PÓST- OG FJARSKIPTASTOFNUN

Ákvörðun nr. 2/2012

varðandi úttekt á samskiptum heildsölu og smásölu Símans vegna meðferðar á trúnaðarupplýsingum

I. Almennt

Mál þetta varðar úttekt sem óháður sérfræðingur í upplýsingatæknimálum framkvæmdi fyrir hönd Póst- og fjarskiptastofnunar (PFS) á samskiptum heildsölu og smásölu Símans að því er varðar meðferð tiltekinna trúnaðarupplýsinga sem félagið öðlast vegna samtengingar fjarskiptaneta. Kveðið var á um umrædda úttekt í ákvörðun PFS nr. 37/2010 þar sem komist var að þeirri niðurstöðu að félagið hefði brotið gegn trúnaðarskyldum sínum samkvæmt 26. gr. fjarskiptalaga með því að nota samtengiupplýsingar í öðrum tilgangi en þær voru fengnar, þ.e.a.s. í markaðslegum tilgangi. Málið varðar einnig úrbætur sem PFS telur nauðsynlegt að Síminn geri í samræmi við niðurstöður skýrslu umrædds sérfræðings.

II. Málavextir

2.1 Ákvörðun PFS nr. 37/2010 varðandi brot Símans á trúnaðarskyldum

Með ákvörðun PFS nr. 37/2010 frá 17. nóvember s.á. komst stofnunin að þeirri niðurstöðu að Síminn hefði brotið gegn trúnaðarskyldum sínum samkvæmt 26. gr. fjarskiptalaga, viðmiðunartilboði félagsins um samtengingu talsímaneta, afleiddum samtengisamningum og jafnræðiskvöðum þeim sem lagðar höfðu verið á félagið,[1] með því að hagnýta sér fjarskiptaumferðarupplýsingar sem vörðuðu heildsölusamskipti fjarskiptafyrirtækja (CDR-gögn) í markaðslegum tilgangi á smásölustigi gagnvart Nova ehf. og Fjarskiptum ehf. (Vodafone). Síminn nýtti því umræddar upplýsingar í öðrum tilgangi en þær voru fengnar.

Síminn öðlaðist umræddar upplýsingar í tengslum við framkvæmd samtengisamninga félagsins við önnur fjarskiptafyrirtæki. Símanum var ekki heimilt að notfæra sér umræddar upplýsingar í markaðslegum tilgangi þar sem tilgangurinn með veitingu þeirra var eingöngu að gera

[1] Umræddar jafnræðiskvaðir voru lagðar á Símann með ákvörðunum PFS frá 20. júlí 2006 (M16 - lúkning í farsíma) og 4. desember 2008 (M9 – lúkning í fastlínu).

samtengingu neta mögulega, ásamt eftirfarandi greiðsluuppgjöri. Því var heildsölu Símans óheimilt að veita smásölu félagsins aðgang að umræddum upplýsingum. Síminn viðurkenndi í málinu að smásalan hefði ekki haft heimild til að nýta umræddar upplýsingar í markaðslegum tilgangi en hafnaði því að smásalan gæti ekki átt rétt á slíkum upplýsingum í ýmsum öðrum tilgangi.

Gögn málsins leiddu í ljós að Síminn hafði gripið til umfangsmikilla markaðsaðgerða sem beindust að öðrum fjarskiptafyrirtækjum. Tilgangurinn var markvisst sá að ná frá félögunum mikilvægum viðskiptavinum með óeðlilegri notkun á trúnaðarupplýsingum sem ekki bæri að nota í markaðslegum tilgangi. Þeir listar sem Síminn vann upp úr umræddum umferðargögnum höfðu að geyma sundurgreinanlegar upplýsingar um mörg þúsund viðskiptavini annarra fjarskiptafyrirtækja. Þar var ekki aðeins um að ræða upplýsingar um símanúmer og nöfn viðkomandi viðskiptavina heldur jafnframt kennitölur, heimilisföng og í mörgum tilvikum starfsheiti, auk upplýsinga um fjölda símtala hvers og eins, lengd í sekúndum og lengd meðalsímtals. Nánar tiltekið var um að ræða skráningu á B-númeri, tíðni og lengd símtala. Samtenging kerfa Símans við kerfi annarra fjarskiptafyrirtækja er eina samskiptalagið sem veitir félaginu umræddar upplýsingar. Því er um að ræða upplýsingar sem verða til á heildsölustigi í starfsemi fjarskiptafyrirtækja og falla þ.a.l. undir viðmiðunartilboð og viðeigandi kvaðir þar að lútandi. Símanum var því óheimilt að afhenda öðrum upplýsingar um lúkningu símtala, þ.m.t. öðrum deildum félagsins.

PFS tók fram að gríðarlega mikilvægt væri fyrir fjarskiptamarkaðinn, sem byggðist á samkeppnislegum sjónarmiðum, að með umræddar upplýsingar væri farið sem fullkomið trúnaðarmál milli fyrirtækja og að slíkar upplýsingar væru ekki nýttar innan fjarskiptafyrirtækjanna í markaðslegum tilgangi eða öðrum óskyldum tilgangi. Þá segir orðrétt:

> *„Að ofangreindu virtu er ljóst að umræddar umferðarupplýsingar sem uppruna eiga að rekja til framkvæmdar Símans á samtengisamningum við önnur fjarskiptafyrirtæki tilheyra heildsöluarmi fyrirtækisins. Símanum ber að haga innri starfsemi sinni þannig að slíkar upplýsingar berist ekki til annarra deilda fyrirtækisins nema brýna nauðsyn beri til. Ef nota þarf slíkar upplýsingar, t.d. til að greina tæknibilanir og villur í fjarskiptasendingu, afstemma reikninga, sundurliða reikninga viðskiptavina Símans eða rekja og/eða fyrirbyggja svikastarfsemi ber Símanum að haga innra skipulagi sínu með þeim hætti að slíkt fari fyrst og fremst fram innan heildsölu félagsins. Reynist nauðsynlegt að miðla smásölunni upplýsingum til tiltekinna afmarkaðra verkefna, sem eðlilegt er að unnin séu innan smásölunnar, ber að haga henni með þeim hætti að einungis þeim upplýsingum sem nauðsynlegar eru til að leysa slík verkefni af hólmi sé miðlað og þeim sé eytt um leið og slíkum verkefnum er lokið. Verkefni tengd markaðssetningu Símans gagnvart viðskiptavinum annarra fjarskiptafyrirtækja koma þarna alls ekki til álita.“*

Í ákvörðunarorðum kom fram að PFS myndi framkvæma eða láta framkvæma fyrir sig úttekt á samskiptum heildsölu og smásölu Símans í kjölfar ákvörðunarinnar. Þá kom fram að kæmi til þess að PFS réði óháðan sérfræðing til að annast umrædda úttekt skyldi Síminn greiða fyrir hana, sbr. heimild í 11. mgr. 14. gr. laga nr. 69/2003 um Póst- og fjarskiptastofnun.[2]

[2] Ennfremur fyrirskipaði PFS Símanum að setja sér verklagsreglur um meðferð persónuupplýsinga og eyðingu gagna í samræmi við ákvæði 7. mgr. 42. gr. fjarskiptalaga og skilyrði sem Persónuvernd kynni að setja. Auk þess framsendi PFS til Persónuverndar þann hluta málsins sem varðaði vinnslu Símans á persónuupplýsingum um áskrifendur annarra fjarskiptafyrirtækja til þóknanlegrar meðferðar.

Ofangreindri ákvörðun PFS nr. 37/2010 var ekki skotið til úrskurðarnefndar fjarskipta- og póstmála né dómstóla, hvorki af hálfu Símans né annarra aðila.

2.2 Ákvörðun Persónuverndar í máli nr. 2010/488 frá 18. janúar 2011

Með ákvörðun Persónuverndar í máli nr. 2010/488, dags. 18. janúar 2011, komst sú stofnun að þeirri niðurstöðu að sú aðgerð Símans að nota samtengiupplýsingar um aðra viðskiptavini en sína eigin, og samkeyra þær við aðrar skrár til að búa til lista til nota í markaðslegum og fjárhagslegum tilgangi, væri heimildarlaus og bryti gegn ákvæðum laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Í ljósi umfangs brotsins og alvarleika þess kærði Persónuvernd umrædda háttsemi Símans til lögreglu.

2.3 Bréf PFS til Símans, dags. 26. janúar 2011

Í bréfi PFS til Símans, dags. 26. janúar 2011, vísaði stofnunin til framangreindrar ákvörðunar PFS nr. 37/2010 og þeirrar úttektar á samskiptum heildsölu og smásölu Símans sem þar var kveðið á um. Fram kom að markmið úttektarinnar væri að greinargóð lýsing fengist á samskiptum heildsölu og smásölu Símans hvað varðaði meðferð samtengiupplýsinga og að tryggja lögmætan og eðlilegan aðgang að upplýsingum í CDR-grunni félagsins og tengdum kerfum, sbr. 26. gr. fjarskiptalaga. Þannig myndi úttektin snúa að kerfunum sjálfum, því starfsfólki sem hefði aðgang að og ynni við þau og skipulagslegum þáttum varðandi fyrirkomulag öryggismála.

Þá kom fram að PFS hefði leitað til Jónasar S. Sverrissonar hjá Theron ehf., sem sérhæfði sig í ráðgjöf á sviði upplýsingatækni til að taka að sér umrædda úttekt. PFS hefði borið fyrirhugaða skipun ofangreinds ráðgjafa undir Símann sem ekki hefði gert athugasemdir. Fyrir lægju drög að verktillögu varðandi úttektina og umfang hennar sem Símanum gæfist hér með tækifæri til að gera athugasemdir við. Eins og fram kæmi í drögum að verktillögu væri gert ráð fyrir að úttektinni yrði skipt í fjóra þætti, þ.e. 1) gagnaöflun og markmiðssetningu, 2) rýni gagna og undirbúning fyrir úttekt, 3) vettvangsathugun og 4) úrvinnslu upplýsinga og skýrslugerð.

Með stoð í 16. gr. reglna nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum, óskaði PFS eftir tilteknum gögnum frá Símanum. Í fyrsta lagi skriflegum og myndrænum lýsingum Símans á miðlunarferli gagna úr CDR-grunninum, m.a. hvaða starfsmenn og kerfi hefðu aðgang að CDR-grunni og tengdum gagnagrunnum, ásamt afleiddum gögnum (pappír og rafræn), og í hvaða tilgangi starfsmenn hefðu aðgang að gögnum úr grunnunum. Í öðru lagi skriflegri *öryggisstefnu* Símans, sbr. 7. gr. ofangreindra reglna. Að lokum viðeigandi kafla úr *áhættumati* og *lýsingu á öryggisráðstöfunum* er tækju til CDR-gagnagrunns og tengdra upplýsingakerfa, sbr. sömu grein reglnanna.

Að lokum kom fram að Síminn bæri að greiða fyrir vinnu umrædds sérfræðings, sbr. 11. mgr. 14. gr. laga nr. 69/2003 um Póst- og fjarskiptastofnun, auk þess sem þagnarskylda hvíldi á honum að viðlagðri ábyrgð.

2.4 Svar Símans til PFS, dags. 9. febrúar 2011

Með bréfi Símans til PFS, dags. 9. febrúar 2011, barst svar félagsins við ofangreindri fyrirspurn PFS, ásamt fylgiskjölum varðandi miðlunarferli gagna úr CDR-grunni Símans, öryggisstefnu félagsins, áhættumat og lýsingu á öryggisráðstöfunum.

2.5 Samningur PFS og Theron um sérfræðilega ráðgjöf frá 15. febrúar 2011

Þann 15. febrúar 2011 undirritaðu forstjóri PFS og Jónas S. Sverrisson, f.h. Theron ehf., samning um sérfræðilega ráðgjöf. Með samningnum tók Theron að sér að veita PFS sérfræðilega ráðgjöf og aðstoð á sviði upplýsingaöryggis. Nánar tiltekið með framkvæmd úttektar á CDR-grunni Símans, samkvæmt nánari lýsingu í verktillögu Theron, dags. 19. janúar 2011, sem PFS og Theron höfðu undirritað og borin hefði verið undir Símann. Starfið fælist m.a. í gagnaöflun, markmiðssetningu, rýni gagna, undirbúningi fyrir úttekt, fundum, vettvangskönnunum, úrvinnslu upplýsinga og skýrslugerð, ásamt öðrum þáttum í tengslum við ofangreinda úttekt eftir nánara samkomulagi.

Samið var um tiltekið tímakaup og gert var ráð fyrir að verkefnið tæki 84 klst. Reyndist verkefnið umfangsmeira en áætlun gerði ráð fyrir gæti verksali innheimt allt að 25% fleiri tíma sem verkkaupi þyrfti að samþykkja. Þá undirritaði verksali sérstaka yfirlýsingu um trúnað og þagmælsku sama dag, sem send var til Símans.

2.6 Verklagsreglur Símans um meðferð persónuupplýsinga, dags. 1. mars 2011

Með bréfi Símans til PFS, dags. 1. mars 2011, sendi félagið stofnuninni verklagsreglur um meðferð og eyðingu persónuupplýsinga til samþykktar, í samræmi við framangreinda ákvörðun PFS nr. 37/2010. Þar er m.a. fjallað um tilgang verklagsreglnanna, umfang þeirra, ábyrgð og birtingu, framkvæmd og stoðskjöl. PFS hefur ekki ennþá samþykkt verklagsreglurnar en ákvörðun þar að lútandi verður tekin innan skamms, þegar máli því sem hér er til umfjöllunar er lokið.

Undir rekstri ofangreinds máls varðandi verklagsreglur um meðferð og eyðingu persónuupplýsinga kom í ljós að Síminn túlkaði ákvæði 2. mgr. 42. gr. fjarskiptalaga með þeim hætti að unnt væri að geyma gögn í allt að 12 mánuði þrátt fyrir að reikningur fyrir þjónustuna hefði verið greiddur. Með ákvörðun PFS nr. 29/2011 komst PFS að þeirri niðurstöðu að slíkt væri ekki í samræmi við ofangreint ákvæði fjarskiptalaga. Lagt var fyrir Símann að taka umrætt ákvæði verklagsreglnanna til endurskoðunar og meta almennan hámarksvarðveislutíma fjarskiptaupplýsinga eingöngu út frá því að geta brugðist við vefengingu reiknings innan hæfilegs tíma frá því að hann hefði verið greiddur. Hefði reikningur verið greiddur skyldi við lok skilgreinds varðveislutíma eyða upplýsingunum eða gera þær ópersónugreinanlegar. Almennur hámarks varðveislutími gæti þó aldrei verið meiri en 6 mánuðir, enda gilti lengri varðveislutími um gögn yfir fjarskiptanotkun sem lægju til grundvallar reikningum í vanskilum.[3]

[3] Við meðferð umræddsmáls aflaði PFS umsagnar Persónuverndar sem var sammála ofangreindri túlkun PFS.

2.7 Úttekt hjá Símanum frá 23. mars til 1. apríl 2011

Á tímabilinu 23. mars til 1. apríl fór fram úttekt hjá Símanum á þremur fundum. Auk Jónasar S. Sverrissonar hjá Theron sóttu fundina Óskar H. Ragnarsson og Stefán Snorri Stefánsson frá PFS. Rætt var við fjölmarga starfsmenn Símans.

2.8 Frumskýrsla Theron frá maí 2011

Í maí 2011 lá fyrir frumskýrsla Theron í málinu og bar hún yfirskriftina „Úttekt á öryggi upplýsinga."

2.9 Bréf PFS til Símans, dags. 22. júní 2011

Í bréfi PFS til Símans, dags. 22. júní 2011, kom fram að áður en Theron gæti lokið skýrslu sinni og PFS tekið endanlega ákvörðun í málinu væri nauðsynlegt að óska eftir frekari upplýsingum frá Símanum um vöruhús gagna. Því var farið fram á að Síminn svaraði nánar tilteknum spurningum, m.a. um það hvaða gögn færu inn í vöruhús gagna, hvernig unnið væri úr grunngögnum til þess að mynda frekari upplýsingar og hvaða upplýsingar væru aðgengilegar í vöruhúsinu eftir meðhöndlun og vinnslu grunnupplýsinga. Að lokum var óskað eftir því að fram kæmi nákvæmari lýsing á aðgangsheimild mismunandi deilda innan fyrirtækisins að gögnum í vöruhúsinu, þ.e. að hvaða þáttum vöruhússins hver deild hefði aðgang að og í hvaða tilgangi. Sérstaklega væri horft til smásölu Símans, m.a. aðgangs markaðsdeildarinnar.

2.10 Svarbréf Símans, dags. 6. júlí 2011

Svör Símans við ofangreindri fyrirspurn PFS bárust stofnuninni með bréfi, dags. 6. júlí 2011.

2.11 Bréf PFS til Símans, dags. 11. október 2011

Vegna óviðráðanlegra orsaka, sem varða verksala, gat hann ekki unnið að málinu frá því að ofangreint bréf var sent í byrjun júlí þar til í október. Er hann hófst handa að nýju taldi hann að enn vantaði nákvæmari svör frá Símanum varðandi vöruhús gagna. Með bréfi, dags. 11. október 2011, sendi PFS því Símanum aðra fyrirspurn. Þar kom fram að áður en Theron gæti lokið skýrslu sinni og PFS tekið endanlega ákvörðun í málinu væri nauðsynlegt að óska eftir nánari upplýsingum frá Símanum um tiltekin atriði er tengdust umræddri úttekt. Óskað var eftir nákvæmari upplýsingum um atriði er tengjast vöruhúsi gagna, auk þess sem óskað var skýringa á skipulagslegum þáttum er varða verkaskiptingu á milli Símans og Skipta.

2.12 Svarbréf Símans til PFS, dags. 8. nóvember 2011

Með bréfi Símans til PFS, dags. 8. nóvember 2011, barst svar Símans við ofangreindri fyrirspurn PFS. Meðal annars kom fram að skilningur Símans á þeirri úttekt sem Theron skyldi framkvæma í samræmi við ákvörðun PFS nr. 37/2010 væri sá að kanna bæri hvernig aðskilnaði á milli heildsölu og smásölu Símans væri háttað, en ekki hvernig meðferð persónuupplýsinga væri almennt háttað hjá fyrirtækinu enda væri það allt annars eðlis og mun víðtækara verkefni. Sá skilningur sem Síminn legði því í fyrirspurn PFS væri að óskað væri eftir upplýsingum sem vörðuðu heildsölu Símans og hvaða gögn frá heildsölu færu í vöruhús gagna og aðgengi eða takmarkanir á aðgengi smásölu að þeim gögnum, m.t.t. 26. gr. fjarskiptalaga.

Þau gögn sem yrðu til vegna viðskipta smásölu Símans við eigin viðskiptavini eða vinnsla upplýsinga um eigin viðskiptavini, s.s. vegna reikningafærslu, féllu því eðli málsins samkvæmt út fyrir ramma þessa máls enda kæmi skýrt fram í ákvörðun PFS nr. 37/2010 að aðeins væri verið að kanna aðskilnað á milli heildsölu og smásölu. Það væri því ljóst að úttekt hins óháða aðila og sá rammi sem honum væri skipaður hlyti að miðast við það verkefni sem honum væri falið, sem væri að kanna aðgangsstýringu á milli heildsölu og smásölu. Almenn vinnsla persónuupplýsinga og eftirlit með vinnslu persónuupplýsinga félli almennt undir valdsvið Persónuverndar, sbr. m.a. ákvörðun PFS nr. 37/2010 þar sem PFS ákvað að framsenda til Persónuverndar þann þátt málsins sem laut að vinnslu og notkun persónuupplýsinga.

PFS hefði hvorki tilkynnt Símanum um að hinum óháða aðila hefði verið falið víðtækara verkefni en í upphafi var tilkynnt um né heldur að PFS hefði til rannsóknar eða skoðunar meðferð persónuupplýsinga hjá Símanum almennt, óháð því hvort um væri að ræða upplýsingar sem lytu að 26. gr. fjarskiptalaga eða upplýsingar um viðskiptavini Símans á smásölustigi. Vegna þessa óskaði Síminn eftir því að PFS útskýrði og rökstyddi með greinargóðum hætti hvað fælist í eftirfarandi texta sem fram kæmi í ákvörðun nr. 29/2011, um varðveislutíma upplýsinga um fjarskiptaumferð hjá Símanum, frá 25. október s.l.:

> *„**Vísar stofnunin til þess að nú stendur yfir formleg úttekt á vegum PFS á meðferð fjarskiptaumferðarupplýsinga í gagnagrunnum Símans,** þ.m.t. í svo kölluðu Vöruhúsi gagna, en þangað mun upplýsingum úr greiðslumiðlunarkerfunum, ásamt fleiri kerfislegum upplýsingum, vera miðlað m.a. í þeim tilgangi að veita viðskiptavinum sundurliðaðar upplýsingar um fjarskiptanotkun sína. Markmið þeirrar úttektar er m.a. að leiða í ljós hvort einhverjir annmarkar eru á þeirri framkvæmd með tilliti til lögmætis og öryggis vinnslunnar.“* (leturbr. Símans)

Þær upplýsingar sem þarna væri vísað til lytu að viðskiptavinum Símans en kæmu ekki til vegna samninga við önnur fjarskiptafyrirtæki. Símanum væri til að mynda skylt að veita viðskiptavinum sínum upplýsingar um fjarskiptanotkun þeirra og því yrði ekki séð hvernig framangreind umfjöllun samræmdist ákvörðun PFS nr. 37/2010. Þar sem Símanum hefði aðeins verið tilkynnt um að verið væri að gera úttekt á samskiptum heildsölu og smásölu væri upplýsinga óskað um á hvaða grunni sú úttekt færi fram sem vísað væri til í ákvörðun PFS nr. 29/2011.

Í bréfi PFS hefði verið tekið fram að umbeðnar upplýsingar væru nauðsynlegar til þess að Theron gæti lokið við gerð skýrslu sinnar og að PFS gæti tekið endanlega ákvörðun í málinu. Í ljósi þess að úttektin ætti að vera óháð óskaði Síminn eftir upplýsingum um hvort og með hvaða hætti PFS og Theron hefðu unnið saman að úttektinni og væntanlegri niðurstöðu. Að lokum kom fram að Síminn myndi svara spurningum PFS eins ítarlega og skilmerkilega og kostur væri að teknu tilliti til eðli spurninganna og þess máls sem væri til meðferðar.

2.13 Lokaskýrsla Theron frá 6. desember 2011

Þann 6. desember 2011 barst PFS lokaskýrsla Theron vegna framangreindrar úttektar á öryggi upplýsinga hjá Símanum. Skýrslan samanstendur annars vegar af frumskýrslu Theron frá maí 2011 og hins vegar viðauka vegna þeirra upplýsinga sem bárust í bréfum Símans, dags. 6. júlí og 8. nóvember s.l.

2.14 Boðunarbréf PFS, dags. 6. desember 2011

Með bréfi PFS til Símans, dags. 6. desember s.l., boðaði stofnunin félaginu fyrirhugaða ákvörðun sína í málinu. Fram kom að í bréfi Símans til PFS, dags. 8. nóvember s.l., hefði félagið óskað eftir upplýsingum um hvort og með hvaða hætti PFS og Theron hefðu unnið saman að úttektinni og væntanlegri niðurstöðu í ljósi þess að úttektin ætti að vera óháð.

PFS kvað skýrsluhöfund algjörlega hafa unnið með sjálfstæðum og óháðum hætti að gerð umræddrar úttektar og gerð skýrslunnar. Skýrsluhöfundur hefði mótað þær spurningar sem PFS hefði beint til Símans í máli þessu. Eðlilegt væri að slík formleg bréfaskipti færu í gegnum eftirlitsstjórnvaldið. Tveir starfsmenn PFS hefðu setið fundi þar sem skýrsluhöfundur heimsótti starfsstöð Símans og ræddi við starfsmenna Símans, en slíkt væri í samræmi við eftirlitsheimildir stofnunarinnar. Umræddir starfsmenn hefðu ekki beitt sér með neinum hætti né reynt að hafa áhrif á efni umræddrar skýrslu. Fyrst og fremst hefði verið um það að ræða að starfsmenn PFS gætu betur áttað sig á gangverki félagsins að þessu leyti þegar kæmi að lestri úttektarskýrslunnar og mótun tillagna til úrbóta í kjölfar hennar.

Starfsmenn PFS og skýrsluhöfundur hefðu fundað í upphafi máls þegar gengið var frá samningi og verkefninu hleypt af stokkunum. Þá áttu starfsmenn PFS og skýrsluhöfundur með sér annan fund í maí 2011 þegar frumskýrslan hefði verið kynnt fulltrúum PFS. Það hefði verið samdóma álit skýrsluhöfundar og starfsmanna PFS að vöruhús gagna væri mesti áhættuþátturinn í rekstri Símans að því er varðaði umrædda úttekt og að Síminn hefði ekki gert nægilega vel grein fyrir virkni og möguleikum þess gagnagrunns í skriflegum svörum sínum frá 9. febrúar 2011. Því hefði verið ákveðið að óska eftir frekari gögnum um vöruhúsið og mótaði skýrsluhöfundur þær spurningar sem PFS sendi síðan Símanum í tvígang, þ.e. í júlí og október s.l. Þá hefðu starfsmenn PFS og skýrsluhöfundur verið í þó nokkrum tölvupóstsamskiptum á meðan á úttektinni stóð. Þar hefði fyrst og fremst verið um það að ræða að PFS beitti sér fyrir því að úttektinni yrði hraðað og henni lokið án ástæðulauss dráttar. Vegna óviðráðanlegra orsaka, sem vörðuðu skýrsluhöfund, hefði vinna við úttektina legið niðri frá byrjun júlí og fram í október s.l.

Í ofangreindu bréfi Símans, dags. 8. nóvember s.l., hefði komið fram að Síminn hefði einnig áhyggjur af því að umrædd úttekt væri komin út fyrir þann ramma sem ákvörðun PFS nr. 37/2010 hefði markað henni, þ.e. að gera úttekt á samskiptum heildsölu og smásölu m.t.t. trúnaðargagna þeirra sem Síminn öðlaðist við gerð samtengisamninga. Svo virtist sem úttektinni væri ennfremur ætlað að kanna hvernig meðferð persónuupplýsinga væri almennt háttað hjá Símanum. Það væri á forræði Persónuverndar en ekki PFS. Þá hefði verið óskað eftir útskýringum og rökstuðingi PFS vegna ummæla stofnunarinnar í ákvörðun nr. 29/2011, þar sem stofnunin vísaði til þess að yfir stæði formleg úttekt á vegum PFS á meðferð fjarskiptaumferðarupplýsinga í gagnagrunnum Símans, m.a. í vöruhúsi gagna.

PFS hafnaði því alfarið að umrædd úttekt Theron næði almennt til meðferðar persónuupplýsinga, án tillits til samskipta heildsölu og smásölu Símans. Eðli málsins samkvæmt varðaði úttekt á umræddum samskiptum heildsölu og smásölu Símans fyrst og fremst skoðun á gagnagrunnum Símans sem mögulega væri unnt að nýta til að vinna með CDR gögn þau sem Síminn hefði öðlast við samtengingu farsímaneta. Óumflýjanlegt væri við slíka úttekt að einhver skörun yrði við málefni er vörðuðu meðferð persónuupplýsinga hjá Símanum,

þótt þau málefni væru ekki sem slík í brennidepli í úttektinni. Umrædd úttekt væri því fyllilega í samræmi við ákvörðun PFS nr. 37/2010, eins og staðfest væri við lestur umræddrar úttektarskýrslu. Úttektin og úttektarskýrslan væru því innan þess ramma sem umrædd ákvörðun hefði markað. Það sama mætti segja um þær tillögur að úrbótum sem skýrsluhöfundur hefði lagt til. Hinn ólögmæti aðgangur smásölu Símans, með tilliti til 26. gr. fjarskiptalaga, hefði varðað aðgang að fjarskiptaumferðarupplýsingum. Umræddar upplýsingar teldust til persónuupplýsinga, enda væru þær persónugreinanlegar. Því væri vandséð hvernig úttekt til að fyrirbyggja aðra eins misnotkun varðaði ekki meðferð persónuupplýsinga.

Varðandi ofangreind ummæli PFS í ákvörðun nr. 29/2011 væri það fyrst að segja að sú ákvörðun hefði aðeins varðað það álitaefni er snéri að varðveislutíma upplýsinga um fjarskiptaumferð hjá Símanum. Í umræddri ákvörðun hefði ekki verið tekin afstaða til þess hvaða upplýsingar úr fjarskiptaneti Símans væri nauðsynlegt að skrá og safna um fjarskiptanotkun viðskiptavina í þeim tilgangi að geta gjaldfært fyrir þjónustuna, eða við hvaða önnur gögn heimilt væri að samkeyra þessar upplýsingar. Því næst vísaði PFS til þess að yfir stæði formleg úttekt á vegum stofnunarinnar á meðferð fjarskiptaumferðarupplýsinga í gagnagrunnum Símans, þ.m.t. svo kölluðu vöruhúsi gagna. Markmið þeirrar úttektar væri m.a. að leiða í ljós hvort einhverjir annmarkar væru á þeirri framkvæmd m.t.t. lögmætis og öryggis vinnslunnar.

Þá kæmi fram að PFS teldi að framangreind ummæli væru í fullu samræmi við raunveruleikann og þann ramma sem umræddri úttekt hefði verið markaður í ákvörðun PFS nr. 37/2010. Ljóst væri að samskipti heildsölu og smásölu yrðu ekki könnuð eða þeim lýst án þess að ítarleg skoðun færi fram á gangvirki upplýsingatæknikerfa og gagnagrunna Símans, eins og gert hefði verið í umræddri úttekt. Með vísan til niðurstöðu meðfylgjandi úttektarskýrslu Theron hefði PFS í hyggju að mæla svo fyrir í ákvörðun að Síminn skyldi framkvæma allar þær úrbætur sem skýrsluhöfundur legði til, alls í 18 liðum, til að tryggja eins og mögulegt væri eðlilegan aðskilnað og eðlileg samskipti á milli heildsölu og smásölu hjá félaginu m.t.t. hagnýtingar CDR gagna. PFS væri sammála niðurstöðum skýrsluhöfundar, ábendingum hans og tillögum að úrbótum. PFS teldi umræddar tillögur að úrbótum nauðsynlegar og í samræmi við meðalhóf til að tryggja eins og unnt væri öryggi umræddra CDR-upplýsinga, án þess að gripið væri til of viðurhlutamikilla úrræða sem skýrsluhöfundur hefði lýst en talið ganga of langt m.t.t. meðalhófs og kostnaðar.

PFS hefði því í hyggju að mæla fyrir um að Síminn gerði eftirtaldar úrbætur:

1. Endurskoðun öryggisstefnu þannig að ábyrgð yrði rétt skilgreind.
2. Áhættumat endurunnið.
3. Formlegt ferli fyrir aðgangsstjórnun innleitt.
4. Formlegt ferli fyrir eftirlit með notkun kerfa og gagna innleitt.
5. Formlegt ferli fyrir rýni á aðgangi notenda innleitt.
6. Formlegt ferli fyrir lögmæta vinnslu gagna innleitt.
7. Þjálfun allra starfsmanna sem koma að aðgangsstjórnun tryggð.
8. Sjá til þess að eitt miðlægt kerfi yrði notað við skráningu beiðna og aðgerða.
9. Geymslu- og grisjunaráætlun gerð fyrir fjarskiptagögn.

10. Gögnum eytt eða þau gerð nafnlaus á öllum stöðum (einnig í þróunarkerfum) þegar lögbundnum líftíma þeirra lyki.
11. Formlegar reglur varðandi meðhöndlun persónugreinanlegra upplýsinga settar, ásamt reglum um gerð fyrirspurna.
12. Formlegar reglur varðandi vinnslu fyrirspurna í vöruhúsi gagna settar.
13. Tryggt að fyrirspurnir í vöruhús gagna teldust ekki vera ólögmætar. Þetta væri mögulegt með því að gefa Viðskiptagreind heimild til þess að synja fyrirspurn þar sem t.d. óskað væri eftir upplýsingum um samkeppnisaðila eða þar sem númer hjá samkeppnisaðilum og nafn einstaklinga væru pöruð saman.
14. Formleg aðgangsstýring og rýni á aðgang að grunngögnum og vöruhúsi gagna tryggð, ásamt geymslu á niðurstöðum slíkrar vinnu.
15. Tryggt að símanúmer í CDR gögnum, sem geymd væru í Datamart hluta vöruhússins, geymdu t.d. aðeins fyrstu fimm tölustafi í símanúmerum viðskiptavina samkeppnisaðila.
16. Tryggt að grunngögn CDR færslna yrði einungis aðgengileg þeim aðilum sem starfs síns vegna þyrftu á þeim að halda.
17. Tryggt að allar óskir um fyrirspurnir yrðu skráðar niður og formleg ákvörðun tekin um framkvæmd þeirra. Þessar skráningar gæti PFS skoðað í úttektum og sannreynt hvort framkvæmdar hefðu verið ólögmætar fyrirspurnir eða eftir þeim óskað.
18. Formlegar reglur settar um stöðugt eftirlit með notkun upplýsinga úr vöruhúsi gagna, t.d. með því að framkvæma stikkprufur á notkun vöruhússins.

Að lokum kom fram að PFS hefði í hyggju að mæla fyrir um að ofangreindar úrbætur skyldu að fullu hafa verið innleiddar fyrir 1. júlí 2012.

2.15 Svarbréf Símans til PFS, dags. 22. desember 2011

Með bréfi, dags. 22. desember s.l., barst PFS svarbréf Símans við framangreindu boðunarbréfi. Fram kom að Síminn teldi ekki ástæðu til þess að gera athugasemdir við tillögur PFS um framangreindar úrbætur.[4] Þá kom fram að félagið myndi leitast við að ljúka innleiðingu úrbótanna fyrir 1. júlí 2012 eins og PFS hefði í hyggju að mæla fyrir um. Hins vegar áætlaði Síminn að flóknari tæknileg atriði gætu tekið lengri tíma og óskaði því eftir að PFS veitti félaginu heimilt til að ljúka innleiðingu síðar en 1. júlí 2012 ef þess reyndist þörf. Síminn myndi þó að sjálfsögðu hraða innleiðingu eins mikið og kostur væri, en í ljósi fjölda tillagna væri fyrirsjáanlegt að innleiðingu yrði ekki að fullu lokið fyrir umrætt tímamark. Það væri álit Símans að það skilaði meiri árangri og festi breytingar betur í sessi ef tilteknar úrbætur yrðu unnar sem verkþættir í einu og sama úrbótaverkefninu. Síminn ynni nú að því að skilgreina þessi verkefni og setja saman áætlun og verkefnislýsingu fyrir hvert þeirra.

[4] Síminn taldi þó að eðli málsins samkvæmt væri þörf á ákveðnum viðræðum og samskiptum milli PFS, eða Theron eftir atvikum, og Símans við innleiðingu úrbótanna, m.a. til þess að staðreyna að skilningur Símans á þeim væri réttur. PFS telur ekkert því til fyrirstöðu að fulltrúar stofnunarinnar og fulltrúar Símans hafi með sér samskipti við innleiðingu og eftirfylgni úrbótanna á næstu mánuðum.

III. Skýrsla Theron

3.1 Almennt

PFS mun hér að neðan gera stuttlega grein fyrir helstu niðurstöðum skýrslu Theron varðandi úttekt á öryggi upplýsinga hjá Símanum og tillögum skýrsluhöfundar til úrbóta. Að öðru leyti vísast til skýrslunnar, sem er meðfylgjandi ákvörðun þessari.

3.2 Frumskýrsla Theron frá maí 2011

Frumskýrsla Theron lá fyrir í maí 2011. Fyrsti kafli hennar hefur að geyma inngangskafla. Þar kemur m.a. fram um aðdraganda úttektarinnar að skýrsluhöfundur hafi að beiðni PFS framkvæmt úttekt á öryggisráðstöfunum hjá Símanum í tengslum við CDR færslur og úrvinnslu þeirra og að umfang verkefnisins hefði náð til allra upplýsingakerfa Símans sem vinna með eða meðhöndla CDR gögn. Fram kom að rætt hafi verið við 10 starfsmenn Símans við úttektina. Markmið úttektarinnar hefði verið að fá greinargóða lýsingu á samskiptum heildsölu og smásölu Símans hvað varðaði meðferð samtengiupplýsinga og tryggja lögmætan og eðlilegan aðgang að upplýsingum í CDR-grunni félagsins og tengdum kerfum, sbr. 26. gr. fjarskiptalaga. Þannig snéri úttektin að kerfunum sjálfum, því starfsfólki sem hefði aðgang að og ynni við þau og skipulagslegum þáttum varðandi fyrirkomulag öryggismála.

Í öðrum kafla frumskýrslunnar er fjallað um mat á gögnum. Grein er gerð fyrir afhentum gögnum sem samanstóðu af myndrænni og skriflegri lýsingu á miðlunarferli gagna úr CDR-grunni, skriflegri öryggisstefnu, áhættumati, öryggisráðstöfunum og afleiddum gögnum. Þá er gerð grein fyrir skoðun á kerfum og viðtölum við starfsmenn og m.a. fjallað um […][5]. Þá er sérstaklega fjallað um CDR-gögn, dagbækur, rýni á aðgangsréttindum og kínamúra í umræddum kafla.

Í þriðja kafla getur að líta niðurstöður skýrsluhöfundar og ábendingar um það sem betur mætti fara. Kaflinn skiptist í fjóra hluta, þ.e. stjórnkerfi upplýsingaöryggis, áhættumat, öryggisráðstafanir og annað. PFS birtir umræddan kafla hér í heild sinni:

> **Stjórnkerfi upplýsingaöryggis**
>
> Út frá þeim gögnum sem Síminn afhenti kemur fram að til staðar er formlegt stjórnkerfi upplýsingaöryggis. Öryggisstefna hefur verið samþykkt af forstjóra og kröfur um markmið skilgreindar. Eftir skoðun er hins vegar erfitt að sjá hvernig öryggisstefnu og markmiðum er fylgt eftir. Hluti af starfsemi Símans er vissulega vottuð samkvæmt ISO 27001 en það nær aðeins yfir hýsingu kerfa og búnaðar fyrir viðskiptavini en ekki vinnslu CDR gagna sem dæmi. Í gögnum frá Símanum var að finna áætlun um upplýsingaöryggi sem gerir ráð fyrir því að umbylta núverandi stjórnkerfi. Eins og staðan er í dag getur núverandi stjórnkerfi upplýsingaöryggis ekki talist vera nægilega virkt.
>
> ***Ábending:***
>
> Mikilvægt er að Síminn endurskoði vel núverandi skipulag stjórnkerfis upplýsingaöryggis og komi í framkvæmd áætlun um upplýsingaöryggi frá því í september 2010. Festa þarf betur í sessi nauðsynlegt verklag við framkvæmd öryggisráðstafana.

[5] Fellt brott vegna trúnaðar.

Áhættumat

Það áhættumat sem Síminn skilaði inn til PFS var aðeins fyrir hluta af þeim kerfum sem Síminn notar við meðhöndlun CDR gagna. Auk þess var matið ekki fullfrágengið þar sem ekki hafði verið lagt mat á skilgreindar ógnir fyrir einstaka kerfi ásamt því að mat á áhrifum ógna var í sumum tilfellum of lágt miðað við alvarleika ógnarinnar og tengingu þeirra við brot Símans.

Síminn gerir ráð fyrir því að nota RM Studio áhættumatskerfið við áhættumat í framtíðinni. Þetta kerfi var ekki notað að þessu sinni. Aðferðafræði við áhættumat er mismunandi eftir því hvort RM Studio er notað eða ekki.

Ábending:

Mikilvægt er að Síminn skilgreini eina aðferðafræði við framkvæmd áhættumats. Í áætlun um upplýsingaöryggi er „handvirka" aðferðafræðin skilgreind en jafnframt er tekið fram að nota eigi RM Studio. Þegar áhættumat er framkvæmt skiptir máli að telja fram ógnir, veikleika, áhrif, líkur, áhættustig, ráðstafanir til að draga úr áhættu og ráðstafanir sem þegar eru komnar í framkvæmd. Þetta mun gefa góða mynd af ástandi áhættu á hverjum tíma. Einnig er mikilvægt að áhættumat fyrir öll mikilvæg kerfi verði framkvæmt.

Öryggisráðstafanir

Öryggisráðstöfunum Símans má skipta í tvo flokka: ráðstafanir sem tengjast rekstri kerfa, t.d. afritun, tvöföldun mikilvægra kerfa, sérhæfðir vélasalir, varaafl o.þ.h.; ráðstafanir sem tengjast formlegum ferlum varðandi aðgangsstýringu, rýni á aðgang, eftirlit með notkun o.þ.h.

Í fyrri flokknum er Síminn með ágæta stöðu en í þeim síðari vantar talsvert upp á. Formleg aðgangsstýring er lítil sem engin. Starfsmenn óska í mörgum tilfellum sjálfir eftir aðgangi að gögnum og kerfum og þurfa ekki neina staðfestingu á heimild til aðgangs. Það er á valdi […][6] að ákveða hvort og þá hvaða aðgang notendur fá. Nánast engin skráning er til staðar um aðgangsveitingar og því ekki hægt að rekja slíkar aðgerðir.

Rýni á aðgang er óformleg. Yfirmenn þurfa ekki að rýna reglulega hvaða aðgang starfsmenn þeirra hafa. Ekki er krafa um að rýna aðgang kerfisstjóra eða stjórnenda kerfa. Þetta veldur því að of margir hafa kerfisstjóraaðgang. Ytri þjónustuaðilar geta í einhverjum tilfellum veitt aðgang að kerfum einnig en engar kröfur hafa verið settar á þá varðandi skráningu aðgerða sem þeir framkvæma. Þó svo […][7] sjái um aðgangsveitingu að mörgum kerfum þá eru samt aðrir aðilar sem einnig sjá um að veita aðgang. Þessir aðilar nota mismunandi kerfi við skráningar á aðferðum þannig að erfitt er að rekja hvernig aðgangsveiting fór fram, þ.e. hver heimilaði aðgang og hver framkvæmdi aðgangsveitingu.

Ábending:

Mjög mikilvægt er að koma á fót formlegum ferlum í tengslum við veitingu aðgangs að kerfum og gögnum. Sama ferli ætti að gilda fyrir öll kerfi og gögn. Allar aðgangsveitingar ætti að skrá í eitt kerfi til þess að auðvelda eftirlit og rýni. Tryggja þarf formlegt ferli þegar starfsmenn hætta störfum eða flytjast á milli starfa þannig að aðgangur verði aðlagaður að nýrri stöðu.

Yfirmenn ættu að rýna reglulega aðgang undirmanna sinna, auk þess sem rýna ætti aðgang kerfisstjóra reglulega. Þetta er eina örugga leiðin til þess að draga úr aðgangi notenda sem hafa hætt eða flust til í starfi.

Mjög mikilvægt er að setja formlegar reglur um lögmætan tilgang úrvinnslu upplýsinga úr Vöruhúsi gagna. Áður en nýjar skýrslur eru unnar úr Vöruhúsinu verður lögmæti þeirra vinnslu að vera ljóst.

[6] Fellt brott vegna trúnaðar.
[7] Fellt brott vegna trúnaðar.

Einnig er mikilvægt að skilgreina ferli við aðgangsveitingu að Vöruhúsi gagna þannig að gögn sem ekki eiga að fara á milli deilda verði ekki gerð aðgengileg, t.d. milli heildsölu og smásölu.

Annað

Varðveisla CDR gagna er 12 mánuðir en eftir það eru þeim eytt úr Vöruhúsi gagna. Það er hins vegar ekki ljóst hvort það sama gildi um aðra gagnagrunna þar sem CDR gögn eru geymd. Afrit af CDR gögnum eru til í þróunarkerfum einnig, en þar eru þau ekki með sömu aðgangsstýringum og í raunkerfum.

Í 42. gr. fjarskiptalaga er gert ráð fyrir því að gögnum verði eytt eða þau gerð nafnlaus á innan við 6 mánuðum enda sé ekki þörf á þeim lengur vegna innheimtu eða rannsókna sakamála.

Ábending:

Síminn þarf að skilgreina geymslu- og grisjunaráætlun fyrir öll fjarskiptagögn til þess að tryggja að gögn verði aðeins varðveitt í þann tíma sem lög gera ráð fyrir. Að þeim tíma loknum verði þeim eytt á öllum stöðum.

Í fjórða kafla getur að líta niðurlagsorð frumskýrslunnar. Fram kom að skoðun á gögnum frá Símanum, ásamt skoðun á kerfum og samtölum við starfsmenn hefðu gefið góða mynd af núverandi ástandi umræddra mála hjá félaginu. Í viðtölum við starfsmenn hefði ekki verið hægt að greina annað en að öll spil hefðu verið lögð á borðið og að vilji væri fyrir hendi að laga það sem að væri.

Þá kom fram að núverandi staða teldist ekki vera nægilega góð hvað varðaði aðgangsstýringar að gögnum og kerfum. Engin formleg ferli væru til staðar né samræmd kerfi sem notuð væru til að skrá beiðnir og aðgerðir þannig að rekjanleiki héldist. Síminn yrði að innleiða formleg ferli varðandi aðgangsstjórnun og eftirlit með notkun kerfa til þess að geta komið í veg fyrir ranga eða ólöglega notkun upplýsinga.

Eftirtalin atriði yrði Síminn að framkvæma:

1. Endurskoða öryggisstefnu þannig að ábyrgð verði rétt skilgreind.
2. Endurvinna áhættumat.
3. Innleiða formlegt ferli fyrir aðgangsstjórnun.
4. Innleiða formlegt ferli fyrir eftirlit með notkun kerfa og gagna.
5. Innleiða formlegt ferli fyrir rýni á aðgangi notenda.
6. Innleiða formlegt ferli fyrir lögmæta vinnslu gagna.
7. Tryggja þjálfun allra starfsmanna sem koma að aðgangsstjórnun.
8. Sjá til þess að eitt miðlægt kerfi verði notað við skráningu beiðna og aðgerða.
9. Gera geymslu- og grisjunaráætlun fyrir fjarskiptagögn.
10. Eyða gögnum eða gera nafnlaus á öllum stöðum, einnig í þróunarkerfum þegar lögbundnum líftíma þeirra líkur.

3.3 Viðaukaskýrsla Theron frá desember 2011

Viðbótarskýrsla Theron lá fyrir þann 6. desember 2011. Fram kom að svör Símans frá 8. nóvember 2011 hefðu svarað spurningum PFS og einungis styrkt fyrri skoðun skýrsluhöfundar frá maí 2011. Úr vöndu væri að ráða. Annars vegar þyrfti Síminn að uppfylla kröfur PFS um

eftirlit með virkni fjarskiptakerfa og hins vegar að gæta þess að vinna ekki með persónugreinanleg gögn samkvæmt fjarskiptalögum. Símanúmer eitt og sér teldist ekki vera persónugreinanlegt fyrr en búið væri að fletta númeri upp í símaskrá og tengja við nafn einstaklings. Samkvæmt svörum Símans væri þetta ekki stundað og engin tenging á símanúmerum samkeppnisaðila við nöfn einstaklinga framkvæmd.

Síminn hefði fulla heimild til reksturs á vöruhúsi gagna til þess að geta framkvæmt greiningar, fylgst með tekjum, gæðum þjónustu og öðrum lykiltölum sem nauðsynlegar væru við rekstur fyrirtækisins. Það sem ylli hins vegar vandræðum væru CDR gögn sem geymd væru í vöruhúsinu. CDR gögnin veittu möguleika á því að draga saman upplýsingar um viðskiptavini samkeppnisaðila Símans. Tekið væri fram að við úttekt á kerfum Símans hefði ekkert komið fram sem benti til misnotkunar á þessum upplýsingum. Hafa yrði þó í huga að úttektin hefði ekki verið tæmandi.

Ljóst væri að upplýsingar úr CDR færslum hefðu verið notaðar til að búa til ólögmætar upplýsingar um viðskiptavini samkeppnisaðila Símans. Einnig væri ljóst að Síminn þyrfti á upplýsingum úr CDR færslum að halda til þess að geta svarað fyrirspurnum eigin viðskiptavina og rækt eftirlitshlutverk sitt hvað varðaði gæði og rýmd. Ekki væri talin þörf á að skipta vöruhúsi gagna niður í hluta þar sem CDR gögn og önnur svipuð gögn væru staðsett í einum grunni meðan öll önnur gögn væru staðsett í sér grunni.

Mikilvægt væri að finna lausn, sem mögulegt væri fyrir Símann að útfæra, án þess að til kæmi óhóflegur kostnaður eða umbylting á núverandi kerfum. Lausnin þyrfti samt sem áður að uppfylla kröfur laga. Eina leiðin til þess að koma alveg í veg fyrir misnotkun CDR færslna væri að eyða upplýsingum úr þeim áður en þær væru fluttar inn í vöruhús gagna. Slíkt kæmi hins vegar í veg fyrir að Síminn gæti uppfyllt eftirlitshlutverk sinn og svarað fyrirspurnum viðskiptavina. Það væri því ljóst að fara þyrfti millileið sem drægi úr möguleikum á misnotkun CDR upplýsinga en kæmi ekki í veg fyrir að Síminn uppfyllti eftirlitshlutverk sitt. Á endanum yrði samt sem áður að treysta á það að starfsmenn Símans færu eftir settum reglum, bæði innri og ytri reglum. Út frá svörum Símans frá 6. júlí og 8 nóvember 2011 væri lagt til að Síminn:

1. Setji formlegar reglur varðandi meðhöndlun persónugreinanlegra upplýsinga ásamt því að setja formlegar reglur varðandi gerð fyrirspurna.
2. Setji formlegar reglur varðandi vinnslu fyrirspurna í vöruhúsi gagna.
3. Tryggi að fyrirspurnir í vöruhús gagna teljist ekki vera ólögmætar. Þetta er mögulegt með því að gefa Viðskiptagreind heimild til þess að synja fyrirspurn þar sem t.d. óskað er eftir upplýsingum um samkeppnisaðila eða þar sem númer hjá samkeppnisaðilum og nafn einstaklinga eru pöruð saman.
4. Tryggi formlega aðgangsstýringu og rýni á aðgang að grunngögnum og vöruhúsi gagna og geymslu á niðurstöðum slíkrar vinnu.
5. Tryggi það að símanúmer í CDR gögnum sem geymd eru í Datamart hluta vöruhússins geymi t.d. aðeins fyrstu fimm tölustafi í símanúmerum viðskiptavina samkeppnisaðila.
6. Tryggi að grunngögn CDR færslna verði einungis aðgengileg þeim aðilum sem starfs síns vegna þurfa á þeim að halda.
7. Tryggi að allar óskir um fyrirspurnir verði skráðar niður og formleg ákvörðun tekin um framkvæmd þeirra. Þessar skráningar geti PFS skoðað í úttektum og sannreynt hvort framkvæmdar hafa verið ólögmætar fyrirspurnir eða eftir þeim óskað.

8. Setja sér formlegar reglur um stöðugt eftirlit með notkun upplýsinga úr vöruhúsi gagna, t.d. með því að framkvæma stikkprufur á notkun vöruhússins.

IV.
Niðurstaða PFS

PFS tekur undir álit skýrsluhöfundar um að öryggisráðstafanir í tengslum við CDR-gagnagrunn Símans hafi verið ófullnægjandi að ýmsu leyti, auk þess sem sumar ráðstafanir reyndust við úttekt ekki vera virkar eða þeim ekki vera framfylgt sem skyldi. Jafnframt er það skoðun PFS að lýsing Símans á virkni og tilgangi s.k. Vöruhúss gagna hafi ekki verið fullnægjandi, en að fyrirtækið hafi bætt úr því undir rekstri málsins með ítarlegri upplýsingagjöf til stofnunarinnar, þannig aðgangsheimildir til samræmis við vinnslumöguleika í grunninum liggi nú fyrir með skjalfestum hætti. Með vísan til tillagna skýrsluhöfundar um eðlilegar og sanngjarnar úrbætur á öryggi CDR-gagnagrunnsins er það niðurstaða PFS að Síminn skuli ráðast í tilteknar úrbætur á öryggisskipulagi sínu sem taldar eru upp hér að neðan í 18 liðum. Fela þessar úrbætur m.a. í sér skipulagslegar og tæknilegar öryggisráðstafanir, svo og starfsmannatengdar ráðstafanir, sem eru til þess fallnar að draga úr, eins og kostur er, hættu á því að upplýsingar í grunninum verði misnotaðar í markaðslegum tilgangi, án þess þó að möguleikum til lögmætrar upplýsingavinnslu í gagnagrunninum verði fórnað, t.d. að geta veitt viðskiptavinum sundurliðar upplýsingar um fjarskiptanotkun sína.

Að öllu ofangreindu virtu, og þar sem Síminn hefur ekki andmælt fyrirhuguðum úrbótum sem PFS mælti fyrir um í framangreindu boðunarbréfi frá 6. desember s.l., mælir stofnunin hér með fyrir um það að Síminn skuli framkvæma eftirfarandi úrbætur varðandi meðferð trúnaðarupplýsinga sem félagið öðlast við gerð samtengisamninga, sér í lagi varðandi samskipti heildsölu og smásölu félagsins:

1. Endurskoðun öryggisstefnu þannig að ábyrgð yrði rétt skilgreind.
2. Áhættumat endurunnið.
3. Formlegt ferli fyrir aðgangsstjórnun innleitt.
4. Formlegt ferli fyrir eftirlit með notkun kerfa og gagna innleitt.
5. Formlegt ferli fyrir rýni á aðgangi notenda innleitt.
6. Formlegt ferli fyrir lögmæta vinnslu gagna innleitt.
7. Þjálfun allra starfsmanna sem koma að aðgangsstjórnun tryggð.
8. Sjá til þess að eitt miðlægt kerfi yrði notað við skráningu beiðna og aðgerða.
9. Geymslu- og grisjunaráætlun gerð fyrir fjarskiptagögn.
10. Gögnum eytt eða þau gerð ópersónugreinanleg á öllum stöðum (einnig í þróunarkerfum) þegar lögbundnum líftíma þeirra lyki.
11. Formlegar reglur varðandi meðhöndlun persónugreinanlegra upplýsinga settar, ásamt reglum um gerð fyrirspurna.
12. Formlegar reglur varðandi vinnslu fyrirspurna í vöruhúsi gagna settar.
13. Tryggt að fyrirspurnir í vöruhús gagna teldust ekki vera ólögmætar. Þetta væri mögulegt með því að gefa Viðskiptagreind heimild til þess að synja fyrirspurn þar sem t.d. óskað væri eftir upplýsingum um samkeppnisaðila eða þar sem númer hjá samkeppnisaðilum og nafn einstaklinga væru pöruð saman.

14. Formleg aðgangsstýring og rýni á aðgang að grunngögnum og vöruhúsi gagna tryggð, ásamt geymslu á niðurstöðum slíkrar vinnu.
15. Tryggt að símanúmer í CDR gögnum, sem geymd væru í Datamart hluta vöruhússins, geymdu t.d. aðeins fyrstu fimm tölustafi í símanúmerum viðskiptavina samkeppnisaðila.
16. Tryggt að grunngögn CDR færslna yrði einungis aðgengileg þeim aðilum sem starfs síns vegna þyrftu á þeim að halda.
17. Tryggt að allar óskir um fyrirspurnir yrðu skráðar niður og formleg ákvörðun tekin um framkvæmd þeirra. Þessar skráningar gæti PFS skoðað í úttektum og sannreynt hvort framkvæmdar hefðu verið ólögmætar fyrirspurnir eða eftir þeim óskað.
18. Formlegar reglur settar um stöðugt eftirlit með notkun upplýsinga úr vöruhúsi gagna, t.d. með því að framkvæma stikkprufur á notkun vöruhússins.

Að mati PFS er umfang ofangreindra úrbóta til marks um það að ástand öryggismála hjá Símanum í tengslum við CDR-gagnagrunninn hafi verið fjarri því að vera viðunandi. Ljóst er því að þær forsendur sem PFS lagði til grundvallar í ákvörðun sinni nr. 37/2010, um þörf á úttekt á umræddum gagnagrunni, reyndust á rökum reistar. Telur PFS mikilvægt að Síminn taki öryggisskipulag sitt til reglubundinnar endurskoðunar og viðhafi fyllsta samstarf við PFS um að stuðla að því að öryggisskipulagið uppfylli á hverjum tíma, eins og kostur er, kröfur reglna PFS nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

PFS hyggst verða við óskum Símans um rýmri frest til innleiðingar ofangreindra úrbóta. Innleiðingu úrbótanna skal að fullu lokið eigi síðar en 31. desember 2012. Auk þess skal a.m.k. helmingi þeirra lokið þann 1. júlí sama ár. Símanum ber að afhenda PFS framkvæmdaáætlun eigi síðar en 15. febrúar n.k., auk stöðuskýrslna þann 1. júlí 2012 og 2. janúar 2013. Símanum ber að tilkynna PFS ef framkvæmdaáætlun tefst.

Ákvörðunarorð

Síminn skal gera úrbætur í neðangreindum 18 liðum, varðandi meðferð trúnaðargagna sem félagið öðlast við gerð samtengisamninga, sér í lagi varðandi samskipti heildsölu og smásölu félagsins. Innleiðingu úrbótanna skal að fullu lokið eigi síðar en 31. desember 2012, auk þess sem a.m.k. helmingi þeirra skal lokið þann 1. júlí sama ár.

1. **Endurskoðun öryggisstefnu þannig að ábyrgð yrði rétt skilgreind.**
2. **Áhættumat endurunnið.**
3. **Formlegt ferli fyrir aðgangsstjórnun innleitt.**
4. **Formlegt ferli fyrir eftirlit með notkun kerfa og gagna innleitt.**
5. **Formlegt ferli fyrir rýni á aðgangi notenda innleitt.**
6. **Formlegt ferli fyrir lögmæta vinnslu gagna innleitt.**
7. **Þjálfun allra starfsmanna sem koma að aðgangsstjórnun tryggð.**
8. **Sjá til þess að eitt miðlægt kerfi yrði notað við skráningu beiðna og aðgerða.**
9. **Geymslu- og grisjunaráætlun gerð fyrir fjarskiptagögn.**

10. **Gögnum eytt eða þau gerð ópersónugreinanleg á öllum stöðum (einnig í þróunarkerfum) þegar lögbundnum líftíma þeirra lyki.**
11. **Formlegar reglur varðandi meðhöndlun persónugreinanlegra upplýsinga settar, ásamt reglum um gerð fyrirspurna.**
12. **Formlegar reglur varðandi vinnslu fyrirspurna í vöruhúsi gagna settar.**
13. **Tryggt að fyrirspurnir í vöruhús gagna teldust ekki vera ólögmætar. Þetta væri mögulegt með því að gefa Viðskiptagreind heimild til þess að synja fyrirspurn þar sem t.d. óskað væri eftir upplýsingum um samkeppnisaðila eða þar sem númer hjá samkeppnisaðilum og nafn einstaklinga væru pöruð saman.**
14. **Formleg aðgangsstýring og rýni á aðgang að grunngögnum og vöruhúsi gagna tryggð, ásamt geymslu á niðurstöðum slíkrar vinnu.**
15. **Tryggt að símanúmer í CDR gögnum, sem geymd væru í Datamart hluta vöruhússins, geymdu t.d. aðeins fyrstu fimm tölustafi í símanúmerum viðskiptavina samkeppnisaðila.**
16. **Tryggt að grunngögn CDR færslna yrði einungis aðgengileg þeim aðilum sem starfs síns vegna þyrftu á þeim að halda.**
17. **Tryggt að allar óskir um fyrirspurnir yrðu skráðar niður og formleg ákvörðun tekin um framkvæmd þeirra. Þessar skráningar gæti PFS skoðað í úttektum og sannreynt hvort framkvæmdar hefðu verið ólögmætar fyrirspurnir eða eftir þeim óskað.**
18. **Formlegar reglur settar um stöðugt eftirlit með notkun upplýsinga úr vöruhúsi gagna, t.d. með því að framkvæma stikkprufur á notkun vöruhússins.**

Ákvörðun þessi er kæranleg til úrskurðarnefndar fjarskipta- og póstmála, sbr. 13. gr. laga nr. 69/2003, um Póst- og fjarskiptastofnun. Kæran skal berast úrskurðarnefnd innan fjögurra vikna frá því viðkomandi var kunnugt um ákvörðun Póst- og fjarskiptastofnunar. Um kostnað vegna málskots fer samkvæmt 5. mgr. 13. gr. sömu laga, auk þess sem greiða ber sérstakt málskotsgjald að upphæð kr. 150.000, skv. 6. gr. reglugerðar nr. 39/2009 um úrskurðarnefnd fjarskipta- og póstmála.

Reykjavík, 6. janúar 2012

_____

Hrafnkell V. Gíslason

_____

Óskar H. Ragnarsson

Fylgiskjöl:

Úttektarskýrsla Theron frá desember 2011. [TRÚNAÐUR]
Reikningur PFS varðandi úttekt á CDR-grunni Símans, dags. 4. janúar 2012. [TRÚNAÐUR]