Meistararitgerð í lögfræði

Hver er ábyrgur?
Hugtökin ábyrgðar- og vinnsluaðili samkvæmt lögum um persónuvernd og meðferð persónuupplýsinga

Steinlaug Högnadóttir

Leiðbeinandi: Trausti Fannar Valsson

Febrúar 2015

FORMÁLI

Áhugi minn á persónuvernd og meðferð persónuupplýsinga vaknaði í skiptinámi við Kaupmannahafnarháskóla haustið 2013. Þar sat ég námskeiðið *European and International Data Protection and Privacy Law* hjá Christopher Kuner, sem ég vitna þónokkuð til í ritgerð þessari. Skrifin áttu sér stað á sumar- og haustmánuðum ársins 2014 í Kaupmannahöfn undir handleiðslu Trausta Fannars Valssonar. Honum vil ég færa þakkir fyrir uppbyggilega gagnrýni og góðar ábendingar á meðan ritferlinu stóð. Þá vil ég sérstaklega færa föður mínum, Högna S. Kristjánssyni og Ásgerði I. Magnúsdóttur þakkir fyrir yfirlestur ritgerðarinnar. Síðast en ekki síst vil ég þakka sambýlismanni mínum, Karli Jóhanni Unnarssyni, fyrir ómetanlegan stuðning við skrif þessi.

EFNISYFIRLIT

1 Inngangur

1.1 Almennt

Persónuréttur sem fræðigrein skiptist í almennan og sérstakan hluta. Páll Sigurðsson lýsir skiptingunni á eftirfarandi hátt:

> Með „almennum hluta“ persónuréttar er hér átt við *höfuðreglurnar – grundvallarreglurnar – um persónuvernd*, eins og þær birtast í fræðigreininni *persónurétti*, þ.e. lögvernd þeirra hagsmuna sem með sterkustum hætti eru tengdir persónu manna, þ.e. frelsi þeirra, persónuleika, lífi og limum. Með „sérstökum hluta“ persónuréttar er hins vegar átt við sérgreind eða afmörkuð viðfangsefni innan persónuréttarins, svo sem þau, er tengjast efnissviði laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.[1]

Persónuvernd sem réttarsvið er mjög víðtækt og geta ýmis réttindi og tilfelli er snerta persónu fólks fallið þar undir, s.s. vernd æru, hugsanafrelsi og réttur til að stofna fjölskyldu.[2] Hugtakið *persónuvernd* er ekki skilgreint í lögum en í daglegu tali er hugtakið notað um vernd á friðhelgi einkalífs fólks og varðar meðferð persónuupplýsinga.[3] Í norskum rétti hefur hugtakið *personvern* verið skilgreint sem vernd á rétti einstaklinga til að stjórna vinnslu upplýsinga um sig sjálfa. Vegna víðtækrar merkingar persónuverndarhugtaksins hafa norsku fræðimennirnir Dag Wiese Schartum og Lee A. Bygrave notast við hugtakið *persónuupplýsingavernd* (no. *personopplysningsvern*) þegar fjallað er um vernd persónuupplýsinga. Schartum og Bygrave líta á persónuupplýsingavernd sem afmarkaðan undirflokk persónuverndar og tekur sá flokkur til reglna um meðferð persónuupplýsinga, sem hafa það að markmiði að vernda friðhelgi einkalífs.[4] Samkvæmt áðurnefndum texta Páls Sigurðssonar falla reglur um vinnslu persónuupplýsinga undir sérstakan hluta persónuverndar sem sérstakt og afmarkað viðfangsefni hennar. Mætti því færa rök fyrir því að hugtakið persónuupplýsingavernd væri hnitmiðaðra og betur til þess fallið að varpa ljósi á viðfangsefni sviðsins, heldur en yfirhugtakið persónuvernd. Persónuupplýsingavernd samsvarar einnig betur því hugtaki sem notað er um vernd persónuupplýsinga í alþjóðasamfélaginu, þ.e. *data protection.*[5] Þrátt fyrir hugleiðingar þessar verður notast við hugtökin persónuvernd og persónuupplýsingavernd jöfnum höndum, eins og tíðkast í sjálfum persónu–upplýsingalögunum.

---

[1] Páll Sigurðsson: *Mannhelgi*, bls. 19.
[2] Sjá Páll Sigurðsson: *Mannhelgi*.
[3] „Mjög sótt að friðhelgi einkalífsins“, http://www.mbl.is.
[4] Sjá Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet*, bls. 17: „Personvern har opprinnelig vært definert som vernet av den enkeltes interesse i å kunne kontrollere behandling av opplysninger om seg selv, spesielt i forbindelse med store organisasjoners bruk av informasjons- og kommunikasjonsteknologi“.
[5] Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet*, bls. 18.

1.2 Þróun persónuverndar og tæknivæðing

Þróun í upplýsingatækni hefur leitt til aukinna möguleika til vinnslu með persónuupplýsingar og á persónuvernd rætur sínar að rekja til þeirrar þróunar.[6] Til marks um þetta er tímaritsgrein frá árinu 1890 eftir lögmennina Samuel D. Warren og Louis D. Brandeis. Aðdragandi greinarinnar var sá að dagblöð birtu í vaxandi mæli, með tilkomu nýrrar tækni, greinar og ljósmyndir um einkamálefni fólks. Settu Warren og Brandeis sér það markmið að meta hvort þágildandi lög fælu í sér einhverskonar meginreglur sem gætu skírskotað til verndar einkalífs einstaklinga við slíkar aðstæður. Rannsókn þeirra lagði grunninn að tveimur grundvallarréttindum einstaklingsins í bandarískum rétti, annars vegar rétt manna til að vera í friði (e. *the right to be left alone*) og hins vegar sjálfsákvörðunarrétt manna (e. *the right to self-determination*).[7]

Undir lok sjöunda áratugar tuttugustu aldar var orðin þörf á löggjöf til verndar á persónuupplýsingum sem afleiðing verulegrar þróunar í upplýsingatækni.[8] Varð það til þess að ríki víða í Evrópu tóku upp einhverskonar persónuverndarlöggjöf. Árið 1981 gerði Evrópuráðið samning um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga[9] sem lagði síðar mikilvægan grunn að persónuupplýsingalöggjöf Evrópusambandsins (hér eftir „ESB“).

Með tilkomu Internetsins[10] hafa skapast fleiri möguleikar til að safna á kerfisbundinn hátt upplýsingum um einstaklinga og nota þær í margvíslegum tilgangi, en unnið er með persónuupplýsingar í mun meiri mæli nú en nokkurn tímann áður. Sú persónuupplýsingalöggjöf sem við búum við í dag hefur aftur á móti verið gagnrýnd fyrir að halda ekki í við þessa þróun, m.a. vegna þess að flóknar tækninýjungar eiga það til að gera skilin á milli ábyrgðar- og vinnsluaðila óskýr.

1.3 Hugtökin ábyrgðaraðili og vinnsluaðili

Hugtökin ábyrgðaraðili og vinnsluaðili eru meðal grundvallarhugtaka persónu–upplýsingalöggjafar. Hugtökin hafa margvíslega þýðingu fyrir framkvæmd laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga[11], en fyrst og fremst afmarka þau hver beri

[6] Ingvi Snær Einarsson: „Sérstök skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga skv. 1. mgr. 9. gr. laga nr. 77/2000“, bls. 44.
[7] Samuel D. Warren og Louis D. Brandeis: „The Right to Privacy“, bls. 193-220.
[8] Alþt. 1999-00, A-deild, bls. 2688.
[9] Á ensku ber samningurinn heitið „Convention nr. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data“.
[10] Hér verður notast jöfnum höndum við orðin Internet og Netið. Einnig tíðkast að rita orðin með stórum staf, sbr. Orðabók Menningarsjóðs.
[11] Hér verður notast jöfnum höndum við skammstöfunina pul. og styttinguna persónuupplýsingalög þegar átt er við lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

ábyrgð á vinnslu persónuupplýsinga samkvæmt ákvæðum laganna. Ábyrgðaraðili ber ábyrgð á að vinnsla persónuupplýsinga uppfylli skilyrði pul.[12] Honum er heimilt að semja við vinnsluaðila um að annast vinnslu fyrir sig, en hlutverk vinnsluaðila er að vinna upplýsingar eftir fyrirmælum ábyrgðaraðila. Þannig eru hugtökin notuð til að greina á milli aðila sem bera ábyrgð á vinnslu persónuupplýsinga og aðila sem eingöngu vinna persónuupplýsingar fyrir hönd þeirra sem bera á þeim ábyrgð. Koma hugtökin einnig til skoðunar við mat á gildissviði pul., þar sem landfræðilegt gildissvið laganna er bundið við *staðfestu* ábyrgðaraðila.[13] Þá skiptir aðgreining hugtakanna máli svo hinn skráði, þ.e. sá aðili sem persónuupplýsingarnar fjalla um, viti hvert hann skal snúa sér til að njóta þeirra réttinda sem ákvæði persónuupplýsingalaga veita honum, en til þess þarf að vera ljóst hver sé ábyrgðaraðili.

Hugtökin eru tæknilega hlutlaus (e. *technology-neutral*) og beiting þeirra á þar með að vera óháð tæknibreytingum. Tækninýjungar hafa þó leitt til óvissu hvað varðar úthlutun ábyrgðar að vinnslu persónuupplýsinga, þar sem óljóst þykir hver gegnir stöðu ábyrgðar- og vinnsluaðila hverju sinni. Óvissa um beitingu hugtakanna getur haft neikvæð áhrif á fylgni við reglur á sviði persónuupplýsingaverndar og á skilvirkni persónuupplýsingalöggjafar í heild sinni.[14] Þegar núgildandi persónuupplýsingalöggjöf var samin um miðjan tíunda áratug síðustu aldar var ekki hægt að sjá þessa þróun fyrir. Internetið var ekki sjálfsagður hlutur á hverju heimili og var vinnsla persónuupplýsinga fyrst og fremst framkvæmd af lögaðilum, opinberum aðilum og einstaklingum í krafti starfs síns. Internetið hefur aftur á móti breytt hlutverki einstaklinga í persónuupplýsingavinnslu. Þeir taka nú meiri þátt í slíkri vinnslu með notkun tölvupósts, samfélagsmiðla og bloggfærslum, þar sem einstaklingar deila sögum og myndum úr eigin lífi og jafnvel annarra.[15] Sú þróun hefur m.a. gefið tilefni til spurninga um hvort einstaklingar séu bærir til að gegna hlutverki ábyrgðaraðila þegar þeir vinna persónuupplýsingar í sínu einkalífi.

1.4 Efnisafmörkun

Í ritgerð þessari verður fjallað um tvö grundvallarhugtök laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Annars vegar hugtakið *ábyrgðaraðili* og hins vegar *vinnsluaðili*. Ekki hefur verið sérstaklega fjallað um hugtök þessi í íslenskum fræðaskrifum og er markmið þessarar ritgerðar að bæta úr því með nákvæmri greiningu á hverju hugtaki

[12] *Opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 4.
[13] Orðið *staðfesta* hefur sérstaka þýðingu að persónuupplýsingalögum, en með því er átt við virka og raunverulega starfsemi með föstu fyrirkomulagi, sbr. 19. lið formála tilskipunar 95/46/EB. Fjallað er um landfræðilegt gildissvið í kafla 3.3.3.
[14] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 2.
[15] Peter Blume: *Databeskyttelsesret*, bls. 355–360.

fyrir sig. Í því skyni að varpa ljósi á raunverulegt gildi þessa hugtaka og hvernig reynt getur á þau í framkvæmd verður sérstaklega fjallað um notkun einstaklinga á *samfélagsmiðlum* og hvernig hún horfir við persónuupplýsingalögum. Endurspeglar samfélagsmiðlanotkun einnig aukna þátttöku einstaklinga í persónuupplýsingavinnslu.

Ábyrgðar- og vinnsluaðilahugtökin eru byggð á sambærilegum hugtökum tilskipunar Evrópuþingsins og Ráðsins 95/46/EB frá 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga.[16] Við greiningu hugtakanna verður því fyrst og fremst litið til Evrópuréttar. Þá verður einnig litið til norrænnar persónuupplýsingalöggjafar, eftir því sem við á, þar sem hún byggist einnig á tilskipun 95/46/EB.

Auk þess sem fjallað hefur verið um persónuvernd sem réttarsvið og þróun þess hér að framan verður í öðrum hluta ritgerðinnar fjallað um uppsprettu hugmyndarinnar um vernd persónuupplýsinga úr grundvallarréttinum til friðhelgi einkalífs. Verður einnig vikið að alþjóðlegum reglum á því sviði sem hafa þýðingu fyrir íslenskan rétt.

Í þriðja hluta ritgerðarinnar verður fjallað um löggjöf um vernd persónuupplýsinga, bæði þær Evrópureglur sem gilda um efnið og lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000. Vikið verður að forsögu núgildandi löggjafar og gerð grein fyrir markmiði, efnislegu gildissviði og helstu hugtökum laganna. Þá verður einnig höfð hliðsjón af þróun upplýsingatækninnar og áhrif hennar á grundvallarhugtök pul. eftir því sem við á.

Í fjórða hluta verður fjallað um ábyrgðaraðilahugtakið. Farið er yfir skilgreiningu þess að íslenskum og norrænum rétti og litið til sambærilegs hugtaks tilskipunar 95/46/EB. Hugtakið verður afmarkað í þrjá þætti og gerð grein fyrir hverjum og einum þeirra. Þá verður vikið að þeim skyldum sem hvíla á ábyrgðaraðila og fjallað um þau tilvik þegar fleiri en einn ábyrgðaraðili kemur að vinnslu persónuupplýsinga.

Í fimmta hluta ritgerðarinnar verður fjallað um vinnsluaðilahugtakið. Farið er yfir skilgreiningu hugtaksins í íslenskum og norrænum rétti og í tilskipun 95/46/EB. Hugtakið verður afmarkað í tvo þætti og gerð grein fyrir þeim. Þá verður vikið að trúnaðarskyldu vinnsluaðila og þeim aðstæðum þegar vinnsluaðili semur við undirverktaka um vinnslu persónuupplýsinga og lagalegar afleiðingar þess að vinnsluaðili eða undirverktaki hafi búsetu utan Evrópska Efnahagssvæðisins.

Í sjötta hluta ritgerðarinnar er fjallað um samfélagsmiðla. Leitast er við að svara þeirri spurningu hver gegni hlutverki ábyrgðaraðila við vinnslu persónuupplýsinga á slíkum miðli

[16] Hér verður notast við „tilskipun 95/46/EB“ þegar átt er við tilskipun 95/46/EB um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga.

og gerð grein fyrir ábyrgð og skyldum sem hvíla á ábyrgðaraðila við slíkar aðstæður. Þá verður lagt mat á hvað mætti betur fara við úthlutun ábyrgðar samkvæmt persónuupplýsingalögum þegar samfélagsmiðlar eiga í hlut.

Í sjöunda og síðasta hluta þessarar ritgerðar verður gerð grein fyrir fyrirhuguðum breytingum á persónuupplýsingalöggjöf Evrópusambandsins sem geta haft áhrif á stöðu ábyrgðar- og vinnsluaðila, verði löggjöfin samþykkt.

2 Friðhelgi einkalífs og vernd persónuupplýsinga

Hugmyndin um vernd persónuupplýsinga varð til út frá grundvallarréttinum til friðhelgi einkalífs, heimilis og fjölskyldu. Vernd persónuupplýsinga og friðhelgi einkalífs eru því nátengd réttindi, en einnig hefur verið litið á persónuupplýsingavernd sem sjálfstæðan rétt einstaklings.[17]

Til ársins 1995 sagði stjórnarskrá lýðveldisins Íslands nr. 33/1944 (hér eftir „stjskr.“) það eitt um friðhelgi einkalífs að heimilið væri friðheilagt og að hvorki mætti gera húsleit né kyrrsetja eða rannsaka bréf og önnur skjöl nema með dómsúrskurði eða sérstakri lagaheimild. Þrátt fyrir orðalag þágildandi 66. gr. stjskr. var litið svo á að einkalíf og fjölskylda nytu verndar samkvæmt óskráðum grunnreglum.[18]

> *Hrd. 1968, bls. 1007* (Kjörbarn). Hæstiréttur vísaði til grunnreglna laga um þagnarvernd einkalífs, því til stuðnings að maður ætti rétt á því að nöfn náttúrulegra foreldra kjörbarns hans yrðu ekki birt í riti um æviágrip lækna á Íslandi. Þó var ekki talið að þessar grunnreglur um persónuvernd yrðu leiddar af þágildandi 66. gr. stjskr.

Með 71. gr. stjskr. var orðalag ákvæðis 66. gr. víkkað verulega út á eftirfarandi hátt:

> Allir skulu njóta friðhelgi einkalífs, heimilis og fjölskyldu.
> Ekki má gera líkamsrannsókn eða leit á manni, leit í húsakynnum hans eða munum, nema samkvæmt dómsúrskurði eða sérstakri lagaheimild. Það sama á við um rannsókn á skjölum og póstsendingum, símtölum og öðrum fjarskiptum, svo og hvers konar sambærilega skerðingu á einkalífi manns.
> Þrátt fyrir ákvæði 1. mgr. má með sérstakri lagaheimild takmarka á annan hátt friðhelgi einkalífs, heimilis eða fjölskyldu ef brýna nauðsyn ber til vegna réttinda annarra.

Í friðhelgi einkalífs felst réttur manna til þess að ráða yfir lífi sínu og líkama og til að njóta friðar um lífshætti sína, einkahagi, tilfinningalíf sitt og tilfinningasambönd við aðra.[19] Við söfnun og skráningu persónuupplýsinga er hætta á að gengið sé of nærri réttindum þessum með afskiptum af persónulegum málefnum manna. Í skýringum með 71. gr. stjskr. er

[17] Hielke Hijmans og Alfonso Scirocco: “Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?”, bls. 1488.
[18] Alþt. 1994-95, A-deild, bls. 2099, Alþt. 1999-00, A-deild, bls. 2687 og Björg Thorarensen: *Stjórnskipunarréttur - mannréttindi*, bls. 284-285.
[19] Alþt. 1999-00, A-deild, bls. 2687 og Alþt. 1994-95, A-deild, bls. 2099.

sérstaklega tekið fram að skráning persónuupplýsinga sé raunhæft dæmi um svið þar sem álitaefni vaknar um hvort brotið er gegn friðhelgi einkalífs. Í því sambandi reynir á hversu langt megi ganga í skipulagðri skráningu á lífsháttum manna og meðferð slíkra upplýsinga.[20] Hæstiréttur hefur í dómaframkvæmd fellt vernd persónuupplýsinga undir ákvæði 71. gr. stjskr.

> *Hrd. 2003, bls. 4153 (151/2003)* (Gagnagrunnur á heilbrigðissviði). Dæmt var um kröfu konu á hendur íslenska ríkinu um að ógilda synjun landlæknis á að ekki yrðu færðar í gagnagrunn á heilbrigðissviði heilsufarsupplýsingar, sem skráðar hefðu verið í sjúkraskrár um látinn föður hennar. Hæstiréttur leit til þess að í sjúkraskrár væru skráðar yfirgripsmiklar upplýsingar um heilsufar manna, læknismeðferð sem þeir sæta, lifnaðarhætti og félagslegar aðstæður, atvinnu og fjölskylduhagi, ásamt nákvæmri tilgreiningu á því hver sá maður væri sem upplýsingarnar varða. Var það talið ótvírætt að 1. mgr. 71. gr. stjskr. tæki til slíkra upplýsinga og veitti sérhverjum manni friðhelgi um einkalíf sitt að þessu leyti.
>
> *Hrd. 1999, bls. 857 (252/1998)* (Einkamálefni sjúklings). Hæstiréttur fjallaði m.a. um gildissvið 71. gr. stjskr. gagnvart persónuupplýsingum, en í málinu var stjórnarmaður útgáfufélags sakfelldur fyrir hlutdeild í broti gegn friðhelgi einkalífs (230. gr. hgl.) með því að hafa skráð og birt frásögn læknis af einkamálefnum fyrrum sjúklings hans. Í niðurstöðum dómsins segir m.a. að „vernd persónuupplýsinga, og þá ekki síst heilsufarslegra, er nauðsynleg til þess að menn fái notið þeirra réttinda, sem varin eru með ákvæðum 71. gr. stjórnarskrárinnar“.

Með 71. gr. stjskr. er sú skylda lögð á ríkið að forðast afskipti af einkalífi manna og persónulegum högum þeirra. Ekki skapast síður hætta á skerðingu friðhelgi einkalífs af hálfu einstaklinga og lögaðila, t.d. með skráningu fyrirtækja á persónuupplýsingum viðskiptavina sinna og dreifingu einstaklinga á persónuupplýsingum á Internetinu. Ákvæði 71. gr. leggur því einnig þá skyldu á ríkið að binda í löggjöf skýrar reglur um öflun, skráningu og meðferð persónuupplýsinga, hvort sem ríkið eða einkaaðilar eiga í hlut. Með setningu pul. hefur löggjafinn uppfyllt þær skyldur.[21]

Með lögum nr. 62/1994 var Mannréttindasáttmála Evrópu (hér eftir „MSE“) veitt lagagildi á Íslandi, sbr. 1. gr. laga nr. 62/1994. Í 8. gr. sáttmálans er kveðið á um rétt manna til friðhelgi einkalífs, fjölskyldu, heimilis og bréfaskipta:

> Sérhver maður á rétt til friðhelgi einkalífs síns, fjölskyldu, heimilis og bréfaskipta. Opinber stjórnvöld skulu eigi ganga á rétt þennan nema samkvæmt því sem lög mæla fyrir um og nauðsyn ber til í lýðræðislegu þjóðfélagi vegna þjóðaröryggis, almannaheilla eða efnalegrar farsældar þjóðarinnar, til þess að firra glundroða eða glæpum, til verndar heilsu manna eða siðgæði eða réttindum og frelsi annarra.

[20] Alþt. 1994-95, A-deild, bls. 2099.
[21] Alþt. 1994-95, A-deild, bls. 2100, Alþt. 1999-00, A-deild, bls. 2687-2688 og Björg Thorarensen: *Stjórnskipunarréttur - mannréttindi*, bls. 284-285.

Vernd persónupplýsinga er ekki sérstaklega orðuð í ákvæðinu, en Mannréttindadómstóll Evrópu (hér eftir „MDE“) hefur í dómaframkvæmd staðfest að söfnun og geymsla á upplýsingum um einkalíf einstaklings geti falið í sér skerðingu á friðhelgi einkalífs hans undir 8. gr. MSE og falli því undir verndarandlag ákvæðisins. Í *MDE, Leander gegn Svíþjóð, 26. mars 1987 (9248/81)* staðfesti dómstóllinn að leynileg söfnun og skráning persónulegra upplýsinga um einstakling hjá lögreglu fæli í sér takmörkun á rétti viðkomandi til að njóta friðhelgi einkalífs. Dómstóllinn taldi þó þessa takmörkun á réttindum kæranda ekki vera úr hófi miðað við það markmið sem hún stefndi að. Einnig þótti sýnt fram á að öryggi uplýsinganna væri nægilega tryggt gagnvart misnotkun og hafi því ekki verið brotið gegn réttindum kæranda til friðhelgi einkalífs.[22] Einnig má nefna *MDE, Rotaru gegn Rúmeníu, 4. maí 2000 (28341/95)*, en þar taldi dómstóllinn að varðveisla og notkun rúmensku leyniþjónustunnar á gögnum um kæranda bryti í bága við 8. gr. MSE.

Til stuðnings þeirrar kenningar að vernd persónuupplýsinga sé sjálfstæður réttur einstaklings, en ekki eingöngu framhald af réttinum til friðhelgi einkalífs, er sáttmáli Evrópusambandsins um grundvallarréttindi.[23] Í 8. gr. sáttmálans er sérstaklega kveðið á um vernd persónuupplýsinga á meðan friðhelgi einkalífs nýtur verndar 7. gr. sama sáttmála. Í 8. gr. segir:

> Sérhver maður á *rétt til verndar eigin persónuupplýsinga*.
> Vinna skal úr slíkum upplýsingum með sanngjörnum hætti, í yfirlýstum tilgangi og með samþykki hlutaðeigandi eða á einhverjum öðrum réttmætum grundvelli sem mælt er fyrir um í lögum. Sérhver maður á rétt til aðgangs að upplýsingum sem teknar hafa verið saman um hann og rétt á að fá þær leiðréttar.
> Óháð yfirvald skal hafa eftirlit með því að þessum reglum sé fylgt.

Með ákvæði þessu er því gengið skrefinu lengra en í stjskr. og MSE með því að veita persónuupplýsingum sjálfstæða vernd.

Í íslenskum rétti er rétturinn til friðhelgi einkalífs, og þar með verndar persónuupplýsinga, ekki ótakmarkaður. Söfnun og vinnsla persónuupplýsinga er því viðurkennd í margvíslegu tilliti. Ákvæði 71. gr. girðir ekki fyrir opinbera skráningu um menn í þjóðskrá eða aðrar opinberar skrár svo sem kjörskrár og skattskrár.[24] Ganga má á rétt einstaklings undir 1. mgr. 8. gr. MSE ef mælt er fyrir um það í lögum, skerðingin hefur lögmætt markmið og er nauðsynleg í lýðræðislegu samfélagi, sbr. 2. mgr. 8. gr. MSE.[25]

---

[22] *MDE, Leander gegn Svíþjóð, 26. mars 1987 (9248/81)* og Björg Thorarensen: „Friðhelgi einkalífs og fjölskyldu og réttur til að stofna til hjúskapar“, bls. 293.
[23] Á ensku „Charter of Fundamental Rights of the European Union“.
[24] Alþt. 1994-95, A-deild, bls. 2099.
[25] David J. Harris, Michael O’Boyle og Colin Warbrick: *Law of the European Convention on Human Rights*, bls. 397-422.

Ákvæði 3. mgr. 71. gr. stjskr. heimilar jafnframt takmörkun á réttinum til friðhelgi einkalífs með *sérstakri lagaheimild* ef *brýn nauðsyn* ber til *vegna réttinda annarra*. Reynt getur á jafnvægi milli friðhelgi einkalífs og annarra stjórnarskrárverndaðra réttinda og kemur þá tjáningarfrelsi annarra oftast til álita. Niðurstaða slíks hagsmunamats ræðst af atvikum hverju sinni og hvort vegi þyngra, hagsmunir einstaklings til að njóta friðar um einkahagi sína eða nauðsyn þess að viðhalda frjálsri lýðræðislegri umræðu um málefni sem varða almenning.[26] Á þetta reyndi í *Hrd. 4. október 2007 (37/2007)* (Tölvupóstsamskipti í DV). Málsatvik voru sú að Fréttablaðið hafði birt upplýsingar upp úr tölvupóstsamskiptum stefnanda í tengslum við tiltekna lögreglurannsókn og greindi dagblaðið DV frá ástarsambandi stefnanda og nafngreinds manns í tengslum við tölvupóstsamskiptin. Hæstiréttur féllst ekki á að réttur DV til að miðla upplýsingunum um ástarsamband stefnanda væri ríkari en réttindi stefnanda til friðhelgi einkalífs. Um það segir m.a. í dómi Hæstaréttar:

> Þegar virt er sú ríka vernd, sem 1. mgr. 71. gr. stjórnarskrárinnar veitir einkalífi manna, verður á hinn bóginn ekki séð hvaða erindi upplýsingar þessu til viðbótar hafi átt til almennings um önnur og persónuleg samskipti gagnáfrýjanda við nefndan B, enda var hvorki leitast við í fréttaflutningi DV 26. september 2005 að skýra gildi þeirra fyrir málefnið, sem til umræðu var í þjóðfélaginu, né hafa aðaláfrýjendur fært fyrir því haldbærar skýringar í máli þessu.

3 Löggjöf um vernd persónuupplýsinga

Lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga eru byggð á því umfangsmikla persónuverndarregluverki sem þróað hefur verið innan Evrópusambandsins. Sem aðili að samningnum um Evrópska efnahagssvæðið[27] ber Íslandi að taka upp í landsrétt sinn þær reglugerðir og tilskipanir ESB sem teknar hafa verið upp í EES-samninginn.[28] Í íslenskum rétti er gengið út frá meginreglunni um tvíeðli þjóðaréttar og landsréttar. Felur hún m.a. í sér að þjóðréttarreglur fá ekki gildi að landsrétti nema þær hafi verið lögfestar.[29] Hafa gerðir ESB því ekki lagaáhrif gagnvart einstaklingum né lögaðilum að íslenskum rétti, nema reglurnar hafi verið innleiddar í landsrétt.

Hér verður gerð grein fyrir þeim Evrópureglum sem hafa þýðingu fyrir íslenska persónuupplýsingalöggjöf, áður en vikið er nánar að íslenskri löggjöf. Fjallað verður um markmið og gildissvið pul. auk þess sem grundvallarhugtökum laganna er lýst.

[26] Björg Thorarensen: *Stjórnskipunarréttur - mannréttindi*, bls. 305.
[27] Hér verður notast við styttinguna „EES-samningurinn“ þegar vísað er til samningsins, en skammstöfunina „EES“ eða styttinguna „EES-svæðið“ þegar átt er við Evrópska efnahagssvæðið.
[28] *Handbók Stjórnarráðsins um EES*, bls. 9 og 34.
[29] Davíð Þór Björgvinsson: *EES-réttur og landsréttur*, bls. 169.

3.1 Evrópureglur

Samningur Evrópuráðsins um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga (hér eftir „Evrópuráðssamningurinn“) var gerður þann 28. janúar 1981. Ísland fullgilti samninginn 25. mars 1991 og öðlaðist hann gildi 1. júlí sama ár.[30] Hann er því þjóðréttarlega skuldbindandi fyrir Ísland. Samkvæmt 1. gr. Evrópuráðssamningsins er markmið og tilgangur hans að tryggja einstaklingum virðingu fyrir réttindum þeirra og grundvallarfrelsi, einkum rétti til einkalífs að því er varðar vélræna vinnslu á persónuupplýsingum þeirra. Gildissvið samningsins nær einungis til vélrænnar vinnslu persónuupplýsinga, en á í meginatriðum við um alla vinnslu persónuupplýsinga þar sem tölvutækni er beitt.[31] Til að halda samningnum uppfærðum og í samræmi við þróun á sviði upplýsingavinnslu hefur Evrópuráðið beint tilmælum til aðildarríkja samningsins honum til fyllingar. Tilmælin eru nú 16 talsins, en eru ekki þjóðréttarlega skuldbindandi, líkt og samningurinn sjálfur. Þau geta aftur á móti haft mikla þýðingu í starfi eftirlitsaðila á sviði persónuverndar, þar sem tilmælin taka fyrir meðferð persónuupplýsinga á afmörkuðum sviðum og beitingu samningsins við úrlausn álitaefna sem á reynir í nútíma samfélagi.[32] Sem dæmi má nefna tilmæli Ráðherranefndar Evrópuráðsins nr. CM/Rec (2012)4 um vernd mannréttinda við notkun samfélagsmiðla.

Evrópuráðssamningurinn lagði mikilvægan grundvöll að tilskipun 95/46/EB. Tilskipunin var sett í þeim tilgangi að tryggja samræmdar reglur og samræmda persónuvernd í aðildarríkjum ESB og til að tryggja öryggi og aukna vernd einstaklinga við vinnslu persónuupplýsinga. Fyrir tilkomu hennar ríkti mikið ósamræmi meðal aðildarríkja ESB hvað varðar löggjöf um vernd persónuupplýsinga. Í sumum aðildarríkjanna voru engin lög sem veittu einstaklingum vernd um persónuupplýsingar sínar, á meðan önnur aðildarríki tryggðu slíka vernd með þeim hætti sem best þekktist í heiminum. Mismikil vernd á friðhelgi einkalífs í aðildarríkjunum var talin geta staðið í vegi fyrir frjálsu flæði persónuupplýsinga milli aðildarríkja og þar með skapað vandamál í efnahagslegu samstarfi þeirra. Af þeirri ástæðu lagði framkvæmdastjórn ESB fram tillögu að tilskipun, sem varð að tilskipun 95/46/EB.[33]

Samkvæmt 1. gr. tilskipunarinnar er markmið hennar tvíþætt. Annars vegar að tryggja rétt manna til þess að njóta friðhelgi einkalífs í tengslum við meðferð persónuupplýsinga og hins vegar að tryggja frjálst flæði persónuupplýsinga milli aðildarríkja ESB. Með tilskipuninni var því annars vegar stefnt að vernd grundvallarréttinda einstaklinga og hins vegar að efnahagslegu takmarki, með því að greiða fyrir frjálst flæði persónuupplýsinga á innri

[30] Stjórnartíðindi 1991, C-deild, bls. 47.
[31] Alþt. 1999-00, A-deild, bls. 2689.
[32] *Handbook on European Data Protection Law*, bls. 15-17.
[33] Alþt. 1999-00, A-deild, bls. 2690.

markaðnum.[34] Innan ramma tilskipunarinnar er aðildarríkjum heimilt að setja strangari reglur um meðferð persónuupplýsinga, sem tryggja meiri vernd en leiðir af tilskipuninni sjálfri. Sú heimild er aftur á móti ekki ótakmörkuð þar sem 2. mgr. 1. gr. tilskipunarinnar bannar aðildarríkjum að setja reglur um persónuvernd sem banna eða takmarka frjálsan flutning persónuupplýsinga milli aðildarríkjanna. Með ákvörðun sameiginlegu EES-nefndarinnar þann 25. júní 1999 var tilskipunin felld inn í EES-samninginn og var hún síðar innleidd í íslenskan rétt með lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.[35]

Með 29. gr. tilskipunar 95/46/EB var komið á fót starfshópi til að gegna ráðgjafarhlutverki um vernd einstaklinga við vinnslu persónuupplýsinga. Starfshópurinn gengur undir nafninu *29. gr. starfshópurinn* og starfar sjálfstætt. Hefur hann það meginhlutverk að stuðla að samræmdri túlkun á evrópskri persónuupplýsingalöggjöf með því að tjá sig um almenn álitaefni á því sviði. Starfshópurinn gegnir mikilvægu hlutverki á sviði evrópska persónuverndarregluverksins, þar sem hann gefur reglulega út álit um túlkun löggjafarinnar og stuðlar að samræmdri túlkun á lykilhugtökum hennar.[36] Starfshópurinn hefur m.a. gefið út álit um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ sem stuðst er við í ritgerð þessari.

Þann 25. janúar 2012 lagði framkvæmdastjórn ESB fram tillögur að breytingum á persónuupplýsingalöggjöf sambandsins. Í orðsendingu framkvæmdastjórnarinnar frá 4. nóvember 2010 var ályktað að þörf væri á breytingum á löggjöfinni, þar sem hún gæti ekki haldið í við öra tækniþróun og alþjóðavæðingu á sviði persónuupplýsingavinnslu.[37] Tillaga framkvæmdastjórnarinnar er tvíþætt. Um er að ræða tillögu að almennri reglugerð um vernd persónuupplýsinga og frjálsa miðlun slíkra upplýsinga[38] og tillögu að tilskipun um meðferð persónuupplýsinga í refsivörslukerfinu.[39] Í samræmi við viðfangsefni þessarar ritgerðar er þó óþarft að fjalla nánar um tilskipunina. Reglugerðartillaga framkvæmdastjórnar ESB var samþykkt af Evrópuþinginu um miðjan mars 2014 með nánar tilteknum breytingum.[40] Svo reglugerðin verði bindandi fyrir aðildarríki ESB skal hún þó einnig samþykkt af

[34] Christopher Kuner: *European Data Protection Law*, bls. 5.
[35] Alþt. 1999-00, A-deild, bls. 2686 og 2690-2691.
[36] Christopher Kuner: *European Data Protection Law*, bls. 9 og *úrskurður PV 4. mars 2013 (2012/1091)*.
[37] *A comprehensive approach on personal data in the European Union,* COM/2010/609/FINAL, bls. 2.
[38] Á ensku bera drögin heitið „Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“.
[39] Á ensku bera drögin heitið „Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data“.
[40] „European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“, http:// http://www.europarl.europa.eu.

Ráðherraráðinu.[41] Þar sem tillögur framkvæmdastjórnarinnar ganga langt og gríðarlegir hagsmunir búa þeim að baki, hefur verið talið líklegt að frekari breytingar verði gerðar áður en þær verða endanlega samþykktar af Ráðherraráðinu.[42] Verði reglugerðartillagan samþykkt kemur hún í stað tilskipunar 95/46/EB.

3.2 Íslensk löggjöf um vernd persónuupplýsinga

Á Íslandi hafa verið í gildi lög um skráningu og meðferð persónuupplýsinga frá árinu 1981. Fyrstu lög sem sett voru hér á landi til verndar persónuupplýsingum voru lög nr. 63/1981 um skráningu á upplýsingum er varða einkamálefni. Þótti nauðsynlegt að endurskoða lögin reglulega þannig að þau væru á hverjum tíma í samræmi við hinn tæknilega veruleika. Höfðu lög nr. 63/1981 því afmarkaðan gildistíma og féllu úr gildi 31. desember 1985. Tóku þá við lög nr. 39/1985 sem höfðu einnig fyrirfram afmarkaðan gildistíma og féllu úr gildi 31. desember 1989. Af lögum 39/1985 tóku við lög nr. 121/1989 um skráningu og meðferð persónuupplýsinga. Leystu lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga þau af hólmi þann 1. janúar 2001 og voru lögin sett í þeim tilgangi að innleiða í íslenskan rétt tilskipun 95/46/EB sem hafði þá verið tekin upp í EES-samninginn. Við samningu frumvarps þess er varð að lögum nr. 77/2000 var litið til þess hvernig aðrar þjóðir á Norðurlöndunum höfðu innleitt ákvæði tilskipunar 95/46/EB í lög. Sérstaklega var litið til Noregs þar sem lög nr. 121/1989 áttu að mestu fyrirmynd í ákvæðum norskra laga, auk þess sem Ísland og Noregur eru einu ríkin á Norðurlöndunum sem eru aðilar að EES en ekki ESB. Innleiðing tilskipunar 95/46/EB horfði því öðruvísi við Danmörku, Svíþjóð og Finnlandi.[43]

Með lögum nr. 77/2000 var sérstakri stofnun, Persónuvernd, falið eftirlit með framkvæmd laganna. Samkvæmt 1. mgr. 36. gr. pul. er Persónuvernd sjálfstæð stofnun með sérstaka stjórn. Verkefni Persónuverndar eru margvísleg. Um þau er fjallað í 37. gr. pul. en stofnunin úrskurðar m.a. í ágreiningsmálum sem kunna að koma upp um vinnslu persónuupplýsinga.

3.3 Markmið, gildissvið og skilgreiningar pul.

3.3.1 Markmið

Ákvæði 1. gr. pul. hefur að geyma markmiðsyfirlýsingu laganna. Með lögunum er stefnt að tvíþættu markmiði. Annars vegar að tryggja grundvallarréttindi einstaklinga til friðhelgi einkalífs og hins vegar að tryggja frjálst flæði upplýsinga innan EES. Í athugasemdum við 1.

[41] „Progress on EU data protection reform now irreversible following European Parliament vote“, http://europa.eu.
[42] Christopher Kuner: „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law“, bls. 2.
[43] Alþt. 1999-00, A-deild, bls. 2685-2686 og 2688.

gr. frumvarps þess er varð að lögum nr. 77/2000 segir að ætla megi að markmiðsyfirlýsing ákvæðisins muni hafa mikið gildi við túlkun annarra ákvæða frumvarpsins.[44] Persónuvernd hefur túlkað ákvæði laganna í samræmi við markmiðsyfirlýsingu þeirra, en í *úrskurði Persónuverndar*[45]*19. maí 2003 (2003/103)* (Guðfræðingatal) segir t.d. um ákvæðið að það beri með sér að pul. sé ætlað að vernda hagsmuni hins skráða, en ekki ábyrgðaraðila.

3.3.2 Efnislegt gildissvið

Í 3. gr. pul. er efnislegt gildissvið laganna afmarkað. Samkvæmt 1. mgr. ákvæðisins gilda lögin um sérhverja *rafræna* vinnslu persónuupplýsinga og *handvirka* vinnslu persónuupplýsinga sem eru eða eiga að vera hluti af skrá. Út frá persónuverndarsjónarmiðum er mikill munur á handvirkri og rafrænni vinnslu þar sem vinnslumöguleikar eru mun meiri með rafrænni tækni. Með rafrænni vinnslu er bæði dreifing persónuupplýsinga og leit í sjálfum upplýsingunum mun einfaldari en ef um handvirka vinnslu væri að ræða. Vinnsla sem er aðeins að hluta til rafræn er því lögð að jöfnu við vinnslu sem er rafræn að öllu leyti.[46] Þess ber einnig að geta að persónuupplýsingalögin taka bæði til vinnslu persónuupplýsinga af hálfu stjórnvalda og einkaaðila.[47]

Í 1. málsl. 2. mgr. 3. gr. pul. eru nokkur ákvæði laganna felld undan gildissviði þeirra ef unnið er með persónuupplýsingar sem varða almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu.[48]

Í 2. málsl. 2. mgr. 3. gr. er meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu ætlaðar til persónulegra nota undanþegin lögunum.[49] Samkvæmt skýringum með 3. gr. pul. er hér t.d. átt við einkabréfaskipti, færslu skráa með heimilisföngum vina og ættingja og færslu dagbóka, svo lengi sem upplýsingarnar varða eingöngu einkahagi viðkomandi eða eru einungis til persónulegra nota hans.[50] Skilin milli persónulegra nota og annarra nota geta þó verið óljós, t.d. þegar upplýsingum er dreift á Internetinu.[51] Fara skal varlega við beitingu undanþágunnar og skal hún túlkuð þröngt.[52]

Í 5. gr. pul. segir að víkja megi frá ákvæðum laganna í þágu fjölmiðlunar, lista eða bókmennta, ef það er nauðsynlegt til að samræma sjónarmið um rétt til einkalífs annars vegar

[44] Alþt. 1999-00, A-deild, bls. 2713.
[45] Hér eftir skammstafað PV.
[46] Alþt. 1999-00, A-deild, bls. 2717.
[47] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 7.
[48] Um er að ræða ákvæði 16., 18.-21., 24., 26., 31. og 32. gr. laganna.
[49] 29. gr. starfshópurinn vísar til undanþágunnar sem „undanþágu vegna heimilisafnota".
[50] Alþt. 1999-00, A-deild, bls. 2718.
[51] Nánar verður fjallað um 2. málsl. 2. mgr. 3. gr. í kafla 6.1.1.
[52] Christopher Kuner: *European Data Protection Law*, bls. 23.

og tjáningarfrelsis hins vegar. Þegar persónuupplýsingar eru einvörðungu unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi gilda einungis nánar tiltekin ákvæði.[53]

3.3.3 Landfræðilegt gildissvið

Í 6. gr. pul. er landfræðilegt gildissvið laganna afmarkað. Gilda lögin annars vegar um vinnslu persónuupplýsinga á vegum ábyrgðaraðila sem hefur *staðfestu* á Íslandi, og hins vegar um ábyrgðaraðila sem hefur staðfestu utan EES-svæðisins en notar *búnað* á Íslandi til vinnslu persónuupplýsinga.

Með staðfestu er átt við *virka og raunverulega starfsemi með föstu fyrirkomulagi* sbr. 19. lið formála tilskipunar 95/46/EB. Ræður það úrslitum hvort vinnslan sem fer fram á Íslandi sé það umfangsmikil og varanleg að það þyki eðlilegt að beita íslenskum lögum um hana.[54] Hafa má 31. gr. samningsins um Evrópska efnahagssvæðið[55] til hliðsjónar, sem kveður á um staðfesturétt og að með honum sé átt við rétt til að hefja og stunda sjálfstæða atvinnustarfsemi og stofna og reka fyrirtæki. Ábyrgðaraðili getur haft staðfestu í fleiri en einu EES-ríki, en af a-lið 1. mgr. 4. gr. tilskipunar 95/46/EB leiðir að ábyrgðaraðili verður að virða landslög hvers staðfesturíkis. Vinnur fjölþjóðafyrirtæki með persónuupplýsingar á Íslandi, Englandi og í Frakklandi og hefur staðfestu í öllum ríkjunum verður hann að fara að landslögum hvers staðfesturíkis að því er varðar þær upplýsingar sem þar eru.[56]

Íslensk lög gilda um starfsemi ábyrgðaraðila sem hefur staðfestu á Íslandi, þótt einstakir þættir vinnslunnar fari fram í öðru EES-ríki.

> Dæmi um þetta gæti verið ábyrgðaraðili sem hefur staðfestu á Íslandi en framkvæmir ákveðna liði vinnslunnar, t.d. söfnun persónuupplýsinga, í Danmörku. Komi til þess að danski eftirlitsaðilinn vilji stöðva þá söfnun eða setja sérstök fyrirmæli um framkvæmd hennar fer um það eftir íslenskum lögum. Á sama hátt mundi Persónuvernd verða að beita dönskum lögum um meðferð persónuupplýsinga sem fer fram hér á landi sé hún á vegum ábyrgðaraðila með staðfestu í Danmörku.[57]

Ef ábyrgðaraðili hefur staðfestu utan EES-svæðisins en notar *tæki og búnað* sem staðsettur er á Íslandi til vinnslu persónuupplýsinga, verður íslenskum lögum beitt um þann hluta starfseminnar sem fer fram hér á landi, sbr. 2. mgr. 6. gr. pul. Í athugasemdum með 6. gr. frumvarps þess er varð að lögum nr. 77/2000 segir að með búnaði sé átt við tölvur og

[53] Hér er um að ræða 4. gr., 1. og 4. tölul. 7. gr., 11.-13.gr. og 24., 28., 42. og 43. gr. laganna.
[54] Alþt. 1999-00, A-deild, bls. 2720-2721.
[55] Samningurinn um Evrópska Efnahagssvæðið öðlaðist gildi á Íslandi 1. janúar 1994, sbr. auglýsing c-deildar Stjórnartíðinda nr. 31/1993.
[56] Alþt. 1999-00, A-deild, bls. 2721. Þess ber að geta að fyrirhugaðar breytingar á persónuupplýsingalöggjöf ESB gera ráð fyrir samræmdri löggjöf á milli allra aðildarríkja, svo fjölþjóðafyrirtæki þurfi einungis að uppfylla skilyrði þeirrar löggjafar, en ekki mismunandi skilyrði hvers staðfesturíkis.
[57] Alþt. 1999-00, A-deild, bls. 2721.

útstöðvar, fjarskiptatæki, myndfundabúnað o.s.frv.[58] Vegna tækniþróunar er hugtakið *búnaður* orðið opnara fyrir mun rýmri túlkun en áður. Til dæmis hefur 29. gr. starfshópurinn litið svo á að svokölluð *smygildi* (e. *cookies*) geti talist til búnaðar í skilningi tilskipunar 95/46/EB.[59] Vinnsla persónuupplýsinga fellur þó ekki undir landfræðilegt gildissvið pul. þegar tækjabúnaður ábyrgðaraðila er einungis notaður til að flytja persónuupplýsingar frá einu landi til annars um Ísland, án þess að sérstök vinnsla fari fram hér á landi, sbr. 3. mgr. 6. gr. pul. Á þetta t.d. við þegar búnaður hvorki geymir né breytir upplýsingum á neinn hátt, þannig að eina hlutverk hans er í raun að senda upplýsingar á leiðarenda.[60]

3.3.4 Grundvallarhugtök

Í 2. gr. pul. er að finna skilgreiningar helstu hugtaka laganna sem eru byggð á 2. gr. tilskipunar 95/46/EB.

Persónuupplýsingar eru skilgreindar sem sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi, sbr. 1. tölul. 2. gr. pul. Undir hugtakið falla t.d. nöfn einstaklinga, heimilisföng, kennitölur og fingraför.[61] Ljósmyndir geta flokkast sem persónuupplýsingar ef hægt er að bera kennsl á þann sem birtist á myndinni og myndin ber með sér upplýsingar um hann.[62] Persónuupplýsingar eru ekki aðeins upplýsingar um einkamálefni einstaklings, heldur taka þær einnig til upplýsinga um t.d. fjárhagsmálefni og atvinnumál.[63] Skilgreining hugtaksins byggist á a-lið 2. gr. tilskipunar 95/46/EB. Þar segir að maður teljist persónugreinanlegur ef unnt er að rekja upplýsingar til hans, beint eða óbeint, svo sem með tilvísun í kennitölu eða einn eða fleiri þætti sem sérkenna hann í líkamlegu, lífeðlisfræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti. Þannig myndu ónafngreindar upplýsingar um alla karlmenn yfir fimmtugu á Akureyri líklega ekki teljast til persónuupplýsinga, þar sem það þykir ólíkegt að hægt væri að rekja slíkar upplýsingar til tiltekins einstaklings. Væru upplýsingarnar um alla karlmenn yfir fimmtugu á Akureyri, sem starfa sem læknar, eiga tvær dætur, hlusta á Verdi óperur og eiga sumarhús í suður Frakklandi, væri þó líklegra að um væri að ræða persónuupplýsingar, þar sem ríkari

[58] Alþt. 1999-00, A-deild, bls. 2721.
[59] *Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines*, bls. 7.
[60] Christopher Kuner: *European Data Protection Law*, bls. 120 og 127.
[61] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 8.
[62] *Svar PV um myndbirtingar 10. ágúst 2006.*
[63] Christopher Kuner: *European Data Protection Law*, bls. 92. Sjá einnig eldri skilgreiningu á hugtakinu *persónuupplýsingar* í 3. mgr. 1. gr. laga nr. 121/1989: „Með persónuupplýsingum er átt við upplýsingar sem varða einkamálefni, fjárhagsmálefni eða önnur málefni einstaklinga, stofnana, fyrirtækja eða annarra lögpersóna sem sanngjarnt er og eðlilegt að leynt fari.“

möguleiki er á að rekja þessa lýsingu til tiltekinna einstaklinga.[64] Í 26. lið formála tilskipunar 95/46/EB segir:

> Til að ákveða hvort hægt sé að tengja upplýsingarnar við einstakling skal tekið mið af öllum aðferðum sem eðlilegt er að hugsa sér að ábyrgðaraðili eða annar aðili beiti til að bera kennsl á viðkomandi einstakling.[65]

Upplýsingar teljast til persónuupplýsinga jafnvel þótt ekki sé hægt að tengja þær við tiltekinn einstakling nema með hjálp annarra upplýsinga. Hugtakið er því mjög víðfemt og tekur til allra upplýsinga, álita og umsagna, ef hægt er að tengja þær á einhvern hátt við tiltekinn einstakling.[66]

Deilt hefur verið um það hvort IP-tölur og smygildi geti flokkast sem persónuupplýsingar. IP-tala er samkvæmt orðabók Menningarsjóðs einkennistala tölvu. Við mat á því hvort slíkar einkennistölur flokkist sem persónuupplýsingar skiptir máli hvort talan sé breytileg (e. *dynamic*) eða föst (e. *static*). Breytileg IP-tala breytist í hvert skipti sem einstaklingur tengist Netinu, en föst IP tala er ávallt sú sama. Eðli breytilegu IP-tölunnar gerir það erfiðara að rekja hana til tiltekins einstaklings.[67] Í athugasemdum með 1. tölul. 2. gr. í frumvarpi því er varð að lögum nr. 77/2000 er eftirfarandi dæmi tekið:

> Aðili A sem selur þjónustu á netinu skráir einungis nafnlaus auðkenni sem ekki verða tengd tilteknum einstaklingi (netverja) [t.d. IP tala] nema með notkun lykils sem aðeins söluaðili internetsaðgangs, B, hefur undir höndum. Upplýsingarnar sem A skráir yrðu samkvæmt þessu taldar persónuupplýsingar í skilningi frumvarpsins þrátt fyrir að hann hafi ekki umræddan lykil undir höndum.[68]

IP-tala getur því flokkast sem persónugreinanlegar upplýsingar, en það fer eftir því hvort talan sé breytileg eða föst. Persónuvernd hefur litið svo á að IP-tölur séu persónuupplýsingar, þar sem þær geta verið rekjanlegar til einstaklinga.[69] En hvað með smygildi? Tölvuorðasafnið skilgreinir smygildi sem gagnahlut sem vefþjónn vistar í geymslu notanda og hefur síðan aðgang að til að auðvelda samskipti. Flest smygildi eru til þæginda fyrir notendur og geta verið nytsamleg, t.d. svo notandi þurfi ekki að skrifa notandaupplýsingar í hvert sinn sem hann skráir sig inn á tiltekna heimasíðu, en í staðinn eru upplýsingarnar vistaðar með hjálp smygilda. Smygildi vista t.d. IP-tölu netnotenda og sendir þeim aðila sem heldur úti vefsíðu. Tilgangurinn með slíkri upplýsingasöfnun getur t.d. verið sá að nota þær til markaðssetningar

[64] Christopher Kuner: *European Data Protection Law*, bls. 92.
[65] Alþt. 1999-00, A-deild, bls. 2686 og 2690-2691.
[66] Dorte Høilund: *Persondataloven*, bls. 16.
[67] Christopher Kuner: *European Data Protection Law*, bls. 91–95.
[68] Alþt. 1999-00, A-deild, bls. 2714.
[69] *Niðurstaða PV 16. desember 2009 (2009/635)* og *úrskurður PV 28. maí 2013 (2012/1390).*

eða til að telja heimsóknir á heimasíðu.[70] Notkun smygilda hefur verið harðlega gagnrýnd, þar sem fyrirtæki hafa notað þessa tækni til að safna upplýsingum um hegðunarmynstur einstaklinga á vefnum, t.d. með því að safna upplýsingum um innkaupamynstur notenda á Netinu.[71] Þess má geta að í reglugerðartillögu framkvæmdastjórnar ESB, sem er hluti af fyrirhuguðum breytingum á persónuupplýsingalöggjöf sambandsins, er gert ráð fyrir því að smygildi séu persónuupplýsingar. Þó er gerður fyrirvari um að svo þurfi ekki alltaf að vera.[72] Annað álitaefni er hvort smygildi teljast til búnaðar í skilningi 2. mgr. 6. gr. pul, en um það er fjallað nánar í kafla 6.2.

Ef upplýsingar hafa verið aftengdar einstaklingnum (e. *anonymous*), þannig að þær eru algjörlega órekjanlegar og því ekki lengur hægt að greina þann skráða, er ekki um að ræða persónuupplýsingar í skilningi pul.[73]

Eftir því sem upplýsingar standa persónu nær njóta þær ríkari verndar sem *viðkvæmar persónuupplýsingar*. Í 8. tölul. 2. gr. pul. eru eftirfarandi tegundir upplýsinga skilgreindar sem viðkvæmar persónuupplýsingar, en ákvæðið er í samræmi við 1. mgr. 8. gr. tilskipunar 95/46/EB:

> Upplýsingar um uppruna, litarhátt, kynþátt, stjórnmálaskoðanir, svo og trúar- eða aðrar lífsskoðanir.
> Upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað.
> Upplýsingar um heilsuhagi, þar á meðal um erfðaeiginleika, lyfja-, áfengis- og vímuefnanotkun.
> Upplýsingar um kynlíf manna og kynhegðan.
> Upplýsingar um stéttarfélagsaðild.

Í athugasemdum sem fylgdi frumvarpi því er varð að lögum nr. 77/2000 segir að aðrar upplýsingar en þær sem taldar eru upp í 8. tölul. 2. gr. laganna geti verið viðkvæmar. Því verður að meta það sérstaklega hverju sinni hvort um viðkvæmar persónuupplýsingar sé að ræða.[74] Helsta þýðing þess að upplýsingar eru skilgreindar sem viðkvæmar er að einhverju af sérstöku skilyrðum 9. gr. pul. þarf að vera fullnægt við vinnslu þeirra.[75]

Hugtakið *vinnsla* er í 2. tölul. 2. gr. pul. skilgreint sem „sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn“ og sækir ákvæðið fyrirmynd sína í b-lið 2. gr. tilskipunar 95/46/EB. Vinnsluhugtakið er mjög

[70] *Mál PV 8. maí 2013 (2012/1235)* (Umsögn um drög framkvæmdastjórnar ESB).
[71] Christopher Kuner: *European Data Protection Law,* bls. 94–95 og *Vejledning til "Cookie-bekendtgørelsen"*, bls. 6-8.
[72] *Proposal for a General Data Protection Regulation*, COM/2012/11/FINAL, 1. tölul. 4. gr. og 24. lið formála.
[73] Dorte Høilund: *Persondataloven*, bls. 16 og Alþt. 1999-00, A-deild, bls. 2713-2714.
[74] Alþt. 1999-00, A-deild, bls. 2716.
[75] Þórður Sveinsson: „Grunnreglur 7. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga“, bls. 410.

víðtækt og tekur til hvers konar meðferðar á persónuupplýsingum, óháð þeirri aðferð sem notuð er til vinnslunnar. Með því er t.d. átt við söfnun, skráningu, geymslu, breytingu, leit, notkun, eyðingu, dreifingu og aðrar aðferðir til að gera upplýsingarnar tiltækar.[76] Evrópudómstóllinn hefur þar að auki staðfest að dreifing persónuupplýsinga um einstaklinga á Internetinu flokkist sem vinnsla.[77]

Hugtakið *skrá* er í 3. tölul. 2. gr. pul. skilgreint sem sérhvert skipulagsbundið safn persónuupplýsinga þar sem finna má upplýsingar um einstaka menn. Samkvæmt skýringum með 3. tölul. 2. gr. pul. er hér átt við „gagnasafn eða upptalningu þar sem persónuupplýsingum er komið fyrir á þann hátt að þar má á ný finna upplýsingar um einstaka menn“.[78] Skilgreiningin er byggð á c-lið 2. gr. tilskipunar 95/46/EB. Í 27. gr. formála tilskipunarinnar segir að vernda beri einstaklinga, hvort sem um er að ræða rafræna eða handunna vinnslu upplýsinga. Tilskipunin tekur aftur á móti ekki til handvirkar vinnslu persónuupplýsinga, nema þær eigi að verða eða séu nú þegar hluti af skrá.[79]

4 Ábyrgðaraðili

4.1 Inngangur

Í kafla þessum verður gerð ítarleg grein fyrir ábyrgðaraðilahugtaki persónuupplýsingalaga. Fyrst verður vikið að forsögu hugtaksins og mismunandi skilgreiningum þess, bæði að Evrópurétti og í nágrannaríkjum Íslands. Næst verður notast við þríþætta aðgreiningu hugtaksins sem 29. gr. starfshópurinn byggði á í áliti sínu nr. 1/2010 um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ og henni beitt við greiningu á ábyrgðaraðilahugtaki pul, þó með nokkrum breytingum. Þá verður athugað hvaða reglur gilda þegar ábyrgðaraðilar að sömu vinnslu eru fleiri en einn og að lokum gerð grein fyrir þeim skyldum sem hvíla á ábyrgðaraðila á grundvelli pul.

4.2 Skilgreiningar

4.2.1 Tilskipun 95/46/EB

Í d-lið 2. gr. tilskipunar 95/46/EB er hugtakið ábyrgðaraðili (e. *controller*) skilgreint á eftirfarandi hátt:

> „ábyrgðaraðili“: einstaklingur eða lögpersóna, opinbert yfirvald, stofnun eða annar aðili sem ákveður, einn og sér eða í samvinnu við aðra, markmið og aðferðir við vinnslu persónuupplýsinga. Ef markmið og aðferðir við vinnsluna eru ákveðin í innlendum lögum og reglugerðum eða lögum og reglugerðum bandalagsins er heimilt að tilgreina

[76] B-liður 2. gr tilskipunar 95/46/EB og Alþt. 1999-00, A-deild, bls. 2714.
[77] *EBD, mál C-101/01, ECR 2003, bls. I-12971*.
[78] Alþt. 1999-00, A-deild, bls. 2715.
[79] Alþt. 1999-00, A-deild, bls. 2717.

> ábyrgðaraðila eða tilteknar viðmiðanir um útnefningu hans í lögum viðkomandi lands eða bandalagsins.[80]

Eins og fram hefur komið lagði Evrópuráðssamningurinn mikilvægan grunn að tilskipun 95/46/EB og á það einnig við um ábyrgðaraðilahugtak hennar. Hugtakið á rætur sínar að rekja til hugtaksins „skrárhaldari“ (e. *controller of the file*) í Evrópuráðssamningnum, en í d-lið 2. gr. samningsins segir að hugtakið merki:

> […] þann mann eða lögaðila, stjórnvald eða hverja aðra stofnun sem er bær samkvæmt landslögum að ákveða markmið með vélrænu skránni, hvers konar persónuupplýsingar eigi að geyma og hvaða aðgerðum megi beita.

Það sem skilur á milli ábyrgðaraðila- og skrárhaldarahugtakanna er í fyrsta lagi að ákvörðunarvald ábyrgðaraðila er ekki bundið við skrá, heldur við *vinnslu* persónuupplýsinga. Skrárhaldari er sá sem er bær til að ákveða markmiðið með vélrænu *skránni*, en ábyrgðaraðili sá sem ákveður markmið og aðferðir við *vinnslu* persónuupplýsinga. Ábyrgðaraðilahugtakið hefur rýmri merkingu þar sem það er tengt við vinnsluhugtakið sem nær til hverskonar meðferða á persónuupplýsingum.[81]

Í öðru lagi krefst skrárhaldarahugtakið þess að landslög mæli fyrir um hæfi aðila til að vera skrárhaldari, sbr. orðalagið „sá sem er bær samkvæmt landslögum að ákveða“. Er þetta gert annað hvort með því að tilnefna aðila beint í stöðu skrárhaldara, eða með því að lista ótvíræð skilyrði fyrir útnefningu hans í lögum. Ábyrgðaraðilahugtakið felur ekki í sér sömu tilvísun til landslaga og er því ekki bundið við landslög hvers og eins ríkis. Með því að sleppa slíkri tilvísun á að tryggja samræmda túlkun þess á meðal ríkja EES-svæðisins. Markmiðið með því var að veita ábyrgðaraðilahugtakinu sjálfstæða merkingu að sambandsrétti, óháð því hvaða merkingu landslög leggja í hugtakið.[82] Það er þó ekki útilokað að ábyrgðaraðili sé tilnefndur á grundvelli laga, eins og fjallað er um síðar í kafla 4.3.2.1.

Í þriðja lagi gerir ábyrgðaraðilahugtakið ráð fyrir möguleikanum á sameiginlegri ábyrgð, sbr. orðalagið „einn og sér eða í samvinnu við aðra“.[83] Í skrárhaldarahugtakinu er ekki minnst á slíka ábyrgð en hugmyndin um sameiginlega ábyrgð var ekki kynnt til sögunnar fyrr en stuttu fyrir gildistöku tilskipunar 95/46/EB.[84]

---

[80] Á ensku hljóðar skilgreiningin svo: „'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.“

[81] *Article 29 Working Party opinion 1/2010 on the concepts of “controller” and “processor”*, bls. 3.

[82] *Article 29 Working Party opinion 1/2010 on the concepts of “controller” and “processor”*, bls. 8-10.

[83] Um sameiginlega ábyrgð er fjallað nánar í kafla 4.4.

[84] *Article 29 Working Party opinion 1/2010 on the concepts of “controller” and “processor”*, bls. 17-18.

Af ofangreindu leiðir að ábyrgðaraðilahugtakið er rýmra en skrárhaldarahugtakið, þar sem það fyrrnefnda tekur til hverskonar vinnslu persónuupplýsinga og gerir ráð fyrir sameiginlegri ábyrgð. Auk þess er því ætlað að hafa sjálfstæða þýðingu að sambandsrétti og er ekki bundið við landslög hvers ríkis fyrir sig.

4.2.2 Lög 77/2000 og lög nágrannaríkja

Ábyrgðaraðili er sá aðili sem ákveður tilgang vinnslu persónuupplýsinga, þann búnað sem notaður er, aðferð við vinnsluna og aðra ráðstöfun upplýsinganna sbr. 4. tölul. 2. gr. pul. Hugtakið er byggt á d-lið 2. gr. tilskipunar 95/46/EB og var kynnt til sögunnar við setningu pul. Tók það við af hugtakinu *skrárhaldari* í lögum nr. 121/1989 um skráningu og meðferð persónuupplýsinga. Skrárhaldarahugtakið var hvorki skilgreint í lögunum sjálfum, né í lögskýringargögnum. Í eldri lögum sem sett voru hér á landi til verndar persónuupplýsingum, þ.e. lög nr. 63/1981 um skráningu á upplýsingum er varða einkamálefni og lög nr. 39/1985 um sama efni, er ekki að finna hugtak sambærilegt ábyrgðaraðila- eða skrárhaldarahugtakinu.

Í dönskum lögum um meðferð persónuupplýsinga [85] er notast við hugtakið „den dataansvarlige“. Í 4. tölul. 3. gr. dönsku laganna er hugtakið skilgreint sem „den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger“. Skilgreiningin er orðrétt sú sama og birtist í tilskipun 95/46/EB. Það kemur þó ekki á óvart, þar sem Danmörk er aðili að ESB og horfir innleiðing tilskipunarinnar því öðruvísi við þar en hér á landi. Í norskum lögum um meðferð persónuupplýsinga[86] er notast við hugtakið „behandlingsansvarlig“. Skilgreining þess svipar meira til þeirrar íslensku en þeirrar dönsku, en í 4. tölul. 2. gr. laganna segir að ábyrgðaraðili sé „den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.“ Í sænskum lögum um meðferð persónuupplýsinga[87] er notast við hugtakið „personuppgiftsansvarig“ og er það skilgreint í 3. gr. laganna sem „den som ensam eller tillsammans med andra bestämmer ändmålen med och medlen för behandlingen av personuppgifter.“

Ljóst er að ábyrgðaraðilahugtakið hefur verið innleitt á mismunandi hátt í landslög aðildarríkja EES og eru þau mis ítarleg. Það sem stingur í augu þegar hið íslenska hugtak er borið saman við skilgreiningar sambærilegra hugtaka er að hin íslenska útgáfa kveður á um að ábyrgðaraðili ákveði hvaða *búnað* skuli nota við vinnslu persónuupplýsinga. Í dönsku og

[85] Á dönsku bera lögin heitið „Lov nr. 429 af 31/05/2000 om behandling af personoplysninger“
[86] Á norsku bera lögin heitið „Lov 2000-04-14-31 om behandling av personopplysninger“
[87] Á sænsku bera lögin heitið „Personuppgiftslag 1998:204“

norsku skilgreiningunni eru orðin „hjælpemidler“ og „hjelpemidler“ notuð. Þegar litið er til enskrar þýðingar á annars vegar norsku persónuupplýsingalögunum og hins vegar þeim dönsku, kemur í ljós að með þessu orðalagi er átt við þá *aðferð* sem notuð er við vinnslu, sem svara til orðsins „means“ í tilskipun 95/46/EB. Þannig virðist ekki sérstaklega gert ráð fyrir því annars staðar en í íslenskum lögum að ábyrgðaraðili ákveði hvaða *búnað* skuli nota til vinnslu persónuupplýsinga. Að því verður vikið síðar hvort þetta ósamræmi hafi einhverja þýðingu í framkvæmd.

4.3 Afmörkun hugtaksins

Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ er ábyrgðaraðilahugtak tilskipunar 95/46/EB afmarkað í þrjá þætti; persónulega þáttinn (e. *the personal aspect*), sameiginlega þáttinn (e. *the possibility of pluralistic control*) og aðgreiningarþáttinn (e. *the essential elements to distinguish the controller from other actors*).[88] Í þessum kafla verður notast við afmörkun 29. gr. starfshópsins til að greina ábyrgðaraðilahugtak pul., þó með örfáum breytingum. Fyrsti þáttur hugtaksins, eins og það birtist í pul., snýr að því hver getur talist ábyrgðaraðili. Annar þáttur snýr að ákvörðunarvaldi ábyrgðaraðilans. Þriðji þáttur skilgreiningarinnar snýr að andlagi ákvörðunarvaldsins, þ.e. hvað aðili þarf að taka ákvarðanir um svo hann teljist ábyrgaraðili. Verður nú fjallað sjálfstætt um hvern þátt.

4.3.1 Aðildarhæfi

Fyrsti þáttur hugtaksins snýr að því hver getur talist ábyrgðaraðili. Í athugasemdum með frumvarpi því er varð að lögum nr. 77/2000 segir að „skilyrði þess að geta talist ábyrgðaraðili er að hafa aðildarhæfi og að geta svarað til saka fyrir tiltekna vinnslu persónuupplýsinga fyrir dómstólum, ef svo ber undir“.[89] Með hliðsjón af 1. mgr. 16. gr. einkamálalaga nr. 91/1991 má ályktа að aðilar njóti aðildarhæfis ef þeir geta átt réttindi eða borið skyldur að landslögum, en krafa pul. um aðildarhæfi er m.a. byggð á nauðsyn þess að geta leitað réttarúrræða til að fullnægja kröfum gagnvart ábyrgðaraðila. Bæði einstaklingar og lögaðilar geta haft aðildarhæfi í skilningi pul. og þar með talist ábyrgðaraðilar. Ábyrgðaraðili er þó í mörgum tilvikum lögaðili og taka lögin t.a.m. til vinnslu af hálfu atvinnurekenda, fyrirtækja, félaga, stofnana og opinberra aðila.[90] Sem dæmi um aðila sem Persónuvernd hefur talið

[88] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 1.
[89] Alþt. 1999-00, A-deild, bls. 2715.
[90] Alþt. 1999-00, A-deild, bls. 2715.

ábyrgðaraðila vinnslu má nefna ráðuneyti [91], heilsugæslustöð [92], Háskóla Íslands [93], Landsbókasafn Íslands[94] og hlutafélög.[95] Verði ábyrgðaraðili gjaldþrota telst þrotabú hans vera ábyrgðaraðili. [96] Við úrlausn stjórnsýslumála er oftar en ekki unnið með persónuupplýsingar almennra borgara. Við slíkar aðstæður er stjórnvald það sem ber ábyrgð á meðferð málsins og er bært til að taka ákvörðun í því almennt álitinn ábyrgðaraðili persónuupplýsinganna.[97]

Við vinnslu persónuupplýsinga í starfsemi fyrirtækja geta risið vafatilvik um hver sé ábyrgur fyrir vinnslunni í skilningi pul. Það er almennt viðurkennt að fyrirtækið sjálft sé ábyrgðaraðili vinnslunnar, þrátt fyrir að vinnslan sé unnin af einstaklingi innan fyrirtækisins, nema augljósar ástæður bendi til þess að einstaklingurinn skuli bera hina lagalegu ábyrgð.[98] Lögaðilar eru almennt í betri stöðu en einstaklingar til að gæta að réttindum þess skráða. Með því að úthluta lögaðilum stöðu ábyrgðaraðila, í stað þess einstaklings sem annast vinnsluna innan fyrirtækisins, eru réttindi hins skráða því betur tryggð.[99] Í *ákvörðun PV 17. september 2014 (2014/952)* (Heilbrigðisstofnun Austurlands), sem varðaði beiðni kvartanda um endurupptöku á *máli PV 5. júní 2010 (2012/193)*, reyndi á það hvort einstaklingur yrði gerður ábyrgur fyrir vinnslu, eða lögaðilinn sem hann starfaði hjá. Málið laut að uppflettingu starfsmanns Heilbrigðisstofnunar Austurlands í sjúkraskrá kvartanda. Skoðun á sjúkraskránni var í tengslum við tiltekið ágreiningsmál sem starfsmaðurinn átti í persónulega og heilbrigðisstofnunin var ekki aðili að. Starfsmaðurinn notaði þannig upplýsingarnar í eigin þágu, en þegar starfsmaður fer út fyrir umboð sitt og nýtir persónuupplýsingar í eigin þágu getur hann bakað sér sjálfstæða ábyrgð á þeim hluta vinnslunnar. Stuðst var við álit 29. gr. starfshópsins um hugtökin ábyrgðaraðili og vinnsluaðili, en um það segir í niðurstöðu Persónuverndar:

> Í umræddu áliti vinnuhópsins kemur m.a. fram að almenn ákvæði í löggjöf, geta gefið vísbendingu um það, hvaða einstaklinga eða lögaðila beri að líta á sem ábyrgðaraðila. Þá kemur einnig fram í álitinu að til að tryggja fyrirsjáanleika og stöðugleika fyrir hinn skráða, ætti fremur að leitast eftir því að beina eftirliti að lögaðila frekar en að tilteknum einstaklingi sem starfar fyrir viðkomandi lögaðila. Engu að síður segir jafnframt að ef einstaklingur, sem starfar fyrir lögaðila, vinni með persónuupplýsingar í eigin þágu og að sú vinnsla falli utan starfssviðs og ábyrgðar umrædds lögaðila, geti sá einstaklingur talist

[91] *Úrskurður PV 18. janúar 2010 (2010/1046).*
[92] *Úrskurður PV 17. ágúst 2011 (2010/906).*
[93] *Úrskurður PV 15. desember 2004 (2004/315).*
[94] *Úrskurður PV 25. janúar 2013 (2011/766).*
[95] *Úrskurður PV 26. júní 2007 (2007/258).*
[96] Alþt. 1999-00, A-deild, bls. 2715.
[97] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 11.
[98] Til dæmis ef viðkomandi vinnur upplýsingar í eigin þágu.
[99] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 15-17.

> ábyrgðaraðili. Þrátt fyrir það geti upphaflegur lögaðili einnig borið ábyrgð á hluta vinnslunnar hafi vinnsla persónuupplýsinga komið til vegna skorts á öryggisráðstöfunum.

Í samræmi við álit 29. gr. starfshópsins og 12. tölul. 3. gr. laga nr. 55/2009 um sjúkraskrár, sem kveður á um að ábyrgðaraðili sjúkraskrár sé heilbrigðisstofnun eða starfsstofa heilbrigðisstarfsmanna þar sem sjúkraskrár eru færðar, leit Persónuvernd svo á að Heilbrigðisstofnun Austurlands væri ábyrgðaraðili þeirrar vinnslu sem kvörtun kvartanda laut að, en ekki starfsmaður stofnunarinnar sem hafði staðið að uppflettingu sjúkraskrár kvartanda. Þá segir einnig í niðurstöðu Persónuverndar að þótt starfsmenn heilbrigðisstofnunarinnar kunni að hafa notað upplýsingar í eigin þágu, og geti þurft að svara til saka fyrir það, breyti það ekki stöðu stofnunarinnar sem ábyrgðaraðila gagnvart hinum skráða. Það hefur þó mikið vægi fyrir niðurstöðu málsins að í lögum nr. 55/2009 um sjúkraskrár var fjallað um ábyrgðaraðila sjúkraskráa. Sambærilegar aðstæður voru uppi í neðangreindum úrskurði Persónuverndar þar sem formaður Barnaverndarnefndar Reykjavíkur var talinn ábyrgðaraðili vinnslu sem þar fór fram.

> *Úrskurður PV 17. ágúst 2011 (2011/347)* (Formaður barnaverndarnefndar). Kvartandi kvartaði yfir því að Barnaverndarnefnd Reykjavíkur hafi unnið með persónuupplýsingar um sig og fjölskyldu sína, án heimildar. Um var að ræða skólaverkefni A og H, en verkefnið fólst í því að athuga árangur af tilteknu úrræði á vegum Velferðarsviðs og Barnaverndarnefndar Reykjavíkur. Barnaverndarnefnd Reykjavíkur veitti aðgang að persónuupplýsingum kvartanda í þágu verkefnisins, án þess að fá fyrir því samþykki kvartanda eða leyfi Persónuverndar. Það að veita aðgang að persónuupplýsingum telst til vinnslu í skilningi pul. og var Barnaverndarnefnd Reykjavíkur talið óheimilt að veita slíkan aðgang án samþykkis hins skráða eða leyfis Persónuverndar. Í reglugerð 56/2004 er að finna reglur um málsmeðferð fyrir barnaverndarnefnd. Þar segir í 4. mgr. 36. gr. að formaður barnaverndarnefndar beri ábyrgð á því að óviðkomandi eigi ekki aðgang að upplýsingum og gögnum barnaverndarmála. Formaður Barnaverndarnefndar Reykjavíkur var því talinn vera ábyrgðaraðili persónuupplýsinganna í skilningi laga nr. 77/2000 og bæri því ábyrgð á því að varðveisla og ráðstöfun persónuupplýsinga væri með lögmætum hætti.

Mál þetta er frábrugðið *ákvörðun PV 17. september 2014 (2014/952)* (Heilbrigðisstofnun Austurlands) að því leyti að ábyrgð á aðgangi að upplýsingum og gögnum var með reglugerð lögð á einstakling en ekki á lögaðilann sjálfan. Almennt er lögaðilinn talinn ábyrgðaraðili persónuupplýsinga og ber því að varast að draga of víðtækar ályktanir af þessum úrskurði. Úrskurðurinn sýnir þó réttilega að einstaklingar geta talist ábyrgðaraðilar, en einstaklingar vinna persónuupplýsingar í auknum mæli, t.a.m. með notkun Internetsins og samfélagsmiðla, og geta talist ábyrgðaraðilar þeirra upplýsinga sem þeir deila þar með öðrum. Um ábyrgðaraðila og samfélagsmiðla er fjallað ítarlega í kafla 6.

4.3.2 Ákvörðunarvald

Annar þáttur hugtaksins snýr að ákvörðunarvaldi ábyrgðaraðilans, en með ábyrgðaraðila er átt við þann aðila sem hefur ákvörðunarvald um vinnslu persónuupplýsinga. Lög og reglugerðir geta tilnefnt ábyrgðaraðila, en við mat á því hvort aðili fari með ákvörðunarvald um vinnslu skal þó ávallt litið til heildarmats á aðstæðum og hver fari með *raunverulegt* ákvörðunarvald hverju sinni. Verður nú vikið að þýðingu raunverulegs ákvörðunarvalds annars vegar og lögbundins ákvörðunarvalds hins vegar.

4.3.2.1 Lögbundið ákvörðunarvald

Í seinni hluta ábyrgðaraðilahugtaksins eins og það birtist í d-lið 2. gr. tilskipunar 95/46/EB segir:

> Ef markmið og aðferðir við vinnsluna eru ákveðin í innlendum lögum og reglugerðum eða lögum og reglugerðum bandalagsins er heimilt að tilgreina ábyrgðaraðila eða tilteknar viðmiðanir um útnefningu hans í lögum viðkomandi lands eða bandalagsins.

Samkvæmt þessu geta lög og reglugerðir tilnefnt aðila beint í stöðu ábyrgðaraðila eða tilgreint viðmiðanir um útnefningu hans ef kveðið er á um markmið og aðferðir við vinnsluna í lögum. Þetta á einnig við í íslenskum rétti, þó það sé ekki tekið sérstaklega fram í skilgreiningu hugtaksins í pul.[100]

Dæmi um tilnefningu ábyrgðaraðila má finna í reglugerð 235/2010 um upplýsingaskyldu framhaldsskóla um skólahald, aðra kerfisbundna skráningu og meðferð persónuupplýsinga um nemendur. Í 1. mgr. 5. gr. reglugerðarinnar segir:

> Hver framhaldsskóli er ábyrgðaraðili í skilningi laga um persónuvernd og meðferð persónuupplýsinga. Skólameistari ber ábyrgð á meðferð og vörslu upplýsinga og að skólinn uppfylli lagalegar kröfur sem gerðar eru til ábyrgðaraðila samkvæmt lögum um persónuvernd og meðferð persónuupplýsinga og laga um Þjóðskjalasafn Íslands, nr. 66/1985.

Í nýlegri *ákvörðun PV 13. mars 2014 (2013/1192)* (Prófskírteini) komst Persónuvernd að þeirri niðurstöðu að ákvæði laga nr. 92/2008 um framhaldsskóla, fæli ekki í sér heimild til vinnslu persónuupplýsinga um annað en námsmat og vitnisburð nemenda í umsögn á prófskírteini þeirra. Má jafnframt nefna lög nr. 55/2009 um sjúkraskrár, en í 9. gr. laganna segir að ábyrgðaraðili sjúkraskráa beri ábyrgð á því að varðveisla þeirra sé í samræmi við ákvæði laga nr. 55/2009. Í 12. tölul. 3. gr. sömu laga er ábyrgðaraðili sjúkraskráa skilgreindur sem heilbrigðisstofnun eða starfsstofa heilbrigðisstarfsmanna þar sem sjúkraskrár eru færðar, sbr. *ákvörðun PV 17. september 2014 (2014/952)* (Heilbrigðisstofnun Austurlands) sem reifuð er hér að ofan.

[100] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 11.

Söfnun persónuupplýsinga og vinnsla þeirra getur einnig verið þáttur í lögbundnu hlutverki aðila, s.s. þegar stjórnvöld afla upplýsinga í tengslum við stjórnvaldseftirlit. Ákvörðunarvald ábyrgðaraðila er þá hvorki byggt á tilnefningu né á viðmiðunum um útnefningu hans, heldur á því hlutverki sem hann gegnir samkvæmt lögum eða reglugerðum og nauðsyn þess að afla persónuupplýsinga í því skyni.[101] Samkvæmt 2. mgr. 5. gr. laga nr. 101/2010 um greiðsluaðlögun einstaklinga er umboðsmanni skuldara skylt að afla tiltekinna upplýsinga áður en hann tekur ákvörðun um hvort veita skuli heimild til greiðsluaðlögunar. Í ákvæðinu segir:

> Umboðsmaður skuldara skal auk þess afla frekari upplýsinga sem hann telur geta skipt máli varðandi skuldir, eignir, tekjur og framferði skuldara, áður en hann tekur ákvörðun um hvort veita skuli heimild til að leita greiðsluaðlögunar. Komi til þess skal veita skuldara fræðslu í samræmi við ákvæði 21. gr. laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, um fræðsluskyldu ábyrgðaraðila þegar upplýsinga er aflað frá öðrum en hinum skráða. Ef þörf krefur er umboðsmanni skuldara heimilt að kalla skuldara eða aðra sem málið varðar á sinn fund til að afla upplýsinganna.

Af orðalagi ákvæðisins má ráða að umboðsmaður skuldara fari með ákvörðunarvald um hvenær skuli afla frekari upplýsinga og telst hann því ábyrgðaraðili þeirra.

Vinnumálastofnun er annað dæmi um stjórnvald sem fer með ákvörðunarvald um vinnslu persónuupplýsinga á grundvelli lögbundins hlutverks síns. Um Vinnumálastofnun gilda lög nr. 54/2006 um atvinnuleysistryggingar. Í *úrskurði PV 16. desember 2009 (2009/635)* (Vinnumálastofnun) reyndi á það hvort vinnsla á IP-tölu bótaþega væri nauðsynleg svo Vinnumálastofnun gæti rækt lögbundið hlutverk sitt. Var IP-talan notuð til að ganga úr skugga um að bótaþegi væri í virkri atvinnuleit í skilningi laga nr. 54/2006 um atvinnuleysistryggingar, en IP-talan sýndi að bótaþegi væri staddur erlendis. Persónuvernd taldi vinnslu slíkra upplýsinga vera í samræmi við ákvæði pul., en gerði þó athugasemd við það að Vinnumálastofnun hafði ekki frætt hinn skráða um að IP-tala hans yrði skoðuð.

Jafnvel þótt lög og reglugerðir kveði á um ákvörðunarvald aðila yfir vinnslu persónuupplýsinga þarf ávallt að ganga úr skugga um að slíkt fyrirkomulag endurspegli raunverulegar aðstæður og að sá aðili fari með raunverulegt ákvörðunarvald. Við mat á aðstæðum getur t.d. komið í ljós að hinn lögbundni ábyrgðaraðili er ekki einn um ábyrgðina, þar sem annar aðili hefur einnig ákvörðunarvald um vinnsluna.

4.3.2.2 Raunverulegt ákvörðunarvald

Með raunverulegu ákvörðunarvaldi er átt við hvar ákvarðanir um vinnslu persónuupplýsinga eru teknar í raun og veru, óháð hverskonar samningum, lögum eða öðrum formsatriðum.

[101] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 10.

Raunverulegt ákvörðunarvald snýr því frekar að staðreyndum og mati á aðstæðum hverju sinni, en að formlegu ákvörðunarvaldi.[102]

Ákvörðunarvald aðila getur í vissum tilvikum stuðst við sérstaka og afmarkaða yfirlýsingu, s.s. í skriflegum samningi. Formleg skipun ábyrgðaraðila á grundvelli samnings getur reynst gagnleg og veitt ákveðnar vísbendingar við mat á því hvort aðili gegni stöðu ábyrgðaraðila. Ef engin ástæða er til að efast um að ákvæði samningsins endurspegli raunverulegar aðstæður er ekkert því til fyrirstöðu að fylgja ákvæðum samningsins um hlutverkaskipti aðila að vinnslunni. Samningsskilmálar eru þó ekki afgerandi við slíkt mat, þar sem þeir endurspegla ekki endilega raunveruleikann.

Í áliti 29. gr. starfshópsins nr. 10/2006 um hið svokallaða SWIFT-mál[103] sá starfshópurinn ástæðu til að líta framhjá orðalagi samninga þar sem gefið var í skyn að SWIFT væri vinnsluaðili en þau fjármálafyrirtæki sem SWIFT starfaði fyrir voru tilgreind sem ábyrgðaraðilar. SWIFT stendur fyrir „Society for Worldwide Interbank Financial Telecommunication“. Samtökin eru í eigu fjármálastofnana um allan heim og sjá þau um að reka samskiptakerfi sem notað er til að millifæra fjármagn með öruggum hætti. Sem milliliður í gjaldeyrisfærslum safnaði SWIFT töluverðu magni persónuupplýsinga, m.a. nöfnum viðtakanda greiðslu og greiðanda. Að mati 29. gr. starfshópsins var SWIFT ekki vinnsluaðili þessa upplýsinga, þar sem samtökin færu með mun meiri ábyrgð og ákvörðunarvald um vinnslu upplýsinganna en talist gæti í verkahring vinnsluaðila. Taldi 29. gr. starfshópurinn samtökin því vera ábyrgðaraðila þeirra upplýsinga sem safnað var í tengslum við millifærslur. Auk þess höfðu samtökin tekið ákvörðun um að flytja upplýsingar um ýmis bankaviðskipti úr evrópskum gagnagrunni sínum til Bandaríkjanna, án fyrirmæla þess efnis frá þeim fjármálastofnunum sem það starfaði fyrir. Voru samtökin einnig talin ábyrgðaraðili þeirrar vinnslu. Í áliti 29. gr. starfshópsins segir orðrétt:

> While SWIFT presents itself as a data processor, and some elements might suggest that SWIFT has acted in the past as a processor in certain cases on behalf of the financial institutions, the Working Party, having considered the effective margin of manoeuvre it possesses in the situations described above, is of the opinion that SWIFT is a controller as defined by Article 2 (d) of the Directive.[104]

SWIFT var því talið bera sameiginlega ábyrgð á vinnslunni með þeim fjármálafyrirtækjum sem það starfaði fyrir. Titill í samningi er því ekki afgerandi við mat á

[102] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 8.
[103] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).*
[104] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, bls. 11.

hlutverki aðila, heldur ber að líta til aðstæðna hverju sinni og hjá hverjum hið raunverulega ákvörðunarvald liggur.[105] Hafa skal í huga að ákvörðunarvaldið getur verið hjá fleiri en einum aðila, en nánar er fjallað um SWIFT-málið í kafla 4.4 um sameiginlega ábyrgð.

4.3.3 Andlag ákvörðunarvalds

Þriðji þáttur hugtaksins snýr að andlagi ákvörðunarvaldsins, þ.e. hvað aðili þarf að hafa ákvörðunarvald um til að teljast ábyrgðaraðili persónuupplýsinga. Samkvæmt pul. hefur ábyrgðaraðili ákvörðunarvald um *tilgang* vinnslunnar, þann *búnað* sem notaður er, *aðferð* við vinnsluna og *aðra ráðstöfun* þeirra upplýsinga sem unnið er með. Til að aðili teljist ábyrgðaraðili þarf hann ekki að hafa tekið ákvörðun um alla efnisþætti hugtakins, heldur nægir að hann taki ákvörðun um einn þessa þátta. Til dæmis getur ábyrgðaraðili verið sá sem tekur ákvörðun um ráðstöfun upplýsinga.[106]

Með því að taka ákvörðun um *tilgang* vinnslu er jafnframt tekin ákvörðun um að vinnslan skuli eiga sér stað. Samkvæmt 2. tölul. 1. mgr. 7. gr. pul. skal gæta þess við vinnslu persónuupplýsinga að þær séu fengnar í yfirlýstum, skýrum og málefnalegum *tilgangi* og ekki unnar frekar í öðrum og ósamrýmanlegum *tilgangi*. Hefur þessi regla verið kölluð tilgangsreglan.[107] Ákvörðun um tilgang vinnslu er því mikilvæg til að afmarka hversu langt megi ganga við vinnslu persónuupplýsinga. Einungis ábyrgðaraðili getur tekið slíka ákvörðun. Ef aðili sem kemur að vinnslu persónuupplýsinga tekur ákvörðun um að tiltekin vinnsla skuli eiga sér stað telst hann því ábyrgðaraðili hennar. Til marks um það er álit 29. gr. starfshópsins nr. 10/2006 um SWIFT málið þar sem SWIFT tók þá ákvörðun að afhenda bandarískum yfirvöldum upplýsingar um gjaldeyrisfærslur og var talið ábyrgðaraðili þeirrar vinnslu.[108]

Í athugasemdum með 4. tölul. 2. gr. pul. er ekki að finna frekari skýringu á því hvað felst í hugtakinu *aðferð* (e. *means*) við vinnslu. Af forsögu ábyrgðaraðilahugtaksins má þó draga vissar ályktanir. Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ kemur fram að við meðferð tilskipunardraga, sem síðar urðu að tilskipun 95/46/EB, var efnisþáttum ábyrgðaraðilahugtaksins fækkað úr fjórum í tvo og orðalagi þeirra breytt. Upprunalegu efnisþættirnir voru (a) tilgangur/markmið vinnslunnar (b) hvaða

---

[105] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, bls. 10-11.

[106] Sigrún Jóhannesdóttir: „Áhrif reglna Evrópusambandsins á íslenskan rétt og ný Evrópulöggjöf um persónuvernd“. Erindi flutt á ráðstefnu *Nýjar ógnir við friðhelgi einkalífs og meðferð persónuupplýsinga.*

[107] Þórður Sveinsson: „Grunnreglur 7. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga“, bls. 422.

[108] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).*

persónuupplýsingar skulu unnar (c) aðgerðir við vinnsluna og (d) aðgangur þriðja aðila að upplýsingunum. Efnisþættir hugtaksins í tilskipun 95/46/EB eru í dag tveir; *markmið* og *aðferð* við vinnslu. Breytingin var þó einungis til styttingar og ekki ætlað að hafa í för með sér efnislegar breytingar. Til dæmis heyrir ákvörðun um hvaða persónuupplýsingar skulu unnar undir aðferðarhugtakið, þótt það sé ekki tilgreint sem sérstakur efnisþáttur þess. Mismunandi ákvarðanir falla því undir aðferðahugtakið, en 29. gr. starfshópurinn hefur skipt slíkum ákvörðunum í tvo flokka eftir eðli þeirra. Annars vegar ákvarðanir er lúta að *tækni- og skipulagsatriðum* og hins vegar ákvarðanir um *grundvallaratriði* vinnslu.[109]

Með ákvörðunum um grundvallaratriði vinnslu er átt við ákvarðanir um ráðstöfun persónuupplýsinga, s.s. hvaða persónuupplýsingar skulu unnar, hversu lengi og hver hafi aðgang að þeim. Slíkar ákvarðanir eru einungis teknar af ábyrgðaraðila.[110]

Samkvæmt ofangreindu áliti 29. gr. starfshópsins er með ákvörðunum um tækni- og skipulagsatriði t.d. átt við ákvörðun um hvaða hugbúnaður sé notaður við vinnslu. Ákvörðun um hvaða búnað skuli nota er því felld undir *aðferðarhugtakið*. Í sama áliti telur starfshópurinn það almennt viðurkennt að vinnsluaðili geti tekið ákvarðanir á þessu sviði, án þess að skapa sér sjálfstæða ábyrgð á vinnslunni, þar sem vinnsluaðili getur reynst betur til þess fallinn að ákveða hvaða búnaður hentar henni best. [111] Í skilgreiningu ábyrgðaraðilahugtaksins í 4. tölul. 2. gr. pul. er aftur á móti tekið sérstaklega fram að ábyrgðaraðili sé sá sem ákveður *hvaða búnað* skuli nota við vinnslu persónuupplýsinga. Líkt og stuttlega var gerð grein fyrir hér að framan er ekki að finna sama efnisþátt í skilgreiningum nágrannaþjóða Íslands á ábyrgðaraðilahugtakinu, né í tilskipun 95/46/EB. Það liggur því ekki ljóst fyrir hvað býr að baki þessum efnisþætti hugtaksins í íslenskum rétti, hvort honum sé ætlað að koma fleiri aðilum undir ábyrgðaraðilahugtakið eða hvort honum sé ekki ætlað að hafa frekari áhrif. Í athugasemdum við ábyrgðaraðilahugtakið í frumvarpi því er varð að lögum nr. 77/2000 segir að ábyrgðaraðili hafi ákvörðunarvald um „hvað sá hugbúnaður sem notaður er á að gera“.[112] Þar segir því ekki orðrétt að ábyrgðaraðili þurfi að ákveða hvaða tiltekni búnaður skuli notaður, heldur má draga þá ályktun að hann ákveði hvað slíkur hugbúnaður á að geta gert í því skyni að ná markmiði vinnslunnar. Í samræmi við uppbyggingu ábyrgðaraðilahugtaks tilskipunar 95/46/EB og álit 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ gæti ábyrgðaraðili veitt vinnsluaðila fyrirmæli um hvert markmið vinnslunnar sé en falið honum að ákveða hvaða búnaður skuli notaður til að ná

[109] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 13-15.
[110] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 14.
[111] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 12-15.
[112] Alþt. 1999-00, A-deild, bls. 2715.

því markmiði. Umboð það sem ábyrgðaraðili veitir vinnsluaðila hefur áhrif á það hvort sá síðarnefndi geti tekið ákvarðanir um tækni- og skipulagsatriði, án þess að baka sér sjálfstæða ábyrgð, en lögmæti þess sem vinnsluaðili gerir ræðst af því umboði. Gangi vinnsluaðili lengra en umboðið nær, eða taki hann að einhverju marki sjálfstæðar ákvarðanir, getur hann talist ábyrgur, a.m.k. á þeim þáttum sem hann ræður sjálfur og tekur ákvarðanir um.[113] Jafnframt verður ábyrgðaraðili að hafa úrskurðarvaldið um þær ákvarðanir sem teknar eru um vinnsluna, svo vinnsluaðili teljist ekki bera sameiginlega ábyrgð á vinnslu með upprunalegum ábyrgðaraðila.[114] Hvort þetta eigi einnig við í íslenskum rétti, þ.e. hvort vinnsluaðili sé bær til að taka ákvarðanir um tækni- og skipulagsatriði vinnslunnar, er þó ekki fyllilega ljóst. Hér verður ekki tekin endanleg afstaða til þessa álitaefnis, en er þessum vangaveltum fyrst og fremst varpað fram til umhugsunar. Að mati höfundar væri þó upplagt að útskýra nánar í lögskýringargögnum hvað búi að baki þessum auka efnisþætti, sem hvorki er sjáanlegur í Norrænni persónuupplýsingalöggjöf, né í tilskipun 95/46/EB.

Persónuvernd og umboðsmaður Alþingis hafa deilt um merkingu aðferðarhugtaksins í skilningi 4. tölul. 2. gr. pul., en á túlkun þess reyndi í neðangreindum úrskurði Persónuverndar sem var síðar kvartað yfir til umboðsmanns Alþingis.

> *Úrskurður PV 10. júní 2009 (2009/172)* (Fjölmennt I). Sálfræðingarnir A og B, sem störfuðu hjá Y ehf., höfðu unnið skýrslu að beiðni sjálfseignarstofnunarinnar Fjölmennt í kjölfar kvörtunar starfsmanns Fjölmenntar yfir einelti á vinnustað. Sami starfsmaður kvartaði síðar til Persónuverndar, þar sem hún taldi sálfræðingana tvo ekki hafa veitt sér fræðslu, sbr. 20. gr. pul., um það að frásagnir hennar um samskipti sín við samstarfsfólk yrðu birtar í skýrslunni og henni síðar dreift. Í skýrslunni var m.a. byggt á persónuupplýsingum sem kvartandi veitti um sig sjálfa. Persónuvernd leit svo á að Fjölmennt hafi haft ákvörðunarvald um *tilgang* vinnslunnar, þar sem skýrslugerðin fór fram að beiðni fyrirtækisins, og væri því ábyrgðaraðili vinnslunnar. Aftur á móti taldi Persónuvernd sálfræðingana A og B einnig gegna hlutverki ábyrgðaraðila, þar sem þeir höfðu farið með ákvörðunarvald um það *hvernig* staðið væri að vinnslunni. Komst Persónuvernd því að þeirri niðurstöðu að Fjölmennt og sálfræðingarnir tveir hefðu ekki veitt kvartanda fræðslu í samræmi við 20. gr. pul.

Af orðalagi úrskurðarins, að A og B höfðu farið með ákvörðunarvald um það *hvernig* staðið væri að vinnslunni, má draga þá ályktun að sálfræðingarnir hafi farið með ákvörðunarvald um *aðferð* við vinnsluna. Það kemur þó ekki skýrt fram í úrskurðum og ákvörðunum Persónuverndar um ofangreint mál, nákvæmlega hvað sálfræðingarnir höfðu ákvörðunarvald um. Það lá þó fyrir að sálfræðingarnir höfðu töluvert svigrúm við gerð skýrslunnar og ekki lágu fyrir nákvæm fyrirmæli frá Fjölmennt um hvernig gerð hennar

[113] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25 – 26.
[114] *Handbook on European Data Protection Law*, bls. 52-53 og *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 12-15.

skyldi hagað.[115] Í *ákvörðun PV 13. ágúst 2009 (2009/172)* (Fjölmennt II), þar sem Persónuvernd synjaði um endurupptöku málsins, kemur fram að sérfræðiþekking sálfræðinganna hafi haft áhrif á niðurstöðu Persónuverndar þess efnis að þeir væru ábyrgðaraðilar. Sálfræðingarnir leituðu síðar til umboðsmanns Alþingis og kvörtuðu yfir niðurstöðu Persónuverndar. *Álit umboðsmanns Alþingis 5. september 2012 (6055/2010)* (Fjölmennt III) beindist að því hvort sú forsenda Persónuverndar að sálfræðingarnir tveir væru ábyrgðaraðilar að vinnslunni, hefði verið í samræmi við lög. Í athugun sinni lagði umboðsmaður töluverða áherslu á hvað fælist í hugtakinu *aðferð* við vinnslu, en í álitinu segir:

> Í athugasemdum við 4. tölul. 2. gr. laga nr. 77/2000 er ekki að finna frekari skýringu á efnisþáttum ákvæðisins, s.s. um það hvað felst í hugtakinu „aðferð“ við vinnslu. Við nánari túlkun þessa efnisþáttar verður að mínu áliti að hafa hliðsjón af 2. tölul. 2. gr. Þar er hugtakið „vinnsla“ skilgreint á þann hátt að um sé að ræða „aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn“. Þegar litið er til athugasemda við það ákvæði og önnur í lögskýringargögnum með frumvarpi því er varð að lögum nr. 77/2000 má álykta að átt sé við aðgreinda vinnsluþætti eða vinnsluaðgerðir, s.s. söfnun, skráningu, varðveislu eða miðlun, en ekki þá aðferðarfræði eða þá faglegu sérfræðiaðferð sem talið er heppilegt að leggja til grundvallar við öflun eða úrvinnslu á upplýsingum í tilteknu skyni.

Umboðsmaður beitir síðan sögulegri skýringu til þess að tengja aðferðarhugtakið við vinnsluhugtak persónuupplýsingalaga á eftirfarandi hátt:

> [...] við meðferð tilskipunardraga þeirra er síðar urðu að tilskipun nr. 95/46/EB hafi efnisþáttum ábyrgðaraðilahugtaksins verið fækkað úr fjórum samkvæmt upphaflegri tillögu framkvæmdastjórnar EB í tvö og orðalagi þeirra breytt. Meðal annars hafi verið horfið frá því að nota hugtakið „aðgerðir“ (e. operations). Í stað þess sé nú notað hugtakið „aðferðir“ (e. means). Breytingin hafi þó ekki verið efnisleg heldur hafi hún verið til styttingar. Með þetta í huga bendi ég á að í gildandi ákvæðum tilskipunarinnar er hugtakið „aðgerðir“ (e. operations) notað með sambærilegum hætti og í lögum nr. 77/2000 um hugtakið „vinnslu“ sem í tilskipuninni er skilgreint sem „aðgerð eða röð aðgerða, rafrænna eða annarra en rafrænna, svo sem söfnun, skráning, kerfisbinding, geymsla, aðlögun eða breyting, heimt, leit, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækilegar, samantenging eða samkeyrsla, aðgangstakmörkun, afmáun eða eyðilegging“.

Af ofangreindu virðist sem umboðsmaður telji að undir aðferðarhugtakið falli þær *aðgerðir* sem teljast til vinnslu í skilningi 2. tölul. 2. gr. pul. Á grundvelli þessa taldi umboðsmaður þá faglegu sérfræðiaðferð, sem sálfræðingarnir notuðu við öflun og greiningu á upplýsingum um atburði á vinnustaðnum, ekki teljast til aðferðar í skilningi ábyrgðaraðilahugtaks laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Það var niðurstaða umboðsmanns Alþingis að Persónuvernd hefði ekki sýnt fram á að A og B hefðu farið með ákvörðunarvald um þá vinnslu persónuupplýsinga sem um ræddi í málinu.

[115] *Ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV).

Taldi umboðsmaður sálfræðingana tvo ekki vera ábyrgðaraðila vinnslunnar. Persónuvernd hefur, þrátt fyrir álit umboðsmanns, haldið fast í túlkun sína á aðferðarhugtakinu og synjað beiðnum um endurskoðun á málinu.[116]

Í ofangreindum málum Persónuverndar kom sérfræðiþekking aðila til álita við mat á því hvort þeir hafi farið með ákvörðunarvald um aðferð vinnslunnar. Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ segir að ef aðili sem kemur að vinnslu persónuupplýsinga býr yfir ákveðinni sérfræðiþekkingu er það líklegt til að hafa áhrif á afmörkun á hlutverki hans.[117] Aðilar sem búa yfir sérfræðiþekkingu eru t.d. lögmenn, endurskoðendur, læknar og sálfræðingar.[118] Sérþekking þeirra og sjálfstæði getur bent til þess að þeir fari með ákvörðunarvald um þá vinnslu sem þeir taka að sér og teljist því ábyrgðaraðilar hennar. Um þetta segir í *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV):

> Í löggjöf er lögð áhersla á stöðu sálfræðinga sem sjálfstæðrar fagstéttar. Í því sambandi má t.d. nefna 3. gr. laga nr. 40/1976 um sérstaka trúnaðarskyldu sálfræðinga. Segir að sálfræðingi sé skylt að gæta þagmælsku um atriði sem hann fær vitneskju um í starfi sínu og leynt skulu fara samkvæmt lögum eða eðli máls. [...] Eftir að leitað var eftir vinnslusamningi milli Fjölmenntar og umræddra sálfræðinga í kjölfar álits umboðsmanns Alþingis hefur fengist staðfest að enginn slíkur samningur var gerður. Af því leiðir jafnframt að ekki gátu talist hafa legið fyrir nákvæm fyrirmæli frá Fjölmennt um hvernig sálfræðingunum bæri að haga starfi sínu. Í samræmi við það liggur og fyrir að við umrædda rannsókn unnu sálfræðingarnir eftir nokkuð ítarlegum verklagsreglum sem þeir höfðu sjálfir sett sér […]

Þóttu því öll rök hníga að því að í ljósi sérfræðiþekkingar sinnar höfðu sálfræðingarnir ráðið mestu um það hvernig verkið var unnið og leit Persónuvernd því á þá sem ábyrgðaraðila vinnslunnar. Einnig kemur til álita hversu mikið svigrúm verkbeiðandi hefur veitt verktaka til útfærslu á sjálfu verkinu þótt sá síðarnefndi búi yfir ákveðinni sérþekkingu. Því meira svigrúm sem vinnsluaðili fær í þeim efnum, því meiri líkur eru á því að hann beri ábyrgð á hluta vinnslunnar. Þannig getur skortur á fyrirmælum verkbeiðanda leitt til þess að verktaki hafi ákvörðunarvald um hvernig skuli haga verkinu. Ef verktaki hefur aftur á móti fengið nákvæm fyrirmæli frá verkbeiðanda um hvernig verkið skal útfært bendir það til þess að verktaki gegni hlutverki vinnsluaðila. Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ er rakið raunhæft dæmi um endurskoðendur sem vert er að hafa til hliðsjónar:

> Þegar endurskoðandi veitir þjónustu á grundvelli mjög almennra fyrirmæla frá verkbeiðanda, s.s. fyrirmæla um að útbúa skattaskýrslu, gegnir endurskoðandinn að öllu

[116] *Ákvörðun PV 13. febrúar 2014 (2013/1397)* (Fjölmennt V).
[117] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 28.
[118] Sjá t.d. lög nr. 77/1998 um lögmenn og lög nr. 79/2008 um endurskoðendur.

> jöfnu hlutverki ábyrgðaraðila, þar sem hann ákveður hvaða upplýsingum skal safnað og í hvaða tilgangi. Það horfir þó öðruvísi við ef endurskoðandi er t.d. fenginn til að annast nákvæma og afmarkaða endurskoðun innan fyrirtækis þar sem hann er undir stjórn yfirendurskoðanda þess og tekur við fyrirmælum frá honum. Við slíkar aðstæður væri almennt litið svo á að endurskoðandinn gegndi hlutverki vinnsluaðila vegna skýrleika fyrirmæla og þ.a.l. takmarkaðs svigrúms hans til ákvarðanatöku.[119]

Í eftirfarandi úrskurði Persónuverndar kom sérfræðiþekking sálfræðings til álita, en niðurstaðan var þó önnur en í *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV).

> *Úrskurður PV 25. júní 2013 (2012/964)* (Barnaverndarnefnd Reykjavíkur). Kvartað var yfir miðlun persónuupplýsinga um kvartanda frá barnaverndarnefnd Reykjavíkur til sálfræðingsins B. Kvörtunin var þríþætt, en í því samhengi sem hér er til álita skiptir sá þáttur kvörtunarinnar máli er beindist að því að barnaverndarnefndin hafði ekki gert vinnslusamning við umræddan sálfræðing varðandi vinnslu viðkvæmra persónuupplýsinga. Sálfræðingurinn hafði framkvæmt sálfræðimat á kvartanda m.t.t. forsjárhæfni hennar og fengið afhent gögn frá barnaverndarnefndum til að geta unnið matið. Skilningur sálfræðingsins var sá að hann ynni í umboði barnaverndarnefndar og væri því vinnsluaðili að þeirri persónuupplýsingavinnslu sem átti sér stað í tengslum við forsjárhæfnismatið. Hins vegar hafði hann haft nokkurt sjálfdæmi um hvernig forsjármatið yrði unnið. Bar hann því ábyrgð á þeim hluta vinnslunnar sem hann framkvæmdi í krafti sérfræðiþekkingar sinnar þegar hann aflaði upplýsinga úr sjúkraskrá kvartanda og lagði sérfræðilegt mat á forsjárhæfni hennar, m.a. með viðtölum við hana. Þrátt fyrir að sálfræðingurinn hafi borið ábyrgð á afmörkuðum og sérhæfðum hlutum vinnslunnar var það niðurstaða Persónuverndar að hann starfaði sem vinnsluaðili fyrir barnaverndarnefnd Reykjavíkur, þar sem nefndin hafði meginákvörðunarvald um það hvernig skýrslan skyldi úr garði gerð, m.a. með því að leggja fyrir sálfræðinginn tilteknar spurningar sem skyldi svarað í skýrslunni. Bar stofnuninni því skylda til að gera skriflegan vinnslusamning við sálfræðinginn í samræmi við 13. gr. pul.

Þótt B hafi borið ábyrgð á afmörkuðum hluta vinnslunnar, bar barnaverndarnefnd Reykjavíkur ábyrgð á verkinu í heild sinni. Var því litið svo á að B starfaði fyrir hönd nefndarinnar sem vinnsluaðili. Ólíkt *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV), þar sem engin fyrirmæli voru veitt af hálfu Fjölmenntar til sálfræðinganna tveggja, voru tiltölulega nákvæm fyrirmæli veitt í máli þessu, m.a. með því að leggja fyrir sálfræðinginn tilteknar spurningar sem skyldi svarað í skýrslu um forsjárhæfnimat kvartanda. Því má ætla að þau fyrirmæli sem veitt voru í seinna málinu hafi orðið til þess að B var ekki látinn bera sameiginlega ábyrgð á verkinu ásamt barnaverndarnefnd Reykjavíkur.

Í *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV) er einnig stuttlega vikið að þeim væntingum sem kvartandi hafði til sálfræðinganna tveggja sem önnuðust gerð vinnustaðaskýrslunnar, en í bréfi kvartanda til Persónuverndar kemur fram að hún hafi staðið í þeirri trú að sálfræðingarnir væru ekki síður að vinna fyrir hana en fyrir vinnuveitandann. Samkvæmt áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ ber að líta til þeirra væntinga sem hinn skráði hefur til aðila sem koma að vinnslunni við mat á því

[119] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 29.

hvort um ábyrgðaraðila eða vinnsluaðila sé að ræða, m.ö.o. skal horfa til þess hvernig hinn skráði upplifir hlutverk aðila.[120] Í sama áliti er eftirfarandi dæmi rakið þessu til stuðnings.

> Ábyrgðaraðili fól símaþjónustuveri að annast símaþjónustu við viðskiptavini sína. Þjónustuverinu voru veitt fyrirmæli um að kynna sig undir nafni ábyrgðaraðila í samskiptum sínum við viðskiptavini. Var upplifun viðskiptavina sú að ábyrgðaraðili annaðist vinnsluna, þar sem viðskiptavinurinn upplifði að hann væri að ræða við sjálfan ábyrgðaraðilann, en ekki annan sjálfstæðan aðila. Þjónustuverið var talið starfa fyrir hönd ábyrgðaraðilans og því talið vinnsluaðili.[121]

Af framangreindu leiðir að þegar lagt er mat á það hvort aðili sem kemur að vinnslu persónuupplýsinga sé ábyrgðaraðili þeirra þarf í fyrsta lagi að meta hvort hann hafi tekið ákvörðun um *tilgang* vinnslunnar. Ef svo er telst hann ábyrgðaraðili. Í öðru lagi þarf að meta hvort hann hafi tekið ákvörðun um *aðferð* við vinnsluna. Hafi viðkomandi tekið ákvörðun um grundvallaratriði vinnslunnar telst hann að öllu jöfnu ábyrgðaraðili hennar. Sé tekið mið af áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ veltur það á umboði því sem viðkomandi hefur frá upprunalegum ábyrgðaraðila hvort hann hafi svigrúm og heimild til að taka ákvarðanir er snúa að tækni- eða skipulagsatriðum vinnslunnar, án þess að skapa sér sjálfstæða ábyrgð. Þá kemur einnig til álita hvort viðkomandi búi yfir sérfræðiþekkingu og hvort honum hafi verið veitt fyrirmæli um framkvæmd vinnslu.

4.4 Sameiginleg ábyrgð

Ábyrgðaraðilahugtak tilskipunar 95/46/EB gerir ráð fyrir að ábyrgðaraðilar geti verið fleiri en einn. Ábyrgðaraðilahugtak persónuupplýsingalaga gerir ekki ráð fyrir slíkri sameiginlegri ábyrgð, en það leiðir hinsvegar af úrskurðum Persónuverndar, auk þess sem það er tekið sérstaklega fram á heimasíðu stofnunarinnar, að ábyrgðaraðilar geta verið fleiri en einn.[122]

Almennt á sameiginleg ábyrgð sér stað þegar tveir eða fleiri aðilar ákveða að vinna persónuupplýsingar í sameiningu og ákvarðanir um vinnslu upplýsinganna, s.s. um tilgang og aðferðir, eru teknar í sameiningu.[123] Í því skyni að koma til móts við vaxandi margbreytileika á sviði persónuupplýsingavinnslu hefur 29. gr. starfshópurinn mælt með rúmri túlkun á hugmyndinni um sameiginlega ábyrgð og lítur svo á að samvinna við vinnsluna geti verið mismikil og þurfi ekki að vera með öllu sameiginleg. Í sumum tilfellum geta aðilar unnið mjög náið saman og ákveðið í sameiningu bæði tilgang vinnslunnar og grundvallaratriði er snúa að aðferð hennar. Í öðrum tilvikum ákveða aðilar einungis grundvallaratriði um aðferð

[120] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 28.
[121] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 28.
[122] *Úrskurður PV 10. júní 2009 (2009/172)* og vefsíða Persónuverndar, http://www.personuvernd.is.
[123] Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet*, bls. 152-153.

vinnslunnar í sameiningu, en upplýsingarnar eru unnar í mismunandi tilgangi.[124] Þá eru *Fjölmenntarmálin*[125] til marks um að ákvarðanir þurfa ekki að vera teknar í *sameiningu* svo um sameiginlega ábyrgð sé að ræða. Eins og fram hefur komið voru sálfræðingarnir tveir taldir ábyrgðaraðilar ásamt Fjölmennt vegna sjálfstæði síns og svigrúms við ákvarðanatöku, en ekki vegna sameiginlegrar ákvarðanatöku. Svo lengi sem fleiri aðilar en einn fara með ákvörðunarvald um vinnslu er því um sameiginlega ábyrgð að ræða.

Til marks um mismunandi form sameiginlegrar ábyrgðar er álit 29. gr. starfshópsins nr. 10/2006 um SWIFT málið. SWIFT veitti bandarískum yfirvöldum upplýsingar um tiltekin bankaviðskipti, þ.á.m. viðskipti sem fóru fram innan aðildarríkja ESB. Bandarísk yfirvöld höfðu birt SWIFT stefnu með fyrirmælum um að láta af hendi tiltekin gögn í þágu baráttu Bandaríkjanna gegn hryðjuverkum. SWIFT afhendi umbeðin gögn án þess að bera afhendinguna undir þá banka og fjármálastofnanir sem það starfaði fyrir. Að mati 29. gr. starfshópsins báru fjármálastofnanir þær sem SWIFT starfaði fyrir ekki einungis ábyrgð á eigin persónuupplýsingavinnslu, heldur einnig að einhverju leiti á þeirri vinnslu sem SWIFT framkvæmdi. Taldi starfshópurinn SWIFT og einstaka fjármálastofnanir bera sameiginlega ábyrgð á vinnslu umræddra upplýsinga, þ.á.m. miðlun þeirra til yfirvalda í Bandaríkjunum, jafnvel þótt SWIFT hafi tekið þá ákvörðun að sjálfsdáðum. Ástæða þess var m.a. sú að stofnanirnar áttu að geta haft áhrif á ákvarðanatöku SWIFT, enda sátu fulltrúar sumra þeirra í stjórn SWIFT. Það væri undir bönkunum og fjármálastofnununum komið að velja samstarfsaðila sem sæi til þess að persónuupplýsingavernd væri tryggð og að eftirlit væri haft með vinnslunni. Þar af leiðandi leit 29. gr. starfshópurinn svo á að stofnanirnar tækju þátt í ákvarðanatöku SWIFT um tilgang og aðferð vinnslu og væru, ásamt SWIFT, ábyrgðaraðilar að vinnslu upplýsinganna.[126]

Samvinna á milli aðila við vinnslu persónuupplýsinga getur reynst gagnleg, bæði hjá hinu opinbera og í einkageiranum. Fyrirtæki geta t.d. komið upp sameiginlegu afsláttar- og auglýsingakerfi, sem safnar upplýsingum um innkaup fólks í þeim tilgangi að veita viðskiptavinum betri þjónustu og auglýsingar um tilboð sem falla að innkaupamynstri þeirra. Slíku meðlimakerfi var komið upp af tveimur fyrirtækjum í Danmörku, sem höfðu samráð við Datatilsynet, dönsku eftirlitsstofnunina á sviði persónuverndar, við uppsetningu kerfisins. Í *máli Datatilsynet 30. janúar 2008 (nr. 2007-212-0042)* var leyst úr álitaefnum á sviði

[124] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 19.
[125] *Úrskurður PV 10. júní 2009 (2009/172)* (Fjölmennt I), *ákvörðun PV 13. ágúst 2009 (2009/172)* (Fjölmennt II), *Álit umboðsmanns Alþingis 5. september 2012 (6055/2010)* (Fjölmennt III), *Ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV) og *Ákvörðun PV 13. febrúar 2014 (2013/1397)* (Fjölmennt V).
[126] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*.

persónuupplýsingaverndar vegna uppsetningu kerfisins. Fyrirtækin Fællesforeningen for Danmarks Brugsforeninger (hér eftir „FDB“) og dótturfélag þess, Coop Danmark A/S (hér eftir „Coop“), vildu sameina gagnasöfn sín í þeim tilgangi að veita viðskiptavinum sínum persónulegri þjónustu byggða á innkaupamynstri þeirra, ásamt afsláttum þegar þar til gerð meðlimakort væru notuð. Gagnasafn FDB innihélt upplýsingar um meðlimi, s.s. nafn, heimilisfang og símanúmer, en í gagnasafni Coop var innkaupamynstur hvers meðlims skráð, svo lengi sem meðlimakortið væri notað við innkaup. Upplýsingar úr gagnasafni Coop, s.s. upplýsingar á innkaupastrimli, voru þannig tengdar við upplýsingar úr gagnasafni FDB og var þannig hægt að tengja innkaupin við tiltekinn viðskiptavin. FDB taldi því réttast að bæði Coop og FDB væru ábyrgðaraðilar að meðlimakerfinu. Datatilsynet féllst á það með FDB, svo lengi sem skýrar reglur og leiðbeiningar væru settar um vinnslu persónuupplýsinganna og að þeir skráðu gætu leitað réttar síns hjá báðum fyrirtækjum.

Sameiginleg ábyrgð getur einnig reynst gagnleg við notkun hins opinbera á miðlægum gagnagrunnum, sem notaðir eru þvert á sveitarfélög og önnur umdæmi. Í norskri skýrslu um meðferð lögreglu og ákæruvaldsins á upplýsingum, er mælt með sameiginlegri ábyrgð að slíkum miðlægum gagnagrunnum:

> Utvalget mener det er hensiktsmessig med et delt behandlingsansvar, hvor det er et sentralt organ og flere lokale organer som deler ansvaret. Hvilke oppgaver som tilligger det sentrale organet og hva som ligger på det lokale, vil variere fra system til system. Det som er viktig, er at ansvarsfordelingen klart fastsettes, og da fortrinnsvis i forskriften for det enkelte systemet. En mulig deling vil være at det sentrale organet har ansvaret for systemet som sådant, mens det lokale organet har ansvaret for bruken av systemet på sitt tjenestested.[127]

Í skýrslunni er lögð fram tillaga um að sameiginlegri ábyrgð sé deilt þannig að hið æðra vald beri ábyrgð á gagnagrunninum í heild sinni, á meðan hið staðbundna vald beri ábyrgð á notkun gagnagrunnsins í sínu umdæmi. Í norskum lögum er þessu fylgt eftir og er kveðið sérstaklega á um möguleikann á sameiginlegri ábyrgð í reglugerð um meðferð lögreglu og ákæruvalds á upplýsingum, sem tekur m.a. til miðlægra gagnagrunna lögreglu. Í 2. málsl. 4. mgr. 45. gr. norsku reglugerðarinnar [128] er t.a.m. kveðið á um sameiginlega ábyrgð rannsóknarlögreglu ríkisins og lögreglustjóra á þeim upplýsingum sem eru sendar i DNA-greiningu.[129]

.

[127] *Kriminalitetsbekjempelse og personvern,* bls. 147.
[128] Forskrift om behandling av opplysninger i politiet og påtalemyndigheten (FOR-2013-09-20-1097).
[129] Í 2. málsl. 4. mgr. 45. gr. norsku reglugerðarinnar segir: „Kripos og politimestrene har delt behandlingsansvar for prøver, person- og saksopplysninger som sendes analyseinstitusjoner for DNA-analyse.“ Kripos rannsóknarlögregla norska ríkisins.

Af reglugerð 322/2001 um meðferð persónuupplýsinga hjá lögreglu leiðir að embætti ríkislögreglustjóra heldur skrár sem eru nauðsynlegar í þágu lögreglustarfa. Gagnagrunnur lögreglu er miðlægur og eru öll lögregluembætti tengd þeim grunni.[130] Á ríkislögreglustjóra hvíla ýmsar skyldur samkvæmt reglugerð 322/2001, s.s. að tilkynna um vinnslu persónuupplýsinga til Persónuverndar. Flestum ákvæðum reglugerðarinnar er þó beint að „lögreglu“, s.s. skylda til að veita hinum skráða vitneskju um upplýsingar sem lögreglan hefur um hann, sbr. 8. gr. reglugerðarinnar. Af úrlausnum Persónuverndar má draga þá ályktun að með „lögreglu“ sé átt við einstök lögregluumdæmi. Þannig er það á ábyrgð hvers og eins umdæmis að unnið sé með persónuupplýsingar í samræmi við gildandi lög og reglur.[131] Af ofangreindu virðist sem ríkislögreglustjóri hafi yfirstjórn með meðferð persónuupplýsinga í skrám lögreglu, á meðan hvert og eitt umdæmi sér til þess að meðferð þeirra persónuupplýsinga, sem geymdar eru í skrám lögreglu, fari eftir settum reglum. Slíkt fyrirkomulag er í samræmi við niðurstöðu norsku skýrslunnar um meðferð lögreglu og ákæruvalds á upplýsingum, þ.e. að hið æðra vald beri ábyrgð á gagnagrunninum í heild sinni, á meðan hið staðbundna vald beri ábyrgð á notkun gagnagrunnsins í sínu umdæmi.[132] Við mat á því hvort um sameiginlega ábyrgð sé að ræða gilda þó áfram sömu reglur og ef um hefðbundið mat væri að ræða. Skoða skal hvar hið raunverulega ákvörðunarvald liggur og ef það er að finna hjá tveimur eða fleiri aðilum, er um að ræða sameiginlega ábyrgð.[133]

Þegar fleiri en einn ábyrgðaraðili koma að vinnslu getur reynst flókið að skipta með þeim þeirri ábyrgð sem fylgir hlutverki ábyrgðaraðila, s.s. að gæta að réttindum þess skráða og að unnið sé með persónuupplýsingar í samræmi við gildandi lög og reglur. Þar af leiðandi getur verið óljóst hver sé bótaskyldur vegna tjóns sem verður, þegar unnið hefur verið með persónuupplýsingar í andstöðu við ákvæði pul. Sameiginleg ábyrgð leiðir ekki sjálfkrafa til óskiptrar ábyrgðar[134], þar sem ábyrgð hvers og eins ábyrgðaraðila getur verið mismikil og á mismunandi þáttum vinnslunnar.[135] Í áliti 29. gr. starfshópsins nr. 10/2006 um SWIFT málið er þessu lýst á eftirfarandi hátt:

> [...] the Working Party is of the opinion that sufficient elements support the opinion that a joint responsibility exists with the financial institutions and the cooperative SWIFT where they are represented, for the processing of personal data via the SWIFTNet FIN service.

[130] Þskj. 1199, 140. lögþ. 2011-12, bls. 1 (enn óbirt í A-deild Alþt.).
[131] *Úrskurður PV 22. júní 2011 (2011/272)* og *svar PV 17. ágúst 2011 (2011/681).* Í þessum málum er ábyrgð á vinnslu persónuupplýsinga talinn hvíla á annars vegar Lögreglunni á Suðurnesjum og hins vegar Lögreglunni á höfuðborgarsvæðinu.
[132] *Kriminalitetsbekjempelse og personvern*, bls. 147.
[133] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 18.
[134] Óskipt ábyrgð er þegar fleiri en einn bera ábyrgð á kröfu og ábyrgð hvers og eins tekur til allrar kröfunnar, sbr. *Lögfræðiorðabók með skýringum*, bls. 319.
[135] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 22.

> However *joint responsibility does not necessarily mean equal responsibility*. Whilst SWIFT bears primary responsibility for the processing of personal data in the SWIFTNet FIN service, financial institutions also bear some responsibility for the processing of their clients' personal data in the service.[136]

Í tilfelli sameiginlegrar ábyrgðar er því sérstaklega mikilvægt að það liggi ljóst fyrir hverju sinni, hvernig ábyrgðinni er skipt á milli þeirra ábyrgðaraðila sem koma að vinnslunni, svo fjöldi ábyrgðaraðila verði ekki til þess að gæði upplýsingaverndarinnar minnki eða að réttindi hins skráða séu ekki tryggð.[137] Réttast væri, þótt þess sé ekki krafist að lögum, að ábyrgðaraðilar gerðu með sér skriflegan samning um hvernig ábyrgðinni sé skipt þeirra á milli, líkt og farið er fram á í 13. gr. pul. um vinnslusamninga á milli ábyrgðaraðila og vinnsluaðila.[138] Með fyrirhuguðum breytingum á evrópskri persónuupplýsingalöggjöf er tekið skref í átt að því að gera samband sameiginlegra ábyrgðaraðila skýrara með því að leggja á þá skyldu til að gera samkomulag um hvernig ábyrgð sé skipt þeirra á milli. Um breytingarnar er fjallað nánar í kafla 7.

4.5 Skyldur ábyrgðaraðila

Persónuupplýsingalögin hafa að geyma ýmsar reglur um skyldur ábyrgðaraðila og réttindi hins skráða, en af skilgreiningu ábyrgðaraðilahugtaksins leiðir að sá einstaklingur eða lögaðili sem gegnir hlutverki ábyrgðaraðila ber ábyrgð á vinnslu persónuupplýsinga gagnvart hinum skráða.[139] Það er hlutverk ábyrgðaraðila að gæta að þeim réttindum sem pul. veitir hinum skráða, en óvissa um hver gegnir hlutverki ábyrgðaraðila haft þau áhrif að ekki sé gætt að þessum réttindum. Verður nú gerð grein fyrir helstu skyldum ábyrgðaraðila.

4.5.1 Söfnun og skráning persónuupplýsinga

Það er á ábyrgð ábyrgðaraðila að unnið sé með upplýsingar í samræmi við reglur pul. og að vinnslan sé lögmæt. Samkvæmt 1. mgr. 8. gr. pul. er vinnsla almennra upplýsinga heimil ef einhver eftirfarandi tölulið er uppfylltur:

1. Hinn skráði hafi ótvírætt samþykkt vinnsluna eða veitt samþykki skv. 7. tölul. 2. gr.
2. vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður;
3. vinnslan sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila;
4. vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða;
5. vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna;
6. vinnslan sé nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili, eða þriðji maður sem upplýsingum er miðlað til, fer með;

[136] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, bls. 13.
[137] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 22.
[138] Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet*, bls. 152-153.
[139] Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer*, bls. 117.

7. vinnslan sé nauðsynleg til að ábyrgðaraðili, eða þriðji maður eða aðilar sem upplýsingum er miðlað til, geti gætt lögmætra hagsmuna nema grundvallarréttindi og frelsi hins skráða sem vernda ber samkvæmt lögum vegi þyngra.

Af ákvæðinu leiðir að vinnsla er óheimil nema eitthvert ofangreindra sjö skilyrða sé uppfyllt. Ábyrgðaraðila er því heimilt að safna og vinna með almennar persónuupplýsingar liggi fyrir ótvírætt samþykki hins skráða, eða ef samþykki liggur ekki fyrir, þegar það er talið nauðsynlegt í þágu ákveðinna hagsmuna sem taldir eru upp í 2. – 7. tölul. 1. mgr. 8. gr. pul. Það ræðst af aðstæðum hverju sinni hvort tiltekin vinnsla persónuupplýsinga sé nauðsynleg í skilningi pul., en ábyrgðaraðila er falið visst mat í þeim efnum. Mat á því hvort nauðsyn sé til staðar ræðst af eðli vinnslunnar, en því umfangsmeiri sem vinnslan er, þeim mun meiri kröfur eru gerðar til nauðsynjarinnar. Ábyrgðaraðili þarf að meta hvern áfanga vinnslunnar sjálfstætt. Þannig þarf að meta sjálfstætt hvort það sé nauðsynlegt að safna upplýsingum, skrá þær og miðla þeim, en tegund vinnslunnar skiptir máli fyrir þær kröfur sem eru gerðar til nauðsynjarinnar. Til dæmis eru gerðar mun meiri kröfur til miðlunnar upplýsinga til þriðja aðila, heldur en til söfnunar, skráningu og annarrar vinnslu persónuupplýsinga. Þótt það teljist nauðsynlegt að skrá tilteknar upplýsingar, er ekki sjálfgefið að ábyrgðaraðili hafi heimild til að miðla persónuupplýsingum til þriðja aðila, en í því tilfelli er um að ræða sitt hvora vinnsluna. Þótt ábyrgðaraðili fari með mat á því hvort tiltekin vinnsla teljist nauðsynleg í skilningi 1. mgr. 8. gr. pul. getur Persónuvernd þó ávallt endurskoðað slíkt mat á grundvelli 36.–38. gr. pul.[140]

Því meira sem vinnslan varðar hagsmuni þess skráða, þeim mun meiri kröfur eru gerðar til vinnslunnar svo hún teljist heimil. Þannig eru gerðar ríkari kröfur til vinnslu viðkvæmra persónuupplýsinga, s.s. upplýsinga um kynlífshegðan eða trúarskoðanir, en við vinnslu slíkra upplýsinga þarf ábyrgðaraðili að sjá til þess að ásamt því að uppfylla ákvæði 1. mgr. 8. gr. sé eitt eða fleiri skilyrði 1. mgr. 9. gr. laganna uppfyllt.[141]

4.5.2 Grunnreglur 7. gr. persónuupplýsingalaga

Þótt vinnsla sé heimil á grundvelli þeirra skilyrða sem 1. mgr. 8. gr. og eftir atvikum 9. gr. pul. kveða á um, þarf vinnslan samt sem áður að fara fram í samræmi við öll skilyrði 7. gr. laganna. Í 7. gr. pul. koma fram grunnreglur sem gilda um alla vinnslu persónuupplýsinga og segja til um hvernig megi eða megi ekki vinna með þær.[142] Öll vinnsla persónuupplýsinga

[140] Þuríður Björk Sigurjónsdóttir: „Ákvæði 1. mgr. 8. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga“, bls. 198-199, Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 17 og Alþt. 1999-00, A-deild, bls. 2724-2725.
[141] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 17 og 20.
[142] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 25.

þarf að uppfylla grunnreglur 7. gr. pul., að því undanteknu að einungis 1. og 4. tölul. 1. mgr. 7. gr. gilda um persónuupplýsingar sem eru einvörðungu unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi sbr. 5. gr. pul. Samkvæmt 7. gr. laganna skal eftirfarandi þátta gætt við meðferð persónuupplýsinga:

1. að þær séu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra sé í samræmi við vandaða vinnsluhætti persónuupplýsinga;
2. að þær séu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi, en frekari vinnsla í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi telst ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt;
3. að þær séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar;
4. að þær séu áreiðanlegar og uppfærðar eftir þörfum, persónuupplýsingar sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal afmá eða leiðrétta;
5. að þær séu varðveittar í því formi að ekki sé unnt að bera kennsl á skráða aðila lengur en þörf krefur miðað við tilgang vinnslu.

Samkvæmt 2. mgr. 7. gr. laganna er ábyrgðaraðili sá sem ber ábyrgð á því að unnið sé með persónuupplýsingar í samræmi við 1. mgr. 7. gr. laganna. Grunnreglum 7. gr. er því beint að ábyrgðaraðila og segja til um hvernig hann eigi að bera sig að við vinnslu persónuupplýsinga.

4.5.3 Fræðsluskylda ábyrgðaraðila gagnvart hinum skráða

Í lögum nr. 77/2000 er mælt fyrir um skyldu ábyrgðaraðila til að tilkynna, að eigin frumkvæði, hinum skráða um að unnið verði með ákveðnar persónuupplýsingar um hann. Fræðsluskylda ábyrgðaraðila fer eftir mismunandi ákvæðum pul. eftir því hvort upplýsinga sé aflað hjá hinum skráða eða hjá öðrum en honum sjálfum.

Í 20. gr. laganna er mælt fyrir um fræðsluskyldu ábyrgðaraðila þegar persónuupplýsinga er aflað hjá hinum skráða, en ákvæðið er byggt á 10. gr. tilskipunar 95/46/EB. Markmið þess er að tryggja að hinn skráði geti tekið upplýsta ákvörðun um hvort hann vilji láta af hendi persónuupplýsingar sem verða notaðar við tiltekna vinnslu, hafi hann um það val. Ákvæði 21. gr. pul. kveður aftur á móti á um fræðsluskyldu ábyrgðaraðila þegar persónuupplýsingum er safnað frá öðrum en hinum skráða og er ákvæðið fyrst og fremst byggt á 11. gr. tilskipunar 95/46/EB. Markmið þess er að auka gegnsæi við vinnsluna og veita hinum skráða betri yfirsýn um vinnslu persónuupplýsinga um hann.[143]

Áður var gert ráð fyrir því að fræðsluskylda samkvæmt 20. gr. pul. gæti eftir atvikum hvílt á vinnsluaðila. Því var breytt með 2. gr. laga nr. 81/2002. Í athugasemdum við 2. gr. í

[143] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 38-39.

frumvarpi því er varð að lögum nr. 81/2002 um breytingu á lögum um persónuvernd og meðferð persónuupplýsinga, kemur fram að það þyki ekki í samræmi við ákvæði tilskipunar 95/46/EB, svo og önnur ákvæði laganna, að vinnsluaðila sé skylt að sinna fræðsluskyldu. Fræðsluskylda gæti því einungis hvílt á vinnsluaðila samkvæmt samningi við ábyrgðaraðila skv. 13. gr. laganna.[144]

Í 1. mgr. 20. gr. pul. eru tilgreindar þær upplýsingar sem ábyrgðaraðila ber að veita hinum skráða þegar upplýsinga er aflað hjá honum. Í fyrsta lagi ber að upplýsa um nafn og heimilisfang ábyrgðaraðila og eftir atvikum fulltrúa hans skv. 6. gr. (1. tölul.). Í öðru lagi skal gefa upp tilgang vinnslunnar (2. tölul.). Í þriðja lagi skal veita aðrar upplýsingar, að því marki sem þær eru nauðsynlegar, með hliðsjón af þeim sérstöku aðstæðum sem ríkja við vinnslu upplýsinganna, svo að hinn skráði geti gætt hagsmuna sinna (3. tölul.). Samkvæmt 10. gr. tilskipunar 95/46/EB skal veita slíkar viðbótarupplýsingar ef þær eru „nauðsynlegar, með hliðsjón af þeim aðstæðum sem ríkja við söfnunina, til að tryggja hinum skráða að vinnslan fari fram á sanngjarnan hátt gagnvart honum.“ Í 3. tölul. 1. mgr. 20. gr. pul. eru talin upp þrjú dæmi um viðbótarupplýsingar sem ábyrgðaraðili gæti þurft að veita hinum skráða. Í fyrsta lagi eru þar nefndar upplýsingar um viðtakendur eða flokka viðtakenda upplýsinganna (a-liður). Í öðru lagi upplýsingar um hvort hinum skráða sé skylt eða valfrjálst að veita umbeðnar upplýsingar (b-liður). Í þriðja lagi upplýsingar um upplýsingarétt hins skráða, svo og rétt hins skráða til leiðréttingar og eyðingar rangra eða villandi persónuupplýsinga um hann (c-liður). Af orðalagi 3. tölul. 1. mgr. 20. gr. pul. má leiða að ekki sé um tæmandi talningu að ræða, heldur einungis dæmi um viðbótarupplýsingar, en ábyrgðaraðili skal meta hvaða upplýsingar sé nauðsynlegt að veita hverju sinni. Þá segir einnig í athugasemdum við 20. gr. í frumvarpi því er varð að lögum nr. 77/2000 að ekki sé alltaf nægilegt að veita fræðslu um þau atriði sem tilgreind eru í 1. mgr.[145] Á fræðsluskyldu á grundvelli 20. gr. pul. reyndi í *úrskurði PV 10. júní 2009, (2009/172)* (Fjölmennt I). Komist var að þeirri niðurstöðu að ábyrgðaraðilar hefðu ekki sinnt fræðsluskyldu samkvæmt 20. gr. pul. við gerð tiltekinnar skýrslu. Um mat á því hvaða upplýsingar væri nauðsynlegt að veita þeim skráða segir í úrskurðinum:

> Við ritun skýrslunnar var m.a. byggt á persónuupplýsingum sem kvartandi veitti um sig sjálfa. Við mat á því hversu miklar kröfur megi gera til fræðslu sem veita átti kvartanda, skv. 20. gr. laga nr. 77/2000, verður að líta til þeirra kringumstæðna sem ríktu þegar þeim upplýsingum, sem liggja skýrslunni til grundvallar, var safnað. Af hálfu kvartanda hefur því verið haldið fram að hún hafi litið svo á að viðtöl hennar við sálfræðingana hafi að miklu leyti verið trúnaðarsamtöl sem m.a. hefðu farið fram til að liðsinna henni. Í skýrslunni er hins vegar m.a. fjallað um þau atriði sem talið var að taka þyrfti til afstöðu um hana, þ. á. m. um framtíð hennar í starfi. Í skýrslunni voru gerðar tillögur sem gátu

[144] Alþt. 2001-02, A-deild, bls. 4528-4529.
[145] Alþt. 1999-00, A-deild, bls. 2733.

> fyrirsjáanlega haft bein áhrif á líf hennar og hagsmuni, en ekki einungis fjallað um málsatvik og greiningu á vandamálum sem upp höfðu komið. Var því eðlilegt að gera ríkar kröfur til fræðslu um þau atriði sem talin eru upp í 3. tölul. 1. mgr. 20. gr. laga nr. 77/2000, þ. á m. um atriði sem voru kvartanda nauðsynleg til að hún gæti gætt hagsmuna sinna í tengslum við vinnsluna og til að vinnslan færi fram á sanngjarnan hátt gagnvart henni.

Markmið fræðsluskyldunnar er að veita hinum skráða möguleika á að nýta sér þann rétt sem persónuupplýsingalögin veita honum, t.d. til aðgangs og leiðréttingar.[146] Þannig á fræðsluskyldan að tryggja að hinn skráði viti hver ábyrgðaraðili vinnslu er svo það sé ljóst hvert hann skuli snúa sér, vilji hann nýta sér þau réttindi sín.

Ef upplýsinga hefur verið aflað hjá öðrum en þeim skráða ber ábyrgðaraðila að veita þeim skráða sömu upplýsingar og ef upplýsinganna hefði verið aflað hjá honum sjálfum. Fræðsluskylda ábyrgðaraðila samkvæmt 21. gr. pul. er aðeins að einu leyti frábrugðin þeirri skyldu sem mælt er fyrir um í 20. gr. laganna, en samkvæmt b-lið 3. tölul. 3. mgr. 21. gr. skal ábyrgðaraðili einnig veita hinum skráða upplýsingar um hvaðan persónuupplýsingarnar koma sem aflað er um hann frá öðrum en honum sjálfum.[147]

Samkvæmt orðalagi 20. gr. pul. skal veita hinum skráða fræðslu um tiltekin atriði *þegar* persónuupplýsingunum er safnað frá honum. Ber ábyrgðaraðila almennt að veita fræðsluna í síðasta lagi á þeim tímapunkti þegar upplýsingunum er safnað. Ef upplýsinga er aflað frá öðrum en þeim skráða er meginreglan sú að gera skuli hinum skráða viðvart um leið og upplýsinga er *aflað* frá viðkomandi, sbr. 21. gr. pul. Almennt skal slík viðvörun eiga sér stað um leið og upplýsingarnar eru skráðar, þ.e. færðar inn í gagnagrunn. Það kann að vera hagkvæmt að skipuleggja starfsemi þannig að viðvörun fari sjálfkrafa af stað við skráningu. Er það heimilt svo lengi sem nægilega víðtæk fræðsla sé veitt.[148]

Samkvæmt 2. mgr. 20. gr. pul. þarf ábyrgðaraðili ekki að veita þeim skráða upplýsingar ef hinn skráði hefur þegar fengið vitneskju um þau atriði sem nefnd eru í 1. mgr. 20. gr. laganna. Í 4. mgr. 21. gr. pul. er ábyrgðaraðili undanþegin fræðsluskyldu í nokkrum tilvikum. Í fyrsta lagi ef það er óframkvæmanlegt að láta hinn skráða vita eða það leggur þyngri byrðar á ábyrgðaraðila en með sanngirni má krefjast (1. tölul.). Í öðru lagi ef ætla má að hinum skráða sé þegar kunnugt um vinnsluna (2. tölul.). Í þriðja lagi ef lagaheimild stendur til skráningar eða miðlunar upplýsinganna (3. tölul.) og í fjórða lagi ef hagsmunir hins skráða af því að fá vitneskju um upplýsingarnar þykja eiga að víkja fyrir veigamiklum almannahagsmunum eða einkahagsmunum, þ.m.t. hagsmunum hans sjálfs (4. tölul.). Auk þessa gildir fræðsluskylda

[146] Alþt. 1999-00, A-deild, bls. 2733.
[147] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 45.
[148] Alþt. 1999-00, A-deild, bls. 2733 og Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 39 og 43.

ábyrgðaraðila samkvæmt 20. og 21. gr. pul. ekki um vinnslu persónuupplýsinga sem varða almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu, sbr. 2. mgr. 3. gr. pul.

4.5.4 Upplýsingaréttur hins skráða og almennur upplýsingaréttur

Ákvæði 16. gr. pul. kveður á um rétt til almennrar vitneskju um vinnslu persónuupplýsinga, en samkvæmt 1. mgr. ákvæðisins er ábyrgðaraðila skylt að veita hverjum sem þess óskar almenna vitneskju um þá vinnslu persónuupplýsinga sem fer fram á hans vegum. Á grundvelli 2. mgr. ákvæðisins getur hver sem er fengið upplýsingar um tiltekna tegund eða tegundir vinnslu persónuupplýsinga, en sá sem vill nýta sér þann rétt þarf að tilgreina nákvæmlega hvaða vinnslu hann vill fá vitneskju um. Þannig getur hver sem er, á grundvelli 2. mgr. 16. gr. laganna, fengið upplýsingar um nafn ábyrgðaraðila, tilgang vinnslu, lýsingu á þeim tegundum persónuupplýsinga sem unnið er með, hvaðan upplýsingarnar koma og hverjir viðtakendur upplýsinganna eru.[149]

Í athugasemdum við 16. gr. frumvarps þess er varð að lögum nr. 77/2000 segir að markmiðið með hinum almenna upplýsingarétti sé tvíþættur. Annars vegar er ákvæðinu ætlað að veita hverjum sem er færi á að ganga úr skugga um hvort honum þyki vinnslan áhugaverð og ástæða til að fá um hana gleggri upplýsingar samkvæmt 2. mgr. 16. gr. pul. Hins vegar er markmið ákvæðisins að skapa manni forsendur til að meta hvort hann kæri sig um að umræddur ábyrgðaraðili vinni með upplýsingar um sig eða ekki. Til dæmis getur einstaklingur, á grundvelli 16. gr. pul., beðið um almennt yfirlit um þá vinnslu persónuupplýsinga sem fer fram á vegum vildarklúbbs áður en hann gengur í klúbbinn.[150]

18. gr. pul. mælir fyrir um upplýsingarétt hins skráða. Samkvæmt 1. mgr. ákvæðisins á hinn skráði rétt á því að fá nánar tilgreindar upplýsingar um það hvernig er unnið með persónuupplýsingar um hann sjálfan. Markmiðið með upplýsingarétti hins skráða er að tryggja að ákveðið gegnsæi ríki um vinnslu persónuupplýsinga. Auk þess gefur upplýsingarétturinn hinum skráða tækifæri til að fylgjast með því að unnið sé með persónuupplýsingar um hann á löglegan hátt.[151] Þær upplýsingar sem ábyrgðaraðila er skylt að veita þeim skráða eru taldar upp í fimm töluliðum í 1. mgr. ákvæðisins. Í ákvæði 1. tölul. 1. mgr. 18. gr. felst sú meginregla að hinn skráði hefur rétt til aðgangs að upplýsingum um sjálfan sig.[152] Reglan hefur verið skýrð á þann hátt að hinn skráði eigi ekki einungis rétt á að

[149] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 49.
[150] Alþt. 1999-00, A-deild, bls. 2730.
[151] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 49.
[152] Alþt. 1999-00, A-deild, bls. 2731.

fá vitneskju um hvaða upplýsingar um hann ábyrgðaraðili hefur unnið með, heldur eigi hann einnig rétt á að kynna sér efni þeirra.[153] Ákvæði 2. tölul. 1. mgr. 18. gr. veitir hinum skráða rétt á að fá vitneskju um tilgang vinnslu upplýsinga sem varða hann sjálfan og kveður 3. tölul. á um rétt hins skráða til að fá vitneskju um viðtakendur upplýsinga um hann. Regla 3. tölul. gildir þegar upplýsingunum er miðlað til utanaðkomandi aðila, en hefur verið túlkuð svo að hún eigi ekki við þau tilvik þegar upplýsingar berast eingöngu á milli ábyrgðaraðila og starfsmanna hans. Á það reyndi í *úrskurði PV 28. febrúar 2005 (144/2004)* (Íslandsbanki) þar sem Persónuvernd hafnaði kröfu manns um að fá lista yfir nöfn starfsmanna Íslandsbanka sem skoðað hefðu fjárhagsupplýsingar um hann, hvenær það hefði verið gert og í hvaða útibúi bankans, en ekki var ráðið hvort persónuupplýsingum um fjárhagsstöðu kvartanda hefði verið miðlað frá bankanum til utanaðkomandi aðila. Eins og gerð er grein fyrir í kafla 5.3.1 liggur það í eðli vinnsluaðilahugtaksins að vinnsluaðili er ávallt utanaðkomandi. Þannig leiðir af 3. tölul. 1. mgr. 18. gr. að ábyrgðaraðila er skylt að upplýsa hinn skráða um vinnsluaðila upplýsinganna. Samkvæmt 4. tölul. 1. mgr. 18. gr. skal ábyrgðaraðili veita hinum skráða upplýsingar um hvaðan persónuupplýsingarnar um hann koma. Ábyrgðaraðili þarf aðeins að veita þessar upplýsingar ef hann býr yfir þeim, en ekki hefur verið talið að sú skylda hvíli á honum að útvega slíkar upplýsingar ef hann hefur þær ekki tiltækar. Ákvæði 5. tölul. 1. mgr. 18. gr. laganna veitir jafnframt þeim skráða rétt á að fá vitneskju um hvaða öryggisráðstafanir eru notaðar við vinnsluna, en sá fyrirvari er gerður að það skerði ekki öryggi vinnslunnar.

Hinn skráði þarf sjálfur að hafa frumkvæði að því að nýta sér upplýsingarétt sinn og leggja fram beiðni þess efnis við ábyrgðaraðila vinnslu. Vegna þess er mikilvægt að ábyrgðaraðili sinni fræðsluskyldu sinni samkvæmt c-lið 3. tölul. 1. mgr. 20. gr. og d-lið 3. tölul. 3. mgr. 21. gr. og vekji athygli hins skráða á upplýsingarétti hans undir 18. gr. laganna. Upplýsingaréttur hins skráða er ekki skilyrðislaus, en í 19. gr. pul. er að finna ýmsar takmarkanir á upplýsingarétti hins skráða, sem óþarft er að kafa dýpra í hér.

4.5.5 Leiðrétting og eyðing persónuupplýsinga

Samkvæmt 25. gr. pul. ber ábyrgðaraðila skylda til að leiðrétta, eyða, bæta við eða stöðva notkun á röngum, villandi eða ófullkomnum persónuupplýsingum eða persónuupplýsingum sem skráðar hafa verið án heimildar. Ákvæðið er byggt á d-lið 1. mgr. 6. gr. og b- og c-lið 12. gr. tilskipunar 95/46/EB. Ábyrgðaraðila er skylt að sinna þessari skyldu sinni að eigin

[153] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 51.

frumkvæði, en í framkvæmd gæti þó þurft ábendingu frá hinum skráða um að upplýsingarnar séu ekki áreiðanlegar.[154]

Í 26. gr. pul. er mælt fyrir um eyðingu og bann við notkun persónuupplýsinga þegar ekki er lengur málefnaleg ástæða til að varðveita upplýsingarnar, þótt þær séu hvorki rangar né villandi. Í athugasemdum með 26. gr. frumvarps þess er varð að lögum nr. 77/2000 segir að ákvæðið taki mið af sambærilegu ákvæði eldri laga, þar sem fram kemur að afmá skuli upplýsingar sem vegna aldurs, eða af öðrum ástæðum, hafa glatað gildi sínu. Með öðrum orðum ætti að afmá upplýsingar sem væru orðnar úreltar. Samkvæmt 2. mgr. 26. gr. getur skráður aðili krafist þess að upplýsingum um hann samkvæmt 1. mgr. sé eytt eða notkun þeirra bönnuð, ef slíkt telst réttlætanlegt út frá heildstæðu hagsmunamati. Fer því oft fram umfangsmikið hagsmunamat á grundvelli 26. gr. pul. Sem dæmi gætu persónuverndar–sjónarmið mælt með eyðingu persónuupplýsinga en önnur og veigamikil samfélagssjónarmið geta mælt gegn eyðingu.[155]Á þetta reyndi í nýlegum dómi Evrópudómstólsins, *EBD, mál C-131/12* (Google)[156], sem kveðinn var upp 13. maí 2014. Í því máli staðfesti dómstóllinn rétt manna til að gleymast (e. *the right to be forgotten*) á grundvelli b-liðar 12. gr. og a-liðar 1. mgr. 14. gr. tilskipunar 95/46/EB. Samkvæmt athugasemdum með 26. gr. ber að túlka ákvæðið í ljósi 1. mgr. 14. gr. tilskipunar 95/46/EB.[157] Í ofangreindu máli Evrópudómstólsins hafði Hæstiréttur Spánar leitað álits dómstólsins vegna máls þar sem einstaklingur fór fram á að Google fjarlægði upplýsingar úr leitarniðurstöðum sínum sem tengdust fjárnámi sem gert var í eignum hans árið 1998. Auglýsing um uppboð á fasteign kæranda var birt í dagblaði árið 1998 og ef leitað var að nafni hans á leitarvél Google var hlekkur á auglýsinguna meðal efstu leitarniðurstöðum sem birtust. Í dóminum segir að það hvort upplýsingum skuli eytt fari eftir mati á hagsmunum hverju sinni. Annars vegar af hagsmunum almennings að leitarniðurstaðan sé aðgengileg og hins vegar hagsmunum viðkomandi einstaklings af að svo sé ekki. Í dóminum segir orðrétt:

---

[154] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*, bls. 54. Á samfélagsmiðlum er t.d. algengt að notast sé við einhversskonar tilkynningakerfi sem gerir notendum kleift að benda á að mynd eða aðrar upplýsingar um viðkomandi séu rangar, villandi eða ófullkomnar. Um það er fjallað nánar í kafla 6 um samfélagsmiðla.

[155] Alþt. 1999-00, A-deild, bls. 2736.

[156] Á þeim tíma sem þetta er skrifað hefur dómurinn enn ekki verið birtur í European Court Reports.

[157] Alþt. 1999-00, A-deild, bls. 2736. Samkvæmt b-lið 12. gr. tilskipunarinnar skulu aðildarríkin tryggja öllum skráðum aðilum rétt til að krefjast af ábyrgðaraðila eftir því sem við á, leiðréttingar, afmáunar eða aðgangstakmarkana á upplýsingum ef vinnsla þeirra uppfyllir ekki ákvæði tilskipunarinnar, einkum ef þær eru ófullkomnar eða óáreiðanlegar. A-liður 1. mgr. 14. gr. tilskipunar kveður á um rétt þess skráða til að andmæla upplýsingum um sjálfan sig ef hann hefur til þess lögmætar og knýjandi ástæður vegna sérstakra aðstæðna sinna, nema kveðið sé á um annað í innlendum lögum. Ef andmælin eiga rétt á sér er ekki lengur heimilt að nota þessar upplýsingar í vinnslu þeirri sem ábyrgðaraðili stofnaði til.

> […] inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a *fair balance should be sought* in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter.[158] Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.[159]

Varð niðurstaðan sú að hagsmunir einstaklingsins vógu þyngra í þessu tilfelli og féllst Evrópudómstóllinn því á kröfu hans um að niðurstöðu á leitarsíðu Google skyldi eytt á grundvelli ofangreindra ákvæða tilskipunar 95/46/EB. Var Google talið ábyrgðaraðili þeirra persónuupplýsinga sem unnar voru í leitarvélinni og bar fyrirtækinu að sjá til þess að skilyrði tilskipunar 95/46/EB væru uppfyllt. Sjálfu efninu á heimasíðu dagblaðsins skyldi aftur á móti ekki eytt, þar sem birting auglýsingar um uppboð fasteignar væri lögmæt.[160] Í fyrirhuguðum breytingum á persónuupplýsingalöggjöf ESB er kveðið á um réttinn til að gleymast sem sjálfstæðan rétt þess skráða, en um hann er fjallað nánar í kafla 7.

4.5.6 Áhættumat, öryggi og gæði persónuupplýsinga

Samkvæmt 3. mgr. 11. gr. pul. ber ábyrgðaraðili ábyrgð á því að áhættumat og öryggisráðstafanir við vinnslu persónuupplýsinga séu í samræmi við lög, reglur og fyrirmæli Persónuverndar um hvernig tryggja skuli öryggi upplýsinga. Á grundvelli öryggisstefnu og áhættumats skal ábyrgðaraðili gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysni og gegn óleyfilegum aðgangi, sbr. 1. mgr. 11. gr. laganna. Ákvæði 11. gr. hvílir á þeim viðhorfum að rafræn vinnsla persónuupplýsinga, sérstaklega þegar hún fer fram á Internetinu, auki verulega hættuna á því að óviðkomandi aðilar fái aðgang að upplýsingunum, en sífellt algengara er að tölvuþrjótar brjótist inn í tölvukerfi fyrirtækja og stofnana.[161] Í þessu samhengi má vísa til úrskurða Persónuverndar vegna innbrots í tölvukerfi Vodafone, sem rekið er af Fjarskiptum hf.[162] Innbrotið leiddi til þess að persónuupplýsingar um þúsundir viðskiptavina félagsins, sem þar höfðu verið varðveittar, komust í hendur óviðkomandi aðila og voru síðar birtar á Netinu. Þar sem sú þjónusta sem veitt var á vefkerfi

[158] Er hér átt við sáttmála Evrópusambandsins um grundvallarréttindi.
[159] Dómur Evrópudómstólsins 13. maí 2014 í máli *C-131/12,* málsl. 81.
[160] Sjá t.d. *Myth-Busting – The Court of Justice of the EU and the "Right to be Forgotten"* fyrir nánari umfjöllun um dóm Evrópudómstólsins.
[161] Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála,* bls. 61.
[162] Sjá t.d. *úrskurð PV 13. maí 2014, (2014/378)* og *úrskurð PV 13. maí 2014, (2014/377).*

Vodafone fellur undir gildissvið laga um fjarskipti nr. 81/2003 voru valdmörk Póst- og fjarskiptastofnunar og Persónuverndar í tengslum við öryggisatvikið ákveðin þannig að Póst- og fjarskiptastofnun fjallaði um öryggi umræddra gagna, en Persónuvernd fjallaði um lögmæti varðveislu Fjarskipta hf. á þeim persónuupplýsingum sem þau hafa að geyma. Þar af leiðandi hefur ekki verið leyst úr ofangreindu öryggisatviki á grundvelli 11. gr. pul.[163]

Þegar ábyrgðaraðili semur við vinnsluaðila um að annast vinnslu persónuupplýsinga sem hann ber ábyrgð á ber honum skylda til að sannreyna að vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir, sbr. 1. mgr. 13. gr. pul. Auk þess skal ábyrgðaraðili viðhafa innra eftirlit hjá vinnsluaðila til að ganga úr skugga um að sá síðarnefndi vinni persónuupplýsingar í samræmi við gildandi lög og reglur, sbr. 1. mgr. 12. gr. pul.

Í reglum nr. 299/2001 um öryggi persónuupplýsinga er fjallað nánar um hvernig ábyrgðaraðila ber að móta öryggisstefnu, framkvæma áhættumat og velja viðeigandi öryggisráðstafanir.

4.5.7 Tilkynningar- og leyfisskylda

Á grundvelli 31. gr. pul. ber ábyrgðaraðila, sem beitir rafrænni tækni við vinnslu persónuupplýsinga, að tilkynna Persónuvernd um vinnsluna tímanlega áður en hún hefst. Í athugasemdum með 31. gr. í frumvarpi því er varð að lögum nr. 77/2000 segir að tilkynningarskylda skuli að meginstefnu til gilda um alla rafræna vinnslu almennra persónuupplýsinga og um handvirka og rafræna vinnslu viðkvæmra persónuupplýsinga. Í 32. gr. pul. er afmarkað hvað skuli koma fram í slíkri tilkynningu. Hefja má vinnslu um leið og tilkynning hefur verið send, þar sem tilkynningin er til upplýsinga fyrir Persónuvernd en er ekki í eðli sínu leyfisumsókn. Persónuvernd getur þó stöðvað vinnslu sem hún telur ólögmæta eða sett skilmála fyrir því að halda megi vinnslu áfram, sbr. 40. gr. pul.[164] Verði fyrirhugaðar breytingar á evrópskri persónuupplýsingalöggjöf samþykktar að öllu óbreyttu, mun tilkynningarskylda ábyrgðaraðila vera afnumin en í staðinn yrði ábyrgðaraðilum skylt að tilkynna viðeigandi persónuverndarstofnun um öryggisbrest við vinnslu persónuupplýsinga.[165]

Í 33. gr. pul er afmarkað hvenær vinnsla persónuupplýsinga er leyfisskyld. Sé um er að ræða vinnslu sem getur falið í sér sérstaka hættu á að farið verði í bága við réttindi skráðra aðila getur Persónuvernd ákveðið að vinnslan megi ekki hefjast fyrr en hún hefur verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar. Sé vinnsla leyfisskyld

[163] *Ákvörðun Póst- og fjarskiptastofnunar 24. mars 2014 (1/2014).* Sjá einnig *úrskurð PV 13. maí 2014 (2014/378)* og *úrskurð PV 13. maí 2014 (2014/377).*
[164] Alþt. 1999-00, A-deild, bls. 2741-2742.
[165] Um frekari umfjöllun um fyrirhugaðar breytingar á evrópskri persónuupplýsingalöggjöf vísast til kafla 7.

má ekki hefja hana nema Persónuvernd hafi veitt til þess leyfi, en þegar vinnsla er eingöngu tilkynningarskyld kemur að öllu jöfnu ekki til afskipta Persónuverndar fyrr en eftir á.[166]

Í reglum 712/2008 um tilkynningarskylda og leyfisskylda vinnslu persónupplýsinga er að finna ítarlegar reglur um tilkynningar- og leyfisskyldu og vísast til þeirra fyrir frekari umfjöllun um efnið.

4.5.8 Bótaskylda

Samkvæmt 43. gr. pul., er ábyrgðaraðili bótaskyldur vegna tjóns sem verður, þegar unnið hefur verið með persónuupplýsingar í andstöðu við ákvæði laganna. Samkvæmt ákvæðinu skal ábyrgaraðili bæta hinum skráða *fjárhagslegt tjón* sem hin ólögmæta vinnsla hefur valdið honum, en hér er ekki um að ræða ábyrgð á öðru tjóni en fjárhagslegu. Ábyrgðaraðili ber ekki einungis ábyrgð á því tjóni sem hann veldur sjálfur, heldur líka á því tjóni sem vinnsluaðili hefur valdið. Í athugasemdum með 43. gr. í frumvarpi því er varð að lögum nr. 77/2000 segir að þar sem við því er að búast að ábyrgðaraðilar muni í auknum mæli láta vinnsluaðila vinna persónuupplýsingar fyrir sig í framtíðinni, væri nauðsynlegt að taka af öll tvímæli um ábyrgð ábyrgðaraðila á því tjóni sem vinnsluaðili veldur. Jafnframt þætti óeðlilegt að ábyrgðaraðili gæti losnað undan skaðabótaábyrgð með því að fela öðrum aðila vinnslu upplýsinga fyrir sig.[167] Það fellur aftur á móti ekki í hlut Persónuverndar að meta hvort bótaábyrgð skv. 43. gr. laganna skuli beitt, heldur er það verkefni dómstóla.[168]

4.6 Samantekt

Vinnsla persónuupplýsinga getur ekki átt sér stað án þess að ábyrgðaraðili komi að vinnslunni, þar sem hann ákveður tilgang vinnslunnar og að hún skuli eiga sér stað. Það er því ávallt að finna ábyrgðaraðila að vinnslu, þó það geti reynst flókið að meta hver gegni því hlutverki og geta þeir jafnvel verið fleiri en einn.

Í kafla þessum hefur verið fjallað um ábyrgðaraðilahugtakið eins og það birtist í pul. og það greint í þrjá mismunandi þætti í samræmi við álit 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“. Í fyrsta lagi var persónulegi þáttur hugtaksins tekinn fyrir, sem snýr að því hver getur talist ábyrgðaraðili. Í honum felst að ábyrgðaraðili verður að hafa aðildarhæfi og geta svarað til saka fyrir tiltekna vinnslu persónuupplýsinga fyrir dómstólum, ef svo ber undir. Í öðru lagi var gerð grein fyrir þeim þætti er snýr að ákvörðunarvaldi um vinnslu persónuupplýsinga, en sá sem fer með ákvörðunarvald um vinnsluna telst almennt

[166] Alþt. 1999-00, A-deild, bls. 2743.
[167] Alþt. 1999-00, A-deild, bls. 2748.
[168] *Ákvörðun PV 17. apríl 2013 (2013/426).*

ábyrgðaraðili hennar. Lögð var áhersla á mikilvægi þess að líta til raunverulegra aðstæðna hverju sinni, þó lög- og samningsbundið ákvörðunarvald veiti í flestum tilfellum áreiðanlegar upplýsingar um hlutverkaskipti að vinnslu. Í þriðja lagi var litið til andlags ákvörðunarvaldsins, þ.e. hvað aðili þarf að hafa ákvörðunarvald um svo hann teljist ábyrgðaraðili. Dregin var sú ályktun að einungis ábyrgðaraðili getur tekið ákvarðanir um tilgang og önnur grundvallaratriði vinnslu. Samkvæmt 29. gr. starfshópnum geta vinnsluaðilar undir vissum kringumstæðum tekið ákvarðanir er snúa að tækni- og skipulagsatriðum vinnslunar. Er þó ekki ljóst hvort það sama eigi við í íslenskum rétti.

Mat á því hver hefur raunverulegt ákvörðunarvald um vinnslu persónuupplýsinga getur leitt í ljós að fleiri en einn aðili hafi slíkt ákvörðunarvald, er þá um að ræða sameiginlega ábyrgð. Slík ábyrgð leiðir ekki sjálfkrafa til óskiptrar ábyrgðar, þar sem ábyrgð hvers og eins ábyrgðaraðila getur verið mismikil og á mismunandi þáttum vinnslunnar.

Persónuupplýsingalögin veita þeim skráða ýmis réttindi, en það er á ábyrgð ábyrgðaraðila að þeirra sé gætt. Ríki óvissa á milli þeirra aðila sem koma að vinnslunni um hver þeirra gegnir hlutverki ábyrgðaraðila getur það orðið til þess að ekki sé gætt að réttindum þess skráða og vinnslan þ.a.l. í ósamræmi við ákvæði pul., sbr. *úrskurð PV 10. júní 2009 (2009/172)* (Fjölmennt I).

5 Vinnsluaðili

5.1 Inngangur

Líkt og frumvarp það er varð að lögum nr. 77/2000 gerði ráð fyrir, hafa ábyrgðaraðilar í auknum mæli fengið vinnsluaðila til að vinna persónuupplýsingar fyrir sína hönd.[169] Þá hefur mikið vatn runnið til sjávar frá gildistöku persónuupplýsingalaganna á árinu 2001 og gríðarleg þróun átt sér stað á sviði upplýsingavinnslu. Persónuupplýsingar eru orðnar að verslunarvöru og fyrirtæki sérhæfa sig orðið í vinnslu þeirra.[170] Dæmi um vinnsluaðila eru fyrirtæki sem hýsa heimasíður, Internet þjónustuaðilar (e. *Internet Service Providers*), fyrirtæki sem annast gagnasafn þriðja aðila og svo mætti lengi telja.

Í kafla þessum verður gerð grein fyrir vinnsluaðilahugtaki pul. og uppruna þess í tilskipun 95/46/EB. Hugtakið verður afmarkað í tvo þætti og gerð verður grein fyrir trúnaðarskyldu vinnsluaðila samkvæmt 13. gr. pul. Þá verður einnig fjallað um þau tilvik þegar vinnsluaðili semur við undirverktaka um að annast vinnslu og hvaða áhrif það hefur þegar vinnsluaðili og/eða undirverktaki hefur staðfestu utan EES-svæðisins.

[169] Alþt. 1999-00, A-deild, bls. 2748.
[170] Peter Blume: „Data Protection in the Private Sector“, bls. 306–307.

5.2 Skilgreiningar

Í e-lið 2. gr. tilskipunar 95/46/EB er hugtakið vinnsluaðili (e. *processor*) skilgreint sem einstaklingur eða lögpersóna, opinbert yfirvald, stofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila. Hugtakið er ekki að finna í Evrópuráðssamningnum og var því fyrst kynnt til sögunnar með tilskipun 95/46/EB.[171]

Samkvæmt 5. tölul. 2. gr. pul. er vinnsluaðili sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila. Hugtakið er byggt á e-lið 2. gr. tilskipunar 95/46/EB. Í eldri lögum var ekki að finna hugtak sambærilegt vinnsluaðilahugtakinu, en í athugasemdum með 5. tölul. 2. gr. í frumvarpi því er varð að lögum nr. 77/2000 segir að vinnsluaðili eigi sér nokkra samsvörun við aðila sem hefur starfsleyfi til að annast tölvuþjónustu í skilningi 25. gr. laga nr. 121/1989 um skráningu og meðferð persónuupplýsinga, undanfara pul. Ákvæði 13. gr. persónuupplýsingalaganna kveður á um samband ábyrgðaraðila og vinnsluaðila, en í 1. mgr. 13. gr. segir að ábyrgðaraðila sé heimilt að semja við tiltekinn aðila um að annast, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á. Tilvist vinnsluaðila ræðst þar af leiðandi af því hvort ábyrgðaraðili ákveði að nýta sér þá heimild eða ekki.[172]

Í dönskum lögum um meðferð persónuupplýsinga er notast við hugtakið „databehandler“ og er það skilgreint í 4. tölul. 3. gr. laganna sem „den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne“. Hugtakið er, líkt og hið íslenska vinnsluaðilahugtak, byggt á tilskipun 95/46/EB og er raunar bein þýðing á þeirri skilgreiningu hugtaksins sem þar má finna. Kjarninn í hinu danska hugtaki er sá að vinnsluaðili vinni upplýsingar af hálfu ábyrgðaraðila, en noti ekki upplýsingarnar i eigin tilgangi. [173] Í norskum lögum um meðferð persónuupplýsinga er einnig notast við hugtakið „databehandler“. Skilgreining þess svipar meira til þeirrar íslensku en til þeirrar dönsku, en í 5. tölul. 2. gr. laganna segir að vinnsluaðili sé „den som behandler personopplysninger på vegne av den behandlingsansvarlige“. Í sænskum lögum um meðferð persónuupplýsinga er notast við hugtakið „personuppgiftsbiträde“ og er það sambærilegt íslensku og norsku skilgreiningu vinnsluaðilahugtaksins, en í 3. gr. laganna segir að vinnsluaðili sé „den som behandlar personuppgifter för den personuppgiftsansvariges räkning“.

[171] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 24.
[172] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25.
[173] Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer*, bls. 119.

5.3 Afmörkun hugtaksins

Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ segir að tvenn grundvallarskilyrði skuli uppfyllt svo aðili sem komi að vinnslu persónuupplýsinga teljist vinnsluaðili hennar. Annars vegar þarf vinnsluaðili að vera sjálfstæður aðili, einstaklingur eða lögaðili (e. *separate legal entity with respect to the controller*), og hins vegar þarf vinnslan að fara fram fyrir hönd ábyrgðaraðila.[174] Krafan um að þessi skilyrði séu uppfyllt er að nokkru leyti í samræmi við lögskýringargögn að baki 5. tölul. 2. gr. pul. Í athugasemdum með ákvæðinu í frumvarpi því er varð að lögum nr. 77/2000 segir að skilyrði þess að aðili teljist vinnsluaðili tiltekinnar vinnslu sé að vinnslan fari fram fyrir hönd ábyrgðaraðila og að hún byggist á ósk hans. Frumvarpið nefnir þannig einungis annað þeirra skilyrða sem 29. gr. starfshópurinn gerir ráð fyrir. Hér verður þó gerð grein fyrir þeim skilyrðum sem 29. gr. starfshópurinn nefnir í áliti sínu og reynt að svara þeirri spurningu hvort skilyrðið um að vinnsluaðili sé sjálfstæður aðili gildi einnig að íslenskum rétti.

5.3.1 Sjálfstæður aðili

Vinnsluaðilahugtakið gerir ráð fyrir því að ýmsir mismunandi aðilar geti gegnt hlutverki vinnsluaðila. Meðal þeirra sem geta sinnt hlutverkinu eru lögaðilar, einstaklingar, opinber yfirvöld og aðrar stofnanir. Það er algengast að vinnsluaðili sé einkarekið fyrirtæki, þótt aðrar lögpersónur og einstaklingar komi vissulega til greina.[175] Dæmi um aðila sem Persónuvernd hefur talið vinnsluaðila vegna aðkomu þeirra að vinnslu persónuupplýsinga eru fjölbreytt en má t.d. nefna kerfisfræðing starfandi undir verktakasamningi við einkahlutafélag[176], fyrirtæki sem framkvæma lyfjapróf á starfsmönnum annarra fyrirtækja samkvæmt þjónustusamningi[177] og fyrirtæki sem framkvæmir kannanir fyrir ráðuneyti.[178]

Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ segir að aðili þurfi að vera sjálfstæður gagnvart ábyrgðaraðila svo hann geti talist vinnsluaðili í skilningi tilskipunar 95/46/EB, en í því felst fyrst og fremst skilyrði um að upplýsingarnar séu unnar af utanaðkomandi aðila (e. *external organization*). Ef ábyrgðaraðili ákveður að persónuupplýsingar skulu unnar innanhúss, t.d. af hans eigin starfsfólki, er ekki um að ræða utanaðkomandi aðila og starfsfólkið sem annast vinnsluna telst þar af leiðandi ekki til

[174] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor",* bls. 25.
[175] Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer*, bls. 120.
[176] *Úrskurður PV 18. janúar 2011, (2010/907)* (Hraðpeningar ehf.), hluverk kerfisfræðingsins var að útbúa forritunarkóða fyrir sms-kerfi í tengslum við smálánaþjónustu fyrirtækisins.
[177] *Svar PV 8. apríl 2008 við fyrirspurn um eiturlyfjaskimun innan fyrirtækja.*
[178] *Ákvörðun PV 3. mars 2011, (2011/62)* (Miðlun ehf).

vinnsluaðila. Ef ábyrgðaraðili felur utanaðkomandi aðila, einstaklingi eða lögaðila, að annast vinnslu persónuupplýsinga getur sá aðili talist vinnsluaðili.[179]

Í *bréfi PV 22. maí 2006* (Þjófnaður í verslunum) svaraði Persónuvernd erindi frá öryggisdeild A hf. um rafræna vinnslu persónuupplýsinga við þjófnaðartilvik í verslunum A hf., en fyrirtækið hugðist halda rafræna skrá um slík tilvik. Í erindinu segir að A hf. sé verslunarfyrirtæki sem á og starfrækir fjölda verslana og eigi einnig dótturfélög sem reka aðrar verslanir. Þegar einstaklingur verður uppvís að þjófnaði í einhverri verslana A hf. (þ.á.m. dótturfélaga þess) eru upplýsingar um viðkomandi skráðar á þar til gert eyðublað og það síðar afhent öryggisdeild A hf. Í svari Persónuverndar við fyrirspurn A hf. segir að slík skráning geti talist nauðsynlegur og eðlilegur þáttur í starfsemi fyrirtækisins, en yrði þó að uppfylla ýmis skilyrði laga um persónuvernd. Litið var svo á að A hf. væri vinnsluaðili fyrir tiltekin dótturfélög sín og væri því skylt að gera við þau vinnslusamninga. Í svari Persónuverndar segir orðrétt:

> Af hálfu A hefur því verið lýst yfir að félagið hafi sjálft með höndum vinnslu persónuupplýsinga sem tengjast þjófnaðartilvikum í eigin verslunum en það sé vinnsluaðili fyrir *tiltekin* dótturfélög þess. Er því skilyrði að A geri vinnslusamninga við þá aðila sem það annast umrædda vinnslu fyrir, þ.e. þeirra fyrirtækja sem eru *sjálfstæðar lögpersónur* og hafa stöðu ábyrgðaraðila í skilningi 4. tl. 2. gr. laga nr. 77/2000.

Líta má svo á að A hf. hafi verið utanaðkomandi aðili gagnvart þeim dótturfélögum sínum sem talin voru sjálfstæðar lögpersónur og því nauðsynlegt að gerður væri vinnslusamningur þeirra á milli. Hér skal þó tekið fram að ekki er um að ræða úrskurð Persónuverndar, heldur einfaldlega svar við fyrirspurn A hf.

Ofangreint svar Persónuverndar gefur einnig tilefni til að víkja stuttlega að þeim aðstæðum þegar persónuupplýsingar eru unnar innan sömu fyrirtækjasamstæðu. Í fyrirtækjarekstri á sér stað gríðarleg vinnsla persónuupplýsinga, bæði um starfsfólk og viðskiptavini og hafa slíkar upplýsingar ákveðið fjárhagslegt gildi fyrir fyrirtæki, t.d. vegna markaðssetningar sem beint er að viðskiptavini á grundvelli þeirra upplýsinga sem fyrirtækið hefur um viðkomandi.[180] Má einnig nefna kortafyrirtæki og fjármálafyrirtæki, sem eðli málsins samkvæmt vinna mikið með persónuupplýsingar. Þegar fyrirtæki eru hluti af samstæðu er algengt að tilteknar upplýsingar gangi á milli aðila innan samstæðunnar. Til dæmis getur samstæða notast við einn sameiginlegan gagnagrunn fyrir upplýsingar um starfsfólk sitt, til að auðvelda samskipti á milli aðila. Í íslenskum félagarétti er gert ráð fyrir því að hvert félag sé sjálfstæður lögaðili en samstæðan sjálf telst ekki sjálfstæður aðili að

[179] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25 og Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet*, bls. 155-157.
[180] Peter Blume: „Data protection in the Private Sector", bls. 307 og 310.

lögum.[181] Af því leiðir að vinnsla persónuupplýsinga innan samstæðu sem felur í sér einhverskonar samnýtingu á upplýsingum telst ekki til notkunar innan félags (e. *internal usage*) heldur til flutnings (e. *transfer*) upplýsinga á milli aðila. Leiðir myndun fyrirtækjasamstæðu því ekki til auðveldari samnýtingu á persónuupplýsingum, heldur skal vinnsla persónuupplýsinga innan samstæðu uppfylla sömu skilyrði og færi hún fram utan hennar.[182] Við afmörkun á hlutverkum þeirra fyrirtækja sem koma að vinnslu upplýsinga innan samstæðu ber rekstrarform þeirra og eignarhald ekki að hafa áhrif á niðurstöðu á því mati sem fer fram. Er ofangreint svar Persónuverndar til marks um það, þar sem móðurfélag var talið vinnsluaðili fyrir hönd tiltekinna dótturfélaga sinna.[183]

Hvorki persónuupplýsingalögin sjálf né frumvarp það sem varð að lögum nr. 77/2000 kveða á um ofangreint skilyrði um að vinnsluaðili skuli vera sjálfstæður aðili gagnvart ábyrgðaraðila. Það liggur þó í hlutarins eðli að ábyrgðaraðili og vinnsluaðili geta ekki verið einn og sami aðilinn, þar sem tilvist vinnsluaðila ræðst af ákvörðun ábyrgðaraðila um að fá annan aðila en hann sjálfan til að vinna persónuupplýsingar fyrir sína hönd.[184]

5.3.2 Á vegum ábyrgðaraðila

Annað grundvallarskilyrða þess að aðili teljist vinnsluaðili er að vinnsla hans fari fram *fyrir hönd ábyrgðaraðila*. Leiðir þetta bæði af áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ og af athugasemdum með 5. tölul. 2. gr. í frumvarpi því er varð að lögum nr. 77/2000, en þar er jafnframt tekið fram að vinnslan skuli *byggð á ósk ábyrgðaraðila*.[185]

Í skilyrðinu felst að vinnsluaðili þjóni hagsmunum ábyrgðaraðila með þeirri vinnslu sem hann tekur sér fyrir hendur, en ekki sínum eigin. Það er því forsenda þess að vinnsluaðili haldi hlutverki sínu sem slíkur, að hann vinni ekki upplýsingarnar á frekari hátt en krafist er af honum af hálfu ábyrgðaraðila og ekki í eigin þágu, þ.e. að hann framkvæmi fyrirmæli ábyrgðaraðila.[186]

---

[181] Stefán Már Stefánsson: *Samstæður hlutafélaga*, bls. 15 og 20 og Peter Blume: „Data protection in the Private Sector“, bls. 267.
[182] Christopher Kuner: *European Data Protection Law*, bls. 79 og 107–108 og Peter Blume: „Data protection in the Private Sector“, bls. 310-311.
[183] Christopher Kuner: *European Data Protection Law*, bls. 107–108.
[184] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25. Á vefsíðu sænsku Datainspektionen segir að vinnsluaðili sé *ávallt* aðili utan starfsemi ábyrgðaraðila, sjá „Vem är personuppgiftsbiträde och vilket ansvar har ett biträde?“, http://www.datainspektionen.se.
[185] Alþt. 1999-00, A-deild, bls. 2715 og *Article 29 Working Group Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25.
[186] Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer*, bls. 119-120.

Þótt aðili gegni hlutverki vinnsluaðila getur hann þurft að vinna persónuupplýsingar í eigin þágu, t.d. vegna eigin fyrirtækjareksturs. Við slíka vinnslu telst hann ekki vinnsluaðili, heldur ábyrgðaraðili. Þessu til útskýringar má nefna eftirfarandi dæmi:

> Fyrirtækið A hf. sérhæfir sig í vinnslu launa- og mannauðsupplýsinga. Í því hlutverki er fyrirtækið vinnsluaðili. Þegar A hf. vinnur persónuupplýsingar um sitt eigið starfsfólk, í hlutverki sínu sem vinnuveitandi, er fyrirtækið aftur á móti ábyrgðaraðili þeirrar vinnslu.[187]

Við mat á því hvort viðkomandi gegni stöðu vinnsluaðila eða ábyrgðaraðila þarf að líta til þess í hverra þágu aðili er að vinna upplýsingar, þ.e. hvort hann sé að vinna þær eftir ósk og fyrirmælum ábyrgðaraðila og er þar af leiðandi í hlutverki vinnsluaðila, eða hvort unnið sé með upplýsingar sem hann sjálfur ákveður að vinna í krafti stöðu sinnar sem ábyrgðaraðili. Þannig getur sami aðilinn, á sama tíma, verið ábyrgðaraðili vinnslu A en vinnsluaðili vinnslu B. Hlutverk aðila er því ekki tengt *persónu* hans.[188] Með því er átt við að hlutverk viðkomandi að persónuupplýsingalögum er ekki tengt tiltekinni manneskju eða tilteknum lögaðila, heldur er það tengt því *hlutverki* sem viðkomandi gegnir við sjálfa vinnsluna.

5.4 Trúnaðarskylda vinnsluaðila við meðferð persónuupplýsinga

Um samband ábyrgðaraðila og vinnsluaðila er fjallað í 13. gr. pul. Samkvæmt ákvæðinu er ábyrgðaraðila heimilt að fela vinnsluaðila, í heild eða að hluta, þá vinnslu persónuupplýsinga sem hann ber ábyrgð á. Ákvæðið byggist á reglum 16. gr. og 2.–4. mgr. 17. gr. tilskipunar 95/46/EB sem fela í sér tvo meginþætti, þ.e. (a) að vinnsluaðili megi eingöngu meðhöndla persónuupplýsingar í samræmi við lög og fyrirmæli ábyrgðaraðila og (b) að ábyrgðaraðili skuli gera við vinnsluaðila skriflegan samning, svonefndan vinnslusamning, þar sem afmarka skuli skyldur vinnsluaðila við meðferð umræddra persónuupplýsinga.

Ákvæði 13. gr. var fyrst kynnt til sögunnar með lögum nr. 90/2001 um breytingu á lögum um persónuvernd og meðferð persónuupplýsinga nr. 77/2000. Samkvæmt athugasemdum með frumvarpi því er varð að breytingarlögum nr. 90/2001 var 16. gr. og 2. – 4. mgr. 17. gr. tilskipunar 95/46/EB ekki innleidd með nógu skýrum hætti með lögum 77/2000. Markmiðið með breytingu þeirri er gerð var á 13. gr. var að bæta úr þeim galla og lögleiða ofangreind ákvæði tilskipunarinnar með afdráttarlausari hætti.[189]

---

[187] Byggt á eftirfarandi dæmi: „The Everready company specialises in data processing for the administration of human resource data for other companies. In this function, Everready is a processor. Where Everready processes the data of its own employees, however, it is the controller of data-processing operations for the purpose of fulfilling its obligations as an employer“ Sjá nánar *Handbook on European data protection law*, bls. 52.
[188] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25.
[189] Alþt. 2000-01, A-deild, bls. 4117.

5.4.1 Lög og fyrirmæli ábyrgðaraðila

Samkvæmt 3. mgr. 13. gr. pul. er hverjum þeim sem starfar í umboði ábyrgðaraðila eða vinnsluaðila, að vinnsluaðila sjálfum meðtöldum, og hefur aðgang að persónuupplýsingum, aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila, nema lög mæli fyrir á annan veg. Af ákvæðinu leiðir að vinnsluaðili má ekki vinna með upplýsingarnar eftir fyrirmælum neins annars en ábyrgðaraðila.

Öll vinnsla vinnsluaðila sem ekki er í samræmi við fyrirmæli ábyrgðaraðila er, samkvæmt athugasemdum með 13. gr. pul., ólögmæt. Á þetta reyndi í *úrskurði PV 18. janúar 2011 (2010/907)* (Hraðpeningar ehf.).

> Málsatvik voru þau að fyrirtækið Hraðpeningar ehf. hafði fengið kerfisfræðing til að vinna forritunarkóða fyrir sms-kerfi í tengslum við smálánaþjónustu fyrirtækisins, en við þá vinnu fékk hann lista yfir viðskiptavini þar sem mátti finna upplýsingar um kennitölu, bankanúmer, símanúmer og tölvupóstföng yfir 3000 einstaklinga. Hraðpeningar ehf. hafði gert verksamning og trúnaðarsamning við umræddan kerfisfræðing og gegndi hann stöðu vinnsluaðila. Lagt var fyrir hann að eyða umræddum lista þegar verki hans væri lokið. Kerfisfræðingurinn gleymdi aftur á móti að eyða listanum og vistaði hann á lokuðu heimasvæði sínu. Varð það til þess að upplýsingarnar urðu aðgengilegar á tiltekinni vefsíðu sem var opin almenningi. Taldi Persónuvernd að með því að vista upplýsingarnar á heimasvæði sínu í stað þess að eyða þeim hafði vinnsluaðili gengið gegn skýrum fyrirmælum ábyrgðaraðila og var sú vinnsla að birta lista yfir viðskiptamenn Hraðpeninga ehf. á vefsíðunni talin ólögmæt.

Helst þetta í hendur við þá staðreynd að ábyrgðaraðili ber ábyrgð á því tjóni sem vinnsluaðili veldur sbr. 43. gr. pul. Er því mikilvægt að vinnsluaðili fari eftir fyrirmælum ábyrgðaraðila, svo vinnsluaðili geri ábyrgðaraðila ekki bótaskyldan fyrir vanrækslu sinni.

Skortur á fyrirmælum frá ábyrgðaraðila getur gefið til kynna að sá aðili sem annast vinnslu af hálfu ábyrgðaraðila sé einnig ábyrgðaraðili vinnslunnar, en ekki einvörðungu vinnsluaðili hennar.[190] Um skort á fyrirmælum og áhrif þess var fjallað í eftirfarandi úrskurði:

> *Ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV). Úrskurður þessi varðaði endurupptökubeiðni á máli Persónuverndar nr. 172/2009 sem lokið var með *úrskurði PV 10. júní 2009, (2009/172)* (Fjölmennt I), en málsatvik þess eru reifuð í kafla 4.3.3. Sálfræðingarnir A og B töldu sig ekki vera ábyrgðaraðila umræddrar vinnslu og leituðu því eftir endurupptöku málsins í kjölfar *álits umboðsmanns Alþingis 5. september 2012, (6055/2010)* (Fjölmennt III). Við mat á því hvort tilefni væri til endurupptöku málsins (þ.e. hvort endurskoða þyrfti þá forsendu Persónuverndar að sálfræðingarnir A og B væru ábyrgðaraðilar vinnslunnar) leit Persónuvernd m.a. til þess svigrúms sem sálfræðingarnir höfðu við vinnslu upplýsinganna. Ekki lágu fyrir nákvæm fyrirmæli frá verkbeiðanda um hvernig sálfræðingunum bæri að haga starfi sínu og fóru sálfræðingarnir því eftir ítarlegum verklagsreglum sem þeir höfðu sjálfir sett sér. Sálfræðingarnir höfðu þannig að mestu ráðið hvernig verkið var unnið og þar með talist ábyrgðaraðilar vinnslunnar. Þótti því ekki tilefni til að endurskoða niðurstöðu Persónuverndar og var synjað um endurupptöku máls.

[190] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 28–29.

Samkvæmt athugasemdum með 13. gr. pul. getur skortur á fyrirmælum orðið til þess að vinnslan teljist ólögmæt, þar sem hún fer ekki fram á grundvelli fyrirmæla frá ábyrgðaraðila.[191] Með vísan til ofangreinds úrskurðar Persónuverndar er þó sennilegra að skortur á fyrirmælum leiði til þess að aðili sem tekur að sér vinnslu fyrir hönd ábyrgðaraðila reynist sameiginlegur ábyrgðaraðili að vinnslunni, þar sem skortur á fyrirmælum leiðir til frekara svigrúms vinnsluaðila um hvernig verk skuli unnið. Styðst þetta einnig við álit 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“.[192]

Framangreindur fyrirvari um að ekki megi vinna með upplýsingar eftir fyrirmælum neins annars en ábyrgðaraðila, nema *lög mæli fyrir á annan veg*, leiðir til þess að vinnsluaðili þarf í vissum tilvikum að meta hvort ákvæði laga hamli því að hann fylgi fyrirmælum ábyrgðaraðila.

> *Álit PV 19. janúar 2006 (2005/593)* (Tölvunotkun starfsmanns). Persónuvernd barst fyrirspurn frá starfsmanni félagsins A um heimildir þess til að afhenda fyrirtækinu B, sem A rak upplýsingakerfi fyrir, upplýsingar um tölvunotkun starfsmanns hjá félaginu A. Persónuvernd veitti almenna leiðsögn um lagasjónarmið og réttarstöðu aðila sem veita sambærilega þjónustu og A og var þar m.a. vikið að stöðu vinnsluaðila gagnvart ábyrgðaraðila. A var talið gegna stöðu vinnsluaðila, en B hafði stöðu ábyrgðaraðila. Persónuvernd vísaði til fyrirvara 3. mgr. 13. gr. pul. um að *lög mæli fyrir á annan veg* og að fyrirvari sá leiddi til þess að vinnsluaðili þyrfti í vissum tilvikum að meta hvort ákvæði laga hamli því að hann hlíti fyrirmælum ábyrgðaraðila. Persónuvernd benti á fyrirmæli um vernd persónuupplýsinga og friðhelgi einkalífs í IX. kafla fjarskiptalaga nr. 81/2003 og 228. gr. almennra hegningarlaga nr. 19/1940, en seinna ákvæðið mælir m.a. fyrir um refsingu fyrir að hnýsast í gögn, þ.á.m. tölvugögn, sem hafa að geyma upplýsingar um einkamál annars manns. Ganga þyrfti úr skugga um að afhending upplýsinga um tölvunotkun starfsmanns til ábyrgðaraðila, myndi ekki brjóta í bága við ofangreind ákvæði.

Ráða má af áliti Persónuverndar að hér hafi tekist á réttur starfsmanns til friðhelgi einkalífs og fyrirmæli ábyrgðaraðila um afhendingu upplýsinga. Var þó ekki skorið úr um ágreiningsmál, heldur einungis veitt almenn leiðsögn um lagasjónarmið, og því ekki komist að bindandi niðurstöðu um það hvort fyrirmæli laga hafi hamlað A í að fylgja fyrirmælum ábyrgðaraðila.

Við mat á því hvort vinnsluaðili hafi farið eftir fyrirmælum ábyrgðaraðila skiptir máli að líta til þess umboðs sem ábyrgðaraðili hefur veitt vinnsluaðila. Gangi vinnsluaðili lengra en umboðið nær, eða taki hann að einhverju marki sjálfstæðar ákvarðanir, getur hann talist ábyrgur, a.m.k. á þeim þáttum sem hann ræður sjálfur og tekur ákvarðanir um.[193] Er því mikilvægt að reglum 13. gr. pul. um vinnslusamninga sé fylgt eftir, þar sem þeir geta veitt

[191] Alþt. 2000-01, A-deild, bls. 4117.
[192] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25.
[193] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 25–26.

ýmsar vísbendingar um samband ábyrgðaraðila og vinnsluaðila og hvaða fyrirmæli vinnsluaðili hefur fengið um framkvæmd verksins.

5.4.2 Vinnslusamningur

Ef ábyrgðaraðili felur vinnsluaðila að annast vinnslu persónuupplýsinga ber ábyrgðaraðili ábyrgð á því að gerður sé vinnslusamningur þeirra á milli, sbr. 13. gr. pul. Ákvæði 2. mgr. 13. gr. laganna krefst þess að slíkur samningur sé skriflegur og a.m.k. í tveimur eintökum, en ákvæðið er byggt á 3. mgr. 17. gr. tilskipunar 95/46/EB.

Skriflegur vinnslusamningur er ekki forsenda þess að samband ábyrgðaraðila og vinnsluaðila sé fyrir hendi, þar sem slíkt samband getur verið til staðar þótt enginn samningur hafi verið gerður. Skortur á slíkum samningi, eða ófullnægjandi samningur, leiðir til þess að vinnslan standist ekki ákvæði pul. og sé því óheimil.[194] Í *úrskurði PV 27. nóvember 2012 (2012/818)* (Sjóvá) leiddi skortur á vinnslusamningi til þess að afhending persónuupplýsinga frá Sjóvá til verktakans Z var talin óheimil. Vinnslusamningi er ætlað að afmarka skyldur vinnsluaðila við meðferð persónuupplýsinga, en norska persónuverndarstofnunin (no. *Datatilsynet*) hefur gefið út leiðbeiningar um hvað slíkur samningur skuli innihalda sem hér verða hafðar til hliðsjónar, ásamt fyrirmælum úr áliti 29. gr. starfshópsins.

Vinnsluaðila er óheimilt að vinna með persónuupplýsingar í öðrum tilgangi en þeim sem ábyrgðaraðili hefur lýst yfir, sbr. 3. mgr. 13. gr. pul. Er þess vegna brýnt að greina frá tilgangi vinnslunnar í vinnslusamningnum en þar skal einnig koma fram að vinnsluaðila sé einungis heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila, sbr. 2. mgr. 13. gr. pul. Þá skal það einnig vera skýrt hvernig upplýsingarnar skulu unnar, t.d. hvort verkið feli í sér umfangsmikla vinnslu upplýsinga eða hvort vinnsluaðili skuli einungis annast geymslu upplýsinganna. Vinnslusamningur skal einnig innihalda ákvæði um skilyrði þess að upplýsingarnar séu afhentar þriðja aðila, t.d. getur afhending upplýsinga til þriðja aðila verið háð skriflegu samþykki ábyrgðaraðila sbr. *leiðbeinandi svar PV 7. ágúst 2012 (2010/1079)* (Alcoa Fjarðarál sf.) þar sem vinnslusamningur milli Alcoa Fjarðaráls sf. og Alcoa Inc. innihélt slíkt ákvæði. Ef það liggur fyrir að verkið krefst þess að vinnsluaðili afhendi upplýsingarnar þriðja aðila skal vinnslusamningurinn kveða skýrt á um hver sá þriðji aðili er. Jafnframt skal þess getið í samningi ef vinnsluaðili notast við undirverktaka við framkvæmd verksins.[195]

Til að koma í veg fyrir að ábyrgðaraðili geti hlaupist frá ábyrgð sinni með því að fá vinnsluaðila til að annast vinnslu persónuupplýsinga sem hann ber ábyrgð á, hvílir sú ábyrgð

[194] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 26–27.
[195] *Data processor agreements pursuant to the Personal Data Act and the Personal Health Data Filing System Act*, bls. 5.

á ábyrgðaraðila samkvæmt 1. mgr. 13. gr. pul. að sannreyna að umræddur vinnsluaðili geti framkvæmt viðeigandi öryggisráðstafanir, áður en samið er við hann um framkvæmd verksins. [196] Vinnslusamningurinn skal því kveða á um þær öryggisráðstafanir sem vinnsluaðili verður að framkvæma.[197] Það leiðir jafnframt af 2. málsl. 2. mgr. 13. gr. pul. að ákvæði laganna um skyldur ábyrgðaraðila gilda einnig um þá vinnslu sem vinnsluaðili annast. Í því felst m.a. að vinnsluaðila ber að gæta viðeigandi upplýsingaöryggis sbr. 11. gr. pul., þ.e. að upplýsingarnar séu verndaðar gegn ólöglegri eyðileggingu, gegn því að þær breytist og gegn óleyfilegum aðgangi. Á upplýsingaöryggi vinnsluaðila reyndi í *ákvörðun PV 3. mars 2011 (2011/62)* (Miðlun ehf.). Miðlun ehf. gegndi hlutverki vinnsluaðila fyrir fjármálaráðuneytið vegna eineltiskönnunar sem fór fram á vegum ráðuneytisins, en persónuupplýsingar sem unnið var með vegna könnunarinnar voru teknar ófrjálsri hendi frá Miðlun ehf. af fyrrum starfsmanni fyrirtækisins. Um skyldur vinnsluaðila til að gæta öryggis upplýsinga segir í ákvörðun Persónuverndar:

> Samkvæmt 3. mgr. 13. gr. er vinnsluaðila aðeins heimilt að starfa í samræmi við fyrirmæli ábyrgðaraðila nema lög mæli fyrir á annan veg. Verður vinnsluaðili að haga vinnslunni í samræmi við lög nr. 77/2000, sbr. 2. málsl. 2. mgr. sömu greinar. Í því felst m.a. að vinnsluaðila ber að gæta viðeigandi upplýsingaöryggis, sbr. 11. gr. laga nr. 77/2000, sbr. reglur nr. 299/2001 um öryggi persónuupplýsinga. Meðal þess sem fram kemur í 11. gr. er að við vinnslu persónuupplýsinga skal gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingarnar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysni og gegn óleyfilegum aðgangi (1. mgr.). Þá segir m.a. að beita skuli ráðstöfunum sem tryggja nægilegt öryggi miðað við áhættu af vinnslunni og eðli þeirra gagna sem verja á, með hliðsjón af nýjustu tækni og kostnaði við framkvæmd þeirra (2. mgr.)

Miðlun ehf. hafði einnig brotið í bága við ákvæði pul. þar sem vinnslusamningur á milli ráðuneytisins og fyrirtækisins kvað á um að eyða ætti öllum persónugreinanlegum gögnum innan tveggja vikna frá því að lokið yrði við að safna svörum í eineltiskönnuninni. Miðlun ehf. varðveitti hins vegar upplýsingarnar í u.þ.b. tvö ár. Taldi Persónuvernd öryggis ekki hafa verið gætt og var varðveisla Miðlunar ehf. á persónuupplýsingunum kærð til lögreglu. Jafnframt var fyrirtækinu gert að senda Persónuvernd öryggisstefnu, áhættumat og skjalfestingu á öryggisráðstöfunum þar sem lýst væri verkferlum til að girða fyrir heimildarlausa varðveislu persónuupplýsinga.[198]

[196] Alþt. 2000-01, A-deild, bls. 4118.
[197] *Data processor agreements pursuant to the Personal Data Act and the Personal Health Data Filing System Act*, bls. 6.
[198] Ákvörðun þessi er einnig til marks um það að til þess getur komið að vinnsluaðili sæti refsiábyrgð fyrir brot gegn pul. Í ákvörðun Persónuverndar segir að það geti t.d. gerst fari hann gegn fyrirmælum ábyrgðaraðila eða ef hann hlýðir fyrirmælum sem brjóta í bága við ákvæði pul.

Hafi vinnsluaðili staðfestu í öðru ríki innan EES en ábyrgðaraðili skal jafnframt mælt svo fyrir í vinnslusamningi að lög og reglur þess ríkis þar sem vinnsluaðili hefur staðfestu gildi um öryggisráðstafanir við vinnslu persónupplýsinga, sbr. 4. mgr. 13. gr. pul. Þannig getur staðfesta vinnsluaðila í öðru ríki haft áhrif á þær öryggisráðstafanir sem vinnsluaðila er gert að framkvæma og gætu landslög þess ríkis t.a.m. gert ríkari kröfur til slíkra ráðstafana.[199]

Þar sem ákvæði pul. um skyldur ábyrgðaraðila gilda einnig um þá vinnslu sem vinnsluaðili annast, sbr. 2. mgr. 13. gr. pul., gæti hann t.d. þurft að verða við beiðni á grundvelli 16. gr. pul um almenna vitneskju.[200] Það er því gagnlegt að kveða á um verkaskiptingu milli ábyrgðaraðila og vinnsluaðila í sjálfum vinnslusamningnum um hvor þeirra annist slíkar beiðnir frá hinum skráða. Jafnframt skal því umboði sem vinnsluaðili hlýtur frá ábyrgðaraðila lýst á fullnægjandi hátt í vinnslusamningnum, svo það sé ljóst hvað vinnsluaðila er heimilt að gera og hvað ekki.[201]

Líkt og gerð hefur verið grein fyrir hér að framan verður að líta til raunverulegra aðstæðna hverju sinni, þótt vinnslusamningur titli aðila sem vinnsluaðila. Ef viðkomandi tekur sér meira vald en samningurinn kveður á um eða vinnur upplýsingar í eigin þágu, eru líkur á því að hann gegni í raun hlutverki ábyrgðaraðila vinnslu.[202] Þá hefur skortur á vinnslusamningi einnig þótt benda til þess að vinnsluaðili væri í raun og veru ábyrgðaraðili vinnslu, sbr. *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV).

Þess má geta að Staðlastofnun Evrópu (e. *European Committee for Standardisation*) hefur gefið út staðlaðan vinnslusamning sem stenst kröfur tilskipunar 95/46/EB og hægt er að styðjast við við gerð slíkra samninga.[203]

5.5 Vinnsluaðili og undirverktakar utan EES

Vinnsluaðilar geta, líkt og ábyrgðaraðilar, verið fleiri en einn að sömu vinnslunni. Ábyrgðaraðili getur t.d. valið að fela fleiri vinnsluaðilum að annast vinnslu upplýsinga fyrir sína hönd, en einnig er algengt að vinnsluaðilar notist við svokallaða undirverktaka (d. *underdatabehandler*, e. *sub processor*) og feli þeim ákveðinn hluta vinnslunnar. Sem dæmi gæti vinnsluaðili fengið undirverktaka til að annast viðhald á gagnasafni sínu eða til að annast

[199] Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger*, bls. 449.
[200] Samkvæmt athugasemdum með 3. mgr. 16. gr í frumvarpi því er varð að lögum nr. 77/2000 segir að ekki sé hægt að beina kröfu samkvæmt ákvæðinu til vinnsluaðilans, en hins vegar stendur því ekkert í vegi að ábyrgðaraðili feli vinnsluaðila að veita umbeðnar upplýsingar og uppfylli þannig skyldur sínar skv. 16. gr. pul. Sjá Alþt. 1999-00, A-deild, bls. 2731.
[201] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 26.
[202] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 26–27.
[203] *Standard form contract to assist compliance with obligations imposed by Article 17 of Data Protection Directive 95/46/EC.* Sjá einnig Christopher Kuner: *European Data Protection Law*, bls. 73 og 453-459.

afmarkaðan hluta tiltekinnar vinnslu.[204] Samkvæmt 29. gr. starfshópnum er ekkert því til fyrirstöðu að vinnsluaðilar séu fleiri en einn, eða að undirverktakar séu fengnir til að annast tiltekinn hluta vinnslu, en allir skulu þeir þó fylgja fyrirmælum ábyrgðaraðila. Það að fleiri aðilar séu fengnir til að annast vinnsluna á ekki að leiða til þess að vernd persónuupplýsinga verði minni en ella.[205]

Fyrirtæki leita í síauknum mæli til vinnsluaðila í löndum á borð við Indland og Kína til að forðast háan kostnað við gagnavinnslu í Evrópu.[206] Þá hefur það einnig færst í aukana að vinnsluaðilarnir sjálfir ráði undiverktaka utan EES. Við þessar aðstæður er mikilvægt að hafa í huga að lög þess ríkis þar sem ábyrgðaraðili hefur staðfestu gilda um vinnslu persónuupplýsinga, sbr. a-lið 1. mgr. 4. gr. pul. Þannig gilda íslensk lög um vinnslu sem á sér stað í Indlandi ef vinnslan er unnin fyrir hönd ábyrgðaraðila sem hefur staðfestu á Íslandi.[207]

Um flutning á upplýsingum út fyrir EES gilda sérstakar reglur, en vísað er til landa utan EES sem „þriðju lönd“.[208] Samkvæmt 1. mgr. 29. gr. pul. er flutningur persónuupplýsinga til annars ríkis heimill ef lög þess veita persónuupplýsingum fullnægjandi vernd. Í 2. mgr. 29. gr. segir að þau ríki sem framfylgja tilskipun 95/46/EB teljast fullnægja skilyrðum 1. mgr. Það sama á við um lönd eða staði sem framkvæmdastjórn ESB hefur viðurkennt að veiti fullnægjandi vernd.[209] Samkvæmt 1. mgr. 30. gr. pul. er flutningur persónuupplýsinga til lands sem ekki veitir fullnægjandi persónuupplýsingavernd óheimill. Samkvæmt 2. mgr. 30. gr. pul. getur Persónuvernd aftur á móti heimilað miðlun persónuupplýsinga til þriðju landa, þótt þau hafi ekki verið talin veita persónuupplýsingum fullnægjandi vernd. Slíkt er háð því að ábyrgðaraðili hafi, að mati stofnunarinnar, veitt nægilegar tryggingar fyrir slíku. Til dæmis getur Persónuvernd áskilið að ábyrgðaraðili geri skriflegan samning við vinnsluaðilann sem hefur staðfestu í þriðja ríki og að samningur sá hafi að geyma tiltekin stöðluð samningsákvæði um flutning persónuupplýsinga til þriðju landa.

[204] Christopher Kuner: *European Data Protection Law*, bls. 171.
[205] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 27.
[206] Christopher Kuner: *European Data Protection Law*, bls. 152.
[207] Um landfræðilegt gildissvið pul. er fjallað í kafla 3.3.3.
[208] *Datatilsynets årsberetning 2011*, bls. 34.
[209] Þegar ritgerð þessi er skrifuð eru þau lönd og staðir sem talin eru veita persónuupplýsingum fullnægjandi vernd í skilningi 29. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga eftirfarandi: Andorra, Argentína, Kanada, Sviss, Færeyjar, Guernsey, Ísrael, Mön, Jersey, Nýja Sjáland og Úrúgvæ sbr. 1. gr. auglýsingar nr. 228/2010 um flutning persónuupplýsinga til annarra landa með síðari breytingum. Jafnframt er heimilt að flytja persónuupplýsingar til aðila í Bandaríkjunum sem fara að reglum, útgefnum af viðskiptaráðuneyti Bandaríkjanna, um örugga höfn fyrir friðhelgi einkalífs, sbr. 2. gr. sömu auglýsingar. Sjá Stjórnatíðindi 2010, B-deild, bls. 1163.

Ákvörðun framkvæmdastjórnar ESB 2010/87/ESB[210] (hér eftir „ákvörðun 2010/87/ESB“) kveður á um stöðluð samningsákvæði (e. *standard contractual clauses*) sem taka til flutninga á persónuupplýsingum frá ábyrgðaraðila innan EES til vinnsluaðila í þriðja landi.[211] Ákvörðunin var tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar þann 1. júlí 2011.[212] Kosturinn við notkun staðlaðra samningsákvæða er að ábyrgðaraðili þarf ekki að sannfæra Persónuvernd um að þau uppfylli skilyrði 30. gr. pul. um fullnægjandi vernd, þar sem þau eru hönnuð af framkvæmdastjórn ESB í þeim tilgangi að veita þá vernd sem krafist er af tilskipun 95/46/EB. Aðildarríki EES geta því ekki neitað að viðurkenna að stöðluðu samningsákvæðin tryggi fullnægjandi vernd persónuupplýsinga.[213]

Ákvörðun 2010/87/ESB staðfestir heimild vinnsluaðila til að semja við undirverktaka, en í 11. gr. stöðluðu skilmálanna sem ákvörðunin kveður á um, er fjallað um samband vinnsluaðila við undirverktaka sína. Samkvæmt 16. lið formála ákvörðunarinnar var samningsákvæðum milli vinnsluaðila og undirverktaka komið á til þess að taka tillit til þróunar viðskiptavenja í átt að síaukinni hnattvæðingu á sviði gagnavinnslu. Í c-lið 3. gr. ákvörðuninnar er hugtakið undirverktaki skilgreint á eftirfarandi hátt:

> „undirverktaki“: vinnsluaðili sem ráðinn er af gagnainnflytjanda [þ.e. vinnsluaðila] eða einhverjum af undirverktökum hans og sem samþykkir að taka við persónuupplýsingum frá gagnainnflytjanda eða einhverjum af undirverktökum hans, sem eru eingöngu ætlaðar til vinnslu fyrir hönd gagnaútflytjandans [þ.e. ábyrgðaraðila] eftir flutninginn, í samræmi við fyrirmæli gagnaútflytjandans, föstu samningsákvæðin sem sett eru fram í viðaukanum og skilmála skriflega samningsins um ráðstöfun gagnavinnslu til undirverktaka.

Í c-lið 1. gr. ákvörðunar 2010/87/ESB er gagnainnflytjandi skilgreindur sem vinnsluaðili sem samþykkir að taka við persónuupplýsingum frá gagnaútflytjanda. Felst það í skilgreiningu hugtaksins að vinnsluaðili heyri ekki undir kerfi þriðja lands sem tryggir fullnægjandi vernd í skilningi 1. mgr. 25. gr. tilskipunar 95/46/EB. Þannig er gert ráð fyrir því að vinnsluaðilinn hafi staðfestu í þriðja landi, sem veitir ekki fullnægjandi persónuupplýsingavernd. Í b-lið 1. gr. ákvörðunarinnar er gagnaútflytjandi skilgreindur sem ábyrgðaraðilinn sem flytur persónuupplýsingar. Undiverktakahugtakið tekur ekki einungis til undirverktaka vinnsluaðila, heldur einnig til undirverktaka sem undirverktaki vinnsluaðila

[210] Ákvörðunin heitir fullu nafni: Ákvörðun framkvæmdastjórnar ESB frá 5. febrúar 2010 um föst samningsákvæði vegna flutnings persónuupplýsinga til vinnsluaðila með staðfestu í þriðju löndum samkvæmt tilskipun Evrópuþingsins og ráðsins 95/46/EB (2010/87/ESB).
[211] Ákvörðunin gildir ekki um flutning ábyrgðaraðila sem hefur staðfestu innan EES á persónuupplýsingum til annars ábyrgðaraðila sem hefur staðfestu utan EES. Um slíkan flutning gildir ákvörðun framkvæmdastjórnarinnar 2001/497/EB frá 15. júní 2001 um föst samningsákvæði vegna flutnings persónuupplýsinga til þriðju landa, samkvæmt tilskipun nr. 95/46/EB.
[212] Ákvörðun sameiginlegu EES-nefndarinnar 1. júlí 2011, nr. 79/2011 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) við EES-samninginn.
[213] Christopher Kuner: *European Data Protection Law*, bls. 195 og 5. liður formála ákvörðunar 2010/87/ESB.

kann að semja við um vinnslu upplýsinga. Þannig er þess gætt að persónuupplýsingar njóti áfram samsvarandi verndar skilmálanna, og eru enn á ábyrgð ábyrgðaraðila, þótt þær séu fluttar á milli fleiri aðila.

Mikilvægt er að persónuupplýsingar njóti ekki verri verndar þótt þeim sé miðlað til undirverktaka og unnar frekar. Ákvæði 11. gr. stöðluðu skilmála ákvörðunar 2010/87/ESB kveður á um þau skilyrði sem skulu uppfyllt svo flutningur frá vinnsluaðila til undirverktaka sé lögmætur. Í fyrsta lagi skal vinnsluaðili ekki fela undirverktaka neina gagnavinnslu, nema skriflegt fyrirframsamþykki ábyrgðaraðila liggi fyrir. Samkvæmt 29. gr. starfshópnum er það undir ábyrgðaraðila komið hvort eitt almennt fyrirframsamþykki um flutning upplýsinga til undirverktaka sé fullnægjandi, eða hvort samþykki skuli veitt fyrir hverjum og einum flutningi. Það veltur m.a. á eðli upplýsinganna sem stendur til að flytja, þ.e. hvort þær séu viðkvæmar, og umfang þeirrar vinnslu sem undirverktaki annast.[214] Í öðru lagi skal vinnsluaðili semja við undirverktaka með skriflegum samningi þar sem undirverktakinn tekur á sig sömu skyldur og lagðar eru á vinnsluaðilann samkvæmt stöðluðu samningsákvæðunum.[215] Ef undirverktaki uppfyllir ekki þær skyldur sem á honum hvíla samkvæmt samningnum ber vinnsluaðili ábyrgð á því gagnvart ábyrgðaraðila að skyldur undirverktaka samkvæmt samningnum séu uppfylltar, sbr. 1. mgr. 11. gr. skilmálanna.

Tilvik þar sem persónuupplýsingar eru fluttar frá vinnsluaðila til undirverktaka í þriðja landi má flokka í tvennt eftir því hvort vinnsluaðili hafi staðfestu innan EES eða utan þess. Stöðluðu samningsákvæði ákvörðunar 2010/87/ESB eiga einungis við þegar vinnsluaðili hefur staðfestu utan EES. Það leiðir af 23. lið formála ákvörðunar 2010/87/ESB að við aðstæður þar sem vinnsluaðili hefur staðfestu innan EES og undirverktaki utan þess er ekki hægt að notast við hin stöðluðu samningsákvæði, þar sem vinnsluaðili getur ekki talist *gagnainnflytjandi* í skilningi samningsákvæðanna þegar hann hefur staðfestu innan EES.[216] Til að mæta skorti á stöðluðum samningsákvæðum á milli vinnsluaðila innan EES og undirverktaka utan þess, hefur 29. gr. starfshópurinn lagt fram drög að nýjum

[214] *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU*, bls. 5.
[215] Einnig er hægt að fullnægja þessari kröfu með því að undirverktaki skrifi líka undir samninginn sem ábyrgðaraðili og vinnsluaðili gera sín á milli á grundvelli stöðluðu samningsskilmálanna.
[216] Í 23. lið formála ákvörðunar framkvæmdastjórnar ESB 2010/87/ESB segir orðrétt: „Þar sem þessi ákvörðun gildir einungis um þær aðstæður þegar gagnavinnsluaðili, með staðfestu í þriðja landi, semur við undirverktaka, með staðfestu í þriðja landi, um gagnavinnslu sína gildir hún ekki um þær aðstæður þegar gagnavinnsluaðili með staðfestu í Evrópusambandinu, sem innir af hendi vinnslu persónuupplýsinga fyrir hönd ábyrgðaraðila með staðfestu í Evrópusambandinu, semur við undirverktaka með staðfestu í þriðja landi um gagnavinnslu sína.“

samningsákvæðum sem er ætlað að gilda um slík tilvik.[217] Drögin eru þó einungis lögð fram sem tillaga af hálfu starfshópsins og hafa ekki verið samþykkt af framkvæmdastjórn ESB og hafa því ekki verið tekin í notkun.

29. gr. starfshópurinn hefur gefið út leiðbeiningar um hvernig skuli standa að flutningi persónuupplýsinga frá vinnsluaðila innan EES til undirverktaka í þriðja landi.[218] Leiðbeiningarnar tilgreina þrjá möguleika sem hægt er að notast við svo flutningurinn sé lögmætur. Í fyrsta lagi getur ábyrgðaraðili samið beint við undirverktakann á grundvelli stöðluðu samningsákvæða ákvörðunar 2010/87/EB, í stað þess að vinnsluaðili semji við hann. Undirverktakinn myndi þá gangast undir samninginn sem gagnainnflytjandi, en ekki sem undirverktaki. Í öðru lagi gæti ábyrgðaraðili veitt vinnsluaðila umboð til að gangast undir stöðluðu samningsákvæðin og undirrita þau fyrir sína hönd gagnvart undirverktakanum. Vinnsluaðili myndi þá skrifa undir sem gagnaútflytjandi og undirverktakinn sem gagnainnflytjandi í skilningi stöðluðu samningsákvæðanna. Það er undir ábyrgðaraðila komið hvort sérstakt umboð skuli veitt fyrir hverja vinnslu sem undirverktaki tekur að sér, eða hvort eitt almennt umboð dugi. Í þriðja lagi er hægt að notast við sértæka samninga (e. *ad hoc contracts*) sem skulu innihalda sömu reglur og skilyrði og stöðluðu samningsákvæðin kveða á um, en notkun þeirra er háð samþykki Persónuverndar.[219] Danska Datatilsynet hefur vísað til þessara þriggja möguleika í *máli 15. janúar 2014 (2013-323-0154)* (Undirverktaki) sem varðaði flutning persónuupplýsinga frá vinnsluaðila með staðfestu í Danmörku til tölvuskýjaþjónustu utan EES. Nánar verður fjallað um málið síðar.

Í samræmi við 20. og 21. gr. pul. um fræðsluskyldu ber að upplýsa hinn skráða um flutning upplýsinga um hann til undirverktaka, svo hinn skráði viti hverju sinni hver fer með vinnslu persónuupplýsinga um hann.[220]

5.5.1 Tölvuskýjaþjónusta

Nátengt álitamálum um flutning persónuupplýsinga til vinnsluaðila og undirverktaka í þriðja ríki er notkun svokallaðrar tölvuskýjaþjónustu (e. *cloud computing services*). Dæmi um tölvuský er forrit sem er selt eða veitt í formi þjónustu og þarfnast ekki uppsetningar í eigin tölvu viðskiptavinarins (e. *cloud client*). Forritið er í raun vistað hjá þjónustuaðila

[217] *Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor"*.
[218] Leiðbeiningarnar heita fullu nafni „FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC".
[219] *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU*, bls. 4 - 5.
[220] Christopher Kuner: *European Data Protection Law*, bls. 172–173.

tölvuskýsins (e. *cloud service provider*) og er aðgengilegt í gegnum internetvafra viðskiptavinarins.[221] Tölvupóstþjónusta Gmail er gott dæmi til að styðjast við. Sú þjónusta er aðgengileg notendum í gegnum internetvafra og upplýsingar eru vistaðar í gagnaveri (e. *data center*) þjónustuaðilans, þ.e. í „skýinu“, en ekki á tölvu notenda nema hann velji það sérstaklega til viðbótar við vistun í skýinu.[222]

Þjónusta sem er veitt í gegnum tölvuský getur verið margvísleg og í mörgum tilfellum eru persónuupplýsingar unnar með slíkri þjónustu, sbr. *mál Datatilsynet 11. júlí 2011* (Dropbox), sem varðaði vistun gagna á Dropbox sem höfðu að geyma viðkvæmar persónuupplýsingar. Þegar unnið er með persónuupplýsingar í tölvuskýi þarf slík vinnsla að uppfylla skilyrði persónuupplýsingalaga, en að tölvuskýjaþjónustu geta komið margir mismunandi aðilar. Aðili A vistar t.d. gögn í tiltekinni þjónustu sem haldið er úti af B og B getur samið við undirverktakana C, D og E um að annast geymslu gagna í gagnaverum sínum. En hvernig horfa þessi ólíku hlutverk við ábyrgðar- og vinnsluaðilahugtökunum og hver ber ábyrgð á því að við vinnslu persónuupplýsinga í skýinu sé farið að lögum?

Í ræðu sinni um stöðu persónuverndar og tölvuskýja í Evrópurétti, sem flutt var 13. apríl 2010, kallaði Peter Hustinx, þáverandi forstöðumaður Evrópsku persónuverndar–stofnunarinnar (e. *European Data Protection Supervisor*), eftir nánari umfjöllun um stöðu þjónustuaðila tölvuskýja að Evrópurétti og hvernig hlutverk þeirra passar við hugtakanotkun tilskipunar 95/46/EB.[223] Svaraði 29. gr. starfshópurinn kalli Hustinx og gaf út álit 05/2012 um tölvuský. Fram að útgáfu þess hafði ríkt töluverð óvissa um það hvort þjónustuaðili gegndi hlutverki ábyrgðaraðila eða vinnsluaðila.

Þjónustuaðili tölvuskýs getur farið með ákvörðunarvald um ýmis atriði. Til dæmis hefur verið bent á að þeir taki ákvarðanir um að flytja upplýsingar á milli gagnavera, og jafnvel á milli landa, eftir því sem hentar hverju sinni og gætu því mögulega verið ábyrgðaraðilar þeirrar vinnslu sem á sér stað í skýinu.[224] Í áliti 29. gr. starfshópsins um tölvuský er litið svo á að viðskiptavinur tölvuskýjaþjónustu, þ.e. notandi skýsins, sé ábyrgðaraðili vinnslu sem á sér stað í tölvuskýinu, þar sem hann ákveður tilgang vinnslunnar og að fela utanaðkomandi aðila (í þessu tilfelli tölvuskýjaþjónustu) hluta hennar, með ákveðið markmið í huga. Þjónustuaðili

[221] Í áliti 29. gr. starfshópsins um hugtökin „ábyrgðaraðili“ og „vinnsluaðili“ eru tölvuský skilgreind á eftirfarandi hátt á bls. 6: „Cloud Computing is a kind of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using internet technologies. Typical cloud computing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. In this sense the cloud is not an island but a global connector of the world's information and users.“

[222] *Datatilsynets årsberetning 2011,* bls. 51.

[223] Peter Hustinx: „Data Protection and Cloud Computing under EU law“, bls. 3.

[224] Paolo Balboni: „Data Protection and Data Security Issues Related to Cloud Computing in the EU“, bls. 6–7.

sá sem heldur úti tölvuskýi er því talinn vinnsluaðili þeirrar persónuupplýsingavinnslu sem þar fer fram, svo lengi sem hún fer fram fyrir hönd ábyrgðaraðila. Hlutverk þjónustuaðila skal þó metið í samræmi við atvik máls hverju sinni, þar sem það kunna að koma upp aðstæður þar sem þjónustuaðili gegnir hlutverki ábyrgðaraðila, t.d. ef hann vinnur upplýsingar í eigin þágu. Með öðrum orðum ber að líta til þess hver fari með raunverulegt ákvörðunarvald um vinnsluna. Þannig getur þjónustuaðili annað hvort borið sameiginlega ábyrgð með viðskiptavini sínum, eða jafnvel sjálfstæða ábyrgð.[225] Af úrlausnum norrænna systrastofnana Persónuverndar, sem fjallað er um síðar, má þó draga þá ályktun að notandinn sé oftast ábyrgðaraðili persónuupplýsinga sem unnar eru í skýinu.[226] Það leiðir einnig af leiðbeiningum um notkun tölvuskýja hjá hinu opinbera, sem gefnar voru út á vegum Norrænu ráðherranefndarinnar, að notandi þjónustunnar sé almennt ábyrgðaraðili.[227]

Algengt er að vinnsluaðili sem heldur úti tölvuskýjaþjónustu semji við undirverktaka til að annast tiltekinn hluta vinnslunnar. Ef þörf er á frekara geymsluplássi getur vinnsluaðili t.d. samið við gagnaver um hýsingu á tilteknum upplýsingum. Í samræmi við 11. gr. stöðluðu skilmála ákvörðunar 2010/87/ESB skal fengið skriflegt samþykki frá notanda tölvuskýsins áður en vinnsluaðili semur við undirverktaka, auk þess sem vinnsluaðila ber að gera skriflegan samning við undirverktaka sem endurspeglar skilyrði þess samnings sem gildir á milli þjónustuaðilans og notandans.[228]

Það er á ábyrgð ábyrgðaraðila að farið sé að lögum við vinnslu persónuupplýsinga í tölvuskýi og er því mikilvægt að notandi vandi valið og semji við tölvuskýjaþjónustu sem tryggir að unnið sé með persónuupplýsingar í samræmi við lög.[229] Sú ábyrgð sem hvílir á ábyrgðaraðila vegna vinnslu persónuupplýsinga í tölvuskýi tekur ekki aðeins til þeirrar vinnslu sem fer fram hjá vinnsluaðila, heldur einnig þeirrar sem fer fram hjá undirverktökum. Í nýlegu máli danska Datatilsynet fékkst þetta staðfest.

> *Mál Datatilsynet 15. janúar 2014 (2013-323-0154)* (Undirverktaki). Mál þetta varðaði fyrirspurn sveitarfélagsins K í Danmörku um samband þess við vinnsluaðila sinn. Sveitarfélagið hafði gert samning við vinnsluaðila sem einnig hafði staðfestu í Danmörku, en vinnsluaðilinn samdi síðar við undirverktaka í þriðja landi um tölvuskýjaþjónustu. Datatilsynet áréttaði að ábyrgðaraðili upplýsinganna, sem í þessu tilfelli var sveitarfélagið K, bæri ábyrgð á því að farið væri að lögum við vinnslu upplýsinganna, sama hvar upplýsingarnar væru hýstar. Sveitarfélagið bæri því ábyrgð á þeirri vinnslu sem færi fram hjá þjónustuaðila tölvuskýjaþjónustunnar og undirverktaka hans.

[225] Article 29 Working Party *opinion 05/2012 on Cloud Computing* bls. 7–8.
[226] Sjá t.d. *bréf Datatilsynet 11. júlí 2011* (Dropbox) og *ákvörðun Datainspektionen 10. júní 2014 (358-2014)* (Grunnskólar í Malmö).
[227] *Legal guide to public organisation cloud sourcing in the Nordic countries*, bls. 5.
[228] *Article 29 Working Party opinion 05/2012 on Cloud Computing*, bls. 9–10.
[229] *Article 29 Working Party opinion 05/2012 on Cloud Computing*, bls. 8.

Með því að gera ábyrgðaraðila ábyrgan fyrir vinnslu undirverktaka ætti vernd persónuupplýsinga að vera tryggð, sama hvar upplýsingarnar eru hýstar. Einnig ber þó að líta til þess hvort vinnsla persónuupplýsinga í skýinu falli undir undanþágu 2. málsl. 2. mgr. 3. gr. pul. um meðferð einstaklings á persónuupplýsingum sem eru eingöngu ætlaðar til persónulegra nota eða varða eingöngu einkahagi hans. Undanþágan leiðir til þess að ákvæði pul. eiga ekki við um vinnsluna. Vistun háskólanema á skólagögnum sínum á Dropbox væri t.d. líkleg til að falla undir þá undanþágu.

Eitt helsta einkenni tölvuskýjaþjónustu er að hún er óháð hverskonar staðsetningu (e. *location independent*). Í því felst að þjónustan getur verið veitt hvaðan sem er, þar sem upplýsingar sem vistaðar eru í skýinu geta verið hýstar í gagnaverum hvar sem er í heiminum, en eru aðgengilegar viðskiptavini í gegnum Internetið. Þessi eiginleiki tölvuskýjaþjónustu hefur mætt erfiðleikum vegna reglna tilskipunar 95/46/EB, og þ.a.l. einnig reglna pul., um flutning persónuupplýsinga utan EES. Þannig getur reynt á flutning upplýsinga til þriðju landa þegar tölvuský eru notuð til vinnslu persónuupplýsinga, þar sem þjónustuaðili tölvuskýs eða undirverktaki hans gæti haft staðfestu í þriðja landi. Hafi notandi tölvuskýjaþjónustu ekki vitneskju um hvaðan tölvuskýjaþjónustan er veitt, eða hvar gögn hans eru hýst, getur það reynst honum flókið að uppfylla þau skilyrði sem persónuupplýsingalög EES-ríkja gera til flutnings upplýsinga til þriðju landa, en samkvæmt 1. mgr. 29. gr. pul. er slíkur flutningur óheimill nema persónuupplýsingar njóti þar fullnægjandi verndar.[230] Á þetta reyndi í máli danska Datatilsynet um vistun viðkvæmra upplýsinga á Dropbox, sem er afar gott dæmi um tölvuskýjaþjónustu og er víða notuð.

> *Bréf Datatilsynet 11. júlí 2011* (Dropbox).[231] Með bréfi dagsett 11. júlí 2011 gerði Datatilsynet móttakanda þess grein fyrir að stofnunin hefði rannsakað vinnslu persónuupplýsinga í starfsemi hans. Viðkomandi notaði tölvuskýjaþjónustuna Dropbox til að vista viðkvæmar persónuupplýsingar um skjólstæðinga sína. Stofnunin benti viðkomandi á að honum bæri skylda, sem ábyrgðaraðili upplýsinganna, að gera vinnslusamning við vinnsluaðila sinn, sem í þessu tilviki var Dropbox. Vegna eðlis Dropbox sem tölvuskýs gætu upplýsingarnar *mögulega* verið unnar i Bandaríkjunum eða öðrum löndum utan EES. Vinnslan þyrfti því að uppfylla skilyrði 27. gr. dönsku pul. um flutning upplýsinga til þriðju landa. Þar sem um var að ræða flutning viðkvæmra persónuupplýsinga til þriðju landa var vinnsla ábyrgðaraðila leyfisskyld en stofnunin taldi sig ekki geta veitt slíkt leyfi vegna ofangreindra annmarka, þ.e. skorts á vinnslusamningi og tryggingu á fullnægjandi vernd persónuupplýsinganna í þriðja landi.

[230] Paolo Balboni: „*Data Protection and Data Security Issues Related to Cloud Computing in the EU*“, bls. 3.
[231] Bréfið er án málsnúmers og annarra upplýsinga á heimasíðu Datatilsynet.

Orðalag Datatilsynet um að vinnsla upplýsinganna geti *mögulega* (d. *eventuelt*) átt sér stað utan EES gefur til kynna að ekki sé fullkomlega ljóst hvar í heiminum upplýsingarnar verði unnar.[232]

Þar sem það er á ábyrgð ábyrgðaraðila að farið sé eftir persónuupplýsingalögum við vinnslu persónuupplýsinga í tölvuskýi getur það reynst erfitt að huga að réttindum hins skráða þegar ábyrgaraðili hefur ekki vitneskju um hvar upplýsingar, sem unnar eru af hans hálfu, eru staddar hverju sinni. Hafi ábyrgðaraðili ekki yfirsýn yfir þá undirverktaka sem vinnsluaðili semur við getur hann t.a.m. ekki frætt hinn skráða um móttakendur persónuupplýsinga hans, sbr. 1. mgr. 18. gr., 1. mgr. 20. gr. og 3. mgr. 21. gr. pul. Jafnframt getur ábyrgðaraðili ekki sinnt þeirri skyldu sinni skv. 1. mgr. 13. gr. pul. að framkvæma innra eftirlit hjá aðila áður en samið er við hann um að annast vinnslu, ef hann veit ekki hvar undirverktaki hefur staðfestu. Óvissa um staðsetningu upplýsinga hafði áhrif á niðurstöðu Datatilsynet í máli um notkun sveitarfélagsins Óðinsvé á tölvuskýjaþjónustunni Google Apps.

> *Mál Datatilsynet 3. febrúar 2011 (2010-52-0138)* (Google Apps). Sveitarfélagið Óðinsvé óskaði eftir leyfi Datatilsynet til að vinna viðkvæmar upplýsingar um nemendur í skólum sveitarfélagsins og foreldra þeirra í tölvuskýjaþjónustunni Google Apps. Tölvuskýið yrði m.a. notað til að skrá upplýsingar um kennslu en einnig sem vettvangur fyrir kennara til að skrá athugasemdir um nemendur og senda bréf til foreldra þeirra. Sveitarfélagið lýsti því yfir að athugasemdir og bréf kennara gætu innihaldið viðkvæmar upplýsingar s.s. heilbrigðisupplýsingar, upplýsingar um félagsleg vandamál og önnur einkamál. Það lá fyrir að Google Ireland Limited væri vinnsluaðili upplýsinganna, en upplýsingarnar yrðu hýstar í gagnaverum Google í Bandaríkjunum og *innan Evrópu*. Datatilsynet taldi gagnaver Google í Bandaríkjunum veita fullnægjandi persónuupplýsingavernd, þar sem Google hefði gengist undir regluverkið um „öruggar hafnir“, sem er viðurkennt af framkvæmdastjórn ESB sem regluverk sem tryggir fullnægjandi vernd persónuupplýsinga. Það var þó óupplýst að hvaða marki gagnaver Google í Evrópu hefðu staðfestu í ríkjum innan EES og því óljóst hvort upplýsingarnar frá sveitarfélaginu myndu njóta fullnægjandi verndar í þeim gagnaverum sem þær yrðu hýstar innan Evrópu.

Til þess að mæta þeirri óvissu sem upp getur komið um staðsetningu upplýsinga hafa þær kröfur verið gerðar til vinnslusamninga milli ábyrgðaraðila og vinnsluaðila, sem heldur úti tölvuskýjaþjónustu, að þar komi skýrt fram hverjir undirverktakar vinnsluaðila eru, hvar þeir hafa staðfestu og hverskonar vinnsla fari fram hjá þeim. Í fjölda mála hefur sænska Datainspektionen gert athugasemdir við vinnslusamninga vegna þess að ekki kemur skýrt fram hvar undirverktakar vinnsluaðila hafa staðfestu og þ.a.l. hvar upplýsingar eru unnar.

> *Mál Datainspektionen 10. júní 2014 (358-2014)* (Grunnskólar í Malmö). Í máli þessu skipaði Datainspektionen grunnskólanefnd Malmö í Svíþjóð að hætta notkun tölvuskýjaþjónstunnar „Google Apps for Education“, þar sem vinnslusamningur sá sem gerður var á milli nefndarinnar og Google Ireland Limited uppfyllti ekki skilyrði sænsku pul. Eitt af þeim skilyrðum sem samningurinn uppfyllti ekki var að veita ábyrgðaraðila,

[232] Orðrétt segir í bréfinu: „Når du benytter en databehandler som Dropbox, hvor databehandlingen *eventuelt* sker i USA eller andre lande uden for EU[...]“.

> sem í þessu tilfelli var grunnskólanefndin, upplýsingar um undirverktaka Google. Í vinnslusamningnum samþykkti grunnskólanefndin að Google myndi nýta sér aðstoð undirverktaka sinna við vinnslu upplýsinga. Í samningnum var ekki gerð grein fyrir hverjir þessir undirverktakar væru, en á heimasíðu Google var að finna lista yfir undirverktaka fyrirtækisins. Datainspektionen taldi upplýsingarnar sem þar var að finna ekki fullnægjandi, þar sem það vantaði upplýsingar um hvar undirverktarnir hefðu staðfestu og hverskonar vinnsla færi fram hjá þeim. Forsenda þess að ábyrgðarðili geti fylgst með þeirri vinnslu sem fer fram fyrir hans hönd er að hann viti hvar vinnslan á sér stað. Datainspektionen setti það skilyrði fyrir notkun tölvuskýjaþjónustunnar að grunnskólanefndin fengi ávallt ofangreindar upplýsingar um undirverktaka vinnsluaðila tafarlaust.

Af ofangreindu leiðir að í flestum tilvikum er notandi tölvuskýjaþjónustunnar ábyrgðaraðili þeirra persónuupplýsinga sem unnar eru í skýinu, en sá aðili sem heldur úti þjónustunni og þeir undirverktakar sem hann semur við teljast almennt vinnsluaðilar upplýsinganna í skilningi persónuupplýsingalöggjafar. Vegna eðlis tölvuskýjaþjónustu og þess svigrúms sem þjónustuaðilar slíkrar þjónustu hafa við útfærslu hennar getur þó reynst erfitt fyrir notanda þjónustunnar að sinna hlutverki sínu sem ábyrgðaraðili. Bent hefur verið á að gagnlegt væri að leggja frekari ábyrgð á þjónustuaðilana sjálfa, bæði svo að vernd þeirra persónuupplýsinga sem unnar eru í skýinu sé tryggð og til að tryggja gegnsæi vinnslunnar fyrir ábyrgðaraðila og þann skráða.[233]

5.6 Samantekt

Í þessum kafla hefur verið fjallað um vinnsluaðilahugtakið eins og það birtist í pul. og í tilskipun 95/46/EB. Hugtakið má greina í tvo lykilþætti. Annars vegar þarf vinnsluaðili að vera sjálfstæður gagnvart ábyrgðaraðila, en í því felst fyrst og fremst að vinnsluaðili verður að vera utanaðkomandi aðili. Hins vegar þarf vinnslan að fara fram fyrir hönd ábyrgðaraðila.

Vikið var að trúnaðarskyldu vinnsluaðila við meðferð persónuupplýsinga samkvæmt 13. gr. pul. og greint frá meginþáttum hennar. Samkvæmt 3. mgr. 13. gr. pul. er vinnsluaðila aðeins heimilt að vinna með persónuupplýsingar í samræmi við fyrirmæli ábyrgðaraðila nema lög mæli fyrir á annan veg. Fjallað var um áhrif þess að vinnsluaðila sé ekki veitt fyrirmæli um vinnsluna. Það virðist sem ákveðin þróun hafi átt sér stað í þeim efnum, þar sem í athugasemdum með 13. gr. pul. segir að skortur á fyrirmælum geti orðið til þess að vinnslan teljist ólögmæt, en af framkvæmd Persónuverndar og af áliti 29. gr. starfshópsins leiðir að svigrúm það sem vinnsluaðili hefur vegna skorts á fyrirmælum er líklegra til að leiða til þess að vinnsluaðili teljist sameiginlegur ábyrgðaraðili að vinnslunni, frekar en að vinnslan í heild sinni teljist ólögmæt. Í trúnaðarskyldu vinnsluaðila samkvæmt 13. gr. pul. felst einnig að gera

[233] *Article 29 Working Party opinion 05/2012 on Cloud Computing*, bls. 23.

skuli vinnslusamning á milli ábyrgðaraðila og vinnsluaðila. Vinnslusamningur er verkfæri til að koma í veg fyrir misskilning um hvert hlutverk vinnsluaðila er með því að afmarka skýrlega hver tilgangur vinnslunnar er og hvernig upplýsingarnar skulu unnar.

Vinnsluaðilar geta samið við undirverktaka til að annast vinnslu fyrir sig, en gerð hefur verið grein fyrir þeim reglum sem gilda þegar undirverktaki hefur staðfestu utan EES og þeim skilyrðum sem uppfylla þarf svo flutningur upplýsinga til undirverktaka sé lögmætur. Meginþátturinn sem ber að hafa í huga þegar vinnsluaðili semur við undirverktaka um að annast vinnslu er að ábyrgð á vinnslunni breytist ekki. Það er ennþá ábyrgðaraðili vinnslunnar sem ber ábyrgð á henni, sama hversu margir undirverktakar tvinnast síðar inní vinnsluna. Vinnsluaðila er því óheimilt að nýta sér þjónustu undirverktaka án þess að fyrirframsamþykki ábyrgðaraðila liggi fyrir.[234] Jafnframt skal gerður skriflegur samningur á milli vinnsluaðila og undirverktaka, sem leggur sömu skyldur á herðar undirverktaka og hvíla á vinnsluaðila. Tölvuskýjaþjónusta er gott dæmi um starfsemi þar sem notkun undirverktaka er mjög algeng, ef ekki óhjákvæmileg. Undirverktakar geta haft staðfestu út um allan heim, sem gerir ábyrgðaraðila erfitt fyrir að sinna hlutverki sínu og gæta þess að unnið sé með persónuupplýsingar á lögmætan hátt hjá hverjum og einum undirverktaka. Forsenda þess að ábyrgðaraðili geti sinnt hlutverki sínu er að það komi skýrt fram í skriflegum samningi við vinnsluaðila hvar undirverktakar hans hafa staðfestu og hvernig vinnsla fari þar fram.

Af umfjölluninni hér að framan leiðir að grundvöllur árangursríkrar samvinnu á milli ábyrgðaraðila, vinnsluaðila og undirverktaka er að slíku sambandi séu gerð góð skil í skriflegum samningi, þar sem gerð er grein fyrir hlutverki og ábyrgð hvers og eins aðila á eins skýran hátt og kostur er.[235]

6 Samfélagsmiðlar

Samfélagsmiðlar eru með einum eða öðrum hætti orðnir hluti af daglegu lífi flestra. Á slíkum miðlum er unnið með gríðarlegt magn persónuupplýsinga, bæði af hálfu notenda og miðilsins sjálfs. Sprottið hafa upp deilur um lagalegt umhverfi samfélagsmiðla, m.a. hvort persónuupplýsingalöggjöf eigi yfirleitt við um persónuupplýsingavinnslu sem þar á sér stað og ef svo er, hver sé ábyrgðaraðili hennar.

[234] Í fyrirhuguðum breytingum á persónuupplýsingalöggjöf ESB er skilyrði þetta lögfest, sbr. d-liður 2. mgr. 26. gr. reglugerðartillögunnar. Um þetta er fjallað nánar í kafla 7.
[235] *Article 29 Working Party opinion 1/2010 on the concepts of "controller" and "processor"*, bls. 27.

29. gr. starfshópurinn hefur skilgreint samfélagsmiðla (e. *social network services*) sem vettvang fyrir rafræn samskipti, sem gerir notendum kleift að mynda tengslanet sín á milli.[236] Þessi skilgreining verður þó að teljast frekar rúm. Samfélagsmiðlar hafa mismunandi tilgang, en eiga það þó flestir sameiginlegt að notendur gefa upp tilteknar persónuupplýsingar til þess að stofna aðgang að miðlinum og gerir slíkur aðgangur þeim kleift að deila efni hver með öðrum eins og textum, myndum og hljóðskrám.[237] Samfélagsmiðlar hafa náð gríðarlegri útbreiðslu á síðustu árum, en þekkt dæmi um slíka miðla eru Facebook, Twitter og LinkedIn. Mikið hefur verið fjallað um vernd persónuupplýsinga á slíkum miðlum og hvort skilmálar þeirra uppfylli almennt reglur um friðhelgi einkalífs og persónuvernd. Það eitt er efni í heila ritgerð, en í kafla þessum verður einblínt á það hver beri ábyrgð á þeim persónuupplýsingum sem birtar eru á samfélagsmiðlum, þ.e. hver sé ábyrgðaraðili þeirra í merkingu laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

Ekki hafa fallið margir dómar um vernd persónuupplýsinga á samfélagsmiðlum og verður því notast við Facebook sem raunhæft dæmi þar sem við á.[238] Þykir það einkum viðeigandi vegna gríðarlegra vinsælda miðilsins, en á seinni hluta ársins 2014 hafði notendafjöldi síðunnar náð 1.35 milljörðum.[239]

6.1 Hver er ábyrgðaraðili?

Á samfélagsmiðlum fer fram rafræn vinnsla persónuupplýsinga og fellur hún því undir efnislegt gildissvið tilskipunar 95/46/EB og eftir atvikum pul.[240] Greina má vinnslu persónuupplýsinga sem á sér stað á samfélagsmiðlum í tvennt, þ.e. fyrri hluta vinnslu og seinni hluta vinnslu. Til hægðarauka verður hér notast við aðgreiningu þessa. Með fyrri hluta vinnslu er átt við vinnslu sem notandi samfélagsmiðils framkvæmir með því að gera persónuupplýsingar sínar, og jafnvel annarra, aðgengilegar á miðlinum. Með seinni hluta vinnslu er átt við frekari vinnslu þjónustuaðilans á þeim upplýsingum sem notandi hefur gert aðgengilegar. Til dæmis geta samfélagsmiðlar notað persónuupplýsingar notenda við markaðssetningu og myndi slík vinnsla teljast seinni hluta vinnsla.[241]

---

[236] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 4. Á ensku hljómar skilgreiningin svo: „SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users."

[237] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 4 og *Álit neytendastofnana á Norðurlöndunum varðandi markaðssetningu í samskiptamiðlum*, bls. 3.

[238] Þegar vísað er til skilmála Facebook er átt við skilmála þá sem tóku gildi 1. janúar 2015, nema annað sé tekið fram.

[239] Vefsíða fréttaveitu Facebook, https://newsroom.fb.com/company-info/.

[240] Ákvæði pul. eiga við ef eitthvert skilyrða 6. gr. laganna um landfræðilegt gildissvið þeirra er uppfyllt, t.d. ef ábyrgðaraðili hefur staðfestu á Íslandi.

[241] *Álit neytendastofnana á Norðurlöndunum varðandi markaðssetningu í samskiptamiðlum*, bls. 3.

Ýmsir aðilar koma að vinnslu persónuupplýsinga á samfélagsmiðlum og leggja verður mat á hver þeirra gegnir hlutverki ábyrgðaraðila og vinnsluaðila. Gerð verður grein fyrir hlutverki notanda (e. *social network service user*) annars vegar og þjónustuaðila sem heldur úti samfélagsmiðli (e. *social network service provider*) hins vegar, auk þess sem stuttlega verður fjallað um hlutverk þriðju aðila sem keyra viðbótarforrit við samfélagsmiðil.

6.1.1 Notandi

Í flestum tilfellum er notandi samfélagsmiðils ekki talinn gegna öðru hlutverki að lögum en að vera hinn skráði (e. *data subject*), þ.e. sá aðili sem upplýsingarnar fjalla um. Notandi hefur ákvörðunarvald um það hvaða miðil hann notar, hverju hann deilir og með hverjum. Undir vissum kringumstæðum getur notandi því talist ábyrgðaraðili þeirra upplýsinga sem hann birtir á samfélagsmiðli.[242] Þegar notandi gegnir hlutverki ábyrgðaraðila leiðir það af a-lið 1. mgr. 4. gr. tilskipunar 95/46/EB að landslög þess ríkis þar sem hann er búsettur gilda um þann hluta vinnslunnar sem hann ber ábyrgð á.[243] Sé notandi búsettur á Íslandi gilda því lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Í neðangreindri umfjöllun verður gert ráð fyrir því að notandi sé búsettur á Íslandi og því vísað til ákvæða pul.

Tilgangur persónuupplýsingalöggjafar er að vernda einstaklinga, en ekki að takmarka aðgerðir þeirra.[244] Notendum samfélagsmiðla er því frjálst að deila persónuupplýsingum um sig sjálfa með öðrum notendum. Peter Blume hefur komist svo að orði að þegar notandi deilir sínum eigin persónuupplýsingum sé hann *nokkurs konar ábyrgðaraðili* fyrir sjálfan sig, þar sem hann þarf að huga að afleiðingum þess að birta upplýsingar á Netinu. Í lagalegum skilningi getur einstaklingur þó ekki verið ábyrgðaraðili upplýsinga sem hann deilir um sig sjálfan.[245] Í þessu samhengi ber að hafa í huga ákvæði 6. tölul. 1. mgr. 9. gr. pul. sem segir að vinnsla viðkvæmra persónuupplýsinga sé heimil ef vinnslan tekur til upplýsinga sem hinn skráði hefur sjálfur gert opinberar. Í dönskum rétti er litið svo á að þetta eigi einnig við um vinnslu almennra persónuupplýsinga.[246] Með því að opinbera viðkvæmar upplýsingar um sig á Facebook, s.s. um kynhneigð sína eða stjórnmálaskoðanir, gerir notandi öðrum í raun frjálst að vinna slíkar upplýsingar frekar, þó með þeim hætti að meginreglum 7. gr. pul. um gæði gagna og vinnslu sé fylgt. Staðreyndin er aftur á móti sú að notendur samfélagsmiðla birta

[242] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 5. Hér ber að hafa í huga að það að deila persónuupplýsingum á Internetinu telst til *vinnslu* í skilningi tilskipunar 95/46/EB og pul.
[243] Þess má geta að á heimasíðu danska Datatilsynet segir að notandi samfélagsmiðils skuli fara eftir dönskum persónuupplýsingalögum þegar hann birtir persónuupplýsingar á miðlinum, þar sem hann gegnir hlutverki ábyrgðarðila. Sjá „Persondataloven og sociale netværk“, http://www.datatilsynet.dk.
[244] Peter Blume: „Data protection in the Private Sector“, bls. 304.
[245] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 179 og Peter Blume: *Databeskyttelsesret*, bls. 377.
[246] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 104.

ekki einungis sínar eigin persónuupplýsingar. Til dæmis er algengt að notendur Facebook birti myndir af sér ásamt öðrum og merki (e. *tag*) þá sem fram koma á myndinni. Með því að taka ákvörðun um að birta upplýsingar annarra getur notandi orðið ábyrgðaraðili gagnvart þeim sem upplýsingarnar fjalla um (þ.e. þeim skráðu).[247] Í bókinni *Internetretten* er að finna eftirfarandi dæmi.

> Ef móðir birtir mynd af syni sínum, sem er undir 18 ára aldri, á Facebooksíðu sinni og myndin sýnir að hann hafi fótbrotnað og er í gifsi [þ.e. viðkvæmar persónuupplýsingar], hefur það sömu áhrif og ef móðirin hafi deilt upplýsingum um sig sjálfa, þar sem hún fer með forsjá barns til 18 ára aldurs. Henni er því heimilt að birta myndina án frekari afleiðinga.[248] Ef hún birtir aftur á móti viðkvæmar upplýsingar um kynhneigð vinar síns á Facebooksíðu sinni og án hans samþykkis, getur sú vinnsla persónuupplýsinga brotið í bága við ákvæði persónuupplýsingalaga.[249]

Þegar notendur deila persónuupplýsingum á samfélagsmiðli verður að gera greinarmun á því hvort viðkomandi deilir eigin persónuupplýsingum eða annarra, þar sem aðeins hið síðarnefnda varðar persónuupplýsingalög og virkjar mögulega ábyrgð notanda samkvæmt ákvæðum laganna.

Þótt notandi samfélagsmiðils birti persónuupplýsingar um aðra leiðir það ekki undantekningarlaust til þess að hann þurfi að huga að skilyrðum pul. þar sem greinarmunur er gerður á því sem 29. gr. starfshópurinn kallar *heimilisafnot* (e. *household exemption*) og önnur afnot persónuupplýsinga. Í 2. málsl. 2. mgr. 3. gr. pul. segir að lögin gildi ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða eru einvörðungu ætlaðar til persónulegra nota.[250] Notandi samfélagsmiðils gegnir því ekki hlutverki ábyrgðaraðila ef þær upplýsingar sem hann deilir falla undir persónuleg afnot, þar sem slík vinnsla fellur utan gildissviðs pul. Hér ber að árétta að um undanþágu er að ræða, sem ber því að túlka þröngt.[251]

Í 12. lið formála tilskipunar 95/46/EB segir að undanskilja skuli frá gildissviði tilskipunarinnar vinnslu einstaklings á persónuupplýsingum ef hún er hluti af starfsemi sem er einungis í þágu hans sjálfs eða fjölskyldu hans, svo sem bréfaskriftir og skrár yfir

---

[247] Danska Datatilsynet hefur gefið út leiðbeinandi álit um það hvenær heimilt sé að birta myndir af einstaklingum á Internetinu án þeirra samþykkis. Gerður er greinarmunur á því hvort um er að ræða mynd af viðburði (d. *situationsbilleder*), s.s. mynd tekin af hópi áhorfenda á tónleikum, eða mynd af tilteknum og jafnvel nafngreindum einstaklingi (d. *portrætbillede*). Að mati Datatilsynet má að öllu jöfnu birta þær fyrrnefndu án samþykkis viðkomandi einstaklinga, en samþykkis skuli aflað fyrir birtingu af tilteknum einstaklingum. Sjá „Billeder på internettet“, http://www.datatilsynet.dk.

[248] Hér vakna vissulega spurningar um friðhelgi einkalífs barna á samfélagsmiðlum, sem eru þó utan viðfangsefnis þessarar ritgerðar. Um friðhelgi einkalífs barna vísast til ritsins *Friðhelgi einkalífs* sem gefið var út af umboðsmanni barna árið 2003.

[249] Jan Trzaskowski: *Internetretten*, bls. 561.

[250] Hér verður framvegis vísað til „persónulegra nota“ þegar átt við afnot persónuupplýsinga samkvæmt 2. málsl. 2. mgr. 3. gr.

[251] Christopher Kuner: *European Data Protection Law*, bls. 23.

heimilisföng. Í athugasemdum með 3. gr. í frumvarpi því er varð að lögum nr. 77/2000 segir að með persónulegum notum sé t.d. átt við einkabréfaskipti, færslu skráa með heimilisföngum vina og ættingja og færslu dagbóka.[252] Hvergi er vikið að vinnslu persónuupplýsinga á Internetinu og hvenær slík vinnsla getur talist til persónulegra nota. Evrópudómstóllinn hefur aftur á móti leyst úr því álitaefni í hinu svokallaða Lindqvist máli.

> *EBD, mál C-101/01, ECR 2003, bls. I-12971* (Lindqvist). Í máli þessu var kveðinn upp forúrskurður að beiðni sænsks dómstóls, Göta hovrätt, í máli Bodil Lindqvist. Lindqvist starfaði fyrir kirkjusöfnuð í Svíþjóð og hafði hún sótt námskeið í upplýsingavinnslu, þar sem hún fékk það verkefni að setja upp vefsíðu. Vefsíða hennar hafði að geyma upplýsingar um hana sjálfa og vinnufélaga hennar í söfnuðinum, svo sem nöfn og símanúmer þeirra, en tilgangurinn með því að setja upp síðuna var að gera slíkar upplýsingar aðgengilegar fyrir fermingarbörn í sókninni. Á vefsíðunni var einnig að finna upplýsingar um fjölskylduhagi og áhugamál vinnufélaga hennar, auk þess sem hún upplýsti um að vinnufélagi hennar hefði slasast á fæti og væri því frá vinnu. Enginn félaga hennar hafði veitt samþykki fyrir birtingu þeirra upplýsinga sem var að finna á vefsíðunni. Í kjölfarið var Lindqvist ákærð fyrir brot á persónuupplýsingalögum. Meðal þeirra spurninga sem lagðar voru fyrir Evrópudómstólinn var hvort birting ofangreindra persónuupplýsinga á vefsíðu Lindqvist gæti fallið undir einhverja af þeim undanþágum sem gert er grein fyrir í 2. mgr. 3. gr. tilskipunar 95/46/EB, m.a. undanþágu þeirri er varðar persónuleg afnot. Dómstóllinn taldi vinnslu Lindqvist á persónuupplýsingum um samstarfsfólk sitt ekki varða persónulega einkahagi hennar eða fjölskyldu hennar, þar sem upplýsingunum var dreift á Internetinu og þannig gerðar aðgengilegar *óákveðnum fjölda* fólks.

Af Lindqvist málinu leiðir að undanþága frá gildissviði persónuupplýsingalaga vegna persónulegra afnota á ekki við ef upplýsingum er dreift til *óákveðins fjölda fólks*. Dreifing upplýsinga til óákveðins fjölda fólks svipar meira til opinberrar birtingar (d. *offentliggørelse*), frekar en persónulegra samskipta.[253] Við mat á því hvort birting persónuupplýsinga á samfélagsmiðli falli undir undanþágu 2. málsl. 2. mgr. 3. gr. pul. er því litið til tveggja atriða. Annars vegar hvort upplýsingum sé dreift til óákveðins fjölda fólks og hins vegar hvert markmið vinnslunnar sé, þ.e. hvort vinnslan sé ætluð til persónulegra- eða heimilisafnota.[254] Verður nú fjallað um hvern þátt fyrir sig.

Á samfélagsmiðlum hafa notendur oftast val um hvernig aðgengi að persónulegri síðu þeirra er hagað. Almennt er aðgangur að síðu notanda takmarkaður við vinahóp hans á samfélagsmiðlinum og þarf notandi að samþykkja hverjir fá inngöngu í þann hóp. Slík aðgangsstilling þykir gefa til kynna að notkun síðunnar sé persónuleg. Velji notandi aftur á móti að hafa síðuna opna, án nokkurrar takmörkunar svo hún sé opin öllum notendum miðilsins og jafnvel öllum veraldarvefnum, er litið svo á að upplýsingar sem þar er deilt nái til

[252] Alþt. 1999-00, A-deild, bls. 2718.
[253] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 178.
[254] Henrik Udsen: *De informationsretlige grundsætninger*, bls. 201–202.

ótakmarkaðs fjölda fólks og á undanþágan því ekki við. Við slíkar aðstæður telst notandi að öllu jöfnu ábyrgðaraðili þeirra upplýsinga sem hann birtir.[255]

Hvað ef aðgangur að persónulegu síðu notanda er takmarkaður, en viðkomandi á það stóran vinahóp á samfélagsmiðlinum að persónuupplýsingar sem þar eru birtar gætu talist aðgengilegar óákveðnum fjölda fólks? Að mati 29. gr. starfshópsins getur fjöldi vinatengsla veitt vísbendingu um það hvort vinnsla notanda sé til persónulegra nota eða ekki og þykir stór vinahópur benda til þess að aðgangur að síðu notanda sé í raun ekki takmarkaður við afmarkaðan hóp.[256] Það liggur þó ekki fyrir hvað telst til *stórs vinahóps* og getur því reynst ómarkvisst að líta til vinafjölda notanda.[257] Jafnframt getur skipt máli *hvernig* notandi velur vinasambönd sín á samfélagsmiðlinum. Ef notandi bætir við sig vinatengslum óháð því hvort hann þekkir viðkomandi getur það haft sömu afleiðingar og ef síða hans væri opin.[258] Í nýlegum dómi Hæstaréttar, *Hrd. 20. nóvember 2014 (214/2014),* reyndi á birtingu efnis á Instagram og hvort hún tælist *opinber birting* í skilningi 2. mgr. 236. gr. almennra hegningarlaga nr. 19/1940, sem fjallar um ærumeiðandi ummæli. Stefndi hafði rúmlega 100 fylgjendur á Instagram og hafði þar birt ljósmynd sem talin var ærumeiðandi. Héraðsdómur féllst ekki á að um opinbera birtingu væri að ræða þar sem einungis þeir sem stefndi hafði fallist á að væru fylgjendur hans á síðunni hafi haft aðgang að myndinni. Var niðurstöðu héraðsdóms hins vegar snúið við af Hæstarétti en í dóminum segir að í rauninni munu myndirnar hafa verið aðgengilegar fyrir aðra notendur miðilsins, ekki einungis fylgjendur stefnda. Fjöldi fylgjenda hafði því ekki úrslitaáhrif á niðurstöðu Hæstaréttar.

Svo undanþága 2. málsl. 2. mgr. 3. gr. pul. eigi við þarf vinnslan að stefna að persónulegu markmiði. Þannig á undanþágan ekki við ef stefnt er að fjárhagslegum ávinningi með vinnslu persónuupplýsinganna. Til að auðvelda mat á því hvort vinnsla sé til persónulegra afnota er hægt að líta til mismunandi viðmiða. Í fyrsta lagi hvort persónuleg tengsl séu á milli hins skráða og þess notanda sem birtir upplýsingarnar. Einnig ber að líta til þess hvort persónuleg tengsl séu á milli notanda og móttakenda upplýsinganna.[259] Til dæmis gætu það talist persónuleg not upplýsinga þegar notandi deilir myndum frá fjölskyldumóti á lokaðri síðu sem einungis fjölskyldumeðlimir hafa aðgang að, en þar eru persónuleg tengsl bæði á milli notanda og þeirra skráðu og notanda og móttakenda.[260] Í öðru lagi er hægt að líta til tíðni og

[255] *Article 29 Working Party Opinion 5/2009 on online social networking,* bls. 6.
[256] *Article 29 Working Party Opinion 5/2009 on online social networking,* bls. 6.
[257] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 178.
[258] *Article 29 Working Party Opinion 5/2009 on online social networking,* bls. 6.
[259] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 4.
[260] Brendan Van Alsenoy o.fl.: „Social networks and web 2.0: are users also bound by data protection regulations?“, bls. 74.

umfangs persónuupplýsingavinnslu notanda, þ.e. hvort hún sé svo mikil að það gefi í skyn að um sé að ræða vinnslu sem ekki getur talist til persónulegra nota. Í þriðja lagi hvort notandi komi fram á samfélagsmiðli fyrir hönd hóp fólks, sem kemur saman á skipulagðan hátt.[261] Ef einstaklingur heldur úti síðu á samfélagsmiðli sem er hluti af kosningabaráttu tiltekins flokks er ekki um að ræða persónuleg afnot. Þá er ekki um að ræða persónuleg afnot ef notandi samfélagsmiðils kemur fram fyrir hönd fyrirtækis eða samtaka.[262]

Þegar vinnsla telst eingöngu vera til persónulegra nota fellur hún utan gildissviðs pul. Hvorki notandi né þjónustuaðili samfélagsmiðilsins eru þá ábyrgðaraðilar þeirra upplýsinga sem birtar eru, einfaldlega vegna þess að reglur persónuupplýsingalöggjafar eiga ekki við. Þá ber einnig að hafa aðrar undanþágur pul. í huga, en samkvæmt 5. gr. pul. má víkja frá ákvæðum laganna í þágu fjölmiðlunar, lista eða bókmennta. Í áliti 29. gr. starfshópsins 5/2009 um samfélagsmiðla segir að sambærileg undanþága tilskipunar 95/46/EB geti átt við um vinnslu notanda samfélagsmiðils á persónuupplýsingum.[263] Af *EBD, mál C-73/07, ECR 2008, bls. I-09831* (Satamedia) leiðir að vettvangur persónuupplýsingavinnslu sker ekki úr um það hvort vinnsla sé undanþegin ákvæðum persónuupplýsingalöggjafar í þágu fjölmiðlunar. Í niðurstöðu Evrópudómstólsins segir:

> […] account must be taken of the evolution and proliferation of methods of communication and the dissemination of information. As was mentioned by the Swedish Government in particular, the medium which is used to transmit the processed data, whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken 'solely for journalistic purposes'.

Því virðist sem ekki sé útilokað að beita undanþágu 5. gr. pul. um vinnslu persónuupplýsinga á samfélagsmiðlum, svo lengi sem hún fer einvörðungu fram í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi. Í slíkum tilfellum þarf að meta hvort vegi þyngra – réttur þess skráða til að njóta friðhelgi einkalífs eða tjáningarfrelsi notanda.[264]

Sé efnið ekki talið til persónulegra nota og aðrar undanþágur pul. eiga ekki við, telst notandi ábyrgðaraðili þeirra upplýsinga sem hann deilir. Sé hann búsettur á Íslandi, ber honum því að uppfylla skilyrði pul. þegar unnið er með persónuupplýsingar annarra. Að gera slíkar kröfur til samfélagsmiðlanotenda hefur verið gagnrýnt fyrir að vera bæði óraunhæft og íþyngjandi, en um það er fjallað nánar í kafla 6.3.1.

---

[261] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 4.
[262] Henrik Udsen: *De informationsretlige grundsætninger*, bls. 201.
[263] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 6.
[264] Um árekstra tjáningarfrelsis og friðhelgi einkalífs vísast til Björg Thorarensen: *Stjórnskipunarréttur - mannréttindi*, bls. 305-308.

6.1.2 Þjónustuaðili

Þjónustuaðili er sá sem rekur og heldur úti samfélagsmiðli og veitir þá þjónustu sem miðillinn hefur uppá að bjóða. Hann ákveður tilgang og markmið þeirrar persónuupplýsingavinnslu sem þar fer fram og annast grundvallaratriði þjónustunnar, s.s. að skrá notendur og eyða aðgangi þeirra, sé þess óskað. Þjónustuaðili tekur jafnframt ákvarðanir um það hvernig persónuupplýsingar notenda eru unnar frekar, t.d. hvernig þær eru skráðar, geymdar eða miðlað áfram og að hvaða marki slíkar upplýsingar geta verið notaðar í markaðssetningarskyni af þriðja aðila. Af þessu leiðir að þjónustuaðili er ábyrgðaraðili að vinnslu sem fer fram á persónuupplýsingum notenda sem þeir hafa sjálfir deilt á sinni eigin persónulegu síðu.[265] Hefur þetta einnig verið staðfest í framkvæmd í Noregi, en í *úrskurði norsku kærunefndarinnar Personvernnemnda 23. október 2012 (PVN-2012-03)* (Nettby) var sá aðili sem rak norska samfélagsmiðilinn Nettby talinn ábyrgðaraðili frekari vinnslu þeirra upplýsinga sem notendur höfðu deilt á miðlinum. Samfélagsmiðillinn Nettby hafði verið lagður niður en þjónustuaðili miðilsins hafði hug á að geyma persónuupplýsingar notenda. Bar hann fyrir sig að upplýsingarnar myndu veita innsýn í líf ungs fólks á árunum 2006-2010 og vistun upplýsinganna væri því í sagnfræðilegum tilgangi. Á þetta var ekki fallist og þjónustuaðila gert að eyða upplýsingunum í ljósi þess að hann væri ábyrgðaraðili frekari vinnslu upplýsinganna.

Þjónustuaðili hefur almennt ekki ákvörðunarvald um það hvað sé birt á miðlinum, þar sem það eru notendur miðilsins sem taka ákvörðun um hverju þeir deila með öðrum og bera þeir því ábyrgð á þeirri vinnslu sem felst í því að deila upplýsingum, líkt og fram hefur komið.[266] Með mikilli einföldun má segja að notandi beri ábyrgð á fyrri hluta vinnslu, þ.e. að deila persónuupplýsingum á samfélagsmiðli, á meðan þjónustuaðili ber ábyrgð á seinni hluta vinnslu, þ.e. vinnsla sem á sér stað eftir að upplýsingunum hefur verið deilt.

6.1.3 Viðbótarforrit

Á samfélagsmiðlum er oft að finna ákveðin viðbótarforrit við samfélagsmiðilinn sjálfan, s.s. leikja-, keppnis- og stefnumótaforrit. Slíkar viðbætur geta safnað persónuupplýsingum þeirra notenda sem nota þær. Þegar viðbótarforrit er tekið í notkun, t.d. á Facebook, samþykkir notandi að veita viðbótinni aðgang að tilteknum persónuupplýsingum sínum. Samkvæmt áliti 29. gr. starfshópsins nr. 5/2009 um samfélagsmiðla getur starfrækjandi viðbótarinnar talist

[265] *Article 29 Working Party Opinion 5/2009 on online social networking,* bls. 5.
[266] Þjónustuaðilinn getur þó ákveðið að nauðsynlegt sé að veita tilteknar upplýsingar til þess að gerast notandi samfélagsmiðilsins. Til dæmis gerir Facebook það að skilyrði að notendur gefi upp nafn, netfang, fæðingardag og kyn.

ábyrgðaraðili þeirra persónuupplýsinga sem forritið vinnur með.[267] Í sama áliti er lögð áhersla á að samfélagsmiðlar tryggi að viðbótarforrit þeirra fullnægi skilyrðum tilskipunar 95/46/EB. Ekki verður fjallað frekar um starfsemi viðbótarforrita, þar sem oft getur verið um mjög tæknileg atriði að ræða, sem óþarft er að lýsa hér.

6.2 Lagaumhverfi þjónustuaðila

Eitt megineinkenni samfélagsmiðla er alþjóðlegt eðli þeirra. Notendur eru dreifðir um allan heim og þjónusta samfélagsmiðils er líkleg til að vera veitt frá nokkrum mismunandi stöðum. Getur því reynst flókið að ákveða lög hvaða ríkis gilda um þá vinnslu persónuupplýsinga sem þjónustuaðilar samfélagsmiðla taka sér fyrir hendur. Verður hér leitast við að svara þeirri spurningu. Vísað verður til ákvæða tilskipunar 95/46/EB frekar en pul., þar sem viðfangsefni kaflans er að afmarka lög hvaða ríkis gilda um vinnslu þjónustuaðila en ekki að fjalla um afmörkuð ákvæði laga nr. 77/2000.

Gildissvið tilskipunar 95/46/EB veltur á því hvar ábyrgðaraðili vinnslu hefur staðfestu, en ef vinnsla fellur undir gildissvið tilskipunar 95/46/EB ber að beita þeim landslögum þar sem ábyrgðaraðili hefur staðfestu, sbr. 4. gr. tilskipunarinnar. Um vinnslu notanda gilda því lög þess ríkis þar sem hann hefur búsetu. Hafi þjónustuaðili staðfestu í aðildarríki EES fellur vinnsla hans án efa undir gildissvið landslaga þess aðildarríkis þar sem hann hefur staðfestu, en hafi þjónustuaðili staðfestu utan EES reynist það flóknara að meta hvaða lög eiga við hverju sinni. Tvær leiðir eru færar til þess að fella vinnslu þjónustuaðila sem hefur staðfestu utan EES undir evrópsk persónuupplýsingalög. Annars vegar kemur c-liður 1. mgr. 4. gr. tilskipunar 95/46/EB til álita og hins vegar a-liður sömu greinar.

Þótt ábyrgðaraðili hafi ekki staðfestu innan EES-svæðisins fellur vinnsla hans á persónuupplýsingum undir gildissvið evrópskrar persónuupplýsingalöggjafar noti hann *búnað* sem staðsettur er á yfirráðasvæði aðildarríkis EES til að vinna upplýsingarnar, sbr. c-liður 1. mgr. 4. gr. tilskipunar 95/46/EB. Að mati 29. gr. starfshópsins geta tölvur og smygildi talist til búnaðar í skilningi ofangreinds ákvæðis tilskipunarinnar. Samkvæmt starfshópnum er um að ræða notkun búnaðar á yfirráðarsvæði EES-ríkis þegar vefsíða með staðfestu utan EES vistar smygildi á tölvu einstaklings sem búsettur er innan EES. Sú vinnsla persónuupplýsinga sem fer fram á vefsíðunni á því að uppfylla skilyrði landslaga þess ríkis þar sem tölvan er staðsett, jafnvel þótt vefsíðan sé staðsett utan EES.[268] Mjög algengt er að samfélagsmiðlar notist við smygildi, en sem dæmi má líta til gagnanotkunarstefnu Facebook, sem segir að notast sé við

[267] *Article 29 Working Party Opinion 5/2009 on online social networking,* bls. 5
[268] Christopher Kuner: *European Data Protection Law*, bls. 123.

smygildi til þess að safna persónuupplýsingum um notendur.[269] Á grundvelli rúmrar túlkunar 29. gr. starfshópsins á hugtakinu *búnaður* ber samfélagsmiðli sem vistar smygildi í tölvu notanda, sem búsettur er innan EES, að uppfylla skilyrði persónuupplýsingalaga þess ríkis þar sem notandinn er búsettur.[270] Við þetta verður þó að setja ákveðinn fyrirvara. Sú nálgun, að líta á smygildi sem búnað, hefur verið harðlega gagnrýnd fyrir það að veita tilskipun 95/46/EB og persónuupplýsingalögum EES-ríkja of rúmt gildissvið. Í ljósi þess hversu margar vefsíður notast við smygildi, leiðir nálgunin í raun til þess að Evrópureglur um vernd persónuupplýsinga gilda um allt Internetið. Með þessari nálgun telur Christopher Kuner að gildissvið Evrópureglna sé teygt alltof langt og að það sé óraunhæft og íþyngjandi fyrir ábyrgðaraðila, sem heldur úti vefsíðu utan EES, að þurfa að uppfylla skilyrði landslaga í hverju EES-ríki þar sem vefsíðan er notuð.[271] Ritgerðarhöfundur tekur undir gagnrýni Kuner að vissu leyti, en þó skal hafa í huga að ef Evrópureglur eru ekki látnar gilda við þessar aðstæður er hætta á að ábyrgðaraðilar eltist við hentug varnarþing (e. *forum shopping*), þ.e. að aðilar leitist við að halda viðskiptum sínum innan þeirrar lögsögu sem hentar þeim best. Til þess að forðast persónuupplýsingalöggjöf aðildarríkja EES gætu fyrirtæki einfaldlega flutt starfsemi sína út fyrir EES-svæðið.[272]

Ofangreint álitamál, um beitingu búnaðar og hvað teljist til búnaðar yfirhöfuð, er dæmi um þá óvissu sem ríkir við beitingu tilskipunar 95/46/EB þegar flóknar tækninýjungar eiga í hlut. Í nýrri reglugerðartillögu framkvæmdastjórnar ESB er ekki gert ráð fyrir ákvæði sem kveður á um gildissvið löggjafarinnar á grundvelli búnaðarnotkunar. Það þýðir þó ekki að ábyrgðaraðilar utan EES sleppi að fullu undan evrópulöggjöf á sviði persónuverndar. Reglugerðartillagan gerir ráð fyrir mun rýmra landfræðilegu gildissviði löggjafarinnar gagnvart fyrirtækjum sem hafa staðfestu utan ESB, en selja vöru eða þjónustu innan svæðisins. Fyrirhugaðar breytingar á persónuupplýsingalöggjöf ESB gætu því auðveldað mat á því hvaða lög eiga við hverju sinni. Um fyrirhugaðar breytingar á landfræðilegu gildissviði persónuupplýsingalöggjafar ESB er fjallað nánar í kafla 7.

Þótt skiptar skoðanir séu um beitingu c-liðar 1. mgr. 4. gr. tilskipunar 95/46/EB við vinnslu persónuupplýsinga á samfélagsmiðlum, getur a-liður 1. mgr. 4. gr. tilskipunarinnar átt við um slíka vinnslu. Af a-lið 1. mgr. 4. gr. tilskipunar 95/46/EB leiðir að ef vinnsla persónuupplýsinga fer fram í tengslum við starfsemi ábyrgðaraðila á yfirráðasvæði

[269] „Cookies, pixels and similar technologies“, https://www.facebook.com/help/cookies/update.
[270] *Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines*, bls. 9–11 og *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 5.
[271] Christopher Kuner: *European Data Protection Law*, bls. 123–127.
[272] *Social Network Services and Privacy – a case study of Facebook*, bls. 37.

aðildarríkis EES, skal beita persónuupplýsingalögum þess ríkis. Svo það sé hægt í tilfelli samfélagsmiðla verður það fyrirtæki er heldur úti miðlinum (þ.e. þjónustuaðili) að vera með virka og raunverulega starfsemi með föstu fyrirkomulagi innan EES, sem annast vinnslu persónuupplýsinga í tengslum við starfsemi fyrirtækisins.[273] Rekstrarform slíkrar starfsemi hefur ekki úrslitaáhrif á það hvort starfsemin uppfylli skilyrði a-liðar 1. mgr. 4. gr. tilskipunarinnar, heldur skiptir meginmáli að sú vinnsla persónupplýsinga sem fer fram innan EES fari fram í *tengslum* við starfsemi fyrirtækis ábyrgðaraðila og að starfsemin sé virk og með föstu fyrirkomulagi (þ.e. að starfsemin hafi staðfestu innan EES). Þetta getur t.d. átt við ef þjónustuaðili starfrækir skrifstofu í aðildarríki EES sem ber ábyrgð á samskiptum við notendur samfélagsmiðilsins í þeirri lögsögu.[274]

Facebook hefur sérstakar starfstöðvar innan EES og eru þær staðsettar í Írlandi. Í þjónustuskilmálum Facebook segir að sé notandi búsettur utan Bandaríkjanna eða Kanada sé samningur gerður á milli notanda og Facebook Ireland Limited, en ekki Facebook Inc., sem hefur staðfestu í Bandaríkjunum.[275] Facebook Ireland Limited er því ábyrgðaraðili vinnslu á persónuupplýsingum notenda sem búsettir eru innan EES og eiga írsk persónuupplýsingalög við um þá vinnslu persónuupplýsinga sem Facebook framkvæmir.[276] Telji einstaklingur, búsettur á Íslandi, á sér brotið með vinnslu upplýsinga á Facebook, er því ekki útilokað að hann þurfi að snúa sér til persónuverndarstofnunarinnar á Írlandi.[277] Tilskipun 95/46/EB hefur verið innleidd í írsk persónuupplýsingalög og ná reglur tilskipunarinnar því til vinnslu sem Facebook framkvæmir á persónuupplýsingum aðila sem búsettir er innan EES.[278]

Samkvæmt Christopher Kuner hefur a-liður 1. mgr. 4. gr. tilskipunar 95/46/EB meira vægi en c-liður 1. mgr. 4. gr. tilskipunarinnar sem grundvöllur fyrir landfræðilegu gildissviði hennar.[279] Er það í samræmi við erfiðleika við beitingu c-liðar vegna túlkunar á búnaðarhugtakinu. Við mat á því hvaða lög gilda um vinnslu persónuupplýsinga af hálfu þjónustuaðila ber því fyrst og fremst að líta til þess hvort þjónustuaðilinn hafi staðfestu innan EES í skilningi a-liðar. Ef svo er ekki er hægt að færa rök fyrir því að notkun þjónustuaðila á

[273] Sjá 19. lið formála tilskipunar 95/46/EB, sem hefur að geyma útskýringu á því hvað átt sé við með „staðfestu“ í skilningi 4. gr. tilskipunarinnar.
[274] *Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines*, bls. 10.
[275] Í 1. mgr. 18. gr. þjónustuskilmálanna segir: „If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to “us,” “we,” and “our” mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.“ Sjá nánar https://www.facebook.com/legal/terms/update.
[276] Peter Blume: *Databeskyttelsesret*, bls. 380.
[277] „Óvíst hvað á að gera við skepnuna Facebook“, http://www.visir.is.
[278] Peter Blume og Janne Rothmar Herrmann: *Ret, privatliv og teknologi*, bls. 114–115.
[279] Christopher Kuner: *European Data Protection Law*, bls. 117.

búnaði í merkingu c-liðar væri til þess að hann ætti að uppfylla skilyrði persónuupplýsingalöggjafar þess ríkis þar sem notandi er búsettur.

6.3 Ábyrgð og skyldur ábyrgðaraðila á samfélagsmiðlum

Sem ábyrgðaraðila ber notanda, þjónustuaðila og þriðja aðila sem rekur viðbótarforrit að sjá til þess að vinnsla á persónuupplýsingum á samfélagsmiðli standist kröfur persónuupplýsingalöggjafar og að gætt sé að réttindum þess skráða. Hver og einn ábyrgðaraðili ber þó ábyrgð á mismunandi þáttum þeirrar vinnslu sem fer fram á miðlinum. Til hægðarauka hefur þessum kafla verið skipt upp í umfjöllun um fyrri hluta vinnslu, þ.e. sú vinnsla sem felst í því að deila upplýsingum á samfélagsmiðli, og seinni hluta vinnslu, þ.e. öll frekari vinnsla á upplýsingum sem þegar hefur verið deilt.

6.3.1 Dreifing efnis – fyrri hluti vinnslu

Þegar meðferð notanda samfélagsmiðils á persónuupplýsingum fellur undir gildissvið laga nr. 77/2000 ber hann ábyrgð á því að uppfylla skilyrði laganna.[280] Verður hann að sjá til þess að skilyrði 8. gr. og eftir atvikum 9. gr. pul. séu uppfyllt, áður en hann deilir persónuupplýsingum þriðja aðila með öðrum notendum síðunnar. Notandi ætti því að leggja það í vana sinn að fá samþykki þeirra sem persónuupplýsingarnar varða áður en hann deilir þeim, svo heimild sé fyrir vinnslunni sbr. 1. tölul. 1. mgr. 8. gr. og 1. tölul. 1. mgr. 9. gr. pul.[281] Jafnframt verður hann að sjá til þess að birting á persónuupplýsingum annarra sé í samræmi við meginreglur 7. gr. pul. um gæði gagna og vinnslu, þ.á.m. að birtingin sé framkvæmd með sanngjörnum, málefnalegum og lögmætum hætti og að upplýsingarnar séu fengnar í yfirlýstum, skýrum og málefnalegum tilgangi og séu ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Ennfremur á notandi að gæta að réttindum þess skráða, s.s. upplýsingarétti hans, rétti hans til aðgangs að upplýsingum um sjálfan sig og réttinum til leiðréttingar og eyðingar persónuupplýsinga, sé þess óskað.

Það virðist þó fjarri raunveruleikanum að notendur samfélagsmiðils á borð við Facebook fari í gegnum ofangreindar reglur pul. áður en þeir deila upplýsingum á sínum eigin síðum. Jafnframt þykir það ólíklegt að notendur líti á sjálfa sig sem ábyrgðaraðila í skilningi pul., þótt í lagalegum skilningi sé því ekkert til fyrirstöðu að þeir gegni því hlutverki.[282] Um þetta segir í áliti forstöðumanns Evrópsku persónuverndarstofnunarinnar um eflingu trausts í upplýsingasamfélaginu:

[280] Hér er gert ráð fyrir að notandi sé búsettur á Íslandi og því fjallað um ákvæði pul. Sé notandi búsettur í öðru ríki innan EES gilda landslög þess ríkis.
[281] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 3.
[282] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 187–188.

> Unfortunately, there is a gap between legal requirements and actual compliance. Whereas legally speaking Internet users are considered data controllers and are bound by the EU data protection and privacy legal framework, in reality, they are often unaware of this role. Generally speaking they have a poor understanding that they are processing personal data and that there are privacy and data protection risks involved in publishing such information. Young people in particular post content online underestimating the consequences for them and others, for example, in the context of subsequent enrolment in educational institutions or applications for jobs.[283]

Notendur Facebook gera sér almennt ekki grein fyrir því að með því einu að birta mynd og merkja þá sem þar koma fram, gætu þeir verið að brjóta í bága við persónuupplýsingalög.[284]

Annað álitamál er hvernig fylgja skuli eftir brotum einstaklinga á ákvæðum pul. við notkun samfélagsmiðla. Á heimasíðu danska Datatilsynet er að finna ráðleggingar handa þeim sem telja á sér brotið vegna dreifingu persónuupplýsinga sinna á samfélagsmiðli. Þar er ráðlagt að hafa fyrst samband við þann aðila sem birti persónuupplýsingarnar, þar sem hann ber ábyrgð á dreifingu þeirra, og krefjast þess að upplýsingunum sé eytt. Ef ábyrgðaraðilinn verður ekki við slíkri beiðni getur Datatilsynet mögulega aðstoðað viðkomandi, ef ábyrgðaraðilinn er á annað borð búsettur í Danmörku.[285] Viðkomandi gæti einnig leitað til dómstóla. Það hringir þó ákveðnum viðvörunarbjöllum. Ef hver og einn notandi samfélagsmiðils telst vera ábyrgðaraðili þeirra upplýsinga sem hann birtir opnar það dyr dómstóla fyrir fjölda mála á milli einstaklinga, sem mögulega væri hægt að leysa án aðkomu dómstóla, t.d. með því að leggja ríkari ábyrgð á þjónustuaðila.[286]

Í fljótu bragði virðist ekki vera mjög raunhæft að láta notendur bera fulla ábyrgð á því sem þeir birta á samfélagsmiðlum. Umhugsunarvert er hvort hægt sé að fara aðra leið í þessum efnum, t.d. með því að koma ábyrgð á fyrri hluta vinnslu yfir á þjónustuaðila samfélagsmiðils í stað notanda. Af þeim ástæðum ber að athuga hvort þjónustuaðili geti undir einhverjum kringumstæðum borið ábyrgð á því sem notendur birta á miðlinum.

Í skýrslu um persónuvernd á samfélagsmiðlum, sem tekin var saman af Alþjóðlega starfshópnum um fjarskipti[287], er mælt með því að regluverk það sem lítur að ábyrgð á persónuupplýsingavinnslu skuli endurhugsað, með það að markmiði að færa frekari ábyrgð á

---

[283] *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, liður 76.
[284] Hér ber að minna á ákvæði laga nr. 77/2000 sem geta undanþegið notanda samfélagsmiðils frá ákvæðum laganna. Er um að ræða 2. málsl. 2. mgr. 3. gr. pul. um persónuleg afnot og 5. gr. pul. um fjjölmiðlun, listir eða bókmenntir.
[285] „Persondataloven og sociale netværk“, http://www.datatilsynet.dk.
[286] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 187–189.
[287] Oft nefndur „Berlínarstarfshópurinn“.

herðar þjónustuaðila samfélagsmiðla.[288] Peter Blume hefur jafnframt gefið í skyn að gera megi ríkari kröfur til þjónustuaðila samfélagsmiðla, heldur en til umsjónarmanna hefðbundinna vefsíðna, um að efni sem þar birtist brjóti ekki í bága við lög. Hann tekur þó einnig fram að forðast skuli að gera þjónustuaðila að fullu ábyrga fyrir vinnslu notanda, þar sem slík ábyrgð myndi gera það nánast ómögulegt að reka samfélagsmiðil, en það myndi krefjast þess að þjónustuaðili gengi úr skugga um að hver og ein einasta færsla allra notenda stæðist ákvæði persónuupplýsingalaga.[289]

Í áliti 29. gr. starfshópsins nr. 5/2009 um samfélagsmiðla er sérstaklega kveðið á um mikilvægi þess að þeir skráðu geti leitað réttar síns samkvæmt persónuupplýsingalögum hjá samfélagsmiðlinum sjálfum. Má þar nefna rétt þeirra skráðu til aðgangs að þeim upplýsingum sem samfélagsmiðilinn hefur um viðkomandi sbr. 1. mgr. 18. gr. pul. og rétt á eyðingu persónuupplýsinga, séu þær skráðar án tilskilinnar heimildar sbr. 1. mgr. 25. gr. pul.[290] Líta má svo á að þjónustuaðili sé betur til þess fallinn að gæta að þessum réttindum heldur en notandi samfélagsmiðilsins. Til dæmis hafa samfélagsmiðlar á borð við Facebook notast við ákveðið tilkynningakerfi (e. *report system*) sem gerir notendum kleift að tilkynna þjónustuaðila að persónuupplýsingar hafi verið birtar án samþykkis viðkomandi.

Reglugerðartillaga framkvæmdastjórnar ESB, sem er hluti af fyrirhugaðri breytingu á persónuupplýsingalöggjöf sambandsins, kveður sérstaklega á um að þótt einstaklingar séu undanþegnir ákvæðum persónuupplýsingalöggjafar vegna persónulegra nota nái undanþágan ekki til ábyrgðar- og vinnsluaðila sem halda úti því svæði eða þeim vettvangi þar sem vinnslan á sér stað.[291] Sé breyting reglugerðartillögunnar heimfærð uppá samfélagsmiðla yrði þjónustuaðili að gæta þess að farið sé að lögum við persónuupplýsingavinnslu á miðlinum, þótt notandi sé undanþeginn slíkri ábyrgð. Er þetta breyting frá núverandi ástandi, þar sem persónuleg afnot einstaklings á persónuupplýsingum leiða til þess að ákvæði persónuupplýsingalöggjafar eiga ekki við um þá tilteknu vinnslu í heild sinni og eiga lögin þá hvorki við um notanda samfélagsmiðils né þjónustuaðila miðilsins.[292]

---

[288] *Report and Guidance on Privacy in Social Network Services*, bls. 4–5.
[289] Peter Blume: *Persondataretten – nu og i fremtiden*, bls. 186 og 188–189.
[290] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 11.
[291] *Proposal for a General Data Protection Regulation*, COM/2012/11/FINAL. Í 15. lið formálans segir: „This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The *exemption should also not apply* to controllers or processors which provide the means for processing personal data for such personal or domestic activities."
[292] Þess ber að geta að hér er einungis um að ræða fyrri hluta vinnslu. Þegar þjónustuaðili fer með ákvörðunarvald um vinnslu og gegnir hlutverki ábyrgðaraðila á persónuupplýsingalöggjöf við um þann vinnsluþátt.

Af ofangreindu virðist sem ákveðin þróun sé að eiga sér stað í átt að aukinni ábyrgð þjónustuaðila samfélagsmiðils. Bæði hafa starfshópar mælt með slíkri þróun og 15. liður reglugerðartillögu framkvæmdastjórnar ESB felur í sér að þjónustuaðilar verða ekki undanþegnir ákvæðum reglugerðarinnar þótt notendur samfélagsmiðla njóti góðs af undanþágu vegna persónulegra nota. Þegar hinn skráði telur brotið á rétti sínum samkvæmt ákvæðum pul. virðist hin almenna nálgun vera sú að ef notandi sem birti persónuupplýsingarnar verður ekki við beiðni þess skráða um að fjarlægja þær geti viðkomandi leitað til þjónustuaðilans sjálfs, t.d. með þar til gerðu tilkynningakerfi. Falli vinnsla notanda undir gildissvið pul. á aukin ábyrgð þjónustuaðila ekki að leiða til þess að notandinn sjálfur beri enga ábyrgð á því sem hann birtir, þar sem á honum hvílir enn sú skylda að deila ekki persónuupplýsingum annarra, nema að uppfylltum skilyrðum 7., 8. og eftir atvikum 9. gr. pul. Hvort hægt sé að gera slíkar kröfur til einstaklings er þó álitaefni út af fyrir sig, en ekki verður fjallað um það nánar hér.

6.3.2 Frekari vinnsla – seinni hluti vinnslu

Þegar upplýsingar hafa verið birtar af notendum á samfélagsmiðli er það undir þjónustuaðila komið hvernig þær eru unnar frekar og ber honum að gæta þess að öll frekari vinnsla, s.s. skráning, flokkun, varðveisla og miðlun upplýsinganna uppfylli skilyrði þeirrar persónuupplýsingalöggjafar sem á við hverju sinni.[293] Þjónustuaðili ákveður einnig hvaða upplýsingum skuli safnað svo hægt sé að stofna aðgang að síðunni og ber söfnun slíkra upplýsinga að uppfylla skilyrði persónuupplýsingalaga.

Líkt og notanda samfélagsmiðilsins ber þjónustuaðila að uppfylla skilyrði 8. gr. og eftir atvikum 9. gr. pul. Með því að skrá sig sem notanda miðils og samþykkja skilmála þjónustunnar veitir einstaklingur að öllu jöfnu samþykki sitt fyrir vinnslu persónuupplýsinga sinna og veitir þar af leiðandi þjónustuaðila heimild til vinnslunnar á grundvelli 1. tölul. 1. mgr. 8. gr. og eftir atvikum 1. tölul. 1. mgr. 9. gr. pul., ef um viðkvæmar persónuupplýsingar er að ræða.

Því fleiri persónuupplýsingum sem þjónustuaðili safnar, þeim mun hærri eru tekjur samfélagsmiðilsins vegna möguleika á sölu *markvissra* auglýsingaplássa. Í því felst að auglýsingum er beint að notanda á grundvelli þekkingar miðilsins á viðkomandi, þar með talið aldur hans, kyn, búseta og upplýsingar um notandann sem safnað er með smygildum.[294] Það er því hætta á því að samfélagsmiðill freistist til að safna upplýsingum umfram það sem

[293] Verður hér vísað til ákvæða pul.
[294] *Álit neytendastofnana á Norðurlöndunum varðandi markaðssetningu í samskiptamiðlum,* bls. 3.

nauðsynlegt getur talist. Þjónustuaðila ber þó skylda til að fara eftir meginreglum 7. gr. pul. um gæði gagna og gæta þess að ekki sé gengið of langt í upplýsingasöfnun. Í því samhengi hefur 29. gr. starfshópurinn fært rök fyrir því að þjónustuaðili geti ekki skyldað notendur til að gefa upp raunverulegt nafn sitt, heldur eigi notendum samfélagsmiðla að vera heimilt að nota dulnefni.[295]

Í samræmi við 20. gr. pul. ber þjónustuaðila að upplýsa notendur sína um hver hann er og í hvaða tilgangi upplýsingar notenda eru unnar. Mikilvægt er að þjónustuaðili upplýsi notendur um það þegar persónuupplýsingar þeirra eru notaðar til beinnar markaðssetningar eða þeim miðlað til þriðja aðila. Jafnframt ber þjónustuaðila að upplýsa notendur um hvernig persónuleg síða þeirra er unnin og hvaðan þjónustuaðili fær frekari upplýsingar um notendur.[296] Á grundvelli fræðsluskyldu ábyrgðaraðila hefur 29. gr. starfshópurinn einnig ráðlagt samfélagsmiðlum að vara notendur við þeirri hættu sem það getur haft í för með sér að deila persónuupplýsingum á samfélagsmiðlinum. Ber þjónustuaðila m.a. að fræða notendur um það að birting á persónuupplýsingum annarra í leyfisleysi, þ.e. án samþykkis viðkomandi, geti varðað við lög. Þjónustuaðilar ættu því að mæla með því við notendur að fá samþykki frá viðkomandi áður en þeir deila frekari upplýsingum um hann.[297]

Þegar einstaklingur ákveður að stofna aðgang að samfélagsmiðli þarf hann að gefa upp ákveðnar persónuupplýsingar eins og nafn, netfang og fæðingardag. Ef þjónustuaðili gerir aðila kleift að gefa upp viðkvæmar upplýsingar, t.d. um kynhneigð og stjórnmálaskoðanir, ber þjónustuaðila að taka það skýrt fram að aðila sé ekki skylt að svara slíkum spurningum.[298] Á grundvelli 11. gr. pul. um öryggi persónuupplýsinga, ber þjónustuaðila að tryggja það að staðlaðar notendastillingar taki mið af persónuvernd (e. *privacy-friendly default settings*). Staðlaðar notendastillingar ættu að vera þannig úr garði gerðar að aðgangur að persónulegu síðu notanda sé takmarkaður við þá aðila sem notandi hefur sjálfur samþykkt að skuli hafa aðgang að síðunni.[299]

Síðast en ekki síst ber þjónustuaðila skylda til að eyða aðgangi notanda, sé þess óskað.

---

[295] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 11.
[296] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 7.
[297] Þess má geta að í 9. tölul. 5. gr. þjónustuskilmála Facebook segir „You will not tag users or send email invitations to non-users without their consent. Facebook offers social reporting tools to enable users to provide feedback about tagging.“ Ákvæði þetta bannar þó ekki birtingu ljósmynda, heldur það eitt að merkja einstakling án samþykkis viðkomandi. Sjá nánar „Statement of Rights and Responsibilities“, http://www.facebook.com/legal/terms.
[298] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 7.
[299] *Article 29 Working Party Opinion 5/2009 on online social networking*, bls. 6-7.

6.4 Samfélagsmiðill sem vinnsluaðili

Eins og gerð hefur verið grein fyrir fer afmörkun á hlutverki aðila, sem kemur að vinnslu persónuupplýsinga, eftir því verkefni sem hann sinnir hverju sinni. Hlutverk viðkomandi samkvæmt persónuupplýsingalögum er ekki tengt tiltekinni manneskju eða tilteknum lögaðila, heldur er það tengt því hlutverki sem viðkomandi gegnir við vinnsluna. Hér að ofan hefur einungis verið horft á hlutverk þjónustuaðila samfélagsmiðils sem *ábyrgðaraðili* þeirra upplýsinga sem þar er að finna. Danska Datatilsynet hefur aftur á móti bent á að samfélagsmiðill geti einnig verið vinnsluaðili persónuupplýsinga.

> *Bréf Datatilsynet 8. nóvember 2013 (2013-321-0173)* (Stjórnvald á Facebook). Með bréfi þessu veitti Datatilsynet stjórnvaldi nokkru leiðbeiningar um hvaða reglur það þyrfti að hafa í huga við fyrirhugaða notkun þess á samfélagsmiðlunum Facebook og Twitter. Datatilsynet tók fram að notkun einstaklinga á samfélagsmiðlum sem er persónulegs eðlis félli almennt ekki undir gildissvið persónuupplýsingalaga, en aðstæður væru þó öðruvísi þegar um væri að ræða notkun stjórnvalds á slíkum miðli. Vinnsla stjórnvaldsins á persónuupplýsingum á samfélagsmiðlinum yrði því að uppfylla skilyrði danskra persónuupplýsingalaga. Datatilsynet taldi líkur á því að vinnsla persónuupplýsinga gæti átt sér stað í skilaboðum sem stjórnvaldið fengi frá almenningi í gegnum skilaboðakerfi Facebook. Við slíkar aðstæður taldi Datatilsynet að stjórnvaldið væri ábyrgðaraðili þeirra upplýsinga sem væri að finna í skilaboðunum, en Facebook væri vinnsluaðili fyrir hönd stjórnvaldsins. Skilaboðin væru vistuð hjá Facebook, en ekki hjá sjálfu stjórnvaldinu og bæri stjórnvaldinu því að hafa í huga þær kröfur sem persónuupplýsingalögin gera til notkun vinnsluaðila, t.a.m. um gerð vinnslusamnings.

Hér virðist sem Datatilsynet líti svo á að ef til þess kæmi að stjórnvaldið notaði Facebook til að vera í samskiptum við almenna borgara væri Facebook vinnsluaðili þeirra persónuupplýsinga sem kæmu fram í skilaboðum til stjórnvaldsins. Það verður að teljast varhugavert að stjórnvald noti Facebook til að vera í beinum samskiptum við borgara og lagði Datatilsynet því einnig til við stjórnvaldið að athuga hvort hægt væri að veita fyrirhugaða þjónustu til almennings, án þess að það myndi skapast möguleiki á að senda stjórnvaldinu skilaboð sem gætu innihaldið persónuupplýsingar.

Hér er einnig umhugsunarvert hvort samfélagsmiðill sé vinnsluaðili þeirra upplýsinga sem notendur birta á miðlinum. Í tilfelli Facebook ákveður notandi hvaða upplýsingar hann birtir og í hvaða tilgangi og hann velur Facebook sem miðil til að birta efnið. Því mætti líta á Facebook sem vinnsluaðila fyrri hluta vinnslu. Um leið og Facebook vinnur upplýsingarnar nánar verður Facebook ábyrgðaraðili þeirrar tilteknu vinnslu. Hér verður þó ekki tekin endanleg afstaða til þessa álitaefnis, en þess má geta að í yfirstandandi hópmálsókn gegn Facebook sem höfðuð er fyrir austurrískum dómstólum, hefur stefnandi fært rök fyrir því að Facebook sé vinnsluaðili fyrri hluta vinnslu, þ.e. ákvörðun notanda um að deila

persónuupplýsingum. Málið hefur ekki enn verið tekið fyrir, en áhugavert verður að fylgjast með þróun þess.[300]

6.5 Hvað má betur fara?

Með undanþágu vegna persónulegra nota persónuupplýsinga var lagt upp með að koma í veg fyrir afskipti persónuverndarstofnana og persónuupplýsingalöggjafar af slíkri vinnslu. Frá gildistöku tilskipunar 95/46/EB árið 1995 hefur persónuleg vinnsla einstaklinga á upplýsingum orðið mun umfangsmeiri. Er hún ekki lengur bundin við einfalda hluti s.s. dagbækur eða lista yfir símanúmer og heimilisföng vina og ættingja, heldur hefur vettvangur fyrir slíka vinnslu myndast á samfélagsmiðlum og Internetinu í heild sinni. Á samfélagsmiðlum getur reynst flókið að ákvarða hvort vinnsla notanda sé eingöngu ætluð til persónulegra nota. Eins og fram hefur komið er litið til aðgangsstýringar og vinafjölda viðkomandi og ef mat á þeim þáttum bendir til þess að deiling persónuupplýsinga jafnist á við opinbera birtingu þeirra, leiðir það til þess að umrædd undanþága eigi ekki við og ætti persónuupplýsingalögum því að vera beitt fullum fetum um birtingu notanda á upplýsingum.

Of þröng túlkun á því hvað teljist til *persónulegra nota* getur leitt til þess að reglur á sviði persónuverndar séu látnar gilda um efni sem í raun og veru er persónulegt og ekki notað í öðrum tilgangi en til einkanota. Getur það haft í för með sér skerðingu á tjáningarfrelsi notanda, ef honum er t.d. gert að fjarlægja efni af persónulegri síðu sinni vegna réttinda þess skráða samkvæmt ákvæðum pul., þótt tilgangur meðferðar persónuupplýsinganna hafi einvörðungu verið persónulegs eðlis. Ennfremur getur of þröng túlkun leitt til skerðingar á friðhelgi einkalífs notanda, þar sem einka- og fjölskyldulíf hans yrði undir eftirliti persónuupplýsingalöggjafar.[301] Í því samhengi hefur verið bent á að undanþágan vegna persónulegra nota sé orðin úrelt og að endurskoða þurfi hvað teljist til *persónulegra nota* upplýsinga.[302] Vaknar því sú spurning hvort notkun einstaklinga á samfélagsmiðlum sé í raun orðin meðferð persónuupplýsinga sem *eingöngu varðar einkahagi viðkomandi eða eru einvörðungu ætlaðar til persónulegra nota* í skilningi 2. málsl. 2. mgr. 3. gr. pul. Taka skal fram að sambærileg undanþága tilskipunar 95/46/EB er orðuð á annan hátt, en er þar talað um vinnslu persónuupplýsinga af hálfu einstaklings sem er hluti af starfsemi sem er *einungis í þágu hans sjálfs eða fjölskyldu hans*. Markmið þessara reglna er þó það sama - að undanskilja persónuleg afnot upplýsinga frá gildissviði persónuupplýsingalöggjafar.

---

[300] Sjá t.d. „Class action against Facebook attracts 60,000 users“, http://www.reuters.com. Enska þýðingu á stefnunni má finna hér: http://www.europe-v-facebook.org/sk/sk_en.pdf (skoðað 17. desember 2014).
[301] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 2.
[302] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 1.

Í reglugerðartillögu framkvæmdastjórnar ESB, sem er hluti af fyrirhugaðri breytingu á persónuupplýsingalöggjöf sambandsins, er gert ráð fyrir undanþágu vegna persónulegra nota, en í d-lið 2. mgr. 2. gr. tillögunnar segir:

> This Regulation does not apply to the processing of personal data […] by a natural person without any gainful interest in the course of its own exclusively personal or household activity.

Reglugerðinni er því ekki ætlað að ná til vinnslu persónuupplýsinga af hálfu einstaklinga, sem er án hverskonar ávinnings og er einvörðungu ætluð til persónulegra- eða heimilisafnota.[303] Áður en tillaga þessi var lögð fyrir Evrópuþingið og Ráðherraráðið hafði hún farið í gegnum þó nokkrar breytingar. Í tillögu þeirri sem lögð var fyrir samráðsferli stofnana ESB var gert ráð fyrir því að undanþágan yrði ekki látin gilda þegar upplýsingar væru gerðar aðgengilegar ótakmörkuðum fjölda fólks.[304] Endurspeglar sú nálgun dóm Evrópudómstólsins í *EBD, mál C-101/01, ECR 2003, bls. I-12971* (Lindqvist) og *EBD, mál C-73/07, ECR 2008, bls. I-09831* (Satamedia).[305] Þessu var aftur á móti breytt áður en reglugerðartillagan var lögð fyrir Evrópuþingið og Ráðherraráðið í ofangreindri mynd. Með því að horfa frá *Lindqvist- og Satamedia* nálguninni gefst möguleiki á rýmri túlkun á því hvað teljist til persónulegra nota.

Í 15. lið formála reglugerðartillögu framkvæmdastjórnar ESB er að finna nánari útskýringar á því hvað teljist til vinnslu persónuupplýsinga *í þágu notandans sjálfs eða fjölskyldu hans*. Eru þar nefnd dæmi svo sem bréfaskriftir og skrár yfir heimilisföng. Hvergi er þó að finna nánari útlistun á því hvað teljist til persónulegra afnota þegar vinnsla fer fram á Internetinu og á samfélagsmiðlum. Þetta hefur 29. gr. starfshópurinn gagnrýnt og lagt til að í formála tillögunnar verði sérstaklega tekið fram að persónuupplýsingavinnsla einstaklings á samfélagsmiðli, sem stefnir hvorki að fjárhagslegu né starfstengdu markmiði, sé undanþegin ákvæðum reglugerðarinnar.[306] Með því væri hægt að komast hjá þeim vafa sem nú virðist ríkja um skyldur samfélagsmiðlanotenda að persónuupplýsingalögum. Þegar Evrópuþingið samþykkti reglugerðartillögu framkvæmdastjórnar ESB í mars 2014 var gagnrýni 29. gr. starfshópsins aftur á móti ekki tekin til greina.

---

[303] Með *ávinningi* er að öllum líkindum átt við fjárhagslegan ávinning, sbr. *Proposals for Amendments regarding exemption for personal or household activities*, bls. 8.
[304] Sjá *Proposal for a General Data Protection Regulation*, 29. nóvember 2011, útgáfa 56, bls. 36-37.
[305] Sjá 44. lið í *EBD, mál C-73/07, ECR 2008, bls. I-09831* (Satamedia) og 47. lið *EBD, mál C-101/01, ECR 2003, bls. I-12971* (Lindqvist).
[306] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 10. Á ensku hljóðar tillaga 29. gr. starfshópsins svo: „This Regulation should not apply to processing of personal data by a natural person, which is exclusively personal or domestic, such as correspondence, the holding of addresses of personal contacts or the use of social network sites that is outside the pursuit of a commercial or professional objective."

Þótt meðferð einstaklings á persónuupplýsingum sé undanþegin gildissviði persónuupplýsingalöggjafar á það ekki að hafa í för með sér að réttindi þess skráða til friðhelgi einkalífs séu skert. Í því samhengi hefur 29. gr. starfshópurinn bent á að hægt væri að gera tilteknar kröfur til notanda um að virða réttindi annarra samkvæmt persónuupplýsingalögum, þótt vinnsla hans falli utan gildissviðs löggjafarinnar vegna persónulegs eðlis hennar. Til dæmis væri hægt að krefjast þess af notanda að virða rétt annarra til eyðingu upplýsinga, t.a.m. þegar viðkomandi biður notanda um að fjarlægja upplýsingar sem sá síðarnefndi hefur birt á persónulegri síðu sinni.[307] Kröfur þær yrðu þó gerðar til notanda, án þess að hann væri álitinn ábyrgðaraðili í lagalegum skilningi.

Með fyrirhuguðum breytingum á persónuupplýsingalöggjöf ESB gefst stofnunum sambandsins tækifæri til að skýra réttarstöðu samfélagsmiðlanotenda frekar. Athugasemdir 29. gr. starfshópsins virðast benda til þess að rýmka eigi þann skilning sem lagður er í *persónuleg afnot* persónuupplýsinga af hálfu einstaklinga og að meðferð persónuupplýsinga á samfélagsmiðlum eigi að falla þar undir, svo lengi sem ekki er stefnt að viðskipta- eða starfstengdu markmiði. Hvort athugasemdir starfshópsins verði teknar til greina verður þó að koma í ljós, en tillögur framkvæmdastjórnar ESB hafa ekki verið samþykktar af Ráðherraráðinu og er því enn möguleiki á frekari breytingum á tillögunni.

6.6 Samantekt

Markmiðið með framangreindri umfjöllun um samfélagsmiðla var að varpa ljósi á það hvernig persónuupplýsingalöggjöf getur snert daglegar athafnir fólks og hvernig ábyrgðar- og vinnsluaðilahugtökin horfa við slíkum aðstæðum. Mismunandi aðilar koma að vinnslu persónuupplýsinga á samfélagsmiðlum og bera þeir ábyrgð á aðgreindum vinnsluþáttum. Var af þeim ástæðum gerður greinarmunur á fyrri og seinni hluta vinnslu. Notandi var talinn ábyrgðaraðili fyrri hluta vinnslu og var þjónustuaðili talinn gegna sama hlutverki að seinni hluta hennar.

Það sem vakti mesta athygli ritgerðarhöfundar var réttarstaða notenda samfélagsmiðla. Var því fjallað ítarlega um þær aðstæður þar sem notendur gegna hlutverki ábyrgðaraðila í merkingu persónuupplýsingalöggjafar og í því samhengi litið sérstaklega til undanþágu tilskipunar 95/46/EB og pul. vegna persónulegra nota einstaklings á persónuupplýsingum. Þá kom einnig til álita hvort þörf væri á frekari afmörkun á því hvað teljist til *persónulegra afnota* þegar Internetið og samfélagsmiðlar eiga í hlut. Komist var að þeirri niðurstöðu að þörf

[307] *Proposals for Amendments regarding exemption for personal or household activities*, bls. 5.

væri á að gera réttarstöðu samfélagsmiðlanotenda skýrari, t.a.m. með því að fella slíka notkun undir *persónuleg afnot*, líkt og 29. gr. starfshópurinn hefur bent á.

Hvað varðar þjónustuaðila samfélagsmiðils virðist sem ákveðin þróun sé að eiga sér stað sem leiðir til frekari ábyrgðar þeirra. Var sú ályktun m.a. dregin af skýrslu Berlínarstarfshópsins, áliti 29. gr. starfshópsins nr. 5/2009 um samfélagsmiðla og reglugerðartillögu framkvæmdastjórnar ESB. Tillagan gerir ráð fyrir því að þjónustuaðili samfélagsmiðils, hvort sem hann gegnir stöðu ábyrgðar- eða vinnsluaðila, skuli fara að ákvæðum reglugerðarinnar þótt notandi sé þeim undanþeginn á grundvelli persónulegra afnota.

7 Fyrirhugaðar breytingar

Líkt og stuttlega var greint frá í kafla 3.1 lagði framkvæmdastjórn ESB fram tillögur að breytingum á persónuupplýsingalöggjöf sambandsins í ársbyrjun 2012. Hér er hvorki svigrúm né tilefni til að fara yfir allar breytingar sem reglugerðartillaga framkvæmdastjórnarinnar kveða á um, en leitast er við að gera grein fyrir þeim allra helstu.

7.1 Reglugerðartillaga framkvæmdastjórnar ESB

Með því að færa persónuupplýsingalöggjöf í form *reglugerðar* í stað *tilskipunar* er stuðlað að stórauknu samræmi í persónuupplýsingalöggjöf á milli aðildarríkja ESB. Reglugerðir eru bindandi í heild sinni og hafa bein lagaáhrif í aðildarríkjum ESB, án sérstakrar lögfestingar á þeim. Reglugerðir fá ekki beint gildi í íslenskum rétti fyrr en reglugerðin hefur verið innleidd í landsrétt, en samkvæmt a-lið 7. gr. EES-samningsins skulu þær teknar upp í heild. Í því felst að texti reglugerða sem teknar hafa verið upp í EES-samninginn er þýddur á íslensku og lögfestur í heild, þó með nauðsynlegri aðlögun.[308] Þegar tilskipanir eiga í hlut er hverju ríki í sjálfsvald sett hvernig markmiðum tilskipunar skuli náð og er því veitt meira svigrúm um innleiðingu slíkra gerða.[309] Með *reglugerð* á sviði persónuupplýsingalöggjafar fengist samræmd heildarlöggjöf milli aðildarríkja ESB, í stað sérstakrar löggjafar í hverju aðildarríki.[310] Auðveldar það til dæmis fjölþjóðafyrirtækjum sem vinna persónuupplýsingar í mismunandi ríkjum innan ESB að uppfylla skilyrði persónuupplýsingalöggjafar, þar sem lögin yrðu þau sömu í hverju ríki.

Ein þeirra grundvallarbreytinga sem vakið hefur mikla athygli er rýmkun á landfræðilegu gildissviði persónuupplýsingalöggjafar ESB. Í reglugerðartillögu framkvæmdastjórnar ESB er

[308] Davíð Þór Björgvinsson: *EES-réttur og landsréttur*, bls. 87-88.
[309] Davíð Þór Björgvinsson: *EES-réttur og landsréttur*, bls. 93.
[310] *Mál PV 8. maí 2013 (2012/1235)* (Umsögn um drög framkvæmdastjórnar ESB).

gildissvið löggjafarinnar teygt út fyrir Evrópska Efnahagssvæðið með því að fella aðila undir gildissvið hennar sem hafa staðfestu utan ESB, en bjóða einstaklingum innan ESB uppá *vörur* eða *þjónustu*. Á það einnig við ef í vinnslu felst vöktun á hegðun einstaklinga í aðildarríkjum ESB. Um þetta segir orðrétt í 2. mgr. 3. gr. reglugerðartillögunnar:

> This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.

Ákvæði þetta kæmi í stað c-liðar 1. mgr. 4. gr. tilskipunar 95/46/EB um notkun ábyrgðaraðila á búnaði á yfirráðasvæði aðildarríkis ESB. Í umsögn Persónuverndar um tillögur framkvæmdastjórnar ESB segir að ætla megi að með þessari afmörkun á landfræðilegu gildissviði löggjafarinnar sé sérstaklega reynt að ná til aðila sem bjóða uppá vöru eða þjónustu á Internetinu. Nálgunin myndi að mörgu leyti skýra lagaumhverfi samfélagsmiðla sem hafa staðfestu utan EES og vinna með persónuupplýsingar aðila sem búsettir eru innan EES. Þá yrðu álitamál um hvað telst til *búnaðar* í skilningi c-liðar 1. mgr. 4. gr. tilskipunar 95/46/EB úr sögunni. Þó vaknar sú spurning hvort svo víðtækt landfræðilegt gildissvið sé raunhæft, þar sem reynst gæti flókið að framfylgja reglunum gagnvart aðilum með staðfestu utan EES.[311]

Í umræddri reglugerðartillögu er ekki gert ráð fyrir breytingu á vinnsluaðilahugtakinu.[312] Á ábyrgðaraðilahugtakinu eru lagðar til smávægilegar breytingar með því að bæta við einum efnisþætti við skilgreiningu þess, þ.e. að ábyrgðaraðili ákveði einnig *skilyrði* (e. *conditions*) vinnslu, en ekki eingöngu markmið hennar og aðferðir við vinnsluna.[313] Óljóst er hvort breyting sú muni hafa einhver áhrif í framkvæmd. Þótt ekki sé kveðið á um meiriháttar breytingar á hugtökunum sjálfum leggur reglugerðartillagan frekari skyldur á bæði ábyrgðar- og vinnsluaðila.

Ákvæði 26. gr. tillögunnar leggur frekari skyldur á herðar vinnsluaðila og gerir strangari kröfur til hans en gerðar eru í tilskipun 95/46/EB. Eins og gerð var grein fyrir í kafla 5.3 getur vinnsluaðili bakað sér ábyrgð á vinnslu ef hann fer út fyrir umboð sitt eða framkvæmir vinnslu í ósamræmi við fyrirmæli ábyrgðaraðila. Með 4. mgr. 26. gr. reglugerðartillögunnar er tekið á þessu og kveðið á um að við slíkar aðstæður skuli vinnsluaðili talinn ábyrgðaraðili þeirrar tilteknu vinnslu og ber hann þá sameiginlega ábyrgð með upprunalegum

[311] *Mál PV 8. maí 2013 (2012/1235)* (Umsögn um drög framkvæmdastjórnar ESB). Sjá einnig Christopher Kuner: *European Data Protection Law*, bls. 125.
[312] *Proposal for a General Data Protection Regulation,* COM/2012/11/FINAL, 6. tölul. 4. gr.
[313] *Proposal for a General Data Protection Regulation,* COM/2012/11/FINAL, 5. tölul. 4. gr.

ábyrgðaraðila.[314] Þá er einnig kveðið á um skyldu vinnsluaðila til að ráða einungis starfsfólk sem heitir trúnaði, sbr. b-lið 2. mgr. 26. gr. reglugerðartillögunnar og er vinnsluaðila jafnframt óheimilt að semja við undirverktaka án fyrirframsamþykkis ábyrgðaraðila, sbr. d-lið 2. mgr. 26. gr. tillögunnar. Skilyrði þetta hefur ekki áður verið bundið í persónuupplýsingalöggjöf, en um fyrirframsamþykki ábyrgðaraðila vegna samninga vinnsluaðila við undirverktaka er fjallað í stöðluðum samningsskilmálum ákvörðunar framkvæmdastjórnar ESB 2010/87/ESB.

Reglugerðartillagan gerir ekki einungis ríkari kröfur til vinnsluaðila heldur einnig til ábyrgðaraðila, eins og sjá má af f-lið 5. gr. tillögunnar. Ákvæði 5. gr. er byggt á 6. gr. tilskipunar 95/46/EB og hefur að geyma meginreglur um gæði gagna sem allar skulu uppfylltar svo vinnsla sé lögmæt. Með f-lið 5. gr. er kveðið á um nýja meginreglu sem hljóðar svo:

> Personal data must be [...] processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

Vinnsla persónuupplýsinga myndi því ekki teljast lögmæt nema hún ætti sér stað undir ábyrgð ábyrgðaraðila og að hann tryggi jafnframt að farið sé að reglum reglugerðarinnar við vinnsluna. Þótt leiða megi af ákvæðum tilskipunar 95/46/EB að það sé á ábyrgð ábyrgðaraðila að farið sé að lögum við vinnslu persónuupplýsinga og að gætt sé að réttindum þeirra skráðu, styrkist ábyrgð hans til muna, verði hún lögfest sem ein af meginreglum persónuupplýsingavinnslu.[315] Í 22. gr. reglugerðartillögunnar er gerð nánari grein fyrir hvað felst í ábyrgð ábyrgðaraðila. Þar er m.a. mælt fyrir um skyldu til að halda skjöl um margvísleg atriði varðandi vinnslu persónuupplýsinga skv. 28. gr. tillögunnar. Til dæmis skal skjalfesta hver tilgangur vinnslunnar er og hvaða upplýsingar séu unnar hverju sinni, en skylda til slíkrar skjalfestingar hvílir einnig á vinnsluaðila.

Með reglugerðartillögunni eru gerðar ríkari kröfur um hátt öryggisstig við persónuupplýsingavinnslu og er lögð sú skylda á ábyrgðaraðila í 23. gr. hennar að gæta að svokallaðri *innbyggðri einkalífsvæddri hönnun* (e. *privacy by design*) og að *sjálfgefnar stillingar* séu persónuverndarvænar (e. *privacy by default*).[316] Í innbygðri einkalífsvæddri hönnun felst að kerfi til vinnslu persónuupplýsinga verði ávallt hönnuð með það að markmiði

[314] Í 4. mgr. 26. gr. reglugerðartillögunnar segir „If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24."
[315] Christopher Kuner: „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", bls. 6.
[316] Íslensk heiti þessa hugtaka eru fengin úr erindi Sigrúnar Jóhannesdóttur, *Áhrif reglna Evrópusambandsins á íslenskan rétt og ný Evrópulöggjöf um persónuvernd*, sem flutt var á ráðstefnunni „Nýjar ógnir við friðhelgi einkalífs og meðferð persónuupplýsinga" 19. október 2012.

að persónuupplýsingar verði nægilega verndaðar. Hvað varðar stillingar er gerð sú krafa til ábyrgðaraðila að sjálfgefnar stillingar kerfisins, t.d. stillingar á samfélagsmiðli þegar hann er notaður í fyrsta sinn, séu persónuverndarmiðaðar.[317] Þannig á vinnsluferlið að tryggja nægilega vernd persónuupplýsinga frá byrjun til enda og skal ábyrgðaraðili sjá til þess að þessu sé fylgt eftir. Í samræmi við auknar kröfur til öryggisstigs persónuupplýsingavinnslu er sú krafa gerð til opinberra stofnana og einkarekinna fyrirtækja með fleiri en 250 starfsmenn, sem gegna hlutverki ábyrgðar- eða vinnsluaðila, að tilnefna persónuverndarfulltrúa (e. *data protection officer*), sbr. 35. gr. tillögunnar. Á þetta einnig við ef aðal starfsemi ábyrgðar- eða vinnsluaðila felst í persónuupplýsingavinnslu sem þarf reglulegt og kerfisbundið eftirlit. Hlutverk persónuverndarfulltrúa er m.a. að fylgjast með því hvort aðili uppfylli þær kröfur sem persónuupplýsingalöggjöf gerir til persónuupplýsingavinnslu og að leiðbeina aðilum í þeim efnum, sbr. 37. gr. reglugerðartillögunnar. Að mati Persónuverndar ætti fjöldi starfsmanna ekki að skipta höfuðmáli við mat á því hvort þörf sé á persónuverndarfulltrúa, enda geta fyrirtæki með mjög fáa starfsmenn haft með höndum vinnslu persónuupplýsinga sem lúta þurfa ströngum skilyrðum.[318] Í 33. gr. reglugerðartillögunnar er kveðið á um enn frekari ráðstafanir til að tryggja öryggi upplýsinga og réttindi einstaklinga til verndar persónuupplýsinga sinna með svokölluðu áhrifamati (e. *impact assessment*). Í 33. gr. segir að ef vinnsla er líkleg til að stefna persónuupplýsingavernd eða réttindum hins skráða til friðhelgis einkalífs í hættu vegna eðlis eða umfangs vinnslunnar (t.d vinnsla upplýsinga í erfðarannsókn) skuli ábyrgðaraðili eða vinnsluaðili framkvæma mat á þeim áhrifum sem vinnslan mun hafa á framangreind réttindi. Í áhrifamatinu skal m.a. lýsa því hvernig gætt verði að réttindum þeirra skráðu við vinnsluna.

Í kafla 4.4 var fjallað um sameiginlega ábyrgð og erfiðleika sem geta komið upp við skipti á ábyrgð á milli ábyrgðaraðila. Með 24. gr. reglugerðartillögu framkvæmdastjórnar ESB er leitast við að gera strangari kröfur til sambands ábyrgðaraðila sem bera sameiginlega ábyrgð á tiltekinni vinnslu. Ákvæðið krefst þess að ábyrgðaraðilar geri samkomulag sín á milli um hvernig þeir skipta með sér ábyrgð á vinnslunni og þeim skyldum sem á þeim hvíla. Þó er ekki kveðið á um skriflegan samning, líkt og krafist er um samband vinnsluaðila og ábyrgðaraðila, heldur einungis að gert sé samkomulag (e. *arrangement*).

Reglugerðartillaga framkvæmdastjórnarinnar styrkir einnig rétt þeirra skráðu og mælir fyrir um ný réttindi í þeirra þágu, en með því eru lagðar frekari skyldur á ábyrgðar- og

[317] Christopher Kuner: „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", bls. 7.
[318] *Mál PV 8. maí 2013 (2012/1235)* (Umsögn um drög framkvæmdastjórnar ESB).

vinnsluaðila. Í 2. mgr. 17. gr. reglugerðartillögunnar er fjallað um réttinn til að gleymast. Rétturinn hefur ekki verið orðaður í löggjöf áður, en virðist þó vera viðbót við 12. gr. tilskipunar 95/46/EB sem kveður á um rétt þess skráða til að láta eyða sínum eigin persónuupplýsingum. Evrópudómstóllinn hefur staðfest réttinn til að gleymast undir 12. gr. tilskipunar 95/46/EB í *dómi Evrópudómstólsins 13. maí 2014, C-131/12* (Google), sem reifaður er í kafla 4.5.5. Í 3. mgr. 17. gr. er rétturinn afmarkaður frekar, en þar segir að ábyrgðaraðili skuli eyða upplýsingum tafarlaust, nema það sé nauðsynlegt að varðveita upplýsingarnar af nánar tilteknum ástæðum. Við mat á því er litið til þess hvort réttindi annarra (s.s. tjáningarfrelsi) og/eða almannahagsmunir hindri að upplýsingum um hinn skráða sé eytt.[319] Slíkt hagsmunamat er líklegt til að vera flókið í framkvæmd, en gert er ráð fyrir að ábyrgðaraðili framkvæmi slíkt hagsmunamat.[320]

Með ofangreindum breytingum virðist sem samband ábyrgðaraðila og vinnsluaðila sé betur afmarkað og gert skýrara. Frekari kröfur eru gerðar til vinnsluaðila og hert er á kröfum til öryggisráðstafana, auk þess sem gerðar eru ríkari kröfur til þess að halda skrifleg gögn um persónuupplýsingavinnslu, t.d. með tilkomu áhrifamats og skilyrða um skjalfestingu. Þá má gera ráð fyrir því að ákvæði 79. gr. reglugerðartillögunnar um vald persónuverndarstofnana til að leggja á sektir þegar brotið hefur verið gegn persónuupplýsingalöggjöf muni auka meðvitund um mikilvægi persónuupplýsingaverndar. Gert er ráð fyrir sektum uppá allt að 2% af ársveltu fyrirtækis á heimsvísu. Með svo háar sektir yfirvofandi er líklegra að persónuvernd og meðferð persónuupplýsinga verði sett hærra á forgangslista fyrirtækja.

8 Lokaorð

Þegar heimildarvinna hófst fyrir ritsmíð þessa varð það höfundi fljótt ljóst að hugtökin *ábyrgðaraðili* og *vinnsluaðili* væru gjarnan kveikjan að álitamálum á sviði persónuupplýsingaréttarins. Við nánari grennslan komu í ljós efasemdir fræðimanna um beitingu hugtakanna, einkum þegar tækninýjungar á borð við tölvuskýjaþjónustu og samfélagsmiðla eiga í hlut. Þá gáfu álit Persónuverndar og umboðsmanns Alþingis jafnframt til kynna að aðilar væru ekki alltaf sammála um hvað fælist í hugtökunum. Markmiðið með ritgerð þessari var að kafa dýpra í merkingu hugtakanna tveggja en áður hafði verið gert í íslenskum fræðaskrifum, í von um að skýra innihald og merkingu þeirra á sem bestan hátt. Að mati höfundar hefur því markmiði verið náð.

[319] Í *dómi Evrópudómstólsins 13. maí 2014, C-131/12* (Google), þurfti að meta hvort vægi þyngra, réttur almennings til aðgangs að upplýsingum eða réttur þess skráða til að fá upplýsingum eytt.
[320] Christopher Kuner: „The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", bls. 6.

Ábyrgðar- og vinnsluaðilahugtök laga nr. 77/2000 sækja fyrirmynd sína til tilskipunar 95/46/EB. Var því að mestu litið til Evrópuréttar við afmörkun hugtakanna. Einkum var stuðst við greiningu 29. gr. starfshópsins á hugtökunum tveimur og sú greining heimfærð uppá íslenskan rétt. Til þess að ná því markmiði sem stefnt var að var hvert hugtak fyrir sig greint í afmarkaða þætti. Ábyrgðaraðilahugtakið hlaut þríþætta greiningu, en vinnsluaðilahugtakið tvíþætta. Með því að líta á hina afmörkuðu þætti sem *skilyrði* þess að viðkomandi gegni hlutverki ábyrgðar- eða vinnsluaðila gefst ef til vill skýrari mynd af hugtökunum. Til þess að aðili teljist gegna hlutverki ábyrgðaraðila skulu eftirfarandi skilyrði uppfyllt:

> (a) Aðili skal hafa *aðildarhæfi* og þarf að geta svarað til saka fyrir tiltekna vinnslu persónuupplýsinga fyrir dómstólum.
> (b) Aðili skal fara með *raunverulegt ákvörðunarvald*[321] um:
> (c) *tilgang* vinnslu, *aðferð* við hana, hvaða *búnaður* skuli notaður eða *aðra ráðstöfun upplýsinga.*

Við mat á því hvort aðili fari með raunverulegt ákvörðunarvald um aðferð eða tilgang vinnslu kemur ýmislegt til álita. Búi aðili yfir sérfræðiþekkingu getur sjálfstæði hans bent til þess að hann fari með ákvörðunarvald um vinnsluna og teljist því ábyrgðaraðili hennar, sbr. *ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV) og *úrskurður PV 25. júní 2013 (2012/964)* (Barnaverndarnefnd Reykjavíkur). Hafi aðili töluvert svigrúm til að taka sjálfstæðar ákvarðanir um vinnsluna þykir það einnig benda til þess að viðkomandi sé ábyrgðaraðili hennar. Svo að aðili teljist ábyrgðaraðili vinnslu er ekki gerð sú krafa að hann hafi ákvörðunarvald um hvern og einn þeirra þátta sem kveðið er á um í c-lið hér að ofan heldur nægir að hann taki ákvörðun um einn þeirra.

Vinnsluaðilahugtakið var afmarkað í tvo þætti sem endurspegla þau skilyrði sem aðili þarf að uppfylla svo hann teljist vinnsluaðili. Eru þau eftirfarandi:

> (a) Vinnsluaðili skal vera *utanaðkomandi* og *sjálfstæður* gagnvart ábyrgðaraðila.
> (b) Vinnsluaðili skal framkvæma vinnslu persónuupplýsinga *fyrir hönd* ábyrgðaraðila og að hans *ósk*.

Af fyrra skilyrðinu leiðir að vinnsla persónuupplýsinga innanhúss, t.d. af starfsfólki ábyrgðaraðila, telst ekki vinnsla af hálfu vinnsluaðila. Skilyrðisins er hvorki getið sérstaklega í persónuupplýsingalögum, né í lögskýringargögnum. Er það þó talið liggja í hlutarins eðli að ábyrgðaraðili og vinnsluaðili geti ekki verið einn og sami aðilinn að sömu vinnslunni, þar sem tilvist vinnsluaðila ræðst af ákvörðun ábyrgðaraðila um að fá annan aðila en hann sjálfan til að vinna persónuupplýsingar fyrir sína hönd. Af seinna skilyrðinu leiðir að fari vinnsluaðili ekki eftir fyrirmælum ábyrgðaraðila eða vinnur upplýsingar í eigin þágu telst hann ekki lengur

[321] Ákvörðunarvald getur verið lög- eða samningsbundið, en gæta þarf þess að slíkt formlegt ákvörðunarvald endurspegli raunveruleikann, þ.e. að viðkomandi fari einnig með *raunverulegt* ákvörðunarvald.

vinnsluaðili, þar sem vinnslan fer þá ekki lengur fram fyrir hönd ábyrgðaraðila, né að hans ósk. Þegar aðstæður eru með þeim hætti er líklegra að viðkomandi teljist ábyrgðaraðili vinnslunnar.

Þótt afmörkun ábyrgðar- og vinnsluaðilahugtakanna virðist einföld í fyrstu getur sú merking sem hver og einn leggur í hugtökin aftur á móti orðið til vandkvæða í framkvæmd. Til marks um það eru *Fjölmenntarmálin*[322] sem m.a. var fjallað um í kafla 4.3.3. Skiptir því meginmáli að aðilar sem koma að vinnslu persónuupplýsinga séu frá upphafi sammála um það hvernig hlutverkaskiptum er hagað þeirra á milli. Er því brýnt að vinnslusamningur liggi fyrir. Hlutverk aðila samkvæmt samningi er hins vegar ekki grafið í stein og ber ávallt að líta til þess hver fari með *raunverulegt ákvörðunarvald* um tiltekna vinnslu. Til marks um það er *SWIFT-álit* 29. gr. starfshópsins, þar sem litið var fram hjá orðalagi samninga og horft til þeirra raunverulegra aðstæðna sem voru uppi í málinu.[323]

Þær skyldur sem hvíla á ábyrgðar- og vinnsluaðila eru ólíkar sem og mismiklar. Ábyrgðaraðili ber ábyrgð á vinnslu persónuupplýsinga og hvílir á honum skylda til að gæta að þeim réttindum sem persónuupplýsingalögin veita hinum skráðu. Er það einnig á ábyrgð ábyrgðaraðila að vinnsla uppfylli almenn skilyrði persónuupplýsingalaga. Ábyrgðaraðili þarf því að ganga úr skugga um að lagaheimild sé fyrir vinnslunni í samræmi við 8. og eftir atvikum 9. gr. pul. Eins skal hann sjá til þess að öllum grunnreglum 7. gr. laganna sé fylgt eftir. Á vinnsluaðila hvílir trúnaðarskylda samkvæmt 13. gr. pul. og felur sú skylda í sér tvo meginþætti. Annars vegar að vinnsluaðili megi eingöngu meðhöndla persónuupplýsingar í samræmi við lög og fyrirmæli ábyrgðaraðila og hins vegar að gerður skuli vinnslusamningur á milli ábyrgðar- og vinnsluaðila sem afmarkar skyldur þess síðarnefnda við meðferð persónuupplýsinga. Af 2. mgr. 13. gr. pul. leiðir einnig að vinnsluaðili skuli gæta öryggis þeirra upplýsinga sem hann vinnur með, sbr. *ákvörðun PV 3. mars 2011 (2011/62)* (Miðlun ehf.). Með breytingartillögu framkvæmdastjórnar ESB á persónuupplýsingalöggjöf sambandsins eru gerðar skýrari og umfangsmeiri kröfur til vinnsluaðila og lagðar á hann frekari skyldur. Má t.a.m. nefna skyldu til að halda skrifleg gögn um þá vinnslu sem hann framkvæmir sbr. 28. gr. reglugerðartillögunnar og kröfu d-liðar 2. mgr. 26. gr. tillögunnar um samþykki ábyrgðaraðila áður en vinnsluaðili semur við undirverktaka. Þá er einnig kveðið skýrar á um samband vinnslu- og ábyrgðaraðila með því að binda það í lög að fari vinnsluaðili

[322] *Úrskurður PV 10. júní 2009 (2009/172)* (Fjölmennt I), *ákvörðun PV 13. ágúst 2009 (2009/172)* (Fjölmennt II), *Álit umboðsmanns Alþingis 5. september 2012 (6055/2010)* (Fjölmennt III), *Ákvörðun PV 4. mars 2013 (2012/1091)* (Fjölmennt IV) og *Ákvörðun PV 13. febrúar 2014 (2013/1397)* (Fjölmennt V).
[323] *Article 29 Working Party opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).* Sjá reifun í kafla 4.3.2.2.

út fyrir umboð sitt eða framkvæmir vinnslu í ósamræmi við fyrirmæli ábyrgðaraðila, telst vinnsluaðili bera sameiginlega ábyrgð á vinnslunni ásamt upprunalegum ábyrgðaraðila.[324]

Með ritgerð þessari var einnig stefnt að því að kynna samfélagsmiðla sem vettvang persónuupplýsingavinnslu og kanna hvernig ábyrgðar- og vinnsluaðilahugtökunum væri beitt við slíkar aðstæður. Við vissar aðstæður getur meðferð einstaklings á persónuupplýsingum við notkun samfélagsmiðla fallið undir gildissvið pul. Getur notandi því talist ábyrgðaraðili þeirra upplýsinga sem hann birtir á slíkum vettvangi. Sé birting upplýsinganna einungis talinn til *persónulegra afnota* í skilningi 2. málsl. 2. mgr. 3. gr. pul. fellur hún þó utan gildissviðs pul. Reynst getur vandasamt að leggja mat á það hvort dreifing persónuupplýsinga á samfélagsmiðli sé til persónulegra nota. Var því velt upp hvort sú þróun hafi orðið að vinnsla persónuupplýsinga af hálfu einstaklinga á samfélagsmiðlum væri *persónuleg not* og því undanþegin gildissviði pul. Hefur 29. gr. starfshópurinn ítrekað í álitum sínum að slík vinnsla persónuupplýsinga skuli felld undir undanþágu persónuupplýsingalöggjafar vegna meðferðar persónuupplýsinga til einka- eða heimilisafnota. Er það mat höfundar að við þá breytingarvinnu sem nú stendur yfir á persónuupplýsingalöggjöf ESB sé tilefni til að endurskoða hvað telst til persónulegra afnota. Væri þá sérstaklega hægt að meta hvort meðferð einstaklinga á persónuupplýsingum á samfélagsmiðlum falli undir þann flokk.

Ljóst er að á næstu árum mun ný persónuupplýsingalöggjöf ESB líta dagsins ljós. Nú þegar hefur Evrópuþingið samþykkt breytingartillögur framkvæmdastjórnar ESB, en svo tillögur þær verði að lögum skulu þær einnig samþykktar af Ráðherraráðinu. Gangi þær eftir er þó líklegt að þónokkur tími muni líða þar til breytingarnar verða teknar upp í íslenskan rétt, þar sem þær skulu fyrst teknar upp í EES-samninginn. Hversu miklar breytingar verði gerðar á ábyrgðar- og vinnsluaðilahugtökunum verður að koma í ljós, en þær breytingar sem framkvæmdastjórn ESB hefur lagt til eru vissulega skref í átt að skýrari beitingu hugtakanna.

[324] Sjá 4. mgr. 26. gr. reglugerðartillögu framkvæmdastjórnar ESB.

HEIMILDASKRÁ

Alþingistíðindi.

„Álit neytendastofnana á Norðurlöndum varðandi markaðssetningu í samskiptamiðlum“, http://www.neytendastofa.is/lisalib/getfile.aspx?itemid=2878 (skoðað 10. desember 2014).

Björg Thorarensen: „Friðhelgi einkalífs og fjölskyldu“. *Mannréttindasáttmáli Evrópu. Meginreglur, framkvæmd og áhrif á íslenskan rétt.* Reykjavík 2005, bls. 286-341.

Björg Thorarensen: *Stjórnskipunarréttur - mannréttindi*. Reykjavík 2008.

Brendan Van Alsenoy o.fl.: „Social networks and web 2.0: are users also bound by data protection regulations?“. *Identity in the Information Society*, 1. tbl. 2009, 65-79.

Christopher Kuner: „The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law“. *Bloomberg BNA Privacy and Security Law Report*, 2012, bls. 1-15.
Aðgengilegt á: http://ssrn.com/abstract=2162781 (skoðað 9. desember 2014).

Christopher Kuner: *European Data Protection Law. Corporate Compliance and Regulation*. 2. útgáfa. Oxford 2007.

„Class action against Facebook attracts 60,000 users“, http://www.reuters.com, 21. ágúst 2014 (skoðað 10. desember 2014).

Dag Wiese Schartum og Lee A. Bygrave: *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* 2. útgáfa. Bergen 2011.

Datatilsynets årsberetning 2011. Datatilsynet, Kaupmannahöfn 2012.

Data processor agreements pursuant to the Personal Data Act and the Personal Health Data Filing System. Datatilsynet, Oslo 2012.
Birt á: https://www.datatilsynet.no.

„Data Use Policy“, https://www.facebook.com/full_data_use_policy, 15. nóvember 2013 (skoðað 10. desember 2014).

Davíð Þór Björgvinsson: *EES-réttur og landsréttur*. Reykjavík 2006.

Dorte Høilund: *Persondataloven. En indføring.* 2. útgáfa. Kaupmannahöfn 2014.

David J. Harris, Michael O’Boyle og Colin Warbrick: *Law of the European Convention on Human Rights*. 2. útgáfa. Oxford 2009.

Friðhelgi einkalífs. Umboðsmaður barna, Reykjavík 2003. Birt á: http://barn.is/.

Handbook on European data protection law. European Union Agency for Fundamental Rights og Council of Europe, Belgía 2014.

Handbók Stjórnarráðsins um EES. Utanríkisráðuneytið, Reykjavík 2003.

Henrik Udsen: *De informationsretlige grundsætninger. Studier i informationsretten.* Kaupmannahöfn 2009.

Henrik Waaben og Kristian Korfits Nielsen: *Lov om behandling af personoplysninger med kommentarer*. 2. útgáfa. Kaupmannahöfn 2008.

Hielke Hijmans og Alfonso Scirocco: "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?". *Common Market Law Review*, 5. tbl. 2009, bls. 1485-1525.

Ingvi Snær Einarsson: „Sérstök skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga, skv. 1. mgr. 9. gr. laga nr. 77/2000". *Úlfljótur*, 1. tbl. 2005, bls. 41-110.

Jan Trzaskowski o.fl.: *Internetretten*. 2. útgáfa. Kaupmannahöfn 2012.

Kriminalitetsbekjempelse og personvern. Politiets og påtalemyndighetens behandling av opplysninger. Justis- og politidepartementet, Oslo 2003.

Legal guide to public organisation cloud sourcing in the Nordic countries. Norræna Ráðherranefndin, Kaupmannahöfn 2013.

Páll Sigurðsson ritstj.: *Lögfræðiorðabók með skýringum*. Reykjavík 2008.

„Mjög sótt að friðhelgi einkalífsins", http://www.mbl.is/greinasafn/grein/829012/, 14. nóvember 2004 (skoðað 9. desember 2014).

Paolo Balboni: „Data Protection and Data Security Issues Related to Cloud Computing in the EU". *Tilburg University Studies Working Paper Series*, no. 022/2010.
Aðgengilegt á: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437.

Páll Hreinsson: *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála*. Reykjavík 2007.

Páll Sigurðsson: *Mannhelgi. Höfuðþættir almennrar persónuverndar.* Reykjavík 2010.

Peter Blume: *Databeskyttelsesret*. 4. útgáfa. Kaupmannahöfn 2013.

Peter Blume: „Data Protection in the Private Sector". *Scandinavian Studies in Law*. *Vol. 47.* Ritsj. Peter Wahlgren. Stokkhólmur 2004, bls. 297-318.

Peter Blume: *Persondataretten – nu og i fremtiden.* Kaupmannahöfn 2010.

Peter Blume og Janne Rothmar Herrmann: *Ret, privatliv og teknologi.* 3. útgáfa. Danmörk 2013.

Peter Hustinx: „Data Protection and Cloud Computing under EU law“. Birt á: https://secure.edps.europa.eu/ (skoðað 10. desember 2014).

„Progress on EU data protection reform now irreversible following European Parliament vote“, http://europa.eu/rapid/press-release_MEMO-14-186_en.htm, 12. mars 2014 (skoðað 9. desember 2014).

„Óvíst hvað á að gera við skepnuna Facebook“, http://www.visir.is, 31. janúar 2013 (skoðað 17. desember 2014).

Report and Guidance on Privacy in Social Network Services. "Rome Memorandum". International Working Group on Data Protection in Telecommunications, Róm 2008. Aðgengilegt á: http://www.datenschutz-berlin.de/.

Samuel D. Warren og Louis D. Brandeis: „The right to Privacy“. *Harvard Law Review*, 4. tbl. 1890, bls. 193-220.

Sigrún Jóhannesdóttir: „Áhrif reglna Evrópusambandsins á íslenskan rétt og ný Evrópulöggjöf um persónuvernd“. Erindi flutt á ráðstefnu *Nýjar ógnir við friðhelgi einkalífs og meðferð persónuupplýsinga,* Reykjavík 19. október 2012. Aðgengilegt á: https://www.youtube.com/watch?v=tRGoBzLblAk&feature=youtu.be (skoðað 10. desember 2014).

Social Network Services and Privacy. A case study of Facebook. Datatilsynet, 2011. Aðgengilegt á: https://www.datatilsynet.no/English/Publications/.

Standard form contract to assist compliance with obligations imposed by Article 17 of Data Protection Directive 95/46/EC. European Committee for Standardization, Brussel 2005. Aðgengilegt á: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15292-00-2005-May.pdf.

Stefán Már Stefánsson: *Samstæður hlutafélaga*. Reykjavík, 2008.

Stjórnartíðindi.

Vefsíða Datainspektionen, http://www.datainspektionen.se.
Vefsíða Datatilsynet, http://www.datatilsynet.dk.
Vefsíða Europe v. Facebook, http://www.europe-v-facebook.org.
Vefsíða Facebook, http://www.facebook.com.
Vefsíða Persónuverndar, http://www.personuvernd.is.

Vejledning til bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr, "Cookie-bekendtgørelsen". Erhvervsstyrelsen, Silkiborg 2013.

Þórður Sveinsson: „Grunnreglur 7. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga“. *Úlfljótur*, 3. tbl. 2003, bls. 404-454.

Þuríður Björk Sigurjónsdóttir: „Ákvæði 1. mgr. 8. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga“. *Úlfljótur*, 1. tbl. 2005, bls. 193-227.

Efni frá Evrópusambandinu:
Ákvörðun framkvæmdastjórnar ESB frá 5. febrúar 2010 um föst samningsákvæði vegna flutnings persónuupplýsinga til vinnsluaðila með staðfestu í þriðju löndum samkvæmt tilskipun Evrópuþingsins og ráðsins 95/46/EB (2010/87/ESB).

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. COM/2010/609/FINAL. European Commission, Brussel 2010. Aðgengilegt á: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, (skoðað 10. desember 2014).

„European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)“, http://www.europarl.europa.eu/, (skoðað 9. desember 2014).

Myth-Busting. The Court of Justice of the EU and the "Right to be Forgotten". European Commission, 2014. Birt á: http://ec.europa.eu/justice/data-protection/ (skoðað 10. desember 2014).

„Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy“. Official Journal of the European Union, Volume 53, 2010. Birt á: http://eur-lex.europa.eu/.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 29/11/2011, version 56. European Commission, Brussel 2011. Aðgengilegt á: http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf (skoðað 15. desember 2014).

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/11/FINAL. European Commssion, Brussel 2012. Aðgengilegt á: http://ec.europa.eu/justice/data-protection/ (skoðað 10. desember 2014).

29. gr. starfshópurinn:[325]
FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC. 29. gr. starfshópurinn, Brussel 2010. Aðgengilegt á: http://www.cnil.fr/fileadmin/documents/–Vos_responsabilites/Transferts/FAQ_Clauses_de_responsable_a_sous-traitant_EN.pdf.

Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 29. gr. starfshópurinn, Brussel 2006.

[325] Álit starfshópsins eru aðgengileg á: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

Opinion 1/2008 on data protection issues relating to search engines. 29. gr. starfshópurinn, Brussel 2008.

Opinion 5/2009 on online social networking. 29. gr. starfshópurinn, Brussel 2009.

Opinion 1/2010 on the concepts of "controller" and "processor". 29. gr. starfshópurinn, Brussel 2010.

Opinion 05/2012 on Cloud Computing. 29. gr. starfshópurinn, Brussel 2012.

Proposals for Amendments regarding exemption for personal or household activities. 29. gr. starfshópurinn, Brussel 2013. Aðgengilegt á: http://ec.europa.eu/justice/data-protection/article-29/documentation/.

Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor". 29. gr. starfshópurinn, Brussel 2014.

SKRÁ YFIR DÓMA, ÚRSKURÐI, ÁKVARÐANIR OG ÁLIT

Hæstaréttardómar:
Hrd. 1968, bls. 1007
Hrd. 1999, bls. 857 (252/1998)
Hrd. 2003, bls. 4153 (151/2003)
Hrd. 4. október 2007 (37/2007)
Hrd. 20. nóvember 2014 (214/2014)

Dómar Mannréttindadómstóls Evrópu:
MDE, Leander gegn Svíþjóð, 26. mars 1987 (9248/81)
MDE, Rotaru gegn Rúmeníu, 4. maí 2000 (28341/95)

Dómar Evrópudómstólsins:
EBD, mál C-101/01, ECR 2003, bls. I-12971
EBD, mál C-73/07, ECR 2008, bls. I-09831
EBD, mál C-131/12

Álit umboðsmanns Alþingis:
Álit umboðsmanns Alþingis 5. september 2012 (6055/2010)

Ákvarðanir Póst- og fjarskiptastofnunar
Ákvörðun Póst- og fjarskiptastofnunar 24. mars 2014 (1/2014)

Úrskurðir, ákvarðanir, álit og svör Persónuverndar:
Úrskurður Persónuverndar 19. maí 2003 (2003/103)
Úrskurður PV 15. desember 2004 (2004/315)
Úrskurður PV 28. febrúar 2005 (144/2004)
Álit PV 19. janúar 2006 (2005/593)
Bréf PV 22. maí 2006. Aðgengilegt á: http://www.personuvernd.is/efst-a-baugi/ymislegt-frettnaemt/greinar/nr/277.
Svar PV 10. ágúst 2006 um myndbirtingar
Úrskurður PV 26. júní 2007 (2007/258)
Svar PV 8. apríl 2008 um eiturlyfjaskimun innan fyrirtækja
Úrskurður PV 10. júní 2009 (2009/172)
Ákvörðun PV 13. ágúst 2009 (2009/172)
Niðurstaða PV 16. desember 2009 (2009/635)
Úrskurður PV 18. janúar 2010 (2010/1046)
Úrskurður PV 18. janúar 2011 (2010/907)
Ákvörðun PV 3. mars 2011 (2011/62)
Úrskurður PV 22. júní 2011 (2011/272)
Úrskurður PV 17. ágúst 2011 (2010/906)
Úrskurður PV 17. ágúst 2011 (2011/347)
Svar PV 17. ágúst 2011 (2011/681)
Ákvörðun PV 5. júní 2012 (2012/193)
Leiðbeinandi svar PV 7. ágúst 2012 (2010/1079)
Úrskurður PV 27. nóvember 2012 (2012/818)
Úrskurður PV 25. janúar 2013 (2011/766)
Ákvörðun PV 4. mars 2013 (2012/1091)
Ákvörðun PV 17. apríl 2013 (2013/426)

Umsögn PV 8. maí 2013 (2012/1235)
Úrskurður PV 28. maí 2013 (2012/1390)
Úrskurður PV 25. júní 2013 (2012/964)
Ákvörðun PV 13. febrúar 2014 (2013/1397)
Ákvörðun PV 13. mars 2014 (2013/1192)
Úrskurður PV 13. maí 2014 (2014/377)
Úrskurður PV 13. maí 2014 (2014/378)
Ákvörðun PV 17. september 2014 (2014/952)

Mál dönsku persónuverndarstofnunarinnar Datatilsynet:
Mál Datatilsynet 30. janúar 2008 (nr. 2007-212-0042)
Mál Datatilsynet 3. febrúar 2011 (nr. 2010-52-0138)
Bréf Datatilsynet 11. júlí 2011. Aðgengilegt á: http://www.datatilsynet.dk/afgoerelser.
Bréf Datatilsynet 8. nóvember 2013 (nr. 2013-321-0173)
Mál Datatilsynet 15. janúar 2014 (nr. 2013-323-0154)

Úrskurðir og álit sænsku persónuverndarstofnunarinnar Datainspektionen:
Ákvörðun Datainspektionen 10. júní 2014 (358-2014)

Úrskurðir norsku kærunefndarinnar Personvernnemnda:
Úrskurður 23. október 2012 (PVN-2012-03)