LEIÐBEININGAR
- RAUNHÆF DÆMI UM ÖRYGGISBRESTI -

Almennt

Meðal þeirra skyldna sem hvíla á ábyrgðaraðilum samkvæmt persónuverndarlögum er að bregðast við öryggisbrestum á viðeigandi hátt. Í því getur meðal annars falist að tilkynna þurfi um öryggisbrest til Persónuverndar og, eftir atvikum, til þess sem persónuupplýsingarnar varða.

Til að aðstoða ábyrgðaraðila við að uppfylla skyldur sínar voru í febrúar 2018 gefnar út leiðbeiningar um tilkynningar um öryggisbresti sem nálgast má á vefsíðu Persónuverndar. Var þar byggt á leiðbeiningum sem gefnar höfðu verið út á samevrópskum vettvangi skömmu áður vegna gildistöku nýrrar persónuverndarlöggjafar síðar á árinu. Evrópska persónuverndarráðið hefur nú veitt færi á umsögnum við nýjar leiðbeiningar með raunhæfum dæmum til að aðstoða ábyrgðaraðila við að meta hvenær nauðsynlegt er að tilkynna öryggisbrest til Persónuverndar og hvenær nauðsynlegt er að tilkynna öryggisbrest til hins skráða.

Einnig má nálgast almennar upplýsingar um öryggisbresti, svo sem um hvað öryggisbrestur er og hvenær ábyrgðaraðili telst hafa orðið var við öryggisbrest, á vefsíðu Persónuverndar.

Hér á eftir eru rakin þau raunhæfu dæmi um öryggisbresti, sem fram koma í fyrrnefndum leiðbeiningum Evrópska Persónuverndarráðsins. Þá er því lýst hvernig bregðast ætti við hverjum þeirra og einum.

Gíslatökubúnaður (e. ransomware)

Dæmi 1

Tölvuþrjótar komast í gögn hjá framleiðslufyrirtæki og halda þeim í gíslingu. Öll gögnin eru dulkóðuð og tölvuþrjótarnir fá ekki aðgang að dulkóðunarlykli og hafa enga möguleika á að afkóða gögnin. Bresturinn hefur eingöngu áhrif á fámennan hóp viðskiptavina og starfsmanna. Afrit er til af öllum gögnum og gögnin verða tiltæk örfáum klukkustundum eftir árásina sem hefur ekki áhrif á daglegan rekstur fyrirtækisins, svo sem launagreiðslur til starfsmanna og afgreiðslu pantana frá viðskiptavinum.

Í þessu tilviki eru áhætta og afleiðingar af öryggisbrestinum minni háttar þar sem persónugreinanlegar upplýsingar urðu ekki aðgengilegar og upplýsingar urðu tiltækar aftur á skömmum tíma, auk þess sem bresturinn hafði ekki áhrif á daglegan rekstur ábyrgðaraðila eða á hina skráðu. Hér ætti ábyrgðaraðili að skrá öryggisbrestinn innanhúss, en ekki þarf að tilkynna hann til Persónuverndar eða til hinna skráðu.

Innri skráning: **X**

Tilkynning til Persónuverndar: **0**

Tilkynning til hinna skráðu: **0**

Dæmi 2

Tölvuþrjótar komast í gögn hjá fyrirtæki sem selur landbúnaðarvörur og halda þeim í gíslingu. Öll gögnin eru dulkóðuð og tölvuþrjótarnir fá ekki aðgang að dulkóðunarlykli og hafa enga möguleika á að afkóða gögnin. Bresturinn hefur eingöngu áhrif á fámennan hóp viðskiptavina og starfsmanna og ekki er um að ræða viðkvæmar persónuupplýsingar. Afrit af meirihluta gagnanna er til á pappírsformi og tekur fimm vinnudaga að koma þeim á tölvutækt form. Öryggisbresturinn leiðir til minniháttar tafa á afhendingu pantana til viðskiptavina.

Í þessu tilviki eru áhætta og afleiðingar af öryggisbrestinum minni háttar þar sem persónugreinanlegar upplýsingar urðu ekki aðgengilegar. Nauðsynlegt er að tilkynna brestinn til Persónuverndar þar sem umtalsverðan tíma tekur að gera gögnin tiltæk á nýjan leik, auk þess sem hann leiðir til röskunar á daglegum rekstri fyrirtækisins og þess að töluvert magn lýsigagna (e. meta-data) hefur tapast. Ekki er nauðsynlegt að tilkynna hinum skráðu um öryggisbrestinn þar sem ólíklegt er að hann leiði af sér mikla áhættu fyrir réttindi þeirra og frelsi.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **0**

Dæmi 3

Tölvuþrjótar komast í gögn hjá heilbrigðisstofnun og halda þeim í gíslingu. Öll gögnin eru dulkóðuð og tölvuþrjótarnir fá ekki aðgang að dulkóðunarlykli og hafa enga möguleika á að afkóða gögnin.

Ábyrgðaraðilinn notast við utanaðkomandi sérfræðiaðstoð og hefur nokkra vissu fyrir því að eingöngu hafi verið sótt dulkóðuð gögn sem ekki er mögulegt að afkóða. Bresturinn hefur áhrif á stóran hóp starfsmanna og sjúklinga. Afrit eru til á rafrænu formi og verða gögnin að mestu leyti tiltæk innan tveggja vinnudaga frá því að bresturinn verður. Bresturinn hefur mikil áhrif á starfsemi stofnunarinnar og leiðir til verulegra tafa í meðhöndlun sjúklinga. Þá hefur bresturinn það í för með sér að stofnunin þarf að hætta við og fresta skurðaðgerðum og lækka þjónustustig sitt.

Í þessu tilviki hefur orðið brestur á öryggi viðkvæmra persónuupplýsinga (upplýsinga um heilsufar) sem ekki eru tiltækar vegna brestsins, auk þess sem veruleg röskun verður á starfsemi viðkomandi heilbrigðisstofnunar. Hér er nauðsynlegt er að senda tilkynningu til Persónuverndar. Þá er líklegt að öryggisbresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi hinna skráðu og er því nauðsynlegt að tilkynna um brestinn beint til þeirra sjúklinga sem bresturinn hefur áhrif á, svo sem þeirra sem þáðu heilbrigðisþjónustu hjá heilbrigðisstofnuninni á meðan gögnin voru ekki aðgengileg. Auk þess ætti að upplýsa sem persónuupplýsingarnar varða á almennan hátt, svo sem með yfirlýsingu sem birt er um öryggisbrestinn.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Dæmi 4

Tölvuþrjótar komast í gögn hjá opinberu samgöngufyrirtæki. Öll gögnin eru dulkóðuð, en eftir innri rannsókn uppgötvast að tölvuþrjótunum hefur tekist að afkóða gögnin. Um er að ræða persónuupplýsingar um viðskiptavini, starfsmenn ábyrgðaraðila og þá sem hafa nýtt sér þjónustu fyrirtækisins, svo sem með því að kaupa farmiða á netinu. Auk almennra tengiliðaupplýsinga er meðal annars um að ræða fjárhagsupplýsingar, svo sem um kreditkortanúmer. Afrit eru til af öllum gögnum, en þeim er einnig haldið í gíslingu af tölvuþrjótunum.

Í því tilviki sem hér um ræðir er líklegt að meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi hinna skráðu. Hér er því nauðsynlegt að þeim sé tilkynnt um öryggisbrestinn svo að þeir geti gripið til ráðstafana vegna hans, svo sem að loka kreditkortum. Tilkynna ætti einstaklingunum beint um brestinn þegar það reynist unnt, en jafnframt ætti að tilkynna um hann almennt, svo sem með fréttatilkynningu á vefsíðu fyrirtækisins, svo að tryggt sé tilkynningar berist einnig til þeirra sem það er ekki með tengiliðaupplýsingar um. Þá ætti að tilkynna um öryggisbrestinn til Persónuverndar og skrá hann innanhúss.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Gagnastuldur (e. Data exfiltration attacks)

Dæmi 5

Ráðningarskrifstofa verður fyrir tölvuárás þar sem búnaði er komið fyrir á vefsíðu hennar. Búnaðurinn verður þess valdandi að upplýsingar sem skrifstofunni hafa borist um vefsíðuna, svo sem starfsumsóknir, verða aðgengilegar óviðkomandi. Talið er að öryggisbresturinn nái til 213 starfsumsókna, en eftir skoðun á innihaldi þeirra er komist að þeirri niðurstöðu að ekki sé um að ræða viðkvæmar persónuupplýsingar. Búnaðurinn veitir aðgang að persónuupplýsingum sem sendar hafa verið skrifstofunni í gegnum vefsíðu hennar, auk þess sem hann gefur kost á eftirliti með vefþjóni og þurrkar búnaðurinn út sjálfkrafa hvaða upplýsingum veittur er aðgangur að.

Í þessu tilviki þarf að meta umfang og eðli þeirra upplýsinga sem um ræðir. Þótt þær séu ekki viðkvæmar getur umfang þeirra, svo og möguleikinn á að misnota þær til meðal annars auðkennisþjófnaðar, gert það líklegt að bresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi hinna skráðu. Þeim ætti því að vera tilkynnt um öryggisbrestinn. Jafnframt ætti að tilkynna um hann til Persónuverndar og skrá hann innanhúss.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Dæmi 6

Tölvuþrjótar nýta sér veikleika í tölvukerfi til að fá aðgang að gagnagrunni uppskriftasíðu. Notendur hafa valið sér handahófskennd notendanöfn fyrir síðuna, en þeim hafði verið ráðlagt að notast ekki við tölvupóstföng. Lykilorð eru varðveitt með tætiaðferð (e. hashed) og tölvuþrjótarnir fá ekki aðgang að slembigildinu (e. salt).

Í þessu tilviki er ekki um að ræða viðkvæmar persónuupplýsingar eða tengiliðaupplýsingar um hina skráðu, svo sem símanúmer eða netföng, en þó kann vera unnt að rekja sum notendanafnanna til hlutaðeigandi einstaklinga. Það að lykilorðin voru geymd með tætiaðferð dregur úr hættueiginleikum og umfangi þeirra upplýsinga sem bresturinn hefur áhrif á. Er því ólíklegt að hann hafi áhrif á réttindi og frelsi einstaklinga og ekki er um að ræða tilvik þar sem skylt er að tilkynna Persónuvernd eða hinum skráðu um brestinn. Slík tilkynning til hinna skráðu getur þó verið æskileg svo að hægt sé að draga úr mögulegum neikvæðum afleiðingum af öryggisbrestinum. Skylt er þó að að skrá öryggisbrestinn innanhúss.

Innri skráning: **X**

Tilkynning til Persónuverndar: **0**

Tilkynning til hinna skráðu: **0**

Dæmi 7

Heimabanki viðskiptabanka verður fyrir tölvuárás, en markmið hennar er að afla notendanafna viðskiptavina bankans með því að slá inn handahófskennt, veikt, átta tölustafa lykilorð. Vegna veikleika á vefsíðunni opnast við þetta aðgangur að persónugreinum upplýsingumum viðskiptavini, svo sem um nafn, kyn og kennitölu, og það jafnvel þegar lykilorðið samsvarar ekki því sem úthlutað hefur verið vegna viðkomandi bankareiknings og jafnvel þegar bankareikningur er ekki lengur virkur. Samtals hefur bresturinn áhrif á um 100.000 viðskiptavini bankans og af þeim um 2.000 sem aðgangur opnast að heimabanka hjá og sem notuðust við sama lykilorð og tölvuþrjóturinn sló inn. Að árásinni lokinni tekst bankanum að bera kennsl á allar óheimilar innskráningartiltraunir og fær það staðfest að engar óheimilar millifærslur hafi verið framkvæmdar meðan á árásinni stóð. Bankinn tók eftir árásinni vegna mikils fjölda innskráningartilrauna og lokaði vefsíðunni tímabundið og endurstillti lykilorð þeirra viðskiptavina sem voru með sama lykilorð og notast var við í árásinni.

Í þessu tilviki voru persónuupplýsingar gerðar aðgengilegar og aukin hætta á að viðskiptavinir bankans verði fyrir auðkennisþjófnaði , auk þess sem viðkomandi fékk upplýsingar um lykilorð tiltekins fjölda einstaklinga að heimabanka sínum. Af því leiðir að líklegt er að öryggisbresturinn hafi í för með sér sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Bankanum er því skylt að skrá öryggisbrestinn innanhúss og ber jafnframt að tilkynna hann til bæði Persónuverndar og allra þeirra 100.000 einstaklinga sem bresturinn hefur áhrif á.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Öryggisbrestir vegna mannlegra mistaka

Dæmi 8

Starfsmaður í uppsagnarfresti hjá tilteknu fyrirtæki afritar upplýsingar úr gagnagrunni þess sem honum er heimill aðgangur að og honum eru nauðsynlegar til að sinna starfi sínu. Nokkrum mánuðum seinna, eftir að hann hefur hafið störf annars staðar, notar hann upplýsingarnar (tengiliðaupplýsingar) til að hafa samband við viðskiptavini fyrrum vinnuveitanda til að fá þá til að færa viðskipti sín til núverandi vinnuveitanda.

Í þessu tilviki er ekki líklegt að meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga og því líklega ekki nauðsynlegt að tilkynna um öryggisbrestinn til hinna skráðu. Nauðsynlegt er þó að tilkynna um brestinn til Persónuverndar og að skrá brestinn innanhúss.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **0**

Dæmi 9

Tryggingaáðgjafi tekur eftir því að Excel-skjal sem hann fékk sent í tölvupósti frá ábyrgðaraðila, inniheldur upplýsingar um rúmlega 20 viðskiptavini sem hann átti ekki að fá upplýsingar um. Hann er bundinn þagnarskyldu og er eini viðtakandi tölvupóstsins. Samningur ábyrgðaraðila og tryggingafélagsins tilgreinir að upplýsa eigi um slíka öryggisbresti til ábyrgðaraðila án tafar. Tryggingaáðgjafinn lætur vita um leið og hann áttaði sig á mistökunum. Ábyrgðaraðili leiðréttir Excel-skjalið og sendir það aftur á tryggingaráðgjafann og óskar eftir því að fyrri tölvupósti verði eytt. Tölvupóstinum er eytt og það staðfest með skriflegri yfirlýsingu. Ekki var um að ræða viðkvæmar persónuupplýsingar heldur einungis tengiliðaupplýsingar og upplýsingar um tryggingu sem viðkomandi einstaklingar hafa tekið, svo sem tegund tryggingar og upphæð iðgjalda.

Í þessu tilviki er um að ræða persónuupplýsingar um fámennan hóp. Ekki er um að ræða viðkvæmar persónuupplýsingar og upplýsingarnar hafa einungis verið sendar einum viðtakanda sem bundinn er þagnarskyldu, tilkynnti ábyrgðaraðila um öryggisbrestinn um leið og hann uppgötvaðist og eyddi tölvupóstinum eftir að þess var óskað. Í ljósi eðlis öryggisbrestsins og þeirra aðgerða sem gripið var til í kjölfar hans þá má þykja það ólíklegt að hann leiði til áhættu fyrir réttindi og frelsi einstaklinga. Nauðsynlegt er að skrá brestinn innanhúss, en ekki er nauðsynlegt að tilkynna hann til Persónuverndar eða til hinna skráðu.

Innri skráning: **X**

Tilkynning til Persónuverndar: **0**

Tilkynning til hinna skráðu: **0**

Týndur eða stolinn búnaður eða gögn

Dæmi 10

Brotist er inn í leikskóla og tveimur spjaldtölvum stolið. Í spjaldtölvunum er smáforrit með persónuupplýsingum um börn sem skráð eru í leikskólann, svo sem nöfn, fæðingardag og um skólagöngu barnanna. Slökkt er á báðum spjaldtölvunum, þær dulkóðaðar og smáforritið læst með sterku lykilorði, auk þess sem aðgengileg afrit eru til af öllum gögnum. Þegar skólinn uppgötvar innbrotið getur hann eytt öllum upplýsingum af spjaldtölvunum.

Í þessu tilviki er ólíklegt að innbrotið leiði til þess að óviðkomandi fái aðgang að persónuupplýsingum og þar sem afrit eru til staðar er nauðsynlegt aðgengi að upplýsingunum ekki skert. Í ljósi eðlis öryggisbrestsins og þeirra aðgerða sem gripið var til í kjölfar hans þá má þykja það ólíklegt að hann leiði til áhættu fyrir réttindi og frelsi einstaklinga. Nauðsynlegt er að skrá brestinn innanhúss, en ekki er nauðsynlegt að tilkynna hann til Persónuverndar eða til hinna skráðu.

Innri skráning: **X**

Tilkynning til Persónuverndar: **0**

Tilkynning til hinna skráðu: **0**

Dæmi 11

Spjaldtölvu starfsmanns þjónustufyrirtækis er stolið. Spjaldtölvan inniheldur upplýsingar um nafn, kyn, heimilisfang og fæðingardag um 100.000 viðskiptavina fyrirtækisins. Ekki er hægt að staðreyna hvort aðrar tegundir persónuupplýsinga séu einnig á spjaldtölvunni, en ljóst er þó að ekki er um að ræða viðkvæmar persónuupplýsingar. Spjaldtölvan er ekki læst með lykilorði. Afrit hefur verið tekið af upplýsingum daglega og aðgengi að þeim er ekki skert.

Í þessu tilviki getur öryggisbresturinn leitt til hættu á að hinir skráðu verði fyrir auðkennisþjófnaði. Er því líklegt að öryggisbresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Fyrirtækinu er því skylt að skrá öryggisbrestinn innanhúss og ber jafnframt að tilkynna hann til bæði Persónuverndar og allra þeirra 100.000 einstaklinga sem hann hefur áhrif á.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Dæmi 12

Stílabók er stolið á sjúkrahúsi sem sérhæfir sig í meðferð fíknsjúkdóma. Bókin inniheldur persónuupplýsingar um sjúklinga sjúkrahússins, þ. á m. heilbrigðisupplýsingar. Upplýsingarnar voru eingöngu skráðar í stílabókina og afrit er ekki til staðar fyrir þá lækna sem sinna sjúklingunum. Bókin var ekki varðveitt í læstri hirslu eða á læstri skrifstofu og ekki eru til staðar aðgangsstýringar eða annars konar skipulagslegar öryggisráðstafanir til að tryggja öryggi pappírsgagna.

Í þessu tilviki fékk óviðkomandi aðgang að persónuupplýsingum um sjúklinga, þ. á m. heilbrigðisupplýsingum, auk þess sem aðgengi að þeim skertist. Er því líklegt að öryggisbresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Sjúkrahúsinu er því skylt að skrá öryggisbrestinn innanhúss og ber því jafnframt að tilkynna bæði Persónuvernd og hinum skráðu um öryggisbrestinn.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Öryggisbrestir við póstsendingar

Dæmi 13

Tvær pantanir á skóm eru sendar röngum viðtakendum þannig að tveir viðskiptavinir fá pantanir og reikninga hvor annars. Þegar ábyrgðaraðilanum verður ljóst að mistök hafi átt sér stað innkallar hann póstsendingarnar og sendir þær á rétta viðtakendur.

Í þessu tilviki er ólíklegt að bresturinn leiði til áhættu fyrir réttindi og frelsi hinna skráðu og því ekki skylt að tilkynna hinum skráðu um brestinn. Tiltekin samskipti við hina skráðu eru þó óhjákvæmileg þar sem nauðsynlegt er að óska eftir því að þeir eyði þeim persónuupplýsingum sem áttu ekki að berast til þeirra svo að hægt sé að draga úr mögulegum neikvæðum afleiðingum af öryggisbrestinum. Ekki er nauðsynlegt að tilkynna hann til Persónuverndar, en skrá þarf hann innanhúss.

Innri skráning: **X**

Tilkynning til Persónuverndar: **0**

Tilkynning til hinna skráðu: **0**

Dæmi 14

Mannauðsdeild opinberar stofnunar sendir upplýsingar um námskeið til þeirra sem skráðir eru í virkri atvinnuleit. Vegna mannlegra mistaka er skjal sent í viðhengi sem inniheldur upplýsingar um nöfn, tölvupóst, heimilisföng og kennitölur framangreindra einstaklinga sem samtals eru um 60.000 talsins. Í kjölfar öryggisbrestsins hefur stofnunin samband við viðtakendur og óskar eftir að tölvupóstinum verði eytt og að upplýsingar í honum verði ekki unnar á nokkurn hátt.

Í þessu tilviki er líklegt að öryggisbresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga, bæði vegna eðlis upplýsinganna sem um ræðir og fjölda viðtakenda. Stofnuninni er því skylt að skrá öryggisbrestinn innanhúss og ber jafnframt að tilkynna hann til bæði Persónuverndar og allra þeirra 60.000 einstaklinga sem bresturinn hafði áhrif á.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Dæmi 15

Listi yfir þátttakendur í fimm daga námskeiði, sem átti að vera sendur á hótel þar sem námskeiðið á að fara fram, er fyrir mistök sendur á 15 fyrrum þátttakendur í námskeiðinu. Listinn inniheldur upplýsingar um nöfn, tölvupóstfang, heimilisföng og séróskir um mataræði tveggja þátttakenda sem eru með mjólkuróþol. Námskeiðshaldari áttar sig samstundis á mistökunum, hefur samband við viðtakendur og óskar eftir því að þeir eyði listanum.

Í þessu tilviki er um að ræða lítið umfang persónuupplýsinga sem sendar eru á afmarkaðan hóp einstaklinga. Jafnvel þótt upplýsingar um mjólkuróþol séu upplýsingar um heilsufar viðkomandi, og þar með viðkvæmar persónuupplýsingar, er ósennilegt að hægt sé að nota þær á slíkan hátt að til mikillar áhættu fyrir réttindi og frelsi hinna skráðu komi. Þá eru aðgerðir ábyrgðaraðila í kjölfar öryggisbrestsins til þess fallnar að draga úr áhættunni fyrir hina skráðu.

Innri skráning:	**X**
Tilkynning til Persónuverndar:	**0**
Tilkynning til hinna skráðu:	**0**

Dæmi 16

Tryggingafélag sendir breytingar á skilmálum í bréfpósti til viðskiptavina með ökutækjatryggingar. Bréfin innihalda upplýsingar um nafn, fæðingardag og heimilisfang tryggingartaka, skráningarnúmer ökutækis, iðgjald fyrir núverandi og komandi gjaldár, svo og áætlaðan árlegan akstur. Bréfin eru send sjálfvirkt, en vegna mistaka fara bréf tveggja tryggingartaka í eitt og sama umslag, þ.e. einn tryggingartaki fær upplýsingar um sínar tryggingar, auk upplýsinga um tryggingar annars tryggingartaka.

Í þessu tilviki var óviðkomandi veittur aðgangur að persónuupplýsingum. Ekki verður þó talið líklegt að öryggisbresturinn leiði til mikillar áhættu fyrir réttindi og frelsi hins skráða. Nauðsynlegt er þó að tilkynna öryggisbrestinn til Persónuverndar og að skrá hann innanhúss.

Innri skráning:	**X**
Tilkynning til Persónuverndar:	**X**
Tilkynning til hinna skráðu:	**0**

Annars konar öryggisbrestir

Dæmi 17

Símaver fjarskiptafyrirtækis fær símtal frá einstaklingi sem segist vera viðskiptavinur. Viðkomandi óskar eftir því að breyta skráðu tölvupóstfangi til móttöku reikninga vegna þjónustunnar. Einstaklingurinn er beðinn um upplýsingar til að staðfesta auðkenni sitt og veitir hann umbeðnar upplýsingar. Í kjölfar er skráðu tölvupóstfangi breytt og reikningar sendir á nýtt netfang, en enginn póstur er sendur á eldra netfang til staðfestingar á breyttu netfangi. Mánuði seinna hringir raunverulegur viðskiptavinur í fyrirtækið og óskar eftir upplýsingum um af hverju hann hafi ekki fengið sendan reikning vegna viðskiptanna og segist ekki hafa óskað eftir breytingum á skráðu netfangi sínu

hjá fyrirtækinu. Fyrirtækið áttar sig þá á að átt hefur sér stað öryggisbrestur , þar sem upplýsingar hafa verið sendar óviðkomandi, og leiðréttir breytingu á netfangi viðskiptavinarins.

Í þessu tilviki hefur átt sér stað auðkennisþjófnaður sem leiddi til þess að persónuupplýsingar voru sendar óviðkomandi. Slíkar upplýsingar gætu auðveldað frekari þjófnað á auðkennum hins skráða, en upplýsingar frá fjarskiptafyrirtækinu gætu verið nýttar til frekari auðkenningar á honum skráða hjá öðrum ábyrgðaraðilum. Líklegt er því að öryggisbresturinn leiði af sér mikla áhættu fyrir réttindi og frelsi hins skráða.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**

Dæmi 18

Verslun uppgötvar breytingar á tilteknum pósthólfum og að tölvupóstar sem berast í þau og innihalda tiltekin orð, svo sem „reikningur“, „greiðsla“, „millifærsla“ og „bankareikningur“, fara sjálfkrafa í ónotaða möppu í pósthólfinu framsendast á netfang ótengt ábyrgðaraðila.

Einnig uppgötvar verslunin að greiðsluupplýsingum tiltekins birgis hefur verið breytt á þann hátt að greiðslur fara til tölvuþrjótsins, auk þess sem versluninni eru sendir falskir reikningar með reikningsupplýsingum hans. Öryggisbresturinn kemur í ljós þegar eftirlitskerfi póstþjónustu verslunarinnar vekur athygli á möppunum í pósthólfunum. Ekki tekst að komast að því hvernig viðkomandi fékk aðgang að þeim, en talið er að hans hafi verið aflað með sýktum tölvupósti. Tölvuþrjóturinn fær aðgang að upplýsingum um launagreiðslur til 89 starfsmanna í tilteknum mánuði, auðkenndar með nöfnum þeirra. Að auki fær hann upplýsingar um nöfn 10 fyrrverandi starfsmanna, hjúskaparstöðu þeirra, fjölda barna, laun og vinnutíma, auk annars þess sem fram kemur í launaseðlum þeirra.

Í þessu tilviki getur öryggisbresturinn leitt til hættu á að hinir skráðu verði fyrir auðkennisþjófnaði. Er því líklegt að hann leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Fyrirtækinu er því skylt að skrá öryggisbrestinn innanhúss og ber því jafnframt að tilkynna hann bæði til Persónuverndar og allra þeirra 99 starfsmanna sem bresturinn hefur áhrif á.

Innri skráning: **X**

Tilkynning til Persónuverndar: **X**

Tilkynning til hinna skráðu: **X**
