PÓST- OG FJARSKIPTASTOFNUN

Ákvörðun nr. 37/2014

Úttekt Póst- og fjarskiptastofnunar á verklagsreglum IP fjarskipta ehf. um meðferð persónuupplýsinga og eyðingu gagna um fjarskipti.

I.
Almennt

Póst- og fjarskiptastofnun hefur viðtæku eftirlitshlutverki að gegna á íslenskum fjarskiptamarkaði og hefur umsjón með framkvæmd laga, nr. 81/2003, um fjarskipti, sbr. 2. mgr. 2. gr. þeirra. Þá hefur stofnunin eftirlit með því að starfsemi fjarskiptafyrirtækja sé í samræmi við lög og afleiddar réttarheimildir sem um starfsemina gilda, sbr. 4. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun. Stofnuninni er skylt að fylgjast með að starfsemi fjarskiptafyrirtækja uppfylli þau skilyrði sem ákvæði fjarskiptalaga, og reglna settra með stoð í þeim, kveða á um. Þannig getur stofnunin, til að framfylgja eftirlitshlutverki sínu, m.a. hafið skoðun á ákveðnum atriðum í starfsemi fjarskiptafyrirtækja að eigin frumkvæði.

Póst- og fjarskiptastofnun hefur nú gert úttekt, sem framkvæmd var af Capacent ehf., á framfylgni IP fjarskipta ehf. (Tals), sem og fjögurra annarra fjarskiptafyrirtækja, á 42. gr. fjarskiptalaga og á verklagsreglum félagsins um meðferð persónuupplýsinga og eyðinga ganga, sbr. 7. mgr. 42. gr. fjarskiptalaga.

Að mati Póst- og fjarskiptastofnunar er niðurstaða úttektar Capacent ehf. mjög afgerandi og jákvæð. Ekki fundust í úttekt Capacent ehf. nein *meiriháttar frábrigði* sem kölluðu á tímasetta áætlun til endurbóta eða eftirfylgni af hálfu úttektaraðila. Líkt og gerð verður grein fyrir í ákvörðun þessari fann úttektaraðili einungis þrjú *minniháttar frábrigði* er hann taldi að mögulega vörðuðu 42. gr. fjarskiptalaga nr. 81/2003. Að lokinn málsmeðferð Póst- og fjarskiptastofnunar er niðurstaðan sú að IP fjarskipti ehf. hafi staðist úttekt stofnunarinnar á verklagsreglum félagsins um meðferð persónuupplýsinga og eyðingu gagna, sbr. 7. mgr. 42. gr. laga, nr. 81/2003, þótt minniháttar frávik frá 42. gr. fjarskiptalaga hafi fundist.

II.
Lagaumhverfi

2.1 Almennt

Í IX. kafla laga nr. 81/2003, um fjarskipti er fjallað um vernd persónuupplýsinga og friðhelgi einkalífsins. Er í 42. gr. laganna fjallað um gögn um fjarskipti, meðferð þeirra og eyðingu en í ákvæðinu segir:

> *Gögnum um fjarskiptaumferð notenda sem geymd eru og fjarskiptafyrirtæki vinnur úr skal eyða eða gera nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu ákveðinnar fjarskiptasendingar.*
>
> *Gögn um fjarskiptanotkun sem nauðsynleg eru til reikningsgerðar fyrir áskrifendur og uppgjörs fyrir samtengingu má geyma þar til ekki er lengur hægt að vefengja reikning eða hann fyrnist.*
>
> *Þrátt fyrir ákvæði 1. og 2. mgr. skulu fjarskiptafyrirtæki, í þágu rannsókna sakamála[)] og almannaöryggis, varðveita lágmarksskráningu gagna um fjarskiptaumferð notenda í sex mánuði. Lágmarksskráningin skal tryggja að fjarskiptafyrirtæki geti upplýst hver af viðskiptavinum þess var notandi tiltekins símanúmers, IP-tölu eða notandanafns, jafnframt því að upplýsa um allar tengingar sem notandinn hefur gert, dagsetningar þeirra, hverjum var tengst og magn gagnaflutnings til viðkomandi notanda. Fjarskiptafyrirtæki skal tryggja vörslu framangreindra gagna og er óheimilt að nota eða afhenda umræddar upplýsingar öðrum en lögreglu eða ákæruvaldi í samræmi við ákvæði 3. mgr. 47. gr. Eyða ber umferðargögnunum að þessum tíma liðnum enda sé ekki þörf fyrir þau á grundvelli 2. mgr.*
>
> *Með samþykki áskrifanda er fjarskiptafyrirtæki heimilt að vinna úr gögnum skv. 1. mgr. vegna markaðssetningar fjarskiptaþjónustu eða framboðs á virðisaukandi þjónustu að því leyti sem nauðsynlegt er fyrir slíka þjónustu eða markaðssetningu. Samþykki má afturkalla hvenær sem er.*
>
> *Þjónustuveitandi skal upplýsa áskrifendur fyrir fram um hvaða gögn um fjarskiptanotkun eru tekin til úrvinnslu og hversu lengi úrvinnsla mun standa.*
>
> *Úrvinnslu gagna samkvæmt þessari grein skulu þeir einir sinna sem eru undir stjórn fjarskiptafyrirtækja og sjá um gerð reikninga eða stjórnun fjarskiptaumferðar, fyrirspurnir notenda, upplýstrun misferlis, markaðssetningu fjarskiptaþjónustu eða virðisaukandi þjónustu og skal úrvinnslan einskorðast við það sem er nauðsynlegt í þágu slíkrar starfsemi.*
>
> *Fjarskiptafyrirtæki skulu setja sér verklagsreglur um meðferð persónuupplýsinga og eyðingu gagna í samræmi við ákvæði þessarar greinar og skilyrði sem Persónuvernd kann að setja.*

Ákvæðið fjallar í fyrsta lagi um eyðingu og geymslu fjarskiptaumferðarupplýsinga, sbr. 1.-3. og 7. mgr. ákvæðisins, og í öðru lagi um vinnslu þeirra, sbr. 4.-6. mgr. ákvæðisins og byggir að mestu leyti á 6. gr. tilskipunar Evrópuþingsins og Ráðsins 2002/58/EB um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta. Reglur Evrópusambandsins á þessu sviði eiga sér nokkra sögu og hefur verið talin þörf á að grípa til verndarráðstafana svo ekki sé brotið gegn friðhelgi einkalífs. Með tilskipun nr. 2002/58/EB (og forvera hennar) voru meginreglur, sem settar voru fram í tilskipun nr. 95/46/EB, um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga, yfirfærðar í sértækar reglur fyrir fjarskiptasviðið og eru ákvæði hennar viðbót og nánari

umfjöllun um ákvæði síðarnefndu tilskipunarinnar, sbr. 2. mgr. 1. gr. og 4. lið inngangsorða tilskipunar nr. 2002/58/EB.

Við gildistöku fjarskiptalaga árið 2003 innihélt ákvæði 42. gr. fimm málsgreinar en árið 2005 tóku gildi lög um breytingu á lögum um fjarskipti, nr. 81/2003, sem breytti ákvæðinu með þeim hætti að við bættust tvær nýjar málsgreinar, þ.e. núgildandi 3. mgr., sem kveður á um varðveislu lágmarksskráningu gagna um fjarskiptaumferð í sex mánuði, og núgildandi 7. mgr. sem kveður á um skyldu fjarskiptafyrirtækja að setja sér reglur um meðferð persónuupplýsinga og eyðingu gagna.

2.2 Varðveisla og eyðing gagna um fjarskiptaumferð

2.2.1 Meginregla 1. mgr. 42. gr. um eyðingu upplýsinga

Fyrsta málsgrein 42. gr. felur í sér þá meginreglu að fjarskiptafyrirtækjum er skylt að eyða gögnum um fjarskiptaumferð eða gera þau nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu ákveðinnar fjarskiptasendingar. Frá þessari kröfu er þó að finna tvær undanþágur. Í fyrsta lagi þá er fjarskiptafyrirtækjum heimilt að geyma þau gögn sem nauðsynleg eru til reikningsgerðar fyrir áskrifendur og uppgjörs fyrir samtengingu þar til ekki er lengur hægt að vefengja reikning eða hann fyrnist, sbr. 2. mgr. ákvæðisins. Í öðru lagi er fjarskiptafyrirtækjunum skylt, í þágu rannsókn sakamála og almannaöryggis, að varðveita ákveðna lágmarksskráningu gagna um fjarskiptaumferð í sex mánuði, sbr. 3. mgr. ákvæðisins.

Í frumvarpi er varð að fjarskiptalögum árið 2003 kemur fram að 1. mgr. ákvæðisins geri þá kröfu að gögnum um fjarskiptaumferð áskrifenda sé eytt eftir að þeirra er ekki þörf við stýringu og afgreiðslu fjarskiptanna. Segir í athugasemdunum að við *„ ... sendingu hvers konar fjarskipta verða til í netum og stoðkerfum ýmsar upplýsingar, t.d. um leiðir sem valdar hafa verið fyrir sambandið hverju sinni, lengd þeirra, tímasetningu og magn ... “* en ekki sé nauðsynlegt að geyma öll þessi gögn eftir að samband hefur verið rofið. Í ákvörðun Póst- og fjarskiptastofnunar nr. 29/2011 kom fram sú afstaða stofnunarinnar að þessar upplýsingar væru almennt taldar vera þær *„ ... tengiupplýsingar sem verða til í fjarskiptaneti og greiðslukerfum fjarskiptafyrirtækja vegna fjarskiptanotkunar viðskiptavina og liggja til grundvallar gjaldfærslu fyrir þjónustuna“*.

Ákvæðið fjallar um geymslu, vinnslu og aðra meðhöndlun umferðargagna og byggir, líkt og áður segir, á 6. gr. persónuverndartilskipun Evrópusambandsins á sviði fjarskipta nr. 2002/58/EB. Í 6. gr. hennar er fjallað um umferðargögn, þ.e. gögn sem unnin eru í þeim tilgangi að flytja fjarskiptasendingu á rafrænu fjarskiptaneti eða til að gefa út reikninga vegna þess, sbr. b lið 2. mgr. 2. gr. tilskipunarinnar. Er í 1. mgr. 6. gr. kveðið á um eyðingu umferðargagnanna eða aðskilnað þeirra frá nafni áskrifanda um leið og þau eru ekki lengur þörf til að senda fjarskiptasendingu, sbr. þó undanþáguákvæði annarra málsgreina ákvæðisins. Er í þeim málsgreinum að finna samhljóða undanþágu og í 2. mgr. 42. gr., þ.e. að heimilt er að vinna úr gögnum sem nauðsynleg eru til útgáfu reikninga en slík vinnsla er þó einungis heimil til loka þess tímabils þegar lögum samkvæmt er hægt að vefengja reikning eða krefjast greiðslu.

Í 26. gr. inngangsorða tilskipunarinnar kemur einnig fram að gögn um áskrifendur, sem notuð eru á rafrænum fjarskiptanetum til að koma á tengingum og til að senda upplýsingar,

innihalda upplýsingar um einkalíf einstaklinga og snerta rétt þeirra til að samskiptin séu bundin trúnaði eða þau snerta réttmæta hagsmuni lögaðila. Kemur líka fram að slík gögn megi aðeins geyma að því marki sem nauðsynlegt er til að veita þjónustuna, gefa út reikninga og innheimta gjöld fyrir samtenginu og einungis í takmarkaðan tíma. Samkvæmt 29. lið inngangsorðanna er fjarskiptafyrirtækjum þó heimilt að vinna umferðargögn um áskrifendur í einstökum tilvikum og eins þau umferðargögn sem nauðsynleg eru vegna útgáfu reikninga til koma upp um og stöðva svik sem felast í ógreiddri notkun rafrænu fjarskiptaþjónustunnar.

Þannig er markmið 42. gr. að tryggja einkalíf áskrifenda með sem bestum hætti og er, að mati Póst- og fjarskiptastofnunar, nauðsynlegt að samlesa ákvæðið með tilliti til 47. gr. fjarskiptalaga en saman er þessum ákvæðum ætlað að tryggja fjarskiptaleynd, sbr. 5. gr. framangreindrar tilskipunar. Þannig ber fjarskiptafyrirtækjum að eyða innihaldi fjarskiptasendingar án tafar eftir afgreiðslu hennar. Eins skulu fjarskiptafyrirtækin uppfylla afdráttarlausa kröfu 42. gr. laganna, þ.e. að upplýsingum um fjarskiptaumferð sé eytt eða þau gerð nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu hennar nema þegar undanþáguákvæði 2. og 3. mgr. eiga við.

Að mati Póst- og fjarskiptastofnunar er nokkuð ljóst hvað átt er við eyðingu gagna skv. 1. mgr. ákvæðisins. Aftur á móti er fjarskiptafyrirtækjum heimilt að gera þau nafnlaus en að mati stofnunarinnar verður að telja að í því felist að gögnin séu gerð ópersónugreinanleg, þ.e. að umferðargögnin verði með engum hætti rakin til viðkomandi áskrifanda. Þannig verða fjarskiptafyrirtæki sem einungis gera upplýsingar um fjarskiptaumferð nafnlausar að tryggja að með engum hætti sé hægt, eftir að nafnleysi er tryggt, að upplýsingarnar verða tengdar aftur við viðkomandi áskrifanda. Svo markmiði um fjarskiptaleynd og friðhelgi einkalífs sé náð og virt er það mat Póst- og fjarskiptastofnunar að ekki sé einungis um nafn notenda að ræða í þessu samhegni heldur allar upplýsingar sem geta persónugreint hann, svo sem kennitala, heimilisfang o.s.frv.

2.2.2 Undanþága 2. mgr. 42. gr. vegna reikningagerðar

Í 2. mgr. ákvæðisins kemur fram að geyma megi gögn um fjarskiptanotkun, sem nauðsynleg eru til reikningsgerðar fyrir áskrifendur og uppgjörs fyrir samtengingu, þar til ekki er lengur hægt að vefengja reikning eða hann fyrnist. Í athugasemdum við frumvarp er varð að fjarskiptalögum kemur fram að þótt eyða bera gögnum um fjarskiptaumferð feli 2. mgr. í sér heimild til að geyma þann hluta gagnanna sem nauðsynlegur er fyrir gerð reikninga. Sú heimild gildi til þess tíma þegar reikningur verður ekki vefengdur eða hann fyrnist.

Í framangreindri ákvörðun Póst- og fjarskiptastofnunar nr. 29/2011 komst stofnunin að þeirri niðurstöðu að hámarks varðveislutími fjarskiptaumferðarupplýsinga geti að hámarki verið sex mánuðir þegar reikningur hefur verið greiddur. Þessar upplýsingar, sem reikningar byggja á, séu gjaldfærsluupplýsingar sem í eðli sínu eru persónurekjanlegar. Í samandreginni niðurstöðu stofnunarinnar segir varðveislutími fjarskiptaumferðarupplýsinga, skv. 2. mgr. ákvæðisins, skuli afmarkaður á almennan á sjálfstæðan hátt og eingöngu á grundvelli brýnnar nauðsynjar, svo sem til þess að geta brugðist við vefengingu reiknings innan hæfilegs tíma frá því hann hefur verið greiddur. Sá tími, geti að mati stofnunarinnar, að hámarki verið sex mánuðir, enda gildi lengri varðveislutími fyrir reikninga sem eru í vanskilum. Þannig skuli eyða

upplýsingum eða gera þær ópersónugreinanlegar við lok skilgreinds varðveislutíma hafi reikningur verið greiddur.

Í ákvörðun stofnunarinnar er vísað til álits svo kallaðs 29. gr. starfshóps sem settur var á fót á grundvelli 29. gr. tilskipunar nr. 95/46/EB, sbr. 30. gr. hennar og 3. mgr. 15. gr. tilskipunar nr. 2002/58/EB. Er honum ætlað að vera samráðsvettvangur allra persónuverndarstofnana innan EES-svæðisins, og er ætlað að fjalla um vernd persónuupplýsinga og stuðla að einsleitri framkvæmd löggjafarinnar. Í 48. lið inngangsorða tilskipunarinnar 2002/58/EB kemur fram að við beitingu hennar geti verið gagnlegt að líta til reynslu þessa starfshóps en í áliti starfshópsins nr. 1/2009 kemur fram sú afstaða hans að sex mánaða varðveislutíma fjarskiptaumferðarupplýsinga, vegna reikningagerðar og mögulegrar vefengingar á þeim, sé nægjanlegur, hóflegur og sanngjarn varðveislutími.[1]

2.2.3 Skylda til varðveislu lágmarksskráningar skv. 3. mgr. 42. gr.

Líkt og áður segir kom ákvæði 3. mgr. ákvæðisins inn með breytingarlögum árið 2005 og hefur að geyma undanþágu frá 1. mgr. ákvæðisins. Ákvæðið er sett með vísan til heimildarákvæðis 1. mgr. 15. gr. áðurnefndrar tilskipunar, sbr. 1. mgr. 6. gr. hennar,[2] og gerir 3. mgr. fjarskiptafyrirtækjum skylt, í þágu rannsókna sakamála og almannaöryggis, að varðveita lágmarksskráningu gagna um fjarskiptaumferð notanda í sex mánuði. Slík lágmarksskráning skal tryggja að fjarskiptafyrirtæki geti upplýst hver af viðskiptavinum þess var notandi tiltekins símanúmer, IP-tölu eða notandanafns, jafnframt því að upplýsa um allar tengingar sem notandinn hefur gert, dagsetningar þeirra, hverjum var tengst og magn gagnaflutnings til viðkomandi notanda. Eftir þennan sex mánaða tíma er fyrirtækjunum jafnframt skylt að eyða þeim sé þeirra ekki enn þörf á grundvelli 2. mgr. greinarinnar, þ.e. vegna vanskila.

Undanþáguákvæði 3. mgr. var sett að ósk ríkislögreglustjóra og miðar að því að tryggja lögreglu og ákæruvaldi nægjanlegt svigrúm til að upplýsa brot að uppfylltum skilyrðum ákvæða sakamálalaga nr. 88/2008. Er fjarskiptafyrirtækjum jafnframt óheimilt að nota eða afhenda umræddar upplýsingar öðrum en lögreglu eða ákæruvaldi, sbr. núgildandi 7. mgr. 47. gr. fjarskiptalaga.[3] Í athugasemdum við umrætt breytingarlagafrumvarp segir að eftirfarandi gögn séu nauðsynleg til að tryggja að upplýsa megi brot sem framan eru á internetinu:

> *1. Gögn um hver sé notandi tiltekins fjarskiptatækis.*
>
> ** Tölva sem tengist netinu og er auðkennd með IP-tölu, tryggja þarf að hægt sé að finna hver er notandi IP-tölunnar á hverjum tíma og varðveita þarf skrár með þessum upplýsingum,*
>
> ** IP-tölur kunna að vera breytilegar þannig að tímasetning á notkuninni er skilyrði þess að hægt sé að tengja hana ákveðnum áskrifanda eða notanda. Tenging er þá gerð þannig að þegar viðkomandi viðskiptavinur tengist fær hann úthlutað IP-tölu úr safni internetþjónustuaðilans sem hann hefur yfirráð yfir,*

[1] Opinion 1/2003 of the Article 29 Data Protection Working Party on the storage of traffic data for billing purpose frá 29. janúar 2003

[2] Síðar tók gildi tilskipun Evrópuþingsins og Ráðsins nr. 2006/24/EC.

[3] Í ákvæði 3. mgr. 42. gr. fjarskiptalaga er vísað til 3. mgr. 47. gr. laganna. Breytingar hafa verið gerðar á síðarnefndu greininni, sbr. lög nr. 39/2007, um breytingu á lögum um fjarskipti nr. 81/2003, þar sem fjórum málsgreinum var bætt inn í 47. gr. fjarskiptalaga. Þessar breytingar leiða að tilvísun 3. mgr. 42. gr. ætti að vera í 7. mgr. 47. gr.

** IP-tala þarf að vera rekjanleg til síma eða annars fjarskiptatækis sem áskrifandi notar til að tengjast inn á kerfi internetþjónustuaðila og áfram út á netið. Til þess að hægt sé að staðfesta hvar tenging á uppruna sinn þarf internetþjónustuaðili að varðveita skrá um úr hvaða símanúmeri eða öðru fjarskiptatæki viðkomandi tengist inn á tölvukerfi hans,*

** óskráð farsímanúmer og símanúmer geta valdið vanda í þessu efni þegar tengst er internetþjónustuaðila með farsíma með frelsiskorti og óskráðu símanúmeri.*

2. Gögn um hverjum hann tengist. Við hvaða IP-tölur á viðkomandi samskipti, tengingar? Þegar leiða á í ljós tengsl við ákveðna starfsemi eða aðila, t.d. dreifingu barnakláms, þarf að vera hægt að sanna hvort viðkomandi tengdist ákveðinni IP-tölu.

3. Gögn um hvenær átti sú tenging sér stað. Nauðsynlegt til að finna samhengi atburða við tengingar viðkomandi.

4. Gögn um hversu lengi tenging vari. Atvik geta átt sér stað nokkru eftir að tengingu er komið á, e.t.v. einhverjum klukkustundum.

5. Gögn um hversu mikið af gögnum var flutt á milli aðila.

Í frumvarpinu var lagt til að geymslutími þessarar lágmarksskráningu gagna sem fjarskiptafyrirtækjum væri skylt að varðveita yrðu tólf mánuðir. Í þinglegri meðferð þáverandi samgöngunefndar var gerð sú breyting á frumvarpinu og varðveislutíminn var styttur úr tólf mánuðum niður í sex mánuði. Taldi meiri hluti nefndarinnar að í ákvæðinu vægust á almannahagsmunir og réttur einstaklinga til persónuverndar og á grundvelli meðalhófs og m.t.t. til umsagnar Persónuverndar við frumvarpið, sem taldi tólf mánaða varðveislutíma ekki samrýmast meðalhófssjónarmiðum sem viðra bæri við meðferð persónuupplýsinga, var gerð framangreind breytingartillaga á frumvarpinu, sem síðar var samþykkt af þinginu.

Að öllu framangreindu virtu er ljóst að mati Póst- og fjarskiptastofnunar að rík áhersla er lögð á að tryggja með sem bestum hætti friðhelgi einkalífs einstaklinga þegar kemur að fjarskiptanotkun þeirra. Ákvæði 42. gr. og 47. gr. fjarskiptalaga og framangreindrar tilskipunar Evrópusambandsins gera þá kröfu að innihald fjarskiptasendinga sé ekki geymt og upplýsingum um fjarskiptaumferð skuli eytt þegar reikningur hafi verið greiddur eða verði ekki vefengdur, þ.e. að hámarki eftir sex mánuði. Annað gildir um reikninga í vanskilum. Þá nær skylda 3. mgr. 42. gr. til varðveislu lágmarksskráningar í þágu rannsókna sakamála og almannaöryggis jafnframt til sex mánaða tímabils og skal eytt að því loknu. Þannig ættu ekki að finnast neinar persónugreinanlegar upplýsingar um fjarskiptaumferð í kerfum fjarskiptafyrirtækja að sex mánuðum liðnum nema þegar reikningur hefur ekki verið greiddur.

2.2.4 Krafa 7. mgr. 42. gr. um gerð verklagsreglna

Ákvæði 7. mgr. 42. gr. kom inn með breytingarlögum árið 2005. Í ákvæðinu er set sú skylda á fjarskiptafyrirtæki að þau setji sér verklagsreglur um meðferð persónuupplýsinga og eyðingu gagna í samræmi við ákvæði 42. gr. og skilyrði sem Persónuvernd kann að setja.

Í athugasemdum við frumvarp það er varð að umræddum breytingarlögum segir að um nýmæli sé að ræða og það sé í samræmi við athugasemdir sem m.a. Persónuvernd hefur sett

fram um meðferð og eyðingu gagna í vörslum fjarskiptafyrirtækjanna. Samkvæmt ákvæðinu skulu fjarskiptafyrirtækin setja sér verklagsreglur um hvernig sé staðið að þessum málum í starfsemi þeirra og um eyðingu gagna.

2.3 Vinnsla gagna um fjarskiptaumferðarupplýsingar

2.3.1 Heimild til úrvinnslu upplýsinga um fjarskiptaumferð

Í 4.-6. mgr. 42. gr. fjarskiptalaga er fjallað um mögulega vinnslu gagna um fjarskiptaumferð, skv. 1. mgr. ákvæðisins, vegna markaðssetningar fjarskiptaþjónustu eða framboðs á virðisaukandi þjónustu, að því leyti sem nauðsynlegt er fyrir slíka þjónustu eða markaðssetningu. Slík vinnsla er háð samþykki áskrifenda sem hann getur afturkallað hvenær sem er. Áður en úrvinnsla hefst skal fjarskiptafyrirtækið upplýsa áskrifendur um hvort tveggja hvaða gögn um fjarskiptanotkun eru tekin til úrvinnslu sem og hversu lengi úrvinnslan mun standa. Þá eru jafnframt sett ákveðin skilyrði um hverjir geti komið að úrvinnslunni og við hvað hún skuli einskorðast.

Í athugasemdum við framvarp er varð að fjarskiptalögum segir að þrátt fyrir ákvæði 1. mgr. um eyðingu fjarskiptaumferðarupplýsinga sé fjarskiptafyrirtæki heimilt, að fengnu samþykki áskrifanda, að vinna úr gögnunum. Sem dæmi um vinnslu eru leiðbeiningar um ódýrustu kosti í þjónustunni, upplýsingar um leiðir, upplýsingar um götu- og vegaumferð, veðurspár og ferðamannaupplýsingar. Segir jafnframt að krafa sé *„ ... gerð um það að þjónustuveitandi upplýsi áskrifendur eða notendur fyrir fram um hvaða gögn hann ætlar að taka til vinnslu og hversu lengi unnið verður úr gögnunum í þeim tilgangi sem heimilaður hefur verið.“*

Í áðurnefndri 6. gr. tilskipunar Evrópusambandsins er einnig fjallað um þessa heimild til að vinna úr umræddum gögnum, sbr. 2.-5. mgr. greinarinnar. Eru ákvæðin efnislega samhljóða 4.-6. mgr. 42. gr. fjarskiptalaga, og kveða á um sömu og skilyrði. Er einungis heimilt að vinna úr gögnum um fjarskiptaumferð þegar áskrifandi eða notandi hefur gefið fyrirfram samþykki sitt fyrir vinnslunni. Krafa er gerð um að þjónustuveitandi upplýsi áskrifanda og notenda um þær tegundir umferðargagna sem unnin eru og um það hve lengi vinnslan varir og, áður en samþykki er fengið, í þeim tilgangi sem kveðið er á um í 3. mgr. ákvæðisins, þ.e. markaðslegum tilgangi og við veitingu virðisaukandi þjónustu.

Í 26. lið inngangsorða tilskipunarinnar er að finna frekari umfjöllun um þessa mögulegu vinnslu. Þar segir að öll frekari vinnsla gagna um áskrifendur, sem eru notuð á rafrænum fjarskiptanetum til að koma á tengingum og til að senda upplýsingar, sem fjarskiptafyrirtæki kann að hafa hug á, í því skyni að markaðssetja rafræna fjarskiptaþjónustu eða veita virðisaukandi þjónustu, er einungis leyfileg hafi áskrifandi *„ ... veitt samþykki sitt á grundvelli réttra og ítarlegra upplýsinga frá veitanda rafrænnar fjarskiptaþjónustu, sem er öllum aðgengileg, um það hvers konar frekari vinnslu hann áformar og um rétt áskrifandans til að veita ekki eða afturkalla samþykki sitt fyrir slíkri vinnslu.“* Þá er jafnframt tilgreint að umferðargögnum sem notuð eru til markaðssetningar eða til að veita virðisaukandi þjónustu skuli einnig eytt eða þau aðskilin frá nafni eftir að þjónustan hefur verið veitt. Eins er tilgreint í töluliðnum að fjarskiptafyrirtæki skuli ávallt upplýsa áskrifendur um það hvers konar gögn þeir eru að vinna, tilgang vinnslunnar og tímalengd hennar. Í 29. lið inngangsorðanna segir svo að þjónustuveitanda sé heimilt að vinna umferðargögn um áskrifendur og notendur í

einstökum tilvikum ef nauðsynlegt er til að greina tæknibilanir og villur í fjarskiptasendingum, til að gefa út reikninga og til að koma upp um og stöðva svik sem felast í ógreiddri notkun fjarskiptaþjónustu. Þá segir í 30. lið inngangsorða að kerfi til að bjóða fram fjarskiptanet og fjarskiptaþjónustu skuli hönnuð þannig að magni nauðsynlegra persónuupplýsinga sé haldið í algjöru lágmarki. Hvers konar starfsemi sem gangi lengra en að senda fjarskiptasendingar og skrifa reikning fyrir þeim skuli byggð á samanlögðum umferðargögnum sem ekki væri hægt að tengja áskrifendum eða notendum.

2.3.2 Samþykki áskrifanda fyrir vinnslu upplýsinga um fjarskiptaumferð

Í athugasemdum við frumvarpið er varð að fjarskiptalögum árið 2003 er áréttað að heimild til úrvinnslu gagna um fjarskiptaumferð, í tilgangi markaðssetningar fjarskiptaþjónustu eða vegna framboðs á virðisaukandi þjónustu, sé einungis heimil ef áskrifandi eða notandi, sem gögnin eru um, hafi veitt samþykki sitt fyrir fram. Hugtakið *samþykki* er ekki skilgreint í fjarskiptalögum en í f -lið 2. mgr. 3. gr. títtnefndrar tilskipunarinnar segir að samþykki notanda eða áskrifanda samsvari samþykki skráðs aðila í tilskipun nr. 95/46/EB, sbr. og 17. lið inngangsorða tilskipunar nr. 2002/58/EB.

Í 7. tölul. 1. mgr. 2. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, sem byggir á h -lið 2. gr. tilvitnaðrar tilskipunar nr. 95/46/EB, er *samþykki* skilgreint með eftirfarandi hætti:

> „Sérstök, ótvíræð yfirlýsing sem einstaklingur gefur af fúsum og frjálsum vilja um að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fer fram, hvernig persónuvernd er tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv.“

Hugtakið *samþykki* má jafnframt finna í 46. gr. fjarskiptalaga, sem fjallar um óumbeðin fjarskipti, og byggt er á 12. gr. sömu tilskipunar Evrópusambandsins nr. 2002/58/EB. Póst- og fjarskiptastofnun hefur í fjölmörgum ákvörðunum sínum, er varða túlkun á 46. gr. fjarskiptalaga, skilgreint hvað felst í hugtakinu *samþykki* í skilningi framangreindar tilskipunar og 46. gr. laganna.

Í ákvörðunum Póst- og fjarskiptastofnunar er varðar óumbeðin fjarskipti og skilgreiningu á hugtakinu er litið til álita áðurnefnds 29. gr. starfshóps. Í áliti hans nr. 5/2004, er lýtur að túlkun hugtaksins *samþykki* vegna óumbeðinna fjarskipta, kemur fram að samþykki sem veitt er sem hluti af almennu samþykki á skilmálum samnings, svo sem áskriftarsamnings þar sem samþykkis er óskað fyrir markaðspóst, verður jafnframt að uppfylla framangreind skilyrði tilskipunar 95/46/EB. Hefur starfshópurinn talið að svo að samþykki teljist uppfylla kröfur tilskipunar 95/46/EB, verði samþykkið að fela í sér ákveðna athöfn af hálfu hlutaðeigandi svo það teljist vera ótvírætt, sbr. áliti hópsins nr. 15/2011.[4] Að mati Póst- og fjarskiptastofnunar verður ekki lagður annar skilningur í hugtakið samkvæmt 42. gr. fjarskiptalaga enda byggja ákvæðin á sömu tilskipun.

[4] Opinion 15/2011 on the definition of consent frá 13. júlí 2011.

III.
Málavextir

3.1 Ósk Póst- og fjarskiptastofnunar um verklagsreglur

Líkt og greint var frá í upphafi ákvörðunar þessarar hefur Póst- og fjarskiptastofnun nú gert úttekt á verklagsreglum fimm stærstu fjarskiptafyrirtækja hér á landi sem settar eru á grundvelli 7. mgr. 42. gr. og hlítingu félaganna við ákvæði 42. gr. fjarskiptalaga. Áður hafði Póst- og fjarskiptastofnun óskað, með bréfi dags. 2. apríl 2012, að IP fjarskipti ehf. afhenti stofnuninni afrit af verklagsreglum sem félagið hefur sett samkvæmt 7. gr. 42. gr. fjarskiptalaga. Með bréfi IP fjarskipta ehf., dags. 30. apríl 2012 greindi félagið stofnuninni frá því að verið væri að vinna að gerð umræddra verklagsreglna í samræmi við ákvörðun stofnunarinnar nr. 29/2011 um varðveislutíma upplýsinga um fjarskiptaumferð hjá Símanum hf. Kom fram að félagið myndi afhenda stofnuninni afrit af verklagsreglunum um leið og þær yrðu fullunnar.

IP fjarskipti ehf. afhenti Póst- og fjarskiptastofnun afrit af verklagsreglum félagsins þann 16. júní 2012. Með bréfi stofnunarinnar, dags. 25. október 2013, var félaginu kynnt sú afstaða stofnunarinnar að verklagsreglur félagsins væru ófullnægjandi og félaginu gert að endurbæta þær, m.a. með tilliti til atriða líkt og skilgreiningu upplýsingaeigna og útfærslur á vernd persónuupplýsinga. Var félaginu veittur frestur til 31. desember 2013 til að skila inn nýjum og fullnægjandi verklagsreglum til stofnunarinnar. Stofnuninni bárust nýjar og endurbættar reglur félagsins fyrir lok tilgreinds svarfrests.

Það var svo í kjölfar þess að brotist inn vefkerfi Fjarskipta hf. aðfararnótt 30. nóvember 2013, sem leiddi til þess að persónuupplýsingar um þúsundir viðskiptavina félagsins, sem þar höfðu verið varðveittar, komust í hendur óviðkomandi aðila og síðar birtar á internetinu, að Póst- og fjarskiptastofnun ákvað að framkvæma úttekt á hlítingu fimm stærstu fjarskiptafyrirtækja hér á landi við ákvæði 42. gr. fjarskiptalaga og verklagsreglna þeirra um meðferð persónuupplýsinga og eyðingu gagna, sbr. 7. mgr. ákvæðisins.

3.2 Boðun úttektar

Póst- og fjarskiptastofnun samdi, á grundvelli 3. mgr. 3. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun, við Capacent ehf. um að framkvæma úttektir samkvæmt kröfum ISO/IEC 27001 á verklagsreglum fimm fjarskiptafyrirtækja um meðferð persónuupplýsinga og eyðingu gagna, sbr. ákvæði 7. mgr. 42. gr. fjarskiptalaga, þ.e. IP fjarskiptum ehf., Fjarskiptum hf., Hringdu ehf., Nova ehf. og Símanum hf. Í framhaldi af undirritun samnings sendi stofnunin bréf, dags. 27. febrúar 2014, til framangreindra fjarskiptafyrirtækja og úttektin boðuð.

Fram kom í bréfinu að megináhersla verkefnisins væri að taka út með hvaða hætti meðhöndlun fjarskiptaumferðaupplýsinga samkvæmt 42. gr. laganna er háttað hjá þessum fyrirtækjum. Þá kom fram að markmið úttektar væri jafnframt að auka vitund um öryggi og meðferð þeirra fjarskiptaumferðarupplýsinga en ekki eingöngu að gera athugasemdir við verklag fyrirtækjanna hvað þetta varðar. Þá sagði í bréfinu:

> „Sú aðferðarfræði sem beitt verður við úttekt tekur mið af „Stjórnkerfi upplýsingaöryggis samkvæmt ISO/IEC 27001:2005“. Verða mælikvarðar um gæði

stýringa útfærðir og munu taka mið af völdum stýringum úr „Starfsvenjum fyrir stjórnun upplýsingaöryggis samkvæmt ISO/IEC 27002:2005“.

Í úttektinni verður skoðað hvernig meðhöndlun fjarskiptaumferðaupplýsinga er háttað hjá fjarskiptafyrirtækjunum. Mun úttektaraðili óska eftir kynningu á hvernig staðið er að meðferð þeirra upplýsinga sem um ræðir. Í framhaldi verður ákveðið, í samráði við viðkomandi fyrirtæki, hvaða starfsmenn verður rætt við. Í úttektinni mun úttektaraðili hafa til hliðsjónar verklag, verklagsreglur viðkomandi fjarskiptafyrirtækis, borið saman við valdar stýringar úr ISO/IEC 27002:2005 og gæði stýringa metnar. Úttektin mun að mestu leyti byggjast á viðtölum við starfsmenn fjarskiptafyrirtækjanna sem úttektaraðili óskar eftir að hitta á þeirra starfsstöð.

Komi upp sú staða, að mati úttektaraðila, að gera þurfi töluverðar úrbætur mun viðkomandi fjarskiptafyrirtæki fá frest til að bregðast við. Úttektaraðili mun í framhaldinu funda með viðkomandi fjarskiptafyrirtæki til að staðfesta hvort það hafi orðið við athugasemdum sem gerðar voru. Er þetta í raun síðari hluti úttektar og verður framkvæmd áður en gengið verður frá niðurstöðuskýrslu.“

Var í bréfinu einnig farið yfir fyrirhugaðan tímaramma úttektanna og óskað eftir því að fjarskiptafyrirtækin tilnefndu tengilið sem úttektaraðili og stofnunin myndu beina samskiptum sínum að.

IV.
Skýrsla úttektaraðila

4.1 Helstu niðurstöður

Capacent ehf. framkvæmdi úttekt á verklagsreglum IP fjarskipta ehf. um meðferð persónuupplýsinga og eyðingu gagna þann 14. apríl 2014 og skilaði lokaskýrslu sinni til Póst- og fjarskiptastofnunar þann 28. maí sl. Fram kemur í skýrslunni að tekin hafi verið viðtöl við starfsmenn félagsins og kannað hversu upplýstir þeir voru um lög og reglur félagsins. Þá var m.a. skoðað hvernig þeir geta flett upp fjarskiptaumferðarupplýsingum í notendaviðmóti. Tekin voru viðtöl við starfsmenn sem sýndu úttektaraðila hvernig þeir vinna með og meðhöndla fjarskiptaumferðarupplýsingar og fór viðtalið í flestum tilvikum fram á starfsstöð viðkomandi starfsmanns. Þá var jafnframt viðstaddur verktaki frá OPEX sem IP fjarskipti ehf. hefur fengið til að vinna með félaginu við gerð á heimasíðu og þjónustuvef.

Helstu niðurstöður Capacent ehf. við úttekt hjá IP fjarskiptum ehf. er settar fram á bls. 4 í skýrslunni. Þar segir:

„Niðurstöður úttektar benda til að farið sé eftir 42. gr. fjarskiptalaga sem segir að gögnum skuli eytt innan ákveðins tíma. Í úttekt fannst ekki tilvik þar sem eldri gögn voru til staðar. Sjálfvirkar keyrslur fara í gang á gagnagrunnum á hverjum degi sem annað hvort eyða gögnum eða gera þau ópersónugreinanleg.

Við úttekt komu í ljós þrjú minniháttar frábrigði sem talin eru þess eðlis að mati úttektaraðila að æskilegt væri að Tal geri úrbætur á.

Viðskiptavinum er ekki greint frá hvernig upplýsingar um þá kunna að vera notaðar eða hversu lengi, líkt og 42. gr. fjarskiptalaga segir til um.

Hefur fyrirtækið sett sér reglur um helstu þætti sem varða meðhöndlun fjarskiptaumferðarupplýsinga. Þessar reglur hafa þó ekki verið fyllilega innleiddar.

Tal hefur nýlega sett í loftið nýja heimasíðu, með nýjum þjónustuvef fyrir viðskiptavini. Farið var yfir hvers konar upplýsingar hægt er að fletta upp og staðfest að einungis er hægt að skoða upplýsingar sex mánuði aftur í tímann.

Einnig komu fram fjórar athugasemdir og fimm tækifæri til að bæta, þar á meðal að Öryggishandbók, Starfsmannahandbók, Öryggisstefnu og verklagsreglur mætti samræma nokkuð og gera aðgengilegt þeim starfsmönnum sem þurfa að hafa aðgang.“

4.2 Minniháttar frábrigði

Í úttekt Capacent ehf. komu í ljós þrjú atvik hjá félaginu sem úttektaraðili mat sem *minniháttar frábrigði* og taldi að þörf væri á að félagið bætti úr. Í fyrsta lagi var ekki vísað með réttum hætti til fjarskiptalaga og eru þau sögð vera nr. 77/2000 sem eru lög um persónuvernd og meðferð persónuupplýsinga. Í öðru lagi var um að ræða skort á upplýsingagjöf til viðskiptavina, sbr. 5. mgr. 42. gr. fjarskiptalaga. Í þriðja lagi gátu starfsmenn félagsins ekki bent á verklagsreglur félagsins og voru þær ekki aðgengilegar í öryggishandbók eða starfsmannahandbók þess. Að mati úttektaraðila varðar fyrsti og þriðji liður við 7. mgr. 42. gr. fjarskiptalaga.

4.3 Önnur atriði

Úttektaraðili setti fram fjórar *athugasemdir* og fimm *tækifæri til að bæta* í niðurstöðuskýrslu sinni. Þær *athugasemdir* sem settar voru fram varða ákveðnar umfram upplýsingar sem óheppilegt er að hafa í verklagsreglum, að auka mætti upplýsingagjöf til starfsmanna um öryggismál og skort á upplýsingum í skilmálum um tímalengd úrvinnslu gagna. Hvað varðar *tækifæri til að bæta* benti úttektaraðili á skort á merkingu gagna sem trúnaðarmál, uppfærslu öryggishandbókar og áherslur í henni, tilgreiningu um að rafrænar handbækur séu gildandi handbækur og mótun stefnu og verklags innan félagsins um notkun á skýjaþjónustu.

V.
Athugasemdir IP fjarskipta ehf.

5.1 Bréf Póst- og fjarskiptastofnunar, dags. 11. ágúst 2014

Póst- og fjarskiptastofnun óskaði athugasemda IP fjarskipta ehf. við niðurstöðuskýrslu úttektar Capacent ehf. með bréfi dags. 11. ágúst sl. Var skýrslan sjálf fylgiskjal bréfs stofnunarinnar. Í bréfi stofnunarinnar sagði m.a. að *„*[n]*iðurstöður úttektarinnar sýna að brigður eru á að ákvæði 5. mgr. 42. gr. fjarskiptalaga sé og hafi að fullu verið virt af félaginu. Kallar slíkt á aðgerðir af hálfu Póst- og fjarskiptastofnunar, í formi ákvörðunar þar*

um, enda ber stofnuninni lögum samkvæmt að hafa eftirlit með framkvæmd fjarskiptalaga, sbr. 1. tl. 3. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun og 2. mgr. 2. gr. laga, nr. 81/2003, um fjarskipti. Póst- og fjarskiptastofnun telur að fyrsta og þriðja minniháttar frábrigðin, er stofnunin telur varða 7. mgr. 42. gr. ekki gefa tilefni til sérstakrar íþyngjandi ákvörðunar, að svo stöddu, af hálfu stofnunarinnar.“

Í bréfinu tilgreindi Póst- og fjarskiptastofnun sérstaklega með hvaða hætti hin *minniháttar frábrigði* vörðuðu ákvæði 42. gr. fjarskiptalaga, þ.e. að með því að tryggja ekki að áskrifendur séu upplýstir fyrir fram um hversu lengi úrvinnsla á upplýsingum stendur yfir, hafi félagið ekki að fullu virt ákvæði 5. mgr. 42. gr. fjarskiptalaga.

Þrátt fyrir að þau *minniháttar frábrigði* sem fram komu við úttekt séu, að mati úttektaraðila og Póst- og fjarskiptastofnunar, ekki umfangsmikil er ljóst að Póst- og fjarskiptastofnun hefur það lögbundna hlutverk að hafa eftirlit með framkvæmd fjarskiptalaga. Komi í ljós að í starfsemi fjarskiptafyrirtækja sé að finna frávik frá skýrum ákvæðum laganna verður stofnunin að bregðast við slíku í formi ákvörðunar. Póst- og fjarskiptastofnun boðaði því í framangreindu bréfi sínu, dags. 11. ágúst sl., að stofnunin hygðist taka ákvörðun til samræmis við niðurstöður úttektarinnar varðandi 5. mgr. ákvæðisins.

Líkt og að framan greinir mat stofnunin það svo að ekki væri að svo stöddu forsendur til þess að taka formlega ákvörðun er varðar fyrsta og þriðja minniháttar frábrigðið, er varðar tilvísun til laga og aðgang starfsmanna að verklagsreglunum. Taldi stofnunin rétt að félagið bætti úr þessum ágöllum. Óskaði stofnunin því jafnframt eftir upplýsingum frá félaginu um með hvaða hætti það hyggist bregðast við öllum þeim þremur minniháttar frábrigðum sem að fram kom í úttektarskýrslu.

Í bréfi sínu óskaði stofnunin enn fremur athugasemda IP fjarskipta ehf. við boðaða afstöðu stofnunarinnar, við niðurstöðuskýrslu Capacent ehf. sem og að félaginu var boðið að tjá sig um framkvæmd úttektarinnar að öðru leyti.

Í bréfi Póst- og fjarskiptastofnunar kom fram að niðurstaða úttektarinnar gæfi fulla ástæðu til að kanna betur með hvaða hætti þjálfun og menntun starfsmanna félagsins væri þegar kæmi að upplýsinga- og öryggismálum. Óskaði stofnunin, á grundvelli 5. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun og 16. gr. reglna, nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum, eftir upplýsingum um með hvaða hætti ákvæði 10. gr. reglnanna, sem fjallar um ráðstafanir vegna starfsmanna, væri útfært og uppfyllt hjá félaginu.

5.2 Svarbréf IP fjarskipta ehf., dags. 1. september 2014

Póst- og fjarskiptastofnun barst svarbréf IP fjarskipta ehf., dags. 1. september sl. Í bréfinu kemur fram að félagið hafi farið ítarlega yfir erindi stofnunarinnar og lesið niðurstöðuskýrslu Capacent ehf. Þá muni félagið fara yfir hvernig það hyggst bregðast við þeim *minniháttar frábrigðum* sem fram koma í niðurstöðuskýrslunni ásamt því að fara jafnframt yfir hvernig félagið muni bregðast við *athugasemdum* og *tækifærum til að bæta.* Eins muni félagið svara fyrirspurn stofnunarinnar er lýtur að 10. gr. reglna nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

5.2.1 Minniháttar frábrigði

Í bréfi IP fjarskipta ehf. er farið yfir öll þau minniháttar frábrigði sem úttektaraðili setti fram í niðurstöðuskýrslu sinni.

Hvað varðar ranga tilvísun til laga í verklagsreglum, þ.e. vísun til laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga þá kemur fram að verklagsreglurnar hafi nú verið uppfærðar og tilvísun til fjarskiptalaga sett inn. Ný útgáfa af skjalinu hafi verið sett á staði sem eru aðgengilegir starfsmönnum félagsins.

Hvað varðar aðgengi starfsmanna að verklagsreglum félagsins kemur fram í bréfi félagsins að nú sé sérstaklega upplýst í starfsmannaþjálfun hvar verklagsreglurnar sé að finna á innri vef þess. Þá séu starfsmenn látnir lesa reglurnar líkt og reglan hafi verið í þjálfun starfsmanna.

Hvað varðar skilmála IP fjarskipta ehf. kemur fram að þeir hafi verið *„ ... uppfærðir á þann veg að þar kemur fram að félagið starfi eftir fjarskiptalögum og fer með upplýsingar og gögn um viðskiptavini eins og grein nr. 42 segir til um í lögum nr. 81/2003. Í tilboðsgerðarkerfi Tals sem sér um að senda tilboð á nýja viðskiptavini hefur einnig verið merkt greinilega að viðkomandi viðskiptavinur kynni sér skilmála félagsins þar sem vísað er í ofangreind lög og hann hvattur til að lesa þá vel í sölusamtali.“* Með þessum breytingum telur félagið að það hafi gert umtalsverðar umbætur á því hvernig viðskiptavinir eru upplýstir um hvernig farið er með fjarskiptaumferðarupplýsingar.

Þá greinir félagið frá því að starfsmannahandbók, öryggisstefna og verkalagsreglur um persónuupplýsingar hafa verið sameinaðar í eitt skjal og gert aðgengilegt á innri vef félagsins. Hið nýja skjal sé með útgáfudagsetningu og –númeri sem og sérstaka tilgreiningu sé að finna á því að rafrænt eintak skjalsins gildi umfram útprentað eintak. Þannig sé nú mun einfaldara að nálgast þessar upplýsingar en áður var. Eins kemur fram að starfsmenn séu upplýstir sérstaklega um hvar skjalið sé að finna og þeir hvattir til þess að kynna sér það. Þá hyggst félagið taka sérstaklega á þessu í starfsmannaþjálfun sem og að niðurstöður úttektarinnar og lagfæringar í kjölfar hennar verði kynntar á starfsmannafundi hjá félaginu.

5.2.2 Athugasemdir og tækifæri til að bæta

Þótt ekki hafi sérstaklega verið óskað eftir viðbrögðum félagsins er varðar aðrar niðurstöður úttetktarinnar í bréfi Póst- og fjarskiptastofnunar fer félagið yfir það í svarbréfi sínu hvernig það hefur brugðist við þeim *athugasemdum* og *tækifærum til að bæta* sem fram komu í niðurstöðuskýrslu Capacent ehf.

Hvað varðar *athugasemdir* sem settar voru fram í skýrslunni segir í svarbréfinu að allar gagnagrunnstöflur hafi verið fjarlægðar úr skjölum um reglur sem snúa að varðveislu fjarskiptaumferðaupplýsinga. Þá hafi gögn verið gerð aðgengilegri, vitund starfsfólks um þau aukin og skilmálum félagsins breytt.

Hvað varðar *tækifæri til að bæta* sem sett voru fram af hálfu úttektaraðila þá er tilgreint í svarbréfinu að félagið hafi tekið til skoðunar hvort bæta eigi merkingar trúnaðarskjala og að sameinað skjal í öryggishandbók hafi verið yfirfarið og uppfært í heild sinni. Hins vegar hafi ekki verið tekin ákvörðun um að breyta öryggishandbók þannig að hún miði meira að

viðskiptavinum en félagið hafi á sínum tíma keypt sérfræðiþjónustu við innleiðingu á öryggisreglum sínum. Félagið útilokar þó ekki að meira mið verði tekið af viðskiptavinum við heildarendurskoðun á þessari vinnu. Fram kemur í svarbréfi félagsins að það notist að mjög litlu leiti við skýjaþjónustur (Google Drive) og ákveðið hafi verið að innleiða annað kerfi í það Google Drive. Tilgreinir félagið að ef breyting verði gerð á þessu að nýju sé sjálfsagt að leggja til skýrar verklagsreglur varðandi notkun á slíkum þjónustum. Er bent á ráðleggingar frá úttektaraðilum þess efnis að ekki væri endilega gott að vera með of mikið eða flókið regluverk heldur ætti heldur að halda því einföldu og aðgengilegu. Á grundvelli þess mun félagið því ekki, að svo stöddu, útbúa verklagsreglur yfir það sem ekki er í notkun í dag.

5.2.3 Upplýsingabeiðni Póst- og fjarskiptastofnunar

Líkt og fram hefur komið óskaði Póst- og fjarskiptastofnun eftir upplýsingum frá IP fjarskiptum ehf. um hvernig félagið útfræði og uppfyllti að ákvæði 10. gr. reglna nr. 1227/2007 um meðferð upplýsinga í almennum fjarskiptanetum, sem fjallar um ráðstafanir vegna starfsmanna.

Í bréfi IP fjarskipta ehf. er farið yfir ákvæði 10. gr. reglnanna sem inniheldur sjö töluliði um öryggisráðstafanir, varðandi þá starfsmenn sem vegna starfa sinna hafa aðgang að upplýsingum í fjarskiptanetum, sem fjarskiptafyrirtæki skal grípa til.

Fyrsti töluliður ákvæðisins kveður á um að fjarskiptafyrirtæki skuli kanna hvort tilefni sé til að afla sakavottorðs umsækjanda áður en starf er veitt. Í svari IP fjarskipta ehf. kemur fram að í atvinnuumsóknarferli er umsækjandi beðinn um að svara því hvort hann hafi hreint sakavottorð eða ekki. Sé svar umsækjanda á þá leið að hann hafi skráningu í sakaskrá er í framhaldinu tekin ákvörðun um hvort óskað sé sérstaklega eftir sakavottorði og umsókn hans metin í framhaldi af því.

Í öðrum tölulið ákvæðisins er kveðið á um skyldu fjarskiptafyrirtækis að láta starfsmenn undirrita trúnaðaryfirlýsingar. Er staðfest í bréfi IP fjarskipta ehf. að allir starfsmenn sem hefja störf fyrir félagið séu látnir skrifa undir trúnaðaryfirlýsingu. Með slíkri undirskrift heitir starfsmaðurinn fullum trúnaði gagnvart félaginu sem m.a. snýr að trúnaðarupplýsingum sem hann kann að vinna með.

Í þriðja tölulið ákvæðisins er lögð sú skylda á fjarskiptafyrirtæki að fræða starfsmenn sína um ábyrgð þeirra samkvæmt IX. kafla fjarskiptalaga. Í svar IP fjarskipta ehf. kemur fram að í starfsmannaþjálfun er farið eftir stöðluðum gátlista en samkvæmt honum er starfsmanni kynnt öryggisstefna félagsins, verklagsreglur félagsins vegna geymslu persónuupplýsinga sem og starfsmannahandbók þess. Í þessum skjölum kemur svo skýrt fram hvernig félagið starfar eftir IX. kafla laganna og starfsmanni gerð grein fyrir að ætlast sé til að hann starfi eftir þessu regluverki.

Í fjórða tölulið ákvæðisins er lögð sú skylda á fjarskiptafyrirtæki að skilgreina ábyrgð og skyldur starfsmanna í tengslum við upplýsingaöryggi. Þá skal hlutverkaskipting og ábyrgð á framkvæmd hinna ýmsu ferla, er lúta að öryggi, vera skilgreind með skýrum hætti og kveða á um bann við skoðun upplýsinga nema í starfstengdum tilgangi. Í svari IP fjarskipta ehf. kemur fram að notast er við staðlað aðgangsstýringareyðublað við stofnun aðgangs fyrir starfsmann

hjá fyrirtækinu. Þar er aðgangur viðkomandi starfsmanns skilgreindur, hann áhættumetinn og skilgreint hver veitir aðgang að kerfum sem og tiltekið hver ber ábyrgð á viðkomandi starfsmanni. Þá eru jafnframt skilgreindar skyldur og ábyrgð á starfsmanni í starfslýsingu viðkomandi starfsmanns. Að lokum kemur fram að í starfsmannahandbók IP fjarskipta ehf. séu reglur sem allir starfsmenn félagsins eiga að fara eftir og varðar skoðun á upplýsingum félagsins.

Samkvæmt fimmta tölulið ákvæðisins skal fjarskiptafyrirtæki tryggja að starfsmönnum sé með reglubundnum hætti gerð grein fyrir starfsskyldum sínum og þeim afleiðingum sem það getur haft í för með sér að brjóta þær. Í svari sínu tilgreina IP fjarskipti ehf. að á hverju ári séu haldin frammistöðusamtöl og á um það bil tveggja vikna fresti séu haldin endurgjafarsamtöl. Eru þessi samtöl góður vettvangur til að fara yfir reglur og skerpa á ferlum sé þess þörf.

Í sjötta tölulið ákvæðisins er gerð krafa um að veita skuli starfsmönnum viðeigandi menntun og þjálfun í upplýsingaöryggismálum. Í svarbréfi IP fjarskipta ehf. kemur fram að við nýliðaþjálfun sé farið ítarlega yfir hvernig hugað er að upplýsingaöryggismálum hjá félaginu og er farið eftir gátlistum. Þá eru starfsmenn enn fremur hvattir til að nýta sér námskeiðahald utanhúss ef það nýtist á þessum vettvangi.

Sjöundi töluliður ákvæðisins setur þá skyldu á fjarskiptafyrirtæki að skoða áhættu varðandi lykilmenn upplýsingaöryggis og m.a. tryggja að ávallt sé hægt að ná í þá eða varamenn þeirra í neyð. Fram kemur í svari IP fjarskipta ehf. að félagið hefur skilgreinda kerfisstjóra ásamt öryggisstjóra og að þessir starfsmenn skipti með sér bakvakt sem rekin er allan sólarhringinn allan ársins hring. Tilgreindir aðilar koma að upplýsingaöryggismálum og er það markmið félagsins að hafa þekkingu þeirra sambærilega svo minni líkur sé á að neyðartilfellum sé ekki fylgt sem skyldi.

Að mati IP fjarskipta ehf. hefur félagið gefið svör við þeirri upplýsingabeiðni sem fram var sett í bréfi Póst- og fjarskiptastofnunar, dags. 11. ágúst sl.

VI.
Forsendur og niðurstaða

6.1 Almennt

Í upphafi telur Póst- og fjarskiptastofnun rétt að gera stuttlega grein fyrir aðferðarfræði sem notuð er við úttekt á grundvelli ISO staðla og stýringa og svo mati á því hvort ákvæði fjarskiptalaga teljist uppfyllt.

Póst- og fjarskiptastofnun áréttar að það eiga ekki allar stýringar staðalsins snertiflöt við ákvæði fjarskiptalaga, t.d. þær er varða útgáfunúmer verklagsreglu, flokkun upplýsingaeigna o.þ.h., og leggur stofnunin hvorki beint mat á þær né tekur afstöðu til þeirra. Hlutverk Póst- og fjarskiptastofnunar er hins vegar, í fyrsta lagi, að hafa eftirlit með því að skilyrði lagaákvæða fjarskiptalaga, t.d. kröfu um eyðingu gagna og upplýsingaskyldu fjarskiptafyrirtækja, séu tekin inn í gæðakerfi og, í öðru lagi, að hafa eftirlit með að þeim skilyrðum lagaákvæðanna sé fylgt af fjarskiptafyrirtækjum.

Þegar gæði stýringa samkvæmt ISO eru mældar er þeim skipt niður í fimm mismunandi gæðastig, þ.e. í *framúrskarandi, góð, ásættanleg, ófullnægjandi* og *óviðunandi*. Í úttekt Capacent ehf. voru þessi gæðastig og niðurstöður úttektirnar stillt upp á móti kröfum 42. gr. fjarskiptalaga. Capacent ehf. skipti hlítni við kröfur ákvæðisins jafnframt í fimm flokka, þ.e. *í lagi, tækifæri til að bæta, athugasemd, minniháttar frábrigði* og *meiriháttar frábrigði.*

Í úttekt sem gerð er út frá viðmiðum ISO stýringa er þannig að finna mismunandi stig fyrir alvarleika á fráviki á hlítingu við ákveðnar stýringar. Getur því verið um ákveðið frávik frá stýringu að ræða sem þó leiðir ekki til þess að viðkomandi aðili telst ekki standast skoðun á grundvelli staðalsins. Sambærileg aðferðarfræði getur ekki átt við um skýrar kröfur lagaákvæða. Þótt brot gegn lagaákvæðum geti verið mismunandi að umfangi þá er ekki í lagalegum skilningi hægt að tala um *minniháttar frábrigði* frá skyldum eða kröfum lagaákvæðis sem ekki felur um leið í sér brot gegn viðkomandi ákvæði. Þannig fæst ekki staðist að þótt úttektaraðili hafi ekki fundið nein tilvik um *meiriháttar frábrigði* frá ákvæði 42. gr. fjarskiptalaga, sem kallaði á tímasetta áætlun til að stöðva brot gegn ákvæðinu, að ekki felist í *minniháttar frábrigði* brot gegn skyldum og kröfum lagaákvæðis. Póst- og fjarskiptastofnun getur ekki litið framhjá því ef upp koma tilvik þar sem ákvæði fjarskiptalaga er ekki að fullu virt enda skal stofnunin framfylgja lögunum, sbr. t.d. 1. tl. 1. mgr. 3. gr. og 4. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun. Gildir þá einu hvort sem að um *minniháttar* eða *meiriháttar frábrigði* hafi fundist hjá fjarskiptafyrirtækjum þeim er úttekt var gerð hjá.

Í boðunarbréfi stofnunarinnar, dags. 27. febrúar sl., á fyrirhugaðri úttekt var tilgreint að ef upp kæmi sú staða, að mati úttektaraðila, að gera þurfi töluverðar úrbætur muni koma til annarrar úttektar til að staðreyna hvort að brugðist hafi verið við. Þetta bar ekki að skilja með þeim hætti að stofnunin hygðist ekki bregðast við ef fram kæmi að ákvæði 42. gr. fjarskiptalaga væri ekki uppfyllt. Heldur bar að skilja það svo að ef um *meiriháttar frábrigði* væri að ræða fæli það í sér það umfangsmikið brot að frekari eftirfylgni af hálfu stofnunarinnar væri þörf. Það að niðurstaða úttektar sýndi að einungis væri um *minniháttar frábrigði* að breytir ekki að um frávik var að ræða frá skýrum kröfum ákvæðis 42. gr. laganna um hvernig fjarskiptaumferðarupplýsingar skuli meðhöndlaðar. Er það skylda stofnunarinnar að bregðast við slíkum frávikum frá ákvæðum laganna í starfsemi fjarskiptafyrirtækja.

Í þessu samhengi verður einnig að horfa til þess að í tilvikum *minniháttar frábrigða* er jafnframt að finna frávik frá kröfum 42. gr. fjarskiptalaga. Þótt að fjarskiptafyrirtæki hafi getað brugðist samstundis við umræddu frábrigði og aðlagað verklag sitt að skilyrðum ákvæðisins er ljóst að brigður voru á að skilyrði ákvæðisins væru uppfyllt þegar úttekt átti sér stað. Hvernig brugðist er við slíkri ábendingu úttektaraðila eftir á breytir engu þar um.

6.2 Vinnsla IP fjarskipta ehf. á fjarskiptaumferðarupplýsingum

Líkt og áður segir kom í ljós í úttekt Capacent hf. *minniháttar frábrigði* frá 5. mgr. 42. gr. fjarskiptalaga. Segir í niðurstöðuskýrslunni að viðskiptavinum sé ekki bent sérstaklega á hvaða reglur gilda hjá fyrirtækinu um meðhöndlun gagna um fjarskiptaumferð líkt og því er skylt samkvæmt 5. mgr. 42. gr. laganna.

Í svarbréfi IP fjarskipta ehf. er gerð grein fyrir því að skilmálar félagsins hafi verið uppfærðir í kjölfar úttektarinnar og nú komi þar fram að félagið starfi eftir fjarskiptalögum og fari með upplýsingar og gögn um viðskiptavini í samræmi við ákvæði 42. gr. fjarskiptalaga. Þá er í bréfi félagins jafnframt vísað til vefslóðar þar sem skilmálana er að finna sem og vísað sérstaklega til 13. gr. þeirra þar sem segir að *„Tal starfar eftir fjarskiptalögum og fer með upplýsingar og gögn um viðskiptavini eins og grein 42. segir til um í lögum nr. 81/2003.“*

Eins er í svarbréfi félagsins fjallað um hvernig skilmálarnir eru nú kynntir fyrir nýjum viðskiptavinum, þ.e. að í tilboðskerfi félagsins, sem sendir tilboð á nýja viðskiptavini, hefur verið merkt greinilega að viðkomandi viðskiptavinur kynni sér skilmálanna, þar sé vísað til fjarskiptalaga og að hann er hvattur til að lesa skilmálanna vel.

Póst- og fjarskiptastofnun hefur nú skoðað aðrar greinar skilmála félagsins og má sjá að í 7. gr. þeirra kemur fram að félagið *„ ... áskilur sér rétt til að vinna úr gögnum um fjarskiptanotkun viðskiptavinar í því skyni að bjóða honum nýjar áskriftarleiðir, þjónustu eða önnur tilboð til hagsbóta fyrir hann.“* Ekki koma fram frekari upplýsingar um úrvinnslu gagna, þ.e. með hvaða gögn er unnið og hversu lengi vinnslan stendur, líkt og ákvæði 5. mgr. 42. gr. fjarskiptalaga gerir kröfu um. Þá hefur félagið ekki bent á að þær upplýsingar sé að finna annars staðar eða að áskrifendur þess séu upplýstir með frekari hætti um vinnslu gagna um fjarskiptanotkun þeirra. Verður Póst- og fjarskiptastofnun að ganga út frá að upplýsingar í skilmálum félagsins séu þær upplýsingar sem áskrifendur fá frá félaginu varðandi vinnslu gagna um fjarskiptanotkun þeirra.

Rétt er að gera grein fyrir því að ákvæði 42. gr. fjarskiptalaga tilgreinir ekki sérstaklega að fjalla skuli um úrvinnslu fjarskiptaumferðarupplýsinga í almennum viðskiptaskilmálum fjarskiptafyrirtækja. Hins vegar verður að ætla að almennir viðskiptaskilmálar þeirra geti verið nýttir til að uppfylla skilyrði ákvæðanna, séu þeir rétt útfærðir og kynntir áskrifendum, enda verður að gera þá lágmarkskröfu til neytenda að þeir lesi og kynni sér almenna viðskiptaskilmála þeirrar þjónustu sem þeir hyggjast kaupa af fjarskiptafyrirtæki.

Ef almennir skilmálar fjarskiptafyrirtækis eru notaðir í þessu samhengi verður í slíkum skilmálum að vera að finna ítarlegar upplýsingar um vinnslu fjarskiptaumferðarupplýsinga, eða skýra tilvísun til þess hvar slíkar upplýsingar er að finna, sem og að upplýsts samþykkis áskrifenda er aflað, þ.e. að hann hafi raunverulegt val og geti hafnað úrvinnslu upplýsinga. Sé slíkt að finna í skilmálunum verður að telja að skilyrði ákvæðanna séu uppfyllt af hálfu fjarskiptafyrirtækja. Póst- og fjarskiptastofnun áréttar þó nauðsyn þess að slíkir skilmálar séu bæði aðgengilegir og sýnilegir á heimasíðu félagsins ásamt því að vera kynntir sérstaklega fyrir áskrifendum áður en gengið er til viðskipta. Enda ber fjarskiptafyrirtæki lagaleg skylda til þess að kröfur ákvæðisins um upplýsingaskyldu og öflun upplýsts samþykkis, á grundvelli ítarlegar upplýsinga um fyrirhugaða úrvinnslu, séu uppfylltar.

Uppfylli almennir viðskiptaskilmálar ekki slíkt sem og að viðskiptavinur er ekki sérstaklega upplýstur um umrædda vinnslu og samþykkis hans fyrir henni ekki aflað er það mat Póst- og fjarskiptastofnunar að slíkt samræmist hvorki ákvæðum 4. og 5. mgr. 42. gr. fjarskiptalaga né almennum sjónarmiðum um neytendavernd. Enda verður að veita áskrifanda ítarlegar upplýsingar um vinnsluna áður en hann tekur afstöðu til þess hvort hann samþykki hana.

Viðkomandi fjarskiptafyrirtæki þarf því að afla upplýsts samþykkis hans fyrir vinnslunni. Sönnunarbyrði fyrir því að slíks samþykkis áskrifanda hafi verið aflað hvílir á viðkomandi fjarskiptafyrirtæki.

Almennur áskilnaður fjarskiptafyrirtækis í almennum viðskiptaskilmálum þess um heimild til úrvinnslu upplýsinga, þar sem ekki er jafnframt að finna ítarlegar upplýsingar um hvað felst í slíkri úrvinnslu, samræmist ekki að fullu ríkum kröfum ákvæðis 4. og 5. mgr. 42. gr. fjarskiptalaga, sbr. einnig álit starfshóps 29. gr. um að skilyrði almennra skilmála verði að uppfylla skilyrði ákvæðis persónuverndarlaga um *samþykki*.

Í bréfi IP fjarskipta ehf. er því ekki hafnað að ákvæði 5. mgr. 42. gr. hafi verið brotið. Félagið tilgreinir þó í svarbréfi sínu að það hafi brugðist við niðurstöðu úttektarinnar með þeim hætti sem að framan hefur verið lýst og uppfylli nú skilyrði ákvæðisins. Að mati Póst- og fjarskiptastofnunar er mjög jákvætt að félagið hafi brugðist við, sér í lagi er varðar útsendingu skilmála til verðandi viðskiptavina og þeir hvattir til að kynna sér þá. Sé slíkt gert við upphaf viðskiptasambands er það mat stofnunarinnar að skilyrði 5. mgr. um fyrirfram upplýsingaskyldu félagsins sé virt. Það er þó að því tilskyldu að þær upplýsingar sem skilmálarnir hafi að geyma uppfylli önnur skilyrði ákvæðisins, þ.e. um hvaða gögn séu tekin til úrvinnslu og hversu lengi úrvinnslan muni standa líkt og skýrlega er kveðið á um í 5. mgr. 42. gr. laganna. Slíkar upplýsingar skortir enn í skilmálum IP fjarskipta ehf. og hefur félagið því ekki að fullu brugðist við þeim *minniháttar frábrigðum* sem fram komu í úttekt Capacent ehf.

Á grundvelli framangreinds er það niðurstaða Póst- og fjarskiptastofnunar að IP fjarskipti ehf. hafi ekki sýnt fram á að tryggt sé að áskrifendur þeirra séu nægjanlega og sannanlega upplýstir fyrir fram um hvaða gögn um fjarskiptanotkun eru tekin til úrvinnslu og hversu lengi sú úrvinnsla mun standa, sbr. 5. mgr. 42. gr. fjarskiptalaga. Umfjöllun um slíkt skortir í almenna skilmála félagsins. Ákvæði 7. og 13. gr. þeirra uppfylla ekki skilyrði ákvæðisins um þær upplýsingar sem félaginu bera lagaleg skylda að upplýsa áskrifendur sína um áður en til viðskiptasambands er stofnað. Póst- og fjarskiptastofnun hyggst því taka ákvörðun því til samræmis.

Á k v ö r ð u n a r o r ð

IP fjarskipti hf. stóðst úttekt Póst- og fjarskiptastofnunar á verklagsreglum félagsins um meðferð persónuupplýsinga og eyðingu gagna, sbr. 7. mgr. 42. gr. laga, nr. 81/2003, um fjarskipti.

Ekki er að finna frávik frá skilyrðum ákvæðis 1. mgr., sbr. 2. og 3. mgr. 42. gr. laga, nr. 81/2003, um fjarskipti, um eyðingu gagna um fjarskiptaumferð eða kröfu sama ákvæðis um að þau séu gerð nafnlaus, í starfsemi IP fjarskipta ehf.

Framkvæmd IP fjarskipta ehf. á upplýsingaskyldu þess um úrvinnslu gagna um fjarskiptanotkun og tímalengd hennar uppfyllir ekki skilyrði ákvæði 5. mgr. 42. gr. laga, nr. 81/2003, um fjarskipti.

Ákvörðun þessi er kæranleg til úrskurðarnefndar fjarskipta- og póstmála og skal kæran berast úrskurðarnefnd innan fjögurra vikna frá því viðkomandi varð kunnugt um ákvörðun Póst- og fjarskiptastofnunar sbr. 13. gr. laga, nr. 69/2003, um Póst- og fjarskiptastofnun og 5. gr. reglugerðar um úrskurðarnefnd fjarskipta- og póstmála. Málskotsgjald fjarskiptafyrirtækis og/eða póstrekanda til úrskurðarnefndar er fjárhæð 150.000 kr., sbr. 6. gr. framangreindrar reglugerðar.

Reykjavík, 23. desember 2014

_____

Hrafnkell V. Gíslason, forstjóri

_____

Unnur Kr. Sveinbjarnardóttir