Umræðuskjal 1. desember 2016

Samningsviðauki vegna upplýsingaöryggis

Þessi texti er hugsaður sem leiðbeinandi skjal um samningsviðauka sem skerpir á þeim öryggiskröfum sem gerðar eru til hýsingaraðila, þjónustuaðila og hugbúnaðarhúsa. Hann er hugsaður fyrir alla samninga sem opinberir aðilar gera eða hafa gert við þjónustuaðila, hýsingaraðila og hugbúnaðarhús.

Ef sambærilegar kröfur eru nú þegar í þeim samningum sem gerðir hafa verið, þá munu strangari kröfurnar gilda. Þ.e.a.s. ef strangari ákvæði eru í upphaflegum samningi eða öðrum samningsviðaukum þá ber að fylgja þeim, en ef strangari ákvæði eru í þessum samningsviðauka þá bera að fylgja honum.

Þjónustuaðili skal ljúka innleiðingu á þeim kröfum sem fram koma í þessum samningsviðauka innan 12 mánaða frá undirritun ella áskilur verkkaupi/skipulagsheild sér rétt til að neyta úrræða vegna vanefnda sem kveðið er á um í lögum um samningsgerð, umboð og ógilda löggerninga nr. 7/1936.

Skilgreiningar

Viðskiptavinur: Sá opinberi aðili sem kaupir þjónustu af viðkomandi þjónustu- og/eða vinnsluaðila, s.s. hýsingaraðila eða hugbúnaðarhúsi.

Þjónustuaðili: Með orðinu „þjónustuaðili“ í þessum samningsviðauka er vísað til viðkomandi fyrirtækis sem veitir þjónustu, hýsingu eða hugbúnaðarhúss sem þróar þann hugbúnað sem það selur viðskiptavini.

Formlegt ferli: Þegar talað er um formlegt ferli, þá er átt við að búið sé að hanna og skjalfesta viðkomandi ferli og að unnið sé eftir því á rekjanlegan hátt.

Almennt

1. Stjórnkerfi upplýsingaöryggis

Þjónustuaðili skal innleiða stjórnkerfi upplýsingaöryggis byggt á upplýsingaöryggisstaðlinum ISO/IEC 27001 (ef hann hefur ekki þegar gert það). Eftirfarandi rekstrarþættir þjónustuaðila þurfa að vera innan stjórnkerfisins:

- Sú þjónusta sem þjónustuaðili veitir viðskiptavini.
- Innviðir þjónustuaðila (rekstur net- og upplýsingakerfa).
- Hugbúnaðarþróun (ef þjónustuaðili þróar hugbúnað sem hann selur viðskiptavini).

Ekki er nauðsynlegt að þjónustuaðili hafi fengið vottun á stjórnkerfinu, en mikilvægt er að innleiða alla eftirfarandi kafla í samningsviðaukanum.

1.1 Öryggisstefna

Þjónustuaðili skal hafa skjalfesta skriflega öryggisstefnu, sem er samþykkt af æðstu stjórnendum. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda til öryggismála. Við mótun öryggisstefnu skal taka mið af því hversu mikla vernd upplýsingar þurfi, hvernig skuli vernda þær og þeirri aðferð sem viðhöfð verður við vinnslu þeirra. Þessa öryggisstefnu skal rýna að lágmarki einu sinni á tveggja ára fresti á rekjanlegan hátt.

1.2 Ábyrgð á upplýsingaöryggi

Þjónustuaðili skal hafa öryggisstjóra og úthluta ábyrgð á þáttum tengdum upplýsingaöryggi til eins (eða fleiri aðila). Öryggisstjóri skal vera tengiliður viðskiptavinar vegna öryggisveikleika og öryggisatvika sem kunna að koma upp.

2. Áhættumat

Þjónustuaðili skal vinna eftir formlegu ferli við framkvæmd áhættumats. Þar skal meðal annars koma fram skilgreining á hvað teljist ásættanleg áhætta. Þjónustuaðili skal framkvæma áhættumat samkvæmt því verklagi að lágmarki einu sinni á ári þar sem sú þjónusta sem þjónustuaðili veitir viðskiptavini skal vera innan umfangs. Áhættumatið sjálft skal vera samþykkt formlega af æðstu stjórnendum þjónustuaðila á rekjanlegan hátt.

Í framhaldi af áhættumati skal þjónustuaðili gera skjalfesta áætlun um innleiðingu öryggisráðstafana fyrir þá áhættuþætti sem eru umfram ásættanlega áhættu. Ábyrgðaraðilum skal úthlutuð ábyrgð á öryggisráðstöfunum og skráðar skulu dagsetningar fyrir áætluð lok innleiðinga á úrbótum. Áætluninni skal fylgt eftir af æðstu stjórnendum þjónustuaðila. Viðskiptavinur má óska eftir upplýsingum úr áhættumati og áætlun um öryggisráðstafanir, bæði fyrir þá þætti er snúa beint að viðskiptavini sem og þá þætti er snúa óbeint að viðskiptavini (t.d. tengdum innviðum þjónustuaðila). Í áhættumati skal taka tillit til raunlægra áhættuþátta (e. Physical security), stafrænna þátta og mögulega annarra þátta.

Dæmi um áhættuþætti sem verður að taka tillit til: Gagnagísling (e. Cryptolocker) og raunlægt öryggi (e. Physical Security).
Dæmi um öryggisráðstafanir vegna gagnagíslingar: Applocker, tíð öryggisafritunartaka af gögnum og vírusvarnir.

3. Stjórnun aðgangs

Þjónustuaðili skal vinna eftir formlegu ferli við stjórnun aðgangs að kerfum og upplýsingum hjá þjónustuaðila. Þar skal meðal annars tekið fram hverjir geta óskað eftir stofnun, breytingu og lokun aðgangs. Ferlið skal vera samþykkt af stjórnendum, vera rekjanlegt og tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti.

Stjórnun aðgangs á innviðum þjónustuaðila skal vera innan umfangs hins formlega ferlis auk þess sem sú þjónusta sem viðskiptavinur kaupir af þjónustuaðila skal einnig vera innan umfangs ferlisins.

4. Öryggisuppfærslur

Þjónustuaðili skal vinna eftir formlegu ferli fyrir vöktun og uppsetningu á öryggisuppfærslum fyrir lykilhugbúnað, öll stýrikerfi og netbúnað. Þjónustuaðili skal setja inn mikilvægar (e. critical) öryggisuppfærslur innan án ónauðsynlegra tafa eftir að þær hafa verið gefnar út.

Aðrar öryggisuppfærslur skulu settar upp innan 90 daga frá því að þær eru gefnar út. Þjónustuaðili skal ekki notast við hugbúnað/stýrikerfi sem framleiðandi er hættur að styðja við með öryggisuppfærslum. Þjónustuaðili skal vakta stöðu öryggisuppfærslna á miðlurum og vinnustöðum. Innra eftirlit þjónustuaðila skal taka út stöðu öryggisuppfærslna að lágmarki einu sinni á ári.

5. Veikleikagreiningar og innbrotsprófanir

Þjónustuaðili skal vinna eftir formlegu ferli fyrir framkvæmd veikleikagreininga á net- og upplýsingakerfum. Þjónustuaðili skal framkvæma veikleikagreiningar á net- og upplýsingakerfum að lágmarki einu sinni á hverjum ársfjórðungi. Þjónustuaðili skal bregðast við þeim veikleikum sem finnast og koma þeim í úrbótaferli. Staða veikleikagreininga og úrbóta þeirra veikleika sem finnast skal tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti. Þjónusta sem þjónustuaðili veitir viðskiptavini og stoðkerfi þjónustuaðila skulu vera innan umfangs veikleikagreininga. Einnig skal þjónustuaðili framkvæma innbrotsprófanir að lágmarki einu sinni á tveggja ára fresti.

6. Innbrotsvöktunarkerfi (e. Intrusion Detection System / Intrusion Prevention System)

Þjónustuaðili skal koma á formlegu ferli fyrir tölvuinnbrotsvöktun og/eða fyrirbyggingu tölvuinnbrota (IDS/IPS). Þjónustuaðili skal vakta tölvuinnbrotsvöktunarkerfið sitt að lágmarki einu sinni á dag. Innbrotsvöktunarkerfið skal a.m.k. ná til innviða þjónustuaðila og þeirrar þjónustu sem þjónustuaðili er að selja viðskiptavini.

7. Frávikaskráning (e. Incident Management)

Þjónustuaðili skal vinna eftir formlegu ferli fyrir frávikaskráningu. Verklagið skal vera kynnt öllum starfsmönnum þjónustuaðila og skulu starfsmenn þjónustuaðila vera hvattir til að tilkynna öryggisfrávik sem og frávik frá verklagsreglum. Upplýsingum um frávik skal haldið til haga. Stjórnendur skulu reglulega fara yfir helstu frávik sem hafa verið tilkynnt og taka afstöðu til þess hvort bregðast þurfi við með úrbótum. Frávikaskráningarferlið skal tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti.

Ef öryggisatvik á sér stað sem getur mögulega haft áhrif á öryggi upplýsinga viðskiptavinar eða á þá þjónustu sem þjónustuaðili veitir viðskiptavini ber þjónustuaðila að tilkynna tengilið viðskiptavinar svo fljótt sem auðið er án ónauðsynlegrar tafar ásamt fyrirhuguðum viðbrögðum (ef einhver eru).

8. Innra eftirlit

Þjónustuaðili skal vinna eftir formlegu verklagi fyrir innra eftirlit þar sem lykilferli og verklagsreglur eru teknar út að lágmarki einu sinni á ári. Þessar úttektir skulu vera rekjanlegar og öll frávik sem finnast skulu vera skráð samkvæmt verklagsreglum um frávikaskráningar. Þau ferli sem tengjast þjónustu sem þjónustuaðili veitir viðskiptavini skulu vera innan umfangs verklags um innra eftirlit.

9. Heildrænt samstarf á sviði netöryggismála

Til að stuðla að heildrænu öryggi skal þjónustuaðili leggja áherslu á öryggishagsmuni viðskiptavina sinna og annarra utanaðkomandi aðila. Hann skal tafarlaust sinna beiðnum lögreglu í tengslum við netglæpi í samræmi við íslenska löggjöf. Sama gildir um tilmæli

netöryggissveitarinnar CERT-ÍS um virkt samstarf og viðbrögð við einstökum öryggisatvikum, alvarlegri netvá og viðvarandi háþróuðum ógnum (e. APT).
Viðskiptaskilmálar allra viðskiptavina skulu innihalda virkar tengiliðaupplýsingar. Þjónustuaðilinn skal fylgja tilmælum netöryggissveitarinnar CERT-ÍS hverju sinni um ákvæði þjónustusamninga.

Þjónustuaðilinn skal leggja áherslu á heildrænt öryggissamstarf í höfuð- og öryggisstefnu sinni, með virku samstarfi við lögreglu og netöryggissveitina CERT-ÍS að því marki sem heimilt er samkvæmt íslenskum lögum.

Starfsmenn og verktakar

10. Ráðningar starfsmanna og verktaka

Þjónustuaðili skal vinna eftir formlegu ferli við ráðningar starfsmanna og verktaka. Bakgrunnsskoðun umsækjenda skal vera hluti ráðningarferlis vegna starfa við rekstur net- og upplýsingakerfa. Einnig skal afla sömu upplýsinga varðandiir þá verktaka sem ráðnir eru og munu fá aðgang að innviðum þjónustuaðila, upplýsingum viðskiptavinar eða fá aðgang að þeirri þjónustu sem þjónustuaðili veitir. Sem hluti af bakgrunnsskoðun skal:

- Staðfesta menntun viðkomandi.
- Fá afrit af sakarvottorði viðkomandi.
- Athuga fjárhagslegt hæfi viðkomandi.
- Hafa samband við að minnsta kosti tvo meðmælendur / fyrri atvinnuveitendur.

11. Trúnaðaryfirlýsingar (e. Confidentiality or Non-Disclosure Agreements)

Allir starfsmenn og verktakar þjónustuaðila sem hafa aðgang að trúnaðarupplýsingum, viðkvæmum persónuupplýsingum, þróun kerfa eða koma að rekstri neta eða upplýsingakerfa skulu undirrita sérstaka trúnaðaryfirlýsingu / þagnarskylduyfirlýsingu.

12. Þjálfun starfsmanna og verktaka

Þjónustuaðili skal stuðla að bættri öryggisvitund starfsmanna sinna og verktaka með reglulegum námskeiðum og/eða starfsmannaþjálfun þar sem fjallað er um helstu þætti er tengjast upplýsingaöryggi. Æskilegt er að starfsmenn sæki slíkt námskeið að lágmarki einu sinni á ári.

13. Starfslok

Þjónustuaðili skal koma á formlegu ferli um starfslok. Skilgreina skal verklag um lokun (og mögulega eyðingu) aðgangs þeirra starfsmanna og verktaka sem hætta störfum hjá þjónustuaðila.

Skýrslugjöf og eftirlit

14. Skýrslugjöf

Þjónustuaðili skal skila viðskiptavini skýrslu að lágmarki einu sinni á ári með upplýsingum um niðurstöður innra eftirlits á þeim þáttum sem koma fram í þessum samningsviðauka. Þar skal koma fram fjöldi frávika sem fundust og til hvaða öryggisráðstafana hefur verið gripið (eins og við á).

15. Eftirlit

Þjónustuaðili samþykkir að veita viðskiptvini aðgang að gögnum og upplýsingakerfum til að framkvæma úttektir á stöðu þeirra ferla sem koma fram í þessum samningsviðauka óski viðskiptavinur eftir því. Þetta á t.d. við um innri- og ytri endurskoðendur viðskiptvinar sem og öryggisstjóra og / eða öryggisteymi.

Þjónustuaðili samþykkir einnig að veita eftirlitsaðilum s.s. ríkisendurskoðanda, lögreglu, fjármálaeftirlitinu og örðum eftirlitsaðilum aðgang að gögnum og upplýsingakerfum sínum ef þau óska eftir því í tengslum við rannsókn á / hjá viðskiptavini að fengnu samþykki viðskiptavinar.

Rekstur

16. Breytingastjórnun

Þjónustuaðili skal vinna eftir formlegu ferli fyrir breytingastjórnun vegna meiriháttar breytinga. Í því ferli skal koma fram hver þarf að samþykkja breytingar, hverju stendur til að breyta, hvenær fyrirhuguð breyting mun eiga sér stað, hver er áætlaður tími sem fer í breytingarnar og/eða mögulegan tíma sem þjónusta liggur niðri, hverjir munu framkvæma viðkomandi breytingu, hvernig verði brugðist við ef breyting mistekst (t.d. ef endurheimta þarf kerfi frá öryggisafriti), hversu mikill tími fer í að hætta við breytingar, t.d. ef endurheimta þarf kerfi (komi fram villur) og hvernig breytingar verða prófaðar. Ferlið skal vera tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti.

Ef fyrirhugaðar breytingar kunna að geta valdið rekstrartruflunum fyrir viðskiptavin þá skal láta viðskiptavin vita með a.m.k. 48 klst. fyrirvara og honum gefinn kostur á óska eftir því að uppfærslu sé frestað ef tími breytinga hentar viðkomandi viðskiptavini illa (t.d. í kringum mánaðarmót).

17. Öryggisafritunartaka (e. Backup)

Þjónustuaðili skal vinna eftir formlegu ferli fyrir öryggisafritunartöku og endurheimt upplýsingakerfa og gagna. Þetta verklag skal vera samþykkt formlega og á sannanlegan hátt af æðstu stjórnendum. Umfang öryggisafritunartöku skal vera bæði fyrir innviði þjónustuaðila og fyrir þau gögn sem þjónustuaðili geymir fyrir viðskiptavin, þau kerfi og upplýsingar sem þjónustuaðili rekur og hýsir í tengslum við þá þjónustu sem hann veitir viðskiptavini. Þjónustuaðili skal prófa endurheimt lykilupplýsingakerfa að lágmarki einu sinni á ári á rekjanlegan hátt.

18. Áætlun um samfelldan rekstur

Þjónustuaðili skal vinna eftir formlegu ferli fyrir samfelldan rekstur sem byggir á bestu starfsvenjum og alþjóðlegum stöðlum. Þjónustuaðili skal kortleggja viðbrögð við helstu áhættuþáttum sem gætu valdið rekstrarrofi / rofi í rekstri og forgangsraða endurheimt kerfa og gagna. Prófa skal áætlun um samfelldan rekstur að lágmarki einu sinni á ári á rekjanlegan hátt. Sú þjónusta sem þjónustuaðili veitir viðskiptavini skal vera innan umfangs áætlunarinnar.

18.1 Áætlun um stóráföll (e. Crisis Management Plan)

Þjónustuaðili skal taka tillit til mögulegra stóráfalla í áætlun um samfelldan rekstur eða útbúa sérstaka viðbragðsáætlun vegna stóráfalla. Áætlunin skal ná til þjónustu, sem þjónustuaðili veitir viðskiptaviniog innviða þjónustuaðila. Kynna skal viðskiptavini áætlaðan endurheimtutíma og hámarks endurheimtutíma fyrir þau kerfi og þá þjónustu sem þjónustuaðili veitir.

18.2 Uppfærsla á áætlun um samfelldan rekstur

Í hvert skipti sem áætlun um samfelldan rekstur og stóráföll er uppfærð, og slík uppfærsla getur haft áhrif á áætlaðan endurheimtutíma eða hámarks endurheimtutíma í tengslum við þá þjónustu sem þjónustuaðili veitir viðskiptavini, þá skal þjónustuaðili tilkynna viðskiptavini um það formlega og óska eftir staðfestingu á móttöku tilkynningarinnar frá tengilið viðskiptavinar.

19. Viðbragðsáætlun fyrir öryggisatvik (e. Incident Response Plan)

Þjónustuaðili skal skjalfesta og koma á/vinna eftir formlegu ferli fyrir viðbragðsáætlun vegna öryggisatvika (t.d. tölvuinnbrots). Ef öryggisatvik á sér stað sem er annað hvort beintengt þeirri þjónustu sem þjónustuaðili veitir viðskiptavini eða ef öryggisatvik á sér stað í innviðum þjónustuaðila og getur þ.a.l. á óbeinan hátt haft áhrif á veitta þjónustu hans eða tengist viðkvæmum upplýsingum viðskiptavinar, þá ber þjónustuaðila að tilkynna viðskiptavini um öryggisbrestinn án ástæðulausrar tafar. Í framhaldi skal þjónustuaðili halda viðskiptavini upplýstum á meðan unnið er að úrbótum.

Hugbúnaðarþróun

Eftirfarandi þættir eiga við um þá þjónustuaðila sem þróa hugbúnað sem þeir selja viðskiptavini. Þetta á við bæði þegar þjónustuaðili selur hugbúnað til viðskiptavinar sem og þegar þjónustuaðili selur viðskiptavini aðgang að hugbúnaði / þjónustu sem þjónustuaðilinn þróar sjálfur.

20. Hugbúnaðarþróunarferli

Þjónustuaðili skal tryggja að a.m.k. einn forritari hafi hlotið þjálfun í öruggri hugbúnaðarþróun og allir starfsmenn hans sem að verkefninu koma séu meðvitaðir um öryggiskröfur til verkefnisins.

Sá hugbúnaður sem þróaður er af þjónustuaðila skal styðja dulkóðaðar gagnasendingar innan kerfis/milli kerfa. Þegar við á sér verkkaupi um að útvega/kaupa skilríki til að tryggja öryggi samskipta.

20.1 Breytingastjórnun í hugbúnaðarþróun

Þjónustuaðili skal vinna eftir formlegu ferli fyrir breytingastjórnun vegna meiriháttar breytinga sem þjónustukaupi óskar eftir. Í því ferli skal koma fram hver þarf að samþykkja breytingar, hverju stendur til að breyta, hvenær fyrirhuguð breyting mun eiga sér stað, hver er áætlaður tími sem fer í breytingarnar og/eða mögulegan tíma sem þjónusta liggur niðri, hverjir munu framkvæma viðkomandi breytingu, hvernig verði brugðist við ef breyting mistekst (t.d. ef endurheimta þarf kerfi frá öryggisafriti), hversu mikill tími fer í að hætta við breytingar, t.d. ef endurheimta þarf kerfi (komi fram villur) og hvernig breytingar verða prófaðar. Ferlið skal vera tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti.

Ef fyrirhugaðar breytingar kunna að geta valdið rekstrartruflunum fyrir viðskiptavin þá skal láta viðskiptavin vita með a.m.k. 48 klst. fyrirvara og honum gefin kostur á óska eftir því að uppfærslu sé frestað ef tími breytinga hentar viðkomandi viðskiptavini illa.

20.2 Tilkynning á öryggisveikleikum sem finnast

Þegar öryggisgallar finnast í hugbúnaði sem þjónustuaðili hefur selt viðskiptavini eða selt viðskiptavini aðgang að þá skal þjónustuaðili tilkynna tengilið viðskiptavinar um öryggisveikleikann svo fljótt sem auðið er án ónauðsynlegrar tafar ásamt fyrirhuguðum viðbrögðum (ef einhver eru) og leiðbeiningum um hvernig hægt sé að lágmarka eða fyrirbyggja áhættu tengda öryggisveikleikanum. Þjónustuaðili skal upplýsa viðskiptavin um viðbrögð og lagfæringar sem gerðar verða til að lagfæra gallann og öryggisuppfærslur skulu vera aðgengilegar eins fljótt og auðið er.

Þjónustuaðili skal koma á útgáfustýringu á hugbúnaði sínum þannig að einfalt sé að gefa út öryggisuppfærslur fyrir gamlar útgáfur af hugbúnaðinum. Þannig getur þjónustuaðili gefið út öryggisuppfærslur fyrir viðskiptavini þeim að kostnaðarlausu án þess að viðskiptavinur þurfi að uppfæra í nýjustu útgáfu hugbúnaðarins.

Persónuvernd

Eftirfarandi þættir eiga við um þá þjónustuaðila sem er falið að vinna eða varðveita persónuupplýsingar fyrir hönd viðskiptavinar. Þetta á bæði við þegar þjónustuaðili hýsir persónuupplýsingar fyrir viðskiptavin eða vinnur þær á annan hátt fyrir viðskiptavin m.a. í tengslum við rekstur upplýsingakerfa eða hugbúnaðar.

21. Vinnslusamningur

Í lögum nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, eru persónuupplýsingar skilgreindar sem sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi.

Með hugtakinu „vinnsla“ er átt við sérhverja aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn, sbr. 2. tölul. 2. gr. laga nr. 77/2000. Vinnsluhugtakið er mjög rúmt og nær m.a. til söfnunar, skráningar, kerfisbindingar, miðlunar, aðlögunar eða breytingar, leitar, notkunar, miðlunar með framsendingu, samtengingar eða samkeyrslu, afmáunar, eyðileggingar og varðveislu persónuupplýsinga.

21.1 Vinnslusamningur

Viðskiptavini, ábyrgðaraðila eins og hann er nefndur, er heimilt samkvæmt 13. gr. persónuverndarlaga að semja við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á samkvæmt ákvæðum laga þessara. Slíkt er þó háð því skilyrði að ábyrgðaraðili hafi áður sannreynt að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir og viðhaft innra eftirlit skv. 12. gr. laga þessara.

Viðskiptavinur sem felur þjónustuaðila að hýsa persónuupplýsingar fyrir sína hönd, eða vinna þær að öðru leyti, ber ábyrgð á að samið verði við þjónustuaðila um vinnslu persónuupplýsinga þannig að samrýmist kröfum 13. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga.

Þjónustuaðila skal ekki vinna persónuupplýsingar fyrir viðskiptavin umfram það sem um hefur verið samið í vinnslusamningi. Ef þjónustuaðili veit til þess að vinnsla persónuupplýsinga fari fram án þess að vinnslusamningur hafi verið gerður ber að láta viðskiptavin vita af slíkri vinnslu án tafar. Að sama skapi skal þjónustuaðili upplýsa viðskiptavin án tafar ef fram fer vinnsla persónuupplýsinga sem rúmast ekki innan umfangs gildandi vinnslusamnings.

21.2 Öryggi persónuupplýsinga

Þjónustuaðili skal skjalfesta upplýsingaöryggi vegna vinnslu persónuupplýsinga í starfsemi sinni í samræmi við reglur nr. 299/2001, um öryggi persónuupplýsinga. Í því felst að þjónustuaðili skal setja sér skriflega öryggisstefnu, gera skriflegt áhættumat og skrásetja viðeigandi öryggisráðstafanir.

Þjónustuaðili skal tryggja að vinnsla persónuupplýsinga í starfsemi hans sé í samræmi við lög, reglur og eftir atvikum fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi persónuupplýsinga.

21.3 Lagabreytingar

Vakin er athygli á að ný Evrópureglugerð um persónuvernd hefur verið samþykkt. Áætlað er að hún verði innleidd í íslensk lög í maí 2018. Þjónustuaðili skuldbindur sig til að vakta þær skyldur sem á hann eru lagðar með hinni nýju reglugerð. Að sama skapi skuldbindur viðskiptavinur sig til að vakta þær skyldur sem á hann eru lagðar með reglugerðinni.