Fullgild rafræn undirskrift
GUÐMUNDUR STEFÁN BJÖRNSSON
Kennitala: 030271-5729
2020-10-06 16:16:48 GMT
Ástæða: Undirskrift

Samgöngu- og sveitarstjórnarráðuneytið
Sölvhólsgötu 7
101 Reykjavík

Reykjavík, 6. október 2020

Efni: Umsögn um drög að reglugerð um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu

I. Inngangur

Sensa ehf. (hér eftir „Sensa"), vísar til draga samgöngu- og sveitarstjórnarráðuneytisins til reglugerðar um öryggi net- og upplýsingakerfa veitenda stafrænnar þjónustu. Markmið reglugerðarinnar er að innleiða nánari útfærslur á m.a. umgjörð net- og upplýsingakerfa veitenda stafrænnar þjónustu og öðrum ákvæðum laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða, sem öðluðust gildi þann 1. september sl.

Sensa hefur yfirfarið drögin og vill góðfúslega koma á framfæri eftirfarandi athugasemdum til ráðuneytisins.

II. Umsögn Sensa

I. og II. Kafli: Almenn ákvæði og þjónusta sem skilgreind er nauðsynleg

- *1. gr.*

Sensa gerir athugasemd við þá undantekningu reglugerðarinnar, n.t.t. í 2. mgr. 1. gr., þar sem segir að reglugerðin eigi ekki að taka til félaganna sem teljast örfélög í skilningi laga nr. 3/2006 um ársreikninga. Jafnvel þótt umrædda undantekningu sé að finna í 2. mgr. 2. gr. laga nr. 78/2019, vill Sensa engu að síður benda á að slík undantekning, þegar kemur að veitendum starfænnar þjónustu, skýtur skökku við, sér í lagi í þeim tilvikum sem slíkir aðilar veita t.d. stafræna þjónustu til handa rekstraraðila nauðsynlegrar þjónustu í skilningi laga nr. 78/2019. Telur Sensa fremur, þegar um ræðir þá reglugerð sem hér er til umfjöllunar og markmiðs hennar og laga nr. 78/2019, að undantekningar reglugerðarinnar (skv. 6., 10. og 15. gr.) ættu að duga til handa þeim aðilum sem geta sýnt fram á að tilteknar kröfur séu of íþyngjandi miðað við umfang og eðli starfsemi hans. Óeðlilegt hlýtur að teljast að láta öll örfélög vera undanskilin regluverkinu sjálfkrafa, m.t.t. þeirra gífurlegu hagsmuna sem hér gætu verið um að ræða og þeirra undantekninga sem reglugerðin tilgreinir nú þegar. Sensa hvetur ráðuneytið til að taka umrædda

undantekningu í lögum nr. 78/2019, sem og í 1. gr. reglugerðarinnar, til endurskoðunar í ljósi framangreinds.

III. kafli: Skipulagslegar ráðstafanir

- *1. mgr. 6. gr.*

Samkvæmt drögunum skal áhættumat framkvæmt „reglubundið og aðferðafræði þess endurmetin, hvort tveggja á a.m.k. tveggja ára fresti". Að mati Sensa er óeðlilegt að skilgreina sérstaklega að aðferðafræði áhættumatsins skuli endurmetin sérstaklega á tveggja ára fresti. Telur Sensa fremur að aðferðafræði áhættumatsins skuli uppfærð þegar og ef þörf krefur, m.t.t. aðstæðna og starfseminnar sem um ræðir hjá viðkomandi aðila og atvik sem kunna að koma upp, en eigi síðar en t.d. á *fimm* ára fresti. Ekki sé jafn knýjandi að setja tveggja ára tímamörk á *aðferðafræðina,* þótt það sé eðlilegra varðandi áhættumatið sjálft, nema aðstæður hverju sinni leiði til þess að aðferðafræðin sé endurmetin fyrr.

- *a-liður 1. mgr. 8. gr.*

Í staðinn fyrir orðalagið „[m]eta hvort *tilefni* sé til að afla sakavottorðs[...]", ætti að mati Sensa breyta orðalaginu í „[m]eta hvort *nauðsynlegt* sé að afla sakavottorðs[...]", í ljósi orðalags 8. gr. og 12. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

IV. kafli: Tæknilegar ráðstafanir

- *1. tölul. a-liðar 1. mgr. 11. gr.*

Að mati Sensa ætti ákvæðið fremur að vísa til „[...]viðeigandi aðgangsstýringarkerfis til *auðkenningar* á notendum og kerfum" fremur en „[...]*sannvottunar* á notendum og kerfum".

- *4. tölul. a-liðar 1. mgr. 11. gr.*

Að mati Sensa ætti að bæta við orðinu „viðeigandi" í ákvæðið, svo það hljóði svona:

> „4. Viðhafa *viðeigandi* ráðstafanir sem tryggja rekjanleika uppflettinga og vinnsluaðgerða"

V. kafli: Viðhald, viðbragðsáætlun, innra eftirlit og atvikatilkynningar

- *16. gr.*

Sensa telur það varhugavert að setja fram kröfu í 3. mgr. ákvæðisins um að innra eftirlit skuli „[...]þó framkvæmt eigi sjaldnar en á tveggja ára fresti", í ljósi þeirra gífurlegu hagsmuna sem felast í innra eftirliti í starfsemi sem þessari. Að mati Sensa ætti því innra eftirlit að vera mun tíðara en áhættumatsgerð og endurskoðun þess, en reglugerðin tilgreinir jafnframt tveggja ára tímamark í þeim efnum.

- *19. gr.*

Sensa kallar eftir því að Netöryggissveitin birti við fyrsta tækifæri leiðbeiningar um mat á alvarleika atvika og áhættu skv. 18. gr., a.m.k. fyrir gildistöku reglugerðarinnar, enda hefði að mati Sensa átt að birta slíkar leiðbeiningar fyrir

gildistöku laganna þann 1. september sl., í ljósi þeirra hagsmuna sem hér um ræðir.

Skv. 3. mgr. ákvæðisins skal tilkynning berast Netöryggissveitinni „eigi síðar en 6 klukkustundum eftir að borin hafa verið kennsl á atvik eða áhættu í kerfum veitanda stafrænnar þjónustu". Sensa lítur svo á að með framangreindu orðalagi sé verið að gefa til kynna ákveðinn stigsmun þegar kemur að tímamarkinu sem miða skal við, enda má af orðalaginu skilja að það sé búið að bera kennsl á atvik eða áhættu eftir að hafa orðið vart við það/hana. Félagið lítur því svo á að einhver vinna hljóti að hafa farið fram við að greina atvikið eða áhættuna, til þess að unnt sé að telja að félagið hafi „borið kennsl" á atvikið/áhættuna. Sé sá skilningur ekki réttur telur Sensa að þörf sé á skýrara orðalagi í reglugerðinni svo unnt sé að átta sig á hvaða tímamark skuli miða við í tilvikum sem þessum.

Í tengslum við þá tilkynningarskyldu sem reglugerðin kveður á um, n.t.t. til Netöryggissveitarinnar, vill Sensa benda á að veitendur stafrænnar þjónustu starfa margir hverjir (ef ekki flestir) sem s.k. *vinnsluaðilar* á vegum síns viðskiptavinar sem telst þá *ábyrgðaraðili* í skilningi laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga. Samkvæmt hinum síðarnefndu lögum er meginreglan sú að vinnsluaðili skuli tilkynna *ábyrgðaraðila* um öryggisbrest þegar hann fær vitneskju um slíkan (nema sérstaklega hafi verið samið um annað), svo ábyrgðaraðila sé í kjölfarið unnt að tilkynna Persónuvernd um öryggisbrestinn þegar við á. Miðað við kröfur þessarar reglugerðar skal veitandi stafrænnar þjónustu senda tilkynningu til Netöryggissveitarinnar um atvik, eins og skilgreint er nánar í reglugerðinni. Í ljósi framangreinds gæti því *tilkynningarskylt atvik skv. reglugerðinni* jafnframt verið *tilkynningarskyldur öryggisbrestur í skilningi laga nr. 90/2018*, sem veitandi starfænnar þjónustu ætti því að tilkynna um til Netöryggissveitarinnar *sem og* ábyrgðaraðila persónuupplýsinganna. Sé sá skilningur réttur, að sama atvik gæti verið tillkynningarskylt skv. tveimur lagabálkum og reglugerð, þá ætti að mati Sensa að taka tillit til þess í tilkynningareyðublöðum eftirlitsaðila, t.d. að spurt sé hvort atvikið sé jafnframt tilkynningarskylt skv. öðru regluverki og hvort það hafi verið tilkynnt *viðeigandi* aðila skv. kröfum þess regluverks (og þá hvaða aðila), enda gæti verið að það falli ekki í hlut veitanda stafrænnar þjónustu að tilkynna tilkynningarskylt atvik til Persónuverndar (heldur til ábyrgðaraðila sem svo tilkynnir eftir atvikum til Persónuverndar) þótt honum beri að tilkynna atvikið beint til Netöryggissveitarinnar skv. þessari reglugerð.

- *20. gr.*

Sensa lítur svo á að skv. 2. mgr. ákvæðisins gæti félagið þurft að tilkynna viðskiptavinum sínum um truflanir eða þjónusturof – ekki *endanotendum* þjónustunnar (einstaklingum).

III. Lokaorð

Til viðbótar framangreindum athugasemdum vill Sensa árétta þær athugasemdir sem komu fram í umsögn Símans hf., dags. 23. júní sl., fyrir hönd Símans hf. og

Sensa ehf. í tengslum við drög ráðuneytisins að reglugerð um öryggi net- og upplýsingakerfa mikilvægra innviða, einkum í tengslum við III.-VI. kafla þeirra draga.

Að öðru leyti er kallað eftir því að Netöryggissveitin birti leiðbeiningar sínar, skv. 19. gr. reglugerðarinnar, við fyrsta tækifæri.

(undirritað rafrænt)

f.h. Sensa,

Guðmundur Stefán Björnsson, öryggisstjóri