegan aðgang, árásir, spillikóða og aðrar hættulegar aðstæður. Meta skal sérstaklega hvort setja eigi upp innbrotsvarnir (e. *intrusion prevention*) þar sem þörf er á sterkum vörnum fyrir gögn og vinnslu.
g. Viðhalda órofinni viðeigandi slóð sönnunargagna sem nýst gætu við greiningu atvika og áhættu. Skilgreina skal fyrir fram skráningu í búnaði og vinnslum innan kerfa þannig að mikilvægir atburðir komi með skýrum hætti fram í eftirlitskerfum.
h. Vakta öryggisuppfærslur fyrir net- og upplýsingakerfi og innleiða allar nauðsynlegar uppfærslur eins fljótt og mögulegt er.

12. gr.

Raunlægar ráðstafanir.

Veitandi stafrænnar þjónustu skal að lágmarki viðhafa eftirfarandi raunlægar ráðstafanir fyrir net- og upplýsingakerfi sín:

a. Raunlæg aðgangsstýring:
    1. Hindra óleyfilegan aðgang að öryggisrýmum með traustum hurðum og læsingum. Leitast skal við að hafa öryggisrými gluggalaus eða glugga varða sérstaklega gegn innbrotum og þannig að byrgi ásýnd inn í rýmin.
    2. Stýra aðgengi starfsmanna og þriðju aðila að öryggisrýmum með aðgangskorti eða sambærilegu auðkenni og skal rekjanleiki tryggður. Takmarka skal aðgang inn í mikilvæg öryggisrými við nauðsynlega aðila. Verktakar og aðrir ytri aðilar sem hafa ekki aðgangsheimild að öryggisrýmum skulu ávallt vera undir eftirliti inni í þeim.
b. Raunlægar varnir öryggisrýma:
    1. Tryggja ber að byggingarefni öryggisrýma og annar frágangur byggingar sé úr eldtefjandi efni sem ver öryggisrýmin fyrir eldsvoða utan þeirra í að lágmarki eina klukkustund. Öll gegntök skulu vera reykþétt og eldvarin.
    2. Verja skal mikilvæg öryggisrými fyrir raka- og vökvaskemmdum. Setja lekapönnur undir vökvalagnir kerfa sem eru með takmörkuðu magni vökva, til dæmis kælikerfi, og tryggja að ekki séu vatns- og hitaveitulagnir í gegnum öryggisrýmin.
    3. Haga skal frágangi virks búnaðar og leiðslna þannig að hann verði ekki fyrir skaða ef vökvi lekur inn í öryggisrýmin, t.d. með því að lyfta búnaði í ákveðna hæð frá gólfi.
    4. Öryggisrými skulu alla jafna vera útbúin sjálfvirku slökkvikerfi.
    5. Haga skal frágangi öryggisrýma þannig að viðeigandi ráðstafanir séu gerðar gagnvart innbrotum og skemmdarverkum.
c. Vöktun öryggisrýma:
    1. Öryggisrými skulu útbúin sjálfvirkum vaktbúnaði sem tengist stjórnstöð og gefur viðvörun um eld og ef umhverfisaðstæður breytast umfram það sem búnaðurinn er gerður fyrir og að lágmarki vegna raka, vökvaleka og hita. Þá skal hitastig við virkan búnað jafnframt vaktað sérstaklega.
    2. Setja upp sjálfvirkt innbrotsviðvörunarkerfi með myndavélum og innbrotsskynjurum þar sem það á við, í og við öryggisrými.
d. Varnir gegn straumrofi fyrir net- og upplýsingakerfi:
    1. Tryggja skal varaafl sem getur að lágmarki haldið uppi óbreyttri virkni net- og upplýsingakerfa í samræmi við uppitímaviðmið þjónustu á grundvelli niðurstöðu áhættumats, en þó eigi skemur en í 2 klst.
    2. Verja skal mikilvægan búnað í öruggum rýmum sérstaklega fyrir rofi í raffæðingu og öðrum skammtíma truflunum í rafveitu, t.d. með órofaaflgjafa.
    3. Auk þess skal meta sérstaklega hvort verja skuli net- og upplýsingakerfi sem eru undirstaða fyrir veitingu stafrænnar þjónustu gegn langtíma straumrofi með sérstakri vararafstöð sem getur haldið kerfum gangandi um lengri tíma.

V. KAFLI
Viðhald, viðbragðsáætlun, innra eftirlit og atvikatilkynningar.

13. gr.
Viðhald net- og upplýsingakerfa.

Veitandi stafrænnar þjónustu skal viðhalda áreiðanlegum rekstri net- og upplýsingakerfa sinna, t.a.m. með virkri endurnýjun búnaðar og uppfærslu hugbúnaðar.

Þá skal veitandi stafrænnar þjónustu hafa virka viðbúnaðarumgjörð fyrir net- og upplýsingakerfi sín og tryggja að kerfi séu reist við eins fljótt og kostur er komi til atviks og/eða þjónusturofs. Tryggja skal að til staðar séu afrit af síðustu stillingum búnaðar sem nauðsynlegur er til að viðhalda og reisa við rekstur net- og upplýsingakerfa. Afritunargögnin skulu vistuð á öruggum stað.

Á grundvelli bilana- og truflanaskýrslna eða tilkynninga frá búnaði, skal veitandi stafrænnar þjónustu hafa getu til að gera nauðsynlegar ráðstafanir eins fljótt og verða má til að bregðast við atvikum sem valda mikilli truflun eða rofi á þjónustu. Meiri háttar röskun á stafrænni þjónustu skal svo fljótt sem verða má tilkynna um í samræmi við 18. gr. til að tryggja netöryggissveit sem réttasta stöðumynd vegna netógna sem gæti þurft að bregðast við.

14. gr.
Stjórnun breytinga í net- og upplýsingakerfum.

Breytingar á net- og upplýsingakerfum veitenda stafrænnar þjónustu, eða endurnýjun þeirra, skal framkvæma þannig að þær trufli sem minnst starfsemi hans. Veitandi stafrænnar þjónustu skal setja verklagsreglur um hvernig standa skal að slíkum breytingum sem og hvernig tryggja megi sem minnsta röskun á þjónustu hans.

15. gr.
Viðbragðsáætlun.

Veitandi stafrænnar þjónustu skal útbúa viðbragðsáætlun sem virkja ber ef upp kemur atvik eða áhætta í net- og upplýsingakerfum hans. Viðbragðsáætlunin skal byggja á niðurstöðum áhættumats og m.a. taka mið af því hvernig leysa á úr mögulegum atvikum, hvernig tryggja beri samfelldan rekstur og/eða endurreisn net- og upplýsingakerfa, svo og að takmarka tjón.

Í viðbragðsáætlun skal að lágmarki kveða á um eftirfarandi atriði:

a. Aðila sem ber ábyrgð á því að virkja viðbragðsáætlun þegar við á og aðra lykilstarfsmenn.
b. Verkferla við reglulega prófun viðbragðsáætlana.
c. Hvernig leita skal orsaka atvika og koma aftur á eðlilegu rekstrarástandi.
d. Leiðbeiningar um hvernig bregðast skal við atvikum og áhættu, þar á meðal skilgreina ábyrgðarsvið viðeigandi starfsmanna og boðleiðir, s.s. nauðsynlegar upplýsingar til að ná í viðgerðarmenn eða aðra sérfræðinga, upplýsingar um varabúnað, skipulag tilkynninga og annars sem við á.
e. Hvernig skuli tryggja heildstæða skráningu og greiningu atvika og þeirra ráðstafana sem gripið er til svo unnt sé að byggja á og læra af fyrri reynslu.

Viðbragðsáætlun skal metin og prófuð með reglulegu millibili, þ. á m. með æfingum.

Heimilt er að víkja frá einstaka kröfum samkvæmt d- og e-liðum 2. mgr. ef veitandi stafrænnar þjónustu getur sýnt fram á að þær séu of íþyngjandi miðað við umfang og eðli starfsemi hans. Skylt er að skrásetja slík frávik sérstaklega.

16. gr.
Innra eftirlit og prófanir.

Veitandi stafrænnar þjónustu skal viðhafa virkt innra eftirlit til að tryggja að umgjörð áhættustýringar og viðbúnaðar í starfsemi hans uppfylli kröfur laga nr. 78/2019 og reglugerðar þessarar, þar á meðal með prófunum.

Gerð skal áætlun um framkvæmd kerfisbundins innra eftirlits samkvæmt fyrir fram skilgreindri aðferð. Prófanir geta meðal annars falið í sér úttektir á virkni tæknilegra öryggisráðstafana skv. IV. kafla og viðbragðsáætlun, sbr. 15. gr.

Tíðni og umfang innra eftirlits skal ákveðið út frá öryggislegum markmiðum m.a. með hliðsjón af niðurstöðu áhættumats. Innra eftirlit skal þó framkvæmt eigi sjaldnar en á tveggja ára fresti.

Niðurstöður úttektar samkvæmt kröfum um innra eftirlit skulu skrásettar.

17. gr.

Meðhöndlun atvika.

Veitandi stafrænnar þjónustu skal halda skrá yfir öll atvik og áhættu sem upp koma í eða steðja að net- og upplýsingakerfum hans. Atvikaskrá skal uppfærð reglulega og atvik og áhætta skráð á grundvelli skýrra verkferla.

Þá skal greina orsök og afleiðingu atvika og áhættu og skjalfesta niðurstöður svo unnt sé að koma í veg fyrir að sambærileg atvik eða áhætta endurtaki sig.

Við endurskoðun áhættumats skal taka mið af atvikaskráningu og -greiningu samkvæmt ákvæði þessu.

18. gr.

Tilkynning um alvarleg atvik eða áhættu.

Veitandi stafrænnar þjónustu skal tilkynna netöryggissveit Póst- og fjarskiptastofnunar um öll alvarleg atvik og áhættu sem ógna öryggi net- og upplýsingakerfa hans.

Við mat á því hvort atvik eða áhætta teljist alvarleg skal horft til viðmiða 2. mgr. 8. gr. laga nr. 78/2019 og í samræmi við neðangreint:

a. fjölda notenda þjónustunnar sem atvik eða áhætta hefur áhrif á og skal þar miða við fjölda einstaklinga eða lögaðila sem gert hafa samning um veitingu þjónustu eða fjölda notenda sem notað hafa þjónustu, einkum samkvæmt gögnum úr umferðarskrám;
b. hversu lengi atvik stendur yfir og skal þar miða við tímabilið frá því að truflun verður á eðlilegri veitingu þjónustunnar þar til endurreisn á sér stað að því er varðar aðgengi, sannvottaðan uppruna, réttleika eða leynd;
c. landfræðilegrar útbreiðslu og skal þar líta til hvort atvik eða áhætta hafi eða geti haft áhrif á veitingu þjónustunnar í öðrum ríkjum innan Evrópska efnahagssvæðisins;
d. umfangs áhrifa atviks eða áhættu og skal það mælt með hliðsjón af skerðingu á aðgengi, sannvottuðum uppruna, réttleika eða leynd gagna eða tengdrar þjónustu; og
e. mögulegra áhrifa atviks eða áhættu á aðra mikilvæga innviði og skal þar miðað við hvort atvik eða áhætta hafi eða geti valdið efnislegu eða óefnislegu tjóni fyrir notendur þjónustu, svo sem er varðar heilbrigði, öryggi eða eignir.

Veitanda stafrænnar þjónustu er þó ekki skylt að afla viðbótarupplýsinga sem hann hefur ekki aðgang að til meta alvarleika atviks eða áhættu samkvæmt 1. og 2. mgr.

Þrátt fyrir 2. mgr. skal atvik ávallt teljast alvarlegt í skilningi 1. mgr. ef:

a. stafræn þjónusta er ekki tiltæk í meira en 5.000.000 notendaklukkustundir;
b. atvik hefur valdið tjóni á réttleika, sannvottuðum uppruna eða leynd vistaðra, sendra eða unninna gagna eða tengdrar þjónustu, sem boðin er eða aðgengileg um net- og upplýsingakerfi veitanda stafrænnar þjónustu, og hefur áhrif á meira en 100.000 notendur innan Evrópska efnahagssvæðisins;
c. atvik hefur stofnað almannaöryggi í hættu eða valdið manntjóni; eða
d. atvik hefur valdið efnislegu tjóni sem nemur meira en 150.000.000 kr. hjá a.m.k. einum notanda þjónustunnar innan Evrópska efnahagssvæðisins.

19. gr.

Nánar um miðlun tilkynninga til netöryggissveitar.

Tilkynning skv. 18. gr. skal berast í gegnum tilkynningagátt stjórnvalda, með tölvupósti á tölvupóstfang netöryggissveitarinnar eða, eftir atvikum, símleiðis. Netöryggissveit skal gefa út nánari leiðbeiningar um boðleiðir samkvæmt ákvæði þessu.

Netöryggissveit skal gefa út nánari leiðbeiningar um mat á alvarleika atvika og áhættu samkvæmt 18. gr. og skal veitandi stafrænnar þjónustu, eftir fremsta megni, taka mið af þeim við mat á því hvort tilkynna beri um atvik eða áhættu til sveitarinnar.

Tilkynning til netöryggissveitarinnar samkvæmt 1. mgr. skal berast eins fljótt og verða má og eigi síðar en 6 klukkustundum eftir að borin hafa verið kennsl á atvik eða áhættu í kerfum veitanda stafrænnar þjónustu. Í tilkynningu skal m.a. veita eftirfarandi upplýsingar:

a. hvenær atviks eða áhættu varð fyrst vart í net- og upplýsingakerfum;

b. frummat á eðli og/eða tegund atviks eða áhættu í net- og upplýsingakerfum;

c. frummat á umfangi atviks eða áhættu;

d. frummat á mögulegum smitáhrifum;

e. hver sé rekstraraðili umræddra net- og upplýsingakerfa, t.a.m. ef rekstri þeirra er útvistað.

Liggi ekki allar upplýsingar fyrir við framangreind tímamörk ber veitanda stafrænnar þjónustu að fylgja upprunalegri tilkynningu um atvik eða áhættu eftir með frekari samskiptum við netöryggissveit, eins fljótt og verða má.

Netöryggissveitin skal miðla tilkynningum samkvæmt ákvæði þessu til eftirlitsstjórnvalds eins fljótt og verða má. Þá skal netöryggissveit upplýsa önnur stjórnvöld, eftir því sem við á, enda sé atvik eða áhætta af þeim toga að haft getur alvarleg áhrif á veitingu þjónustu af hálfu annarra mikilvægra innviða.

20. gr.

Tilkynningar til viðskiptavina.

Veitandi stafrænnar þjónustu skal vera með skýra og skilvirka ferla vegna tilkynninga um ósamfellu í virkni eða þjónusturof, svo sem af völdum atviks, bilana, breytinga eða viðhalds. Á heimasíðu hans, eða með öðrum sambærilegum leiðum, skal eftir atvikum tilgreina almenn þjónustuviðmið, svo sem um þjónustustig og reglubundið viðhald.

Veitandi stafrænnar þjónustu skal tilkynna viðskiptavinum um truflanir eða þjónusturof. Í tilkynningu skal að lágmarki koma fram hvaða áhrif truflunin eða þjónusturofið hefur eða getur haft og þær ráðstafanir sem veitandi stafrænnar þjónustu muni grípa til, ásamt ráðleggingum til viðskiptamanna ef svo ber undir. Sé veitandi stafrænnar þjónustu viðskiptavinur annars mikilvægs innviðar skal tilkynna honum slíkt sérstaklega.

VI. KAFLI
Eftirlit, samræmi og viðurlög.

21. gr.

Eftirlitsstjórnvald.

Póst- og fjarskiptastofnun hefur eftirlit með framkvæmd laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og reglugerðar þessarar, gagnvart veitendum stafrænnar þjónustu.

22. gr.

Aðgangur að upplýsingum.

Um aðgang eftirlitsstjórnvalds að upplýsingum fer samkvæmt lögum nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

Ef eftirlitsstjórnvald telur á grundvelli rökstuddra grunsemda að veitandi stafrænnar þjónustu uppfylli ekki kröfur skv. 7. og 8. gr. laga nr. 78/2019 skal veitandi stafrænnar þjónustu að beiðni þess afhenda allar upplýsingar sem óskað er eftir og varða net- og upplýsingaöryggi, þ.m.t. um skipulag net- og upplýsingaöryggis, öryggisstefnu, áhættumat, lýsingu á öryggisráðstöfunum, viðbragðsáætlun, atvikaskrá og skýrslur um innra eftirlit. Þá er eftirlitsstjórnvaldi heimilt að óska eftir nánari skýringum og gögnum í starfsemi veitanda stafrænnar þjónustu við framkvæmd eftirlits.

Veitanda stafrænnar þjónustu ber að verða við beiðni samkvæmt 2. mgr. eins fljótt og auðið er.

Aðgangsheimild eftirlitsstjórnvalds samkvæmt ákvæði þessu nær einnig til persónuupplýsinga í skilningi laga um persónuvernd og vinnslu persónuupplýsinga, að því marki sem nauðsynlegt er vegna eftirlits með framkvæmd laga nr. 78/2019 og reglugerðar þessarar.

Eftirlitsstjórnvaldi er heimilt að óska eftir reglubundinni skýrslugjöf af hálfu veitanda stafrænnar þjónustu um meðhöndlun atvika, í því skyni að leggja mat á uppfyllingu lágmarkskrafna um áhættustýringu og viðbúnað í starfsemi veitanda stafrænnar þjónustu. Við matið skal meðal annars horft til atvikaskrár og niðurstaðna atvikagreiningar.

23. gr.

Bindandi fyrirmæli eftirlitsstjórnvalds.

Eftirlitsstjórnvaldi er heimilt að gefa bindandi fyrirmæli um úrbætur ef mat þess er að veitandi stafrænnar þjónustu uppfylli ekki kröfur laga nr. 78/2019 og reglugerðar þessarar, þ.m.t. um skipulag net- og upplýsingakerfa og einstakar lágmarksöryggisráðstafanir. Skal gefinn til þess hæfilegur frestur. Áður en bindandi fyrirmæli eru gefin skal gefa viðkomandi aðila tækifæri til að koma á framfæri athugasemdum og skýringum.

Vanræki veitandi stafrænnar þjónustu að verða við bindandi fyrirmælum eftirlitsstjórnvalds innan þess frests sem stjórnvaldið setur er eftirlitsstjórnvaldi heimilt að láta vinna verkið fyrir hönd og á kostnað hlutaðeigandi aðila. Kröfur sem kunna að myndast samkvæmt þessu ákvæði eru aðfararhæfar.

Brot á reglugerð þessari varða viðurlögum samkvæmt ákvæðum laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

24. gr.

Heimild og gildistaka.

Reglugerð þessi er sett með heimild í 7., 8. og 28. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, og öðlast þegar gildi.

Samgöngu- og sveitarstjórnarráðuneytinu, 1. desember 2020.

Sigurður Ingi Jóhannsson.

Ragnhildur Hjaltadóttir.

Fyrirvari
Reglugerðir eru birtar í B-deild Stjórnartíðinda skv. 3. gr. laga um Stjórnartíðindi og Lögbirtingablað, nr. 15/2005, sbr. reglugerð um útgáfu Stjórnartíðinda nr. 958/2005.
Sé misræmi milli þess texta sem birtist hér í safninu og þess sem birtur er í útgáfu B-deildar Stjórnartíðinda skal sá síðarnefndi ráða.