PÓST- OG FJARSKIPTASTOFNUN

Ákvörðun nr. 35/2014

Úttekt Póst- og fjarskiptastofnunar á verklagsreglum Fjarskipta hf. 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 Fjarskipta hf., 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 Fjarskipti hf. 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, uppljóstrun 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, 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 Fjarskipti hf. afhenti stofnuninni afrit af verklagsreglum sem félagið hefur sett samkvæmt 7. gr. 42. gr. fjarskiptalaga. Fjarskipti hf. afhenti stofnuninni umbeðnar reglur með bréfi þann 18. júní 2012.

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 óskaði eftir því að félagið endurskoðaði og uppfærði tilgreindar verklagsreglur sínar, meðal annars m.t.t. þessarar ógnar. Óskaði stofnunin eftir því að fá afhentar endurskoðaðar verklagsreglur félagsins og boðaði jafnframt að framkvæmd yrði vettvangsrannsókn hjá félaginu til þess að staðreyna hvort farið væri eftir þeim verkferlum og öryggisráðstöfunum sem lýst er í verklagsreglunum, sbr. bréf stofnunarinnar frá 6. desember 2013. Var jafnframt boðað í bréfi stofnunarinnar að félagið myndi bera hluta útlagðs kostnaðar við framkvæmd úttektarinnar, s.s. vegna aðkeyptrar sérfræðiþjónustu. Fjarskipti hf. afhenti Póst- og fjarskiptastofnun verklagsreglur sínar í byrjun árs 2014.

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. Fjarskiptum hf., IP fjarskiptum ehf. (Tal) 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 skiptingu kostnaðar. Þá var óskað eftir því að fjarskiptafyrirtækin tilnefndu tengilið sem úttektaraðili og stofnunin myndu beina samskiptum sínum að.

3.3 Svarbréf Fjarskipta hf., dags. 10. mars 2014

Póst- og fjarskiptastofnun barst bréf frá Fjarskiptum hf., dags. 10. mars sl., þar sem fram kom að þótt félagið gerði ekki athugasemdir við að aðferðarfræði ISO 27001 yrði notuð við úttektina þá væri ekki gerð krafa um að verklagsreglur fjarskiptafyrirtækjanna væru miðaðar við umræddan staðal. Þannig áréttaði félagið að úttektin gæti *„ … aðeins tekið mið af þeim skilyrðum sem viðeigandi lög og reglur setja, t.d. fjarskiptalaga og persónuverndarlaga sem og reglugerða sem settar eru á grundvelli þeirra, en ekki hvort að félagið uppfylli skilyrði ISO 27001.“* Var óskað eftir, ef þessi skilningur félagsins væri ekki í samræmi við fyrirætlan Póst- og fjarskiptastofnunar, að stofnunin upplýsti félagið þar um.

Í bréfinu gerði félagið jafnframt athugasemdir við að úttektaraðili muni hafa til hliðsjónar verklag og verklagsreglur félagsins og bera þær saman við valdar stýringar úr ISO 27002. Að mati félagsins geta mælingar á gæðum stýringa ekki verið mældar út frá völdum stýringum ISO 27002. Þá var gerð athugasemd við að hvorki lægi fyrir hvaða völdu stýringar væri um að ræða né hvaða lagaskyldur hvíldu á fjarskiptafélögum við innleiðingu þeirra. Á ný vísaði félagið til þess að úttektin geti eingöngu tekið mið af gildandi lögum og afleiddum réttarheimildum og gilda um starfsemi fjarskiptafyrirtækja.

Fram kom í bréfi Fjarskipta hf. að félagið teldi rétt að haldinn yrði kynningarfundur þar sem farið væri yfir uppbyggingu úttektarinnar. Það væri til þess fallið að starfsmenn félagsins gætu undirbúið sig fyrir úttekt, úttektin myndi vera skilvirkari og hægt yrði að byggja á henni til framtíðar.

Í bréfi Vodafone var áréttað mikilvægi þagmælsku úttektaraðila og að fyllsta hlutleysis yrði gætt við hina boðuðu úttekt. Ásamt því að óska eftir afriti af trúnaðaryfirlýsingu úttektaraðila þá greindi félagið frá því að Capacent ehf., hafi á árinu 2012 og 2013 unnið að verkefnum fyrir félagið. Að lokum sagði í bréfinu að félagið gerði hvorki athugasemdir við tímaramma fyrirhugaðrar úttektar né þann kostnað sem Póst- og fjarskiptastofnun tilgreindi í bréfi sínu.

3.4 Bréf Póst- og fjarskiptastofnunar, dags. 17. mars 2014

Póst- og fjarskiptastofnun sendi bréf til Fjarskipta hf., dags. 17. mars sl., þar sem staðfest var að úttektin mundi taka mið af settum lögum og reglum. Ekki væri ætlunin með úttektinni að meta hvort verkalagsreglur fjarskiptafélaganna muni uppfylla kröfur ISO 27001 líkt og um vottun á grundvelli staðalsins væri að ræða. Stofnunin benti þó á að í ákvæði 7. mgr. 42. gr. væri kveðið á um skyldu fjarskiptafyrirtækja að setja sér reglur um meðferð persónu-upplýsinga og eyðingu þeirra. Þá er í ákvæði 47. gr. kveðið á um fjarskiptaleynd m.a. til verndar friðhelgi einkalífs. Samkvæmt síðarnefnda ákvæðinu skulu fjarskiptafyrirtæki gera *viðeigandi ráðstafanir* til að tryggja öryggi þjónustunnar og verja upplýsingar sem fara um fjarskiptanet. Skulu fjarskiptafyrirtækin skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, gera áhættumat og ákveða öryggisráðstafanir á grundvelli þess.

Í bréfinu kom fram að framangreind ákvæði fjarskiptalaga væru, að mati stofnunarinnar, nátengd og ljóst að verklagsreglur fjarskiptafyrirtækja skv. 7. mgr. 42. gr. er liður í öryggisskipulagi fjarskiptafélaga þar sem um væri að ræða persónugreinanlegar upplýsingar um notendur sem tryggja verði að óviðkomandi fái ekki aðgang að. Þá benti stofnunin á að í reglum, nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum, komi m.a. fram að með reglunum sé kveðið á um þær ráðstafanir sem stofnunin telur nauðsynlegar að fjarskiptafyrirtækin geri til að tryggja vernd umferðar og upplýsinga í almennum fjarskiptanetum, sbr. 1. gr. reglnanna. Var jafnframt bent á það að í 3. mgr. 2. gr. reglnanna kemur fram að styðjast megi við staðla ISO/IEC 27001 og ISO/IEC 17799 og fara skuli eftir nýjustu útgáfu staðlanna á hverjum tíma en ISO 27002 er nýrri útgáfa af slíkum starfsvenjum. Eins segir að staðlana megi nota sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.

Fram kom í bréfinu það mat stofnunarinnar að þótt að kveðið sé á um að styðjast megi við tilgreinda staðla er ekkert sem takmarkar að jafnframt sé horft til annarra starfsvenja þegar *viðeigandi ráðstafanir* eru valdar. Stofnunin telji að nægjanlega lagastoð sé að finna í 1. mgr. 47. gr. Í bréfinu áréttaði stofnunin þann mun sem um ræðir á tilgreindum ISO 27001 og 27002 stöðlum en í þeim fyrrnefnda er að finna stjórnunarlegar kröfur um stjórnkerfi upplýsingaöryggis en í hinum síðarnefnda er um að ræða starfsvenjur (*e. Code of practice*). Ætti í úttektinni að velja tilteknar stýringar úr þeim starfsvenjum sem finna má í 27002 sem eiga við um andlag úttektarinnar og hafa þær til hliðsjónar með sama hætti og hafa má til hliðsjónar starfsvenjur samkvæmd ISO/IEC 17799, nú ISO 27002. Að mati stofnunarinnar væru starfsvenjur sem finna má í 27002 hjálplegar við að uppfyllar kröfur sem settar eru fram í 27001 og því sé ekki því um ótengda hluti að ræða.

Að mati Póst- og fjarskiptastofnunar er ljóst að ekki var um að ræða úttekt á grundvelli staðalsins líkt og þegar vottun samkvæmt honum færi fram. Fyrst og fremst fæli úttektin í sér könnun á hlítingu félagsins við ákvæði 42. gr. fjarskiptalaga.

IV.
Skýrsla úttektaraðila

4.1 Helstu niðurstöður

Capacent ehf. framkvæmdi úttekt á verklagsreglum Fjarskipta hf. um meðferð persónuupplýsinga og eyðingu gagna þann 13. maí 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 sem sýndu úttektaraðila hvernig þeir vinna með og meðhöndla fjarskiptaumferðarupplýsingar. Í flestum tilvikum hafi viðtalið farið fram á starfsstöð starfsmannsins. Þá hafi einnig var haldinn vinnufundur með forstöðumönnum félagsins við upphaf og lok úttektar.

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

> *„Niðurstöður úttektar benda til að farið sé að mestu eftir 42. gr. fjarskiptalaga sem segir að gögnum skuli eytt innan ákveðins tíma. Þó fundust tilfelli þar sem eldri gögn voru aðgengileg. Við úttekt komu þrjú minniháttar frábrigði í ljós. Tvö þeirra varða geymslutíma fjarskiptaumferðarupplýsinga og er þar um að ræða einu tilvikin þar sem upplýsingar eldri en 6 mánaða fundust í kerfum Vodafone. Eitt frábrigði varðar að upplýsa beri viðskiptavini fyrirfram um meðhöndlun gagna.*
>
> *Á meðan úttekt stóð yfir var brugðist strax við frábrigði sem fannst í vöruhúsi gagna þar sem upplýsingar voru aðgengilegar lengur en krafa er samkvæmt fjarskiptalögum.*
>
> *Fyrirtækið er þegar í þeirri vegferð að fá vottun á stjórnkerfi upplýsingaöryggis og hefur þ.a.l. lagt töluverða vinnu í innleiðingu á helstu stefnum, reglum og stýringum. Hefur fyrirtækið sett sér reglur um helstu þætti sem varða meðhöndlun fjarskiptaumferðarupplýsinga.*
>
> *Einnig var komið auga á tækifæri til úrbóta sem varðar orðalag í reglu og ítarlegar tæknilegar upplýsingar tiltekinna upplýsingakerfa í verklagsreglu.*
>
> *Farið var yfir hve mikilvægt er að útfæra einfalt skipulag og að aðgangur starfsmanna að mikilvægum upplýsingum sé auðveldur og greiður.*
>
> *Kannað var hvernig vinnsla með fjarskiptaumferðarupplýsinga er háttað í ýmsum kerfum. Í flestum kerfum var staðfest að gögn eru ekki aðgengileg og í mörgum tilfellum er verklag framúrskarandi“.*

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 voru aðgengilegar upplýsingar um fjarskiptaumferð í einum gagnagrunni félagsins sem hefði átta vera búið að eyða eða gera órekjanlegar og varðar við 1.-3. mgr. 42. gr. fjarskiptalaga. Nánar

tiltekið leiddi uppfletting [...][5] á símanúmeri [...][6] í ljós að hægt var að sjá fjarskiptaumferðarupplýsingar um frá hvaða númeri var hringt aftur til 1. ágúst 2013. Í skýrslunni segir að „[í] *þessum reit átti að vera búið að breyta gögnum þannig að fram kæmi -1 í stað númers sem hringt er í (calling party), en í þessu tilviki hafði það ekki verið gert.“* Í skýrslunni kemur þó skýrt fram að gæða- og öryggisstjóri Fjarskipta hf. hefði staðfest að brugðist hafi verið við þessari athugasemd á meðan á úttektinni stóð.

Í öðru lagi var að ræða að gögn um fjarskiptaumferð frá október 2013 sem eru tekin út úr kerfum félagsins og send, í formi Excel-skjals, með almennum tölvupósti á milli starfsmanna og varðar jafnframt 1.-3. mgr. 42. gr. fjarskiptalaga. Nánar tiltekið var óskað eftir sundurliðun á fjarskiptanotkun fyrirtækisins [...][7] í gegnum verkbeiðnakerfi Fjarskipta hf. Segir í skýrslunni að við slíkt séu *„ ... gögn tekin út úr kerfum í Excel skjal og sent í tölvupósti samkvæmt beiðni um slíkt.“* Kemur fram í skýrslunni að „[í] *tölvupósti sem sendur var á* [...][8]*, starfsmann Vodafone, 11.10.13 var Excel skjal sent sem inniheldur upplýsingar um þann viðskiptavin þar sem fram koma upplýsingar um notkun í sept*[ember] *2013.“*

Þriðja *minniháttar frábrigðið* fólst í að áskrifendur eru ekki upplýstir um hversu lengi úrvinnsla upplýsinga stendur yfir, sbr. 5. mgr. 42. gr. fjarskiptalaga, þ.e. upplýsingar um slíkt koma ekki fram í skilmálum félagsins. Segir í skýrslunni að ekki komi *„ ... fram í skilmálum fyrirtækisins hversu lengi úrvinnsla á upplýsingum stendur yfir. Fjarskiptalög segja hins vegar fyrir um að slíkt skuli tekið fram í skilmálum.“*

4.3 Tækifæri til að bæta

Úttektaraðili benti á tvö atriði sem hann taldi vera *tækifæri til að bæta* fyrir Fjarskipti hf. Um var að ræða breytingu á orðalagi í verklagsreglu um meðhöndlun fjarskiptaumferðargagna sem verða til [...][9]. Hið nýja orðalag yrði í betra samræmi við ISO 27002. Þá taldi úttektaraðili að ákveðnar kerfislægar upplýsingar sem fram koma í verklagsreglu félagsins væru of ítarlegar og tilheyrðu hærra öryggisstigi.

V.
Athugasemdir Fjarskipta hf.

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

Póst- og fjarskiptastofnun óskaði athugasemda Fjarskipta hf. 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 1. mgr., sbr. 2. og 3. mgr., og 5. mgr. 42. gr. og fjarskiptalaga séu 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.“*

[5] Fellt út vegna trúnaðar.
[6] Fellt út vegna trúnaðar.
[7] Fellt út vegna trúnaðar.
[8] Fellt út vegna trúnaðar.
[9] Fellt út vegna trúnaðar.

Í bréfinu tilgreindi Póst- og fjarskiptastofnun sérstaklega með hvaða hætti hin *minniháttar frábrigði* vörðuðu ákvæði 42. gr. fjarskiptalaga, þ.e. að, í fyrsta lagi, með því að hafa, þann 13. maí 2014, varðveitt fjarskiptaumferðarupplýsingar fyrir tilgreint símanúmer allt aftur til 1. ágúst 2013 [...][10] og hafa varðveitt, á sömu dagsetningu, fjarskiptaumferðarupplýsingar um annað tilgreint símanúmer í Excel-skjali í tölvupósti frá 11. október 2013 hafi ákvæði 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga ekki verið að fullu virt. Í öðru lagi, 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 er 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.

Í bréfi sínu óskaði stofnunin athugasemda Fjarskipta hf. að þeirri afstöðu stofnunarinnar, við niðurstöðuskýrslu Capacent ehf. sem og að tjá sig um framkvæmd úttektarinnar að öðru leyti. Eins óskaði stofnunin eftir upplýsingum frá félaginu um með hvaða hætti félagið hyggist bregðast við þeim *minniháttar frábrigðum* sem að fram komu í úttektinni og varða ákvæði 42. gr. fjarskiptalaga.

5.2 Svarbréf Fjarskipta hf., dags. 15. september 2014

Póst- og fjarskiptastofnun barst svarbréf Fjarskipta hf., dags. 15. september sl. Í bréfinu tilgreinir félagið að við boðun úttektar hafi komið fram að byggt yrði á aðferðarfræði sem tæki mið Stjórnkerfi upplýsingaöryggis samkvæmt ISO/ICE 27001 sem og völdum stýringum úr Starfsvenjum fyrir stjórnun upplýsingaöryggis samkvæmt ISO/ICE 27002 en niðurstöður úttektar á grundvelli þessara staðla eru skilgreindar eftir alvarleika þeirra í fimm flokka, þ.e. 1) í lagi, 2) tækifæri til að bæta, 3) athugasemd, 4) minniháttar frábrigði og 5) meiriháttar frábrigði.

Í bréfi Fjarskipta hf. er bent á að niðurstöður úttektar hjá félaginu hafi sýnt að einungis þrjú *minniháttar frábrigði* hafi fundist. Ekki hafi því fundist *meiriháttar frábrigði* sem kallaði á sérstakar úrbætur og eftirfylgni. Að mati Fjarskipta hf. stóðst félagið skoðun á tilgreindum öryggisstöðlum þar sem einungis fundust þrjú *minniháttar frábrigði* sem félagið hefur nú brugðist við, sbr. fylgiskjöl við svarbréf félagsins. Þannig hafi gögnum um fjarskiptaumferð umrædds símanúmers sem fannst [...][11] strax verið eytt. Þá kemur einnig fram í bréfi félagsins að verklagi við afgreiðslu verkbeiðna frá viðskiptavinum hafi verið breytt og er ekki lengur sendar í tölvupósti.

Þá segir í bréfi félagsins að viðskiptavinir félagsins séu nú þegar upplýstir um það hve lengi úrvinnsla gagna um fjarskiptaumferð stendur á heimasíðu félagsins, þ.e. á slóðinni

[10] Fellt út vegna trúnaðar.
[11] Fellt út vegna trúnaðar.

www.vodafone/skilmalar/gagnageymsla.is. Félagið telur að *„ ... skilyrði 42. gr. fjarskiptalaga feli ekki í sér skyldu til að upplýsa um lengd úrvinnslu gagna í skilmálum félagsins líkt og Capacent heldur fram í skýrslu sinni.“* Sé það aftur á móti afstaða Póst- og fjarskiptastofnunar að ákvæði 42. gr. feli í sér slíka skyldu muni félagið gera viðeigandi úrbætur á skilmálum sínum.

Að mati Fjarskipta hf. kalla þau *minniháttar frábrigði* sem fundust við úttekt ekki á aðgerðir af hálfu Póst- og fjarskiptastofnunar. Þá geti þau ekki verið grundvöllur fyrir ákvörðunartöku af hálfu stofnunarinnar. Um hafi verið að ræða minniháttar athugasemdir sem nú þegar hefur verið gerð úrbót á. Bendir félagið á þann mikla fjölda kerfa sem sýsla með fjarskiptaumferðargögn, þ.e. um 60 talsins. Komi fram með skýrum hætti í verklagsreglum félagins hvers konar gögn hvert kerfi sýslar með, hvers konar geymslutíma er um að ræða í hverju kerfi og hvaða deild innan félagsins ber ábyrgð á að eyða umræddum gögnum. Segir í svarbréfinu að *„*[í] ***öllum*** *tilvikum í úttektinni þar sem fjarskiptakerfi voru skoðuð, voru ákvæði 42. gr. uppfyllt. Fyrir mistök og algjörlega ómeðvitað voru hluti gagna* [...][12] *geymd lengur en 6 mánuði, en það sjálfvirka ferli var lagað um leið og á þetta var beint af hálfu úttektaraðila.“*

Að mati Fjarskipta hf. geta þau litlu frávik sem fram komu í úttektinni ekki talist brot á 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga og horfa verði til umfangs fráviksins og alvarleika þegar metið er hvort um brot á umræddu ákvæði er að ræða. Þá telur félagið að Póst- og fjarskiptastofnun verði að horfa til meðalhófs í málsmeðferð sinni. Vísar félagið til 2. mgr. 73 gr. fjarskiptalaga þar sem fram komi að stofnunin skuli, komist hún að þeirri niðurstöðu að fjarskiptafyrirtæki fari ekki að lögum, tilkynna félaginu niðurstöðu sína og gefa því kost á að koma sjónarmiðum sínum á framfæri eða lagfæra brot sín innan eins mánaðar frá dagsetningu tilkynningar. Að mati félagsins hefur félaginu ekki verið veitt tækifæri til að lagfæra þau *minniháttar frábrigði* sem fundust. Stofnunin hafi aftur á móti boðað ákvörðun um brot á ákvæði 42. gr. fjarskiptalaga á grundvelli niðurstöðu úttektarinnar. Að mati félagsins fer slík málsmeðferð í bága við framangreint ákvæði 73. gr. fjarskiptalaga og meginreglur stjórnsýsluréttar. Þannig ber stjórnvaldi samkvæmt 12. gr. stjórnsýslulaga nr. 37/1993, að velja það úrræði sem vægast er og að gagni getur komið og er óheimilt að taka íþyngjandi ákvörðun ef hægt er að ná markmiðinu með vægari hætti.

Hvað varðar niðurstöðuskýrsluna sjálfa þá setur félagið einungis fram athugasemd við túlkun Capacent ehf. á ákvæðum fjarskiptalaga er varðar skyldu þeirra til að upplýsa viðskiptavini sína um vinnslu gagna um fjarskiptaumferð en Capacent ehf. haldi því fram að slíkt skuli gera í skilmálum félagsins. Þessu andmæla Fjarskipti hf. og telja að ákvæðið kveði einungis á um skyldu félagsins um að upplýsa um hversu lengi vinnsla upplýsinga standi yfir, en slíkt hafi nú þegar verið gert.

Að lokum kemur fram í svarbréfi Fjarskipta hf. að félagið fari þess á leit við Póst- og fjarskiptastofnun að ekki verði tekin formleg ákvörðun um brot félagsins gegn fjarskiptalögum heldur taki mið af niðurstöðu Capacent ehf. Félagið hafi uppfyllt, í öllum

[12] Fellt út vegna trúnaðar.

meginatriðum, skilyrði 42. gr. fjarskiptalaga og nú þegar brugðist við þeim atriðum sem komu upp í úttektinni.

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.

Ekki er að finna í ákvæði 42. gr. mismunandi stig fyrir alvarleika brota. Ef upplýsingar, eldri en sex mánaða finnast í kerfum, án þess að um vanskil sé að ræða, sbr. 2. mgr. ákvæðisins, er ljóst að brigður eru á að skilyrði ákvæðisins séu uppfyllt. Hvort sem um er að ræða umfangslitlar upplýsingar eða ef einhvers konar tæknileg eða kerfisleg villa leiði til þess, með viðvarandi hætti, að umtalsvert magn persónugreinanlegra fjarskiptaumferðaupplýsinga séu geymd umfram hámarks varðveislutíma, þá eru í hvorugu tilvikinu skilyrði ákvæði 42. gr. uppfyllt. Póst- og fjarskiptastofnun er eftirlitsaðili með fjarskiptalögum hér á landi og hefur

löggjafinn falið stofnuninni það hlutverk að hafa eftirlit með hvort starfsemi fjarskiptafyrirtækja sé í samræmi við ákvæði fjarskiptalaga ásamt því að framfylgja þeim lögum. Komist Póst- og fjarskiptastofnun að því að starfsemi fjarskiptafyrirtækjanna sé ekki í samræmi við ákvæði þeirra ber henni lögum samkvæmt að grípa til aðgerða.

Framangreint á við hvort sem að um *minniháttar* eða *meiriháttar frábrigði* hafi fundist hjá þeim fjarskiptafyrirtækjum er úttekt var gerð hjá. Í boðunarbréfi stofnunarinnar, dags. 27. febrúar sl., var tilgreint að ef upp komi 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* 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 Varðveisla Fjarskipta hf. á fjarskiptaumferðarupplýsingum

Líkt og að framan var rakið komu í ljós við úttekt tvö *minniháttar frábrigði* er vörðuðu 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga.

Í fyrsta lagi var um að ræða tilvik þar sem upplýsingar fundust, þann 13. maí sl., um símanúmerið [...][13] í [...][14]. Uppfletting í gagnagrunni á númerinu sýndi að hægt var að sjá upplýsingar um frá hvaða númeri var hringt aftur til 1. ágúst 2013. Í niðurstöðuskýrslu Capacent kemur fram að í þessum reit átti vera búið að breyta gögnunum þannig að fram kæmi -1 í stað númers.

Í öðru lagi var um að ræða fjarskiptaumferðarupplýsingar fyrirtækisins [...][15] sem geymdar voru í Excel skjali í tölvupósthólfi starfsmanns Fjarskipta hf. Þegar óskað er eftir sundurliðun á fjarskiptanotkun í gegnum verkbeiðnakerfi Fjarskipta hf. þá eru gögn tekin út úr kerfum félagsins og þau sett í Excel skjal sem síðan er sent með tölvupósti samkvæmt beiðni. Þann 13. maí sl., fannst í tölvupósti, sem sendur var á [...][16], starfsmann Fjarskipta hf. þann 11. október 2013, skjal sem innihélt upplýsingar um notkun fyrirtækisins frá því í september 2013.

[13] Fellt út vegna trúnaðar.
[14] Fellt út vegna trúnaðar.
[15] Fellt út vegna trúnaðar.
[16] Fellt út vegna trúnaðar.

Póst- og fjarskiptastofnun getur tekið undir þau sjónarmið sem fram koma í andmælabréfi Fjarskipta hf., dags. 15. september sl., um að athugasemdir Capacent ehf. hafi verið minniháttar. Að mati Póst- og fjarskiptastofnunar er eðlilegt og rétt að líta til umfangs þeirra kerfa sem sýsla með fjarskiptaumferðarupplýsingar en í tilviki Fjarskipta hf. eru þau um 60 talsins. Það að einungis finnist tvö frávik frá skilyrði 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga, annað [...][17] og hitt í tölvupósthólfi starfsmanns, og engin frávik í stærstu kerfum félagsins, sýnir að vel er staðið að meðferð og eyðingu fjarskiptaumferðarupplýsinga hjá félaginu og í samræmi við tilgreint ákvæði. Enda er í niðurstöðuskýrslu Capacent ehf. sérstaklega tilgreint og staðfest að í flestum kerfum voru gögn ekki aðgengileg og í mörgum tilfellum hafi verklag verið framúrskarandi. Að mati Póst- og fjarskiptastofnunar er það megin niðurstaða úttektarinnar sem ber að árétta.

Fram kemur í niðurstöðuskýrslu Capacent ehf. að Fjarskipti hf. hafi, á meðan úttektinni stóð, brugðist við ábendingu úttektaraðila, sbr. verklagsreglur félagsins sem voru fylgiskjöl 1 og 2 með bréfi félagsins.

Póst- og fjarskiptastofnun óskaði, í bréfi sínu dags. 11. ágúst sl., sérstaklega eftir upplýsingum um það verklag sem viðhaft er þegar kemur að beiðnum um sundurliðun fjarskiptanotkunar í gegnum verkbeiðnakerfi félagsins. Í svarbréfi Fjarskipta hf., dags. 15. september kemur fram að verklaginu hafi verið breytt í framhaldi af úttektinni og verkbeiðnir varðandi sundurliðun á fjarskiptanotkun viðskiptavina séu nú ekki sendar í tölvupósti, sbr. einnig verklagsreglu félagsins sem var fylgiskjal 3 með bréfi félagsins.

Líkt og áður greinir þá varða framangreind tilvik sem úttektaraðili mat sem *minniháttar frábrigði* ákvæði 1. mgr. 42. gr., sbr. 2. og 3. mgr. ákvæðisins. Að mati Póst- og fjarskiptastofnunar er um frávik frá skilyrðum ákvæðisins að ræða, þótt í heildarsamhengi verði þau að teljast minniháttar og umfangslítil. Aftur á móti, líkt og skýrt er að framan, gerir tilgreint ákvæði fjarskiptalaga ekki greinarmun á alvarleika brota. Þá hefur það ekki áhrif á það mat, hvort skilyrði ákvæðisins hafi verið uppfyllt eða ekki, þótt að um gáleysisbrot sé að ræða. Í 2. mgr. 74. gr. fjarskiptalaga er sérstaklega kveðið á um að gáleysisbrot skuli eingöngu varða sektum en undanskilur ekki brot á lögunum þótt þau sé gerð af gáleysi. Að mati stofnunarinnar verður því ekki hjá því komist en að taka ákvörðun þess efnis að brigður hafi verið á hjá Fjarskiptum hf. að virða að fullu ákvæði 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga, nr. 81/2003.

Póst- og fjarskiptastofnun getur ekki fallist á tilvísun Fjarskipta hf. til 3. mgr. 73. gr. fjarskiptalaga. Ákvæðið er hluti af viðurlagakafla fjarskiptalaga og á við þegar stofnunin lítur brot fjarskiptafyrirtækis það alvarlegum augum að hún hyggst beita viðurlögum samkvæmt 74. gr. laganna, t.a.m. þegar um fyrirhugaða afturköllun á réttindum er að ræða eða stöðvun netrekstur eða þjónustu fjarskiptafyrirtækis, en ekki þegar um er að ræða almenna ákvörðun.

Póst- og fjarskiptastofnun verður jafnframt að hafna því sjónarmiði Fjarskipta hf. að með töku ákvörðunar sé brotið gegn meðalhófsreglu 12. gr. stjórnsýslulaga nr. 37/1993. Það að stofnunin þurfi að taka sérstaka ákvörðun um að Fjarskipti hf. hafi ekki að fullu virt ákvæði

[17] Fellt út vegna trúnaðar.

fjarskiptalaga getur ekki falið í sér brot á meðalhófi þrátt fyrir að þegar hafi verið brugðist við þeim atriðum sem varða ákvæðið. Ekki er í máli þessu ágreiningur um að tilgreindar upplýsingar um fjarskiptaumferð hafi fundist við úttekt á verklagsreglum félagsins. Að mati Póst- og fjarskiptastofnunar væri óeðlilegt ef fjarskiptafyrirtæki gæti með almennum hætti vísað til meðalhófsreglu stjórnsýslulaga og komist hjá ákvörðun stofnunarinnar með því einu að viðurkenna brot sitt á ákvæðum laganna.

Í þessu tilviki er heldur ekki verið að leggja íþyngjandi skyldu á Fjarskipti hf. sem hægt væri að ná með minna íþyngjandi hætti. Ekki er verið í ákvörðun þessari að leggja nokkra nýja skyldu á félagið heldur fyrst og fremst verið að bregðast við því að hjá félaginu fundust upplýsingar um fjarskiptaumferð tveggja áskrifenda félagsins sem það hefði átt að hafa eytt eða gert ópersónugreinanlegar samkvæmt ákvæði 1. mgr., sbr. 2. og 3. mgr. 42. gr. fjarskiptalaga. Það að frávik frá skyldu ákvæðisins hafi verið minniháttar kemur ekki í veg fyrir að stofnunin taki ákvörðun er lýtur að umræddum frávikum. Póst- og fjarskiptastofnun hyggst því taka ákvörðun þessu til samræmis.

6.3 Vinnsla Fjarskipta hf. á fjarskiptaumferðarupplýsingum
Líkt og áður segir kom í ljós í úttekt Capacent hf. *minniháttar frábrigði* er varðaði 5. mgr. 42. gr. fjarskiptalaga. Segir í niðurstöðuskýrslunni að félagið hafi ekki upplýst áskrifendur um tímalengd úrvinnslu á upplýsingum um fjarskiptaumferð og kemur fram að slíkt sé ekki tilgreint í skilmálum félagsins.

Fjarskipti hf. mótmæla að félagið hafi brotið gegn ákvæði 5. mgr. 42. gr. laganna. Að mati félagsins gerir ákvæðið ekki kröfu um að tilgreindar upplýsingar þurfi að koma fram í skilmálum félagsins. Vísar félagið til þess að á heimasíðu sinni, á vefslóðinni www.vodafone.is/skilmalar/gagnageymsla, séu viðskiptavinir félagsins upplýstir um hve lengi úrvinnsla gagna stendur yfir.

Við skoðun Póst- og fjarskiptastofnunar á framangreindri vefslóð er ljóst að þar koma fram upplýsingar um úrvinnslu gagna, tilgang hennar og tímalengd. Er þar tilgreint að félagið vinni úr gögnum um viðskiptavina sinna á grundvelli samþykkis þeirra, sbr. 9. gr. skilmála félagsins og 42. gr. fjarskiptalaga. Í 9. gr. almennra þjónustuskilmála félagsins segir að félagið *„ ... áskilur sér rétt til að vinna úr gögnum um fjarskiptanotkun áskrifanda í því skyni að bjóða honum nýjar áskriftarleiðir, þjónustu eða önnur tilboð til hagsbóta fyrir hann.”*

Póst- og fjarskiptastofnun fellst á það sjónarmið Fjarskipta hf. að ákvæði 42. gr. fjarskiptalaga tilgreinir ekki sérstaklega að fjalla skuli um úrvinnslu fjarskiptaumferðarupplýsinga í almennum viðskiptaskilmálum félagsins. Aftur á móti verður ekki horft fram hjá ríkum kröfum 4. og 5. mgr. 42. gr. um að áskrifanda séu veittar ítarlegar upplýsingar um vinnsluna áður en hann tekur afstöðu til þess hvort hann samþykki hana. Þannig á það að vera val áskrifanda hvort hann heimili félaginu vinnslu upplýsinga um fjarskiptanotkun sína og þarf viðkomandi fjarskiptafyrirtæki að afla upplýsts samþykkis hans. Sönnunarbyrði fyrir því að slíks samþykkis áskrifanda hafi verið aflað hvílir á viðkomandi fjarskiptafyrirtæki.

Þannig verður áskrifandi að hafa raunverulegt val um það hvort hann heimili úrvinnslu á upplýsingum um fjarskiptanotkun sína. 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.*

Að mati Póst- og fjarskiptastofnunar er ekki tryggt, þegar viðskiptavinur þarf sjálfur að afla sér upplýsinga á mismunandi stöðum á heimasíðu félagsins, áður en að til viðskiptasambands kemur, um atriði sem fjarskiptafyrirtæki ber lagaleg skylda að upplýsa þá um, að kröfur ákvæðisins um upplýsingaskyldu og öflun upplýsts samþykkis á grundvelli ítarlegar upplýsinga um fyrirhugaða úrvinnslu séu uppfylltar.

Hins vegar verður að ætla að almennir viðskiptaskilmálar félags 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. Sé í slíkum skilmálum 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, 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.

Uppfylli almennir viðskiptaskilmálar ekki slíkt, sem og að viðskiptavinur er ekki sérstaklega upplýstur um umrædda vinnslu og samþykkis hans fyrir henni ekki aflað sérstaklega, er það mat Póst- og fjarskiptastofnunar að slíkt samræmist hvorki ákvæðum 4. og 5. mgr. 42. gr. fjarskiptalaga né almennum sjónarmiðum um neytendavernd.

Í bréfi Fjarskipta hf. er því hafnað að ákvæði 5. mgr. 42. gr. hafi verið brotið þar sem finna má, á heimasíðu félagsins, upplýsingar um úrvinnslu á fjarskiptaumferðarupplýsingum áskrifenda. Ekki er í bréfinu gerð frekari grein fyrir með hvaða hætti þessar upplýsingar eru kynntar fyrir áskrifendum og upplýsts samþykkis þeirra aflað fyrir vinnslunni. Þá má, við lestur almennra viðskiptaskilmála félagsins, sjá almennan áskilnað félagsins um heimild til vinnslu á upplýsingum um fjarskiptanotkun.

Á grundvelli framangreinds er það niðurstaða Póst- og fjarskiptastofnunar að Fjarskipti hf. 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. Almenn umfjöllun um slíkt á heimasíðu félagsins, en t.d. ekki í almennum viðskiptaskilmálum félagsins sem viðskiptavinir hafa kynnt sér, tryggir ekki að krafa ákvæðisins um að fjarskiptafyrirtæki veiti ítarlegar upplýsingar um vinnsluna áður en samþykkis fyrir henni er aflað frá áskrifenda sé uppfyllt. Það er því niðurstaða stofnunarinnar að Fjarskipti hf. tryggi ekki með nægjanlegum hætti með núverandi framkvæmd sinni að skilyrði ákvæða 4. og 5. mgr. 42. gr. fjarskiptalaga séu uppfyllt. Hyggst stofnunin taka ákvörðun því til samræmis.

Á k v ö r ð u n a r o r ð

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.

Í ljós komu minniháttar 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, þar sem:

a) **Fjarskipti hf. varðveittu, þann 13. maí 2014, gögn um fjarskiptaumferð símanúmersins [...][18] frá 1. ágúst 2013 [...][19].**
b) **Fjarskipti hf. varðveittu, þann 13. maí 2014, gögn um fjarskiptaumferð fyrirtækisins [...][20] frá 11. október 2013 í Excel skjali í tölvupósthólfi [...][21], starfsmanns félagsins.**

Framkvæmd Fjarskipta hf. á upplýsingaskyldu félagsins um úrvinnslu gagna um fjarskiptanotkun og tímalengd hennar, í formi almennrar kynningar Fjarskipta hf. á vinnslu gagna um fjarskiptaumferð á heimasíðu félagsins, tryggir ekki með nægjanlegum hætti að skilyrði 5. mgr. 42. gr. laga, nr. 81/2003, um fjarskipti séu uppfyllt.

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

[18] Fellt út vegna trúnaðar.
[19] Fellt út vegna trúnaðar.
[20] Fellt út vegna trúnaðar.
[21] Fellt út vegna trúnaðar.