Persónuvernd

LEIÐBEININGAR UM SAMÞYKKI

Almennt

Samþykki er, og verður áfram, ein af heimildum persónuverndarlaga til vinnslu persónuupplýsinga. Persónuverndarreglugerð ESB 679/2016 (pvrg.) skýrir nánar og lögfestir að miklu leyti gildandi framkvæmd en í því felst m.a. að lykilatriði *samþykkis* haldast óbreytt, þó svo að nú séu gerðar mun strangari kröfur til ábyrgðaraðila. Leiðbeiningar þessar byggja á leiðbeiningum 29. gr. vinnuhóps ESB um samþykki (WP259), sem skipaður er forstjórum allra persónuverndarstofnana innan ESB, en Persónuvernd hefur þar áheyrnaraðild.

Efnisyfirlit

1. Inngangur

Samþykki er áfram ein af þeim heimildum sem byggja má vinnslu persónuupplýsinga á samkvæmt reglugerðinni. Samþykki telst einungis hafa verið veitt ef hinn skráði hefur raunverulegt val um hvort hann samþykki, eða hafni, vinnslu persónuupplýsinga um sig. Það er ábyrgðaraðila að meta hvort skilyrðum samþykkis hefur verið fullnægt. Í leiðbeiningunum er farið yfir helstu atriði sem þarf að hafa í huga við slíkt mat.

2. Lagaumhverfi

Grundvallarskilyrði samþykkis eru að miklu leyti sambærileg skilyrðum samþykkis skv. lögum nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga. Þó eru gerðar ákveðnar breytingar. Til að mynda er tekið fram að samþykki verður að vera veitt með aðgerð. Í því felst m.a. að box sem þegar hefur verið hakað í á vefsíðu uppfylla ekki kröfur reglugerðarinnar. Þá er í 8. gr. pvrg. fjallað um sérstök skilyrði fyrir samþykki barna vegna þjónustu í upplýsingasamfélaginu. Í formálsorðum 32, 33, 42 og 43 má einnig finna nánari umfjöllun um notkun samþykkis sem heimildar fyrir vinnslu persónuupplýsinga

Ákvæði 11. tölul. 4. gr. pvrg. skilgreinir samþykki á eftirfarandi hátt:

- „Samþykki“ skráðs einstaklings: óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan.

Í 7. gr. pvrg. er síðan að finna nánari skilyrði fyrir samþykki:

- Þegar vinnsla er byggð á samþykki skal ábyrgðaraðilinn geta sýnt fram á að skráður einstaklingur hafi samþykkt vinnslu persónuupplýsinga sinna.
- Ef hinn skráði gefur samþykki sitt með skriflegri yfirlýsingu, sem einnig varðar önnur málefni, skal beiðnin um samþykki sett fram á þann hátt að hún sé auðgreinanleg frá hinum málefnunum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli. Ef einhver hluti slíkrar yfirlýsingar felur í sér brot á þessari reglugerð skal hann ekki vera bindandi.
- Skráður einstaklingur á rétt á að draga samþykki sitt til baka hvenær sem er. Afturköllun samþykkis skal ekki hafa áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni. Hinum skráða skal tilkynnt um þetta áður en hann gefur samþykki sitt. Jafnauðvelt skal vera að draga samþykki sitt til baka og að veita það.
- Þegar metið er hvort samþykki sé gefið af fúsum og frjálsum vilja skal taka ítrasta tillit til þess m.a. hvort það sé skilyrði fyrir framkvæmd samnings, þ. á m. veitingu þjónustu, að samþykki sé gefið fyrir vinnslu persónuupplýsinga sem ekki er nauðsynleg vegna framkvæmdar samningsins.

3. Hverjir eru helstu þættir samþykkis?

Í 11. tölul. 4. gr. pvrg. segir að samþykki hins skráða feli í sér:

- óþvingaða,
- sértæka (e. specific),
- upplýsta og
- ótvíræða viljayfirlýsingu hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan.

Hér á eftir má finna umfjöllun um hvern þessara þátta og að hvaða marki ábyrgðaraðilar þurfa að uppfæra samþykkiseyðublöð sín til að tryggja að kröfur reglugerðarinnar séu uppfylltar.

3.1 Óþvingað

Það að samþykki sé óþvingað felur í sér að það þarf að vera veitt af fúsum og frjálsum vilja. Ef hinn skráði er undir miklum þrýstingi að veita samþykki sitt eða ef hann þarf að sæta neikvæðum afleiðingum samþykki hann ekki, verður slíkt samþykki ekki talið uppfylla skilyrði þess að vera frjálst og óþvingað.

Sama gildir þegar hinum skráða er ekki mögulegt að afturkalla samþykki sitt án neikvæðra afleiðinga.

Þegar samþykki er sett fram sem órjúfanlegur hluti óumsemjanlegra skilmála þá er jafnframt gengið út frá því að samþykki hafi ekki verið veitt af fúsum og frjálsum vilja. Þá hefur í reglugerðinni einnig verið hugað að þeim aðstæðum þegar til staðar er valdaójafnvægi milli ábyrgðaraðila og hins skráða.

Dæmi 1

Smáforrit sem er hannað til að breyta ljósmyndum óskar eftir upplýsingum um staðsetningu notenda sinna. Forritið segir að tilgangur upplýsingaöflunarinnar sé að selja sérsniðnar auglýsingar (e. behavioural advertising). Hvorki staðsetning notenda né sérsniðnar auglýsingar teljast til kjarnaþjónustu smáforritsins. Ef notendur geta ekki nýtt sér þjónustu smáforritsins án þess að samþykkja vinnsluna þá telst samþykki ekki vera veitt af fúsum og frjálsum vilja.

3.1.1 Valdaójafnvægi

Í formálsorðum 43 kemur með skýrum hætti fram að ólíklegt sé að stjórnvöld geti byggt á samþykki þegar þau starfa innan valdheimilda sinna, þar sem þar sé til staðar valdaójafnvægi á milli ábyrgðaraðila og hins skráða. Þetta er einnig skýrt í tilvikum þegar hinn skráði á enga raunverulega möguleika á að samþykkja skilmála ábyrgðaraðila. Auk þessa eru aðrar heimildir til vinnslu persónuupplýsinga betur til þess fallnar að heimila vinnslu persónuupplýsinga hjá stjórnvöldum.

Þó er ekki þar með sagt að stjórnvöld geti aldrei unnið með persónuupplýsingar á grundvelli samþykkis hins skráða.

Dæmi 2

Sveitarfélag fyrirhugar að fara í verulegar vegaframkvæmdir við stóra umferðargötu, sem munu hafa mikil áhrif á umferð í sveitarfélaginu.

Sveitarfélagið ákveður því að bjóða borgurunum að skrá sig á póstlista þar sem þeir munu fá sendar upplýsingar um stöðu verksins, s.s. upplýsingar um hvaða daga megi gera ráð fyrir miklum töfum á umferð.

Öllum er frjálst að skrá sig á póstlistann, og hann verður ekki notaður í neinum öðrum tilgangi, en allar upplýsingarnar verða að auki birtar á vefsíðu sveitarfélagsins.

Þeir sem kjósa að skrá sig ekki á listann munu ekki verða af neinni kjarnaþjónustu sem sveitarfélagið veitir og telst samþykki þeirra vera frjálst og óháð í þessu tilviki.

Dæmi 3

Einstaklingur þarf að sækja um leyfi til bæði sveitarfélags og ráðuneytis. Nauðsynlegt er að skila inn sömu gögnum til beggja yfirvalda, en þau hafa ekki aðgang að gagnagrunni hvort annars. Hinn skráði sendir gögnin á bæði yfirvöldin, en þau óska eftir heimild hans til að sameina umsóknirnar til að koma í veg fyrir tvíverknað. Bæði yfirvöld leggja áherslu á að þetta sé valkvætt og að umsóknirnar verði afgreiddar aðskilið ef hann veitir ekki samþykki sitt. Í þessu tilviki getur hann veitt frjálst og óháð samþykki.

Dæmi 4

Grunnskóli óskar eftir heimild nemanda til að nota ljósmynd af honum í tímariti nemenda við skólann. Að því gefnu að synjun muni ekki hafa neikvæð áhrif á valkosti hans til náms eða þjónustu innan (eða utan) skólans getur hann eða forsjáraðili hans veitt frjálst og óháð samþykki.

Valdaójafnvægi getur einnig verið til staðar í vinnuréttarsambandi. Ólíklegt er að starfsmaður geti veitt frjálst og óháð samþykki, sem er ekki undir þeim þrýstingi sem fylgir vinnuréttarsambandinu, enda ólíklegt að hann geti synjað án þess að til staðar sé hætta á beinum eða óbeinum neikvæðum afleiðingum.

Það er því vandkvæðum bundið að vinna með persónuupplýsingar í vinnuréttarsambandi á grundvelli samþykkis hins skráða, en það er þó ekki útilokað.

Dæmi 5

Kvikmyndafyrirtæki á að taka upp myndskeið af hluta af skrifstofurými fyrirtækis. Fyrirtækið óskar eftir samþykki þeirra sem starfa á hæðinni fyrir vinnslu persónuupplýsinga um þá, enda geta þeir hæglega birst í bakgrunni myndskeiðsins. Þeir starfsmenn sem kjósa að veita ekki samþykki sitt geta fært sig tímabundið á skrifstofur sem standa þeim til boða þar sem myndataka mun ekki eiga sér stað.

Þrátt fyrir að hér sé einungis fjallað um valdaójafnvægi og aðstöðumun í vinnuréttarsambandi og samskiptum einstaklinga við stjórnvöld þá getur valdaójafnvægi einnig verið til staðar í öðrum tilvikum. Samþykki getur einungis átt við þegar ekki er til staðar hætta á blekkingu, þvingun, nauðung eða verulegum neikvæðum afleiðingum, s.s. auknum kostnaði við þjónustu.

3.1.2 Skilyrði sem ekki eru nauðsynleg vegna framkvæmdar samnings

Þegar metið er hvort samþykki sé veitt af fúsum og frjálsum vilja gegnir 4. mgr. 7. gr. pvrg. mikilvægu hlutverki en þar segir að taka skuli ítrasta tillit til þess m.a. hvort það sé skilyrði fyrir framkvæmd samnings, þ. á m. veitingu þjónustu, að samþykki sé gefið fyrir vinnslu persónuupplýsinga sem ekki er nauðsynleg vegna framkvæmdar samningsins.

Þetta leiðir m.a. til þess að mjög óæskilegt er að skeyta saman samþykki fyrir vinnslu persónuupplýsinga og samþykki fyrir almennum skilmálum (e. terms and conditions). Hið sama á við þegar ákvæði í samningi eða veiting þjónustu eru bundin við beiðni um samþykki fyrir vinnslu persónuupplýsinga. Ef samþykki er gefið við þessar aðstæður verður ekki litið svo á að það hafi verið gefið af fúsum og frjálsum vilja. Tilgangur 4. mgr. 7. gr. er að koma í veg fyrir að ákvæði um tilgang með vinnslu persónuupplýsinga séu ekki falin í samningsskilmálum sem eru oft langir og flóknir. Þá þarf að hafa í huga að heimildirnar tvær, samþykki og nauðsyn vegna samningsgerðar, er ekki hægt að sameina og ekki má gera mörk þeirra óljós.

Skylda til að samþykkja aðra vinnslu persónuupplýsinga en þá sem er algjörlega nauðsynleg við veitingu þjónustunnar dregur úr möguleikum hins skráða og stendur í vegi fyrir frjálsu og óháðu samþykki. Þar sem einn af grundvallarþáttum persónuverndarlöggjafarinnar er að tryggja grundvallarréttindi hins skráða er nauðsynlegt að hann hafi sjálfsákvörðunarrétt um vinnslu persónuupplýsinga um sig og í því skyni er sérstaklega ályktað í reglugerðinni að samþykki fyrir ónauðsynlegri vinnslu persónuupplýsinga geti ekki verið hluti af samningsskilmálum eða skilyrði fyrir veitingu þjónustu.

Þegar beiðni um samþykki er skeytt saman við framkvæmd samnings geta einstaklingar átt það á hættu að fá synjun um þá þjónustu sem þeir hafa óskað eftir. Til að leggja mat á hvort slík samskeyting er til staðar þarf að ákvarða gildissvið samningsins eða þjónustunnar sem veitt er. Samkvæmt áliti 29. gr. vinnuhópsins nr. 6/2014 (WP217) verður að túlka það sem er „nauðsynlegt fyrir framkvæmd samnings“ þröngt. Vinnslan þarf að vera nauðsynleg til að ábyrgðaraðili geti uppfyllt skyldur sínar samkvæmt samningnum, svo sem upplýsingar um heimilisfang til að hinn skráði geti fengið keypta vöru senda á heimilið, eða kreditkortaupplýsingar til að taka á móti greiðslu vegna þjónustunnar. Ef ábyrgðaraðilinn þarf að vinna persónuupplýsingar vegna framkvæmdar samnings þá byggir hann á viðeigandi heimild í b-lið 1. mgr. 6. gr. pvrg. Ekki er þörf á því að byggja á annarri heimild, eins og samþykki, og 4. mgr. 7. gr. á ekki við.[1]

Dæmi 6

Banki óskar eftir samþykki viðskiptavina sinna til að nota persónuupplýsingar um þá í markaðssetningartilgangi. Vinnslan er ekki nauðsynleg til að uppfylla samning við viðskiptavinina um hefðbundna bankaþjónustu. Ef synjun hins skráða leiðir til aukinnar gjaldtöku, synjunar á þjónustu eða lokunar bankareikinga, þá getur samþykki ekki verið grundvöllur fyrir vinnslu persónuupplýsinga.

Ef ábyrgðaraðili tengir vinnslu persónuupplýsinga við þá þjónustu sem hann veitir, en þjónustan er ekki nauðsynleg til að efna samninginn, skal ganga út frá því að samþykki sé ekki veitt af fúsum og frjálsum vilja. Ábyrgðaraðili ber sönnunarbyrði fyrir því að skilyrði samþykkis séu uppfyllt en orðalag 4. mgr. 7. gr. pvrg. gefur til kynna að ábyrgðaraðilar þurfa að gæta sérstakrar varúðar þegar samningur eða þjónusta inniheldur beiðni umn samþykki fyrir vinnslu persónuupplýsinga.[2]

3.1.3 Sérgreint samþykki

Ábyrgðaraðili getur óskað eftir persónuupplýsingum um hinn skráða í þeim tilgangi að framkvæma margar mismunandi vinnsluaðgerðir í mismunandi tilgangi. Í slíkum tilvikum ættu hinir skráðu að hafa val um hvaða tilgang þeir samþykkja, en þeir ættu ekki að þurfa að samþykkja vinnslu í margvíslegum tilgangi í einu lagi. Því getur verið nauðsynlegt að afla nokkurra samþykkisyfirlýsinga frá hinum skráða áður en hægt er að veita þjónustu.

Eins og fram kemur í formálsorðum 43 telst samþykki ekki veitt af fúsum og frjálsum vilja ef ekki er hægt að veita sérstakt samþykki fyrir aðskildum aðgerðum við vinnslu persónuupplýsinga, þótt slíkt ætti við í því einstaka tilviki. Samþykki ætti að ná til allrar vinnslustarfsemi sem fram fer í sama tilgangi, einum eða fleiri. Þegar vinnslan er í margvíslegum tilgangi ætti að gefa samþykki fyrir hverjum og einum þeirra, eins og fram kemur í formálsorðum 32.

---

[1] Athuga skal þó að heimild til vinnslu viðkvæmra persónuupplýsinga getur ekki byggst á samningi. Því þurfa ábyrgðaraðilar sem vinna slíkar upplýsingar að styðja vinnsluna við aðra heimild í 9. gr. reglugerðarinnar.
[2] Sjá nánari umfjöllun um þetta atriði í leiðbeiningum 29. gr. vinnuhópsins um samþykki, bls. 9 og 10.

Dæmi 7

Ábyrgðaraðili óskar eftir samþykki hins skráða til að varðveita tölvupóstfang hans í markaðssetningartilgangi annars vegar og til að deila því með öðrum fyrirtækjum í sömu fyrirtækjasamstæðu hins vegar. Ef ábyrgðaraðili veitir hinum skráða ekki tækifæri til að samþykkja vinnslu í hvorum tilgangi fyrir sig þá telst samþykkið ekki vera frjálst og óháð.

3.1.4 Afturköllun samþykkis og skaðleysi

Ábyrgðaraðili þarf að sýna fram á að hinn skráði geti afturkallað samþykki sitt án þess að verða fyrir neikvæðum afleiðingum, en sem dæmi um neikvæðar afleiðingar má nefna ef hinn skráði verður fyrir auknum kostnaði eða ef hann fær lakari þjónustu. Ef hinn skráði þarf að þola neikvæðar afleiðingar þess að veita ekki samþykki sitt fyrir vinnslu persónuupplýsinga telst samþykkið ekki vera frjálst og óháð.

3.2 Sértækt samþykki

Til að samþykki teljist vera fullnægjandi í skilningi reglugerðarinnar verður hinn skráði að vera upplýstur um hvaða persónuupplýsingar á að vinna með og í hvaða tilgangi. Þá á einstaklingurinn að hafa val um hvaða tilgang hann samþykkir og hvaða tilgang hann samþykkir ekki. Þetta er nátengt skilyrðunum um *upplýst* samþykki og *sérgreint* samþykki, sbr. kafla 2.2.3. Athuga skal að hér er ekki um að ræða breytingu frá gildandi rétti.

Til að uppfylla þetta skilyrði samþykkis þarf ábyrgðaraðili að:

- tilgreina tilgang til að koma í veg fyrir að persónuupplýsingar séu notaðar í öðrum og ósamrýmanlegum tilgangi,
- tryggja að samþykkið sé sérgreint, og
- tryggja að skýrt sé skilið á milli upplýsinga sem tengjast því að fá samþykki fyrir vinnslu persónuupplýsinga og upplýsinga um önnur atriði.

Þessu skilyrði er ætlað að koma í veg fyrir að persónuupplýsingar séu notaðar í tilgangi sem er annar en sá sem persónuupplýsinganna var upphaflega aflað í og upphaflegt samþykki tók til. Ef ábyrgðaraðili óskar eftir að vinna með persónuupplýsingar hins skráða í öðrum tilgangi en þeim sem var tilgreindur upphaflega skal hann jafnframt óska eftir samþykki hins skráða fyrir vinnslu í hinum nýja tilgangi.

Dæmi 8

Sjónvarpsstöð vinnur með persónuupplýsingar um áskrifendur sína á grundvelli samþykkis til að bjóða þeim upp á kvikmyndir sem henta viðkomandi einstaklingum, en tillögur sjónvarpstöðvarinnar byggja á áhorfssögu viðkomandi. Ef sjónvarpsstöðin vill deila upplýsingunum með þriðja aðila, t.d. til að birta fyrir áskrifendunum sérsniðnar auglýsingar, þá þyrfti að afla viðbótarsamþykkis fyrir þeirri vinnslu.

3.3 Upplýst samþykki

Reglugerðin gerir auknar kröfur til þess að samþykki sé upplýst. Þessi skylda er nátengd meginreglunni um sanngirni og lögmæti, sbr. 5. gr. pvrg. Veiting upplýsinga af hálfu ábyrgðaraðila um vinnslu persónuupplýsinga, áður en samþykkis er aflað, er nauðsynleg til þess að hinn skráði skilji hvað hann er að samþykkja, afleiðingar samþykkis og að honum sé heimilt að afturkalla

samþykki sitt. Ef ábyrgðaraðili veitir ekki fullnægjandi og aðgengilegar upplýsingar um vinnsluna getur beiðni um samþykki orðið villandi og samþykkið þ.a.l. talist ófullnægjandi.

3.3.1 Lágmarksfræðsla til að samþykki teljist upplýst

Til að samþykki teljist vera upplýst er nauðsynlegt að upplýsa hinn skráða um tiltekin atriði svo að hann geti tekið ákvörðun um hvort hann samþykki vinnsluna. Af hálfu 29. gr. vinnuhópsins er talið að eftirfarandi atriði þurfi að lágmarki að koma fram:

- Heiti ábyrgðaraðila
- Tilgangur hverrar vinnsluaðgerðar sem óskað er samþykkis fyrir
- Hvaða persónuupplýsingar er fyrirhugað að vinna með
- Rétturinn til að afturkalla samþykki
- Hvort fram fer sjálfvirk ákvörðunartaka, sbr. 22. gr. pvrg.
- Hvort miðla á persónuupplýsingunum til þriðja ríkis án þess að fullnægjandi vernd liggi fyrir.

3.3.2 Hvernig veita skal fræðslu

Reglugerðin gerir engar sérstakar kröfur um á hvaða formi skuli veita fræðslu, en hana má t.d. veita munnlega, skriflega eða með myndbandi. Engu að síður gerir reglugerðin ákveðnar kröfur til framsetningar, sbr. sérstaklega ákvæði 2. mgr. 7. gr. og formálsorð 32.

Þannig þarf fræðslan að vera einföld og á auðskiljanlegu máli. Til að uppfylla þessa skyldu þarf ábyrgðaraðili m.a. að gera sér grein fyrir því hverjir séu hinir skráðu. Ef hinir skráðu eru t.d. börn þarf fræðslan að vera þannig úr garði gerð að hún sé á máli sem þau skilja.

Fræðslan[3] þarf auk þess að vera aðskilin frá öðrum upplýsingum sem ekki varða vinnslu persónuupplýsinga. Sem dæmi má nefna að ef samningur inniheldur fjölda atriða sem koma vinnslu persónuupplýsinga ekki við þá skal sú fræðsla sem liggur samþykkinu að baki að vera áberandi og aðskilin frá öðrum ótengdum upplýsingum, eða í sérskjali. Sömu sjónarmið eiga við þegar um er að ræða samþykki sem er veitt með rafrænum hætti, en líkt og áður greinir er óheimilt að fela samþykki til vinnslu persónuupplýsinga meðal annarra ákvæða í samningi. Þá þarf einnig að skoða þá tækni sem notuð er við að veita fræðsluna. T.a.m. getur verið æskilegt við öflun samþykkis í gegnum smáforrit í snjallsíma að setja upplýsingarnar fram í nokkrum aðskildum skrefum (e. layered way of presenting information).

Dæmi 9

Fyrirtæki hefur fengið ábendingar um að óljóst sé í hvaða tilgangi það ætli að nýta sér þær persónuupplýsingar sem það hefur óskað eftir samþykki fyrir að vinna með. Fyrirtækið ákveður því að grípa til aðgerða til að ganga úr skugga um að fræðslan sé skiljanleg og býr til rýnihópa sem samanstanda af þverskurði af viðskiptavinahópi fyrirtækisins til að kanna skilning þeirra á fræðslunni. Rýnihóparnir lesa fræðslutextann og eru í kjölfarið beðnir að svara spurningalista til að kanna skilning þeirra. Með þessari leið getur fyrirtækið gengið úr skugga um að fræðslan hafi verið á skýru og auðskiljanlegu máli.

Dæmi 10

Fyrirtæki vinnur persónuupplýsingar á grundvelli samþykkis. Fræðslan og samþykkið voru á rafrænu formi og í mörgum skrefum (e. layered) þar sem finna mátti allar nauðsynlegar upplýsingar, að undanskildum

[3] Sjá nánari umfjöllun um fræðsluskyldu ábyrgðaraðila og upplýsingarétt hinna skráðu í leiðbeiningum Persónuverndar um gagnsæi.

upplýsingum um hvernig hafa mætti samband við persónuverndarfulltrúa fyrirtækisins. Samþykkið telst upplýst í skilningi pvrg., sbr. kafla 2.3.1., jafnvel þótt fræðslu um persónuverndarfulltrúann hafi verið ábótavant.

3.4 Ótvírætt samþykki

Í reglugerðinni er skýrt tekið fram að samþykki verði einungis veitt með skýrri staðfestingu sem feli ávallt í sér einhvers konar aðgerð eða yfirlýsingu, eins og nánar er greint frá í formálsorðum 32. Það þarf að vera augljóst að hinn skráði hafi samþykkt vinnsluna. Í lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga er kveðið á um að samþykki þurfi að veita með ótvíræðri yfirlýsingu um að hinn skráði sé samþykkur vinnslunni. Í reglugerðinni er áfram kveðið á um að samþykkið skuli veitt með yfirlýsingu eða ótvíræðri staðfestingu. Í þessu felst að samþykki verður að vera veitt með einhvers konar aðgerð af hálfu hins skráða.

Heimilt er því að veita yfirlýsinguna munnlega, skriflega eða með rafrænum hætti. Aðgerðaleysi, svo sem box sem þegar hefur verið hakað í, fullnægir hins vegar ekki skilyrðum reglugerðarinnar um ótvírætt samþykki. Þá er ekki hægt að líta á þögn hins skráða og það að hann haldi áfram að nota tiltekna þjónustu sem aðgerð í skilningi reglugerðarinnar.

Þá er vakin athygli á því að samþykki er ekki hægt að veita samhliða undirritun samnings eða viðurkenningu á almennum skilmálum. Slíkt telst ekki uppfylla skilyrði reglugerðarinnar til ótvíræðs samþykkis fyrir vinnslu persónuupplýsinga

Ábyrgðaraðilum er í sjálfsvald sett hvaða aðferðir þeir nota til að uppfylla skilyrði til ótvíræðs samþykkis.

Dæmi 11

Þegar einstaklingur hleður niður hugbúnaði óskar forritið eftir samþykki til að nota upplýsingar um nafn notenda til að senda skýrslur um frávik (e. crash reports) til að bæta hugbúnaðinn. Persónuverndarstefna, sem inniheldur nauðsynlegar upplýsingar, fylgir með beiðninni um samþykki. Með því að haka í valkvæðan kassa þar sem við stendur „Ég samþykki“, hefur hinn skráði veitt samþykki með skýrri staðfestingu.

Dæmi 12

Tilteknar aðgerðir á farsíma, t.d. að strjúka til hægri, veifa í myndavélina eða snúa símanum á tiltekinn hátt, geta flokkast undir ótvírætt samþykki ef fullnægjandi upplýsingar eru veittar og aðgerðin er nægilega ótvíræð. Ábyrgðaraðili þarf þó að geta sýnt fram á að samþykki hafi verið veitt á þennan hátt og að hægt sé að afturkalla samþykkið jafnauðveldlega og það var veitt.

Dæmi 13

Að fletta niður á farsíma í gegnum skilmála sem innihalda yfirlýsingu um samþykki, jafnvel þegar sérstaklega er tilkynnt um að litið verði svo á að áframhaldandi fletting feli í sér samþykki, fullnægir ekki kröfum pvrg. Hinn skráði getur auðveldlega farið á mis við aðvörunina þegar hann flettir hratt í gegnum mikinn texta, en í því tilviki er ekki hægt að fullyrða að samþykki hafi ótvírætt verið veitt.

Mörg fyrirtæki í stafrænu umhverfi þurfa að afla persónuupplýsinga til að geta veitt hinum skráðu tiltekna þjónustu. Hinir skráðu geta því jafnvel fengið margar beiðnir á hverjum degi um samþykki, sem þarf að svara. Við þessar aðstæður er hætta á því að það skapist samþykkisþreyta, þ.e.a.s. að hinn skráði lesi ekki þá fræðslu sem honum er veitt og honum sé því ókunnugt um þá vinnslu persónuupplýsinga sem óskað er samþykkis fyrir. Í reglugerðinni er lögð sú skylda á ábyrgðaraðila að útfæra aðferðir til að kljást við þetta vandamál, svo sem með því að hinn skráði veiti samþykki

sitt í viðkomandi netvafra en ekki á einstökum vefsíðum. Athygli er þó vakin á því að slíkt samþykki þarf að uppfylla skilyrði reglugerðarinnar til samþykkis, þ. á m. til sérgreinds samþykkis.

Þrátt fyrir að ekki sé kveðið á um það berum orðum í reglugerðinni að afla þurfi samþykkis áður en hafist er handa við vinnslu persónuupplýsinga, þá segir í 1. tölul. 1. mgr. 6. gr. reglugerðarinnar að vinnsla persónuupplýsinga sé lögmæt ef skráður einstaklingur *hefur* gefið samþykki sitt fyrir vinnslunni. Nauðsynlegt er því að afla samþykkis hins skráða áður en vinnsla persónuupplýsinga hefst, auk þess sem nauðsynlegt er að afla nýs samþykkis ef vinna á með persónuupplýsingar í öðrum tilgangi en upphaflega var áætlað.

4. Afdráttarlaust samþykki

Við þær aðstæður þar sem mikil áhætta er fólgin í vinnslu persónuupplýsinga og eðlilegt þykir að einstaklingurinn hafi mikla stjórn yfir sínum upplýsingum þarf samþykkið að vera afdráttarlaust. Þetta á sérstaklega við þegar um er að ræða vinnslu viðkvæmra persónuupplýsinga, þegar persónuupplýsingar eru fluttar úr landi og við sjálfvirka ákvarðanatöku, þ.m.t. við gerð/notkun persónusniða.

Það að samþykki skuli vera afdráttarlaust felur í sér að hinn skráði þarf að gefa frá sér yfirlýsingu. Auðveldasta leiðin til að gera það er að afla skriflegrar yfirlýsingar, jafnvel undirritaðrar af hinum skráða. Hins vegar er sú aðferð ekki eina leiðin til að afla samþykkis sem er afdráttarlaust. Þannig má sjá fyrir sér að hinn skráði geti veitt afdráttarlaust samþykki með því að fylla út rafrænt eyðublað, senda tölvupóst, skanna skjal sem inniheldur undirskrift hins skráða eða með því að nota rafræna undirskrift.

Dæmi 14

Lýtalæknastofa óskar eftir afdráttarlausu samþykki sjúklings fyrir flutningi á rafrænni sjúkraskrá hans til annars sérfræðings sem óskað er læknisfræðilegs álits hjá. Í ljósi þess hversu viðkvæmar umræddar upplýsingar eru óskar lýtalæknastofan eftir rafrænni undirritun sjúklingsins í þeim tilgangi að fá frá honum afdráttarlaust samþykki og sýna fram á að það hafi verið fengið.

Þá væri einnig hægt að afla samþykkis í tveimur skrefum. Dæmi um þetta er að hinn skráði fær tölvupóst þar sem hann er upplýstur um þá ætlun ábyrgðaraðila að vinna persónuupplýsingar upp úr skrá sem inniheldur heilsufarsupplýsingar. Ábyrgðaraðilinn útskýrir í tölvupóstinum að hann óski eftir samþykki hins skráða fyrir notkun á ákveðnum upplýsingum í afmörkuðum tilgangi. Ef hinn skráði samþykkir notkun þessara upplýsinga óskar ábyrgðaraðilinn eftir því að hinn skráði svari tölvupóstinum með yfirlýsingunni „Ég samþykki“. Eftir að svarið hefur verið sent fær hinn skráði sendan tengil á staðfestingarsíðu eða SMS með staðfestingarkóða, til að hann geti samþykkt fyrirkomulagið.

5. Aðrar kröfur

Reglugerðin leggur auknar skyldur á ábyrgðaraðila til að tryggja að þeir afli samþykkis og geti sýnt fram á að hinn skráði hafi samþykkt vinnslu persónuupplýsinga um sig.

5.1 Ábyrgðarskyldan og samþykki

Ábyrgðaraðili þarf að geta sýnt fram á að hinn skráði hafi veitt samþykki sitt. Ábyrgðaraðila er í sjálfsvald sett hvernig hann uppfyllir þessa skyldu, en það ætti þó ekki að leiða til vinnslu

persónuupplýsinga umfram það sem nauðsynlegt er. Ábyrgðaraðili mætti t.d. varðveita yfirlit yfir veitt samþykki til að hann geti sýnt fram á að samþykki hafi verið veitt, hvernig það var veitt og hvenær það var veitt. Þá skal hann einnig geta sýnt fram á að hinum skráða hafi verið veitt viðeigandi fræðsla.

Á meðan vinnsla á grundvelli samþykkis fer fram þarf ábyrgðaraðili að varðveita sönnun þess að hinn skráði hafi veitt samþykki sitt. Eftir þann tíma ber ábyrgðaraðila að eyða upplýsingunum nema til staðar séu málefnalegar ástæður fyrir varðveislu þeirra, svo sem vegna lagaskyldu eða nauðsynjar til að krafa verði afmörkuð, sett fram eða varin vegna dómsmáls.

Dæmi 15

Framkvæma á vísindarannsókn á heilbrigðissviði á heilbrigðisstofnun sem felur m.a. í sér að nauðsynlegt er að afla upplýsinga um tannheilsu tiltekinna sjúklinga. Haft er samband við sjúklingana símleiðis og þeim boðið að taka þátt í rannsókninni. Sjúklingarnir veita samþykki sitt í símtalinu, en það er hljóðritað og afrit varðveitt til að sýna fram á að samþykki hafi verið veitt.

Þá er vakin athygli á því að þrátt fyrir að ábyrgðaraðila sé það ekki skylt er mælt með því að samþykki sé endurnýjað reglulega.

5.2 Afturköllun samþykkis

Persónuverndarreglugerðin leggur aukna áherslu á afturköllun samþykkis og þannig segir að jafnauðvelt skuli vera að afturkalla samþykki eins og það var að veita það. Það þarf þó ekki endilega að vera gert á sama hátt. Hér má til dæmis nefna að ef samþykki var veitt með því að strjúka til hliðar á snjallsíma, eða haka í kassa á vefsíðu fyrirtækisins, þá ætti að vera jafnauðvelt að afturkalla samþykkið. Þá verður hinn skráði að geta afturkallað samþykki sitt án þess að verða fyrir neikvæðum afleiðingum í kjölfarið, en í því felst m.a. að ábyrgðaraðila er ekki heimilt að rukka gjald fyrir afturköllun samþykkis og hinn skráði má ekki verða fyrir þjónustuskerðingu vegna afturköllunarinnar.

Dæmi 16

Miði á tónlistarhátíð var keyptur á Netinu, en í kaupunum var veitt samþykki fyrir vinnslu persónuupplýsinga í markaðssetningartilgangi. Til að afturkalla samþykkið þarf að hringja í símaver tónlistarhátíðarinnar á skrifstofutíma, þ.e. milli kl. 8-17, en símtalið er gjaldfrjálst.

Í þessu tilfelli er ekki jafnauðvelt að afturkalla samþykkið og það var að veita það. Músarsmellur á Netinu sem má framkvæma hvenær sem er er ekki sambærilegur við að þurfa að hringja símtal á tilteknum tíma.

Ef hinn skráði afturkallar samþykki sitt þarf ábyrgðaraðili að hætta þeirri vinnslu sem fór fram á grundvelli samþykkis. Að meginreglu til skal vinnsla persónuupplýsinga í tilteknum tilgangi einungis fara fram á grundvelli einnar ákveðinnar heimildar, s.s. samþykkis, en hægt er að vinna með persónuupplýsingar í fleiri en einum tilgangi og þá á grundvelli fleiri en einnar heimildar. Grundvöllur vinnslu í tilteknum tilgangi þarf að vera ákveðinn fyrirfram og honum má ekki breyta eftir hentisemi ábyrgðaraðila.

6. Samspil samþykkis og annarra vinnsluheimilda í pvrg.

Eins og fyrr segir er samþykki ein af þeim heimildum sem hægt er að byggja á við vinnslu persónuupplýsinga samkvæmt reglugerðinni. Almennt getur vinnsla persónuupplýsinga í tilteknum tilgangi ekki grundvallast á fleiri en einni vinnsluheimild. Mögulegt er þó að vinnsla sömu

persónuupplýsinga í mismunandi tilgangi hjá sama ábyrgðaraðila geti grundvallast á mismunandi vinnsluheimildum, svo sem samþykki annars vegar og samningi hins vegar. Ábyrgðaraðili þarf að ákveða á grundvelli hvaða vinnsluheimildar vinnsla persónuupplýsinga fer fram áður en vinnsla hefst, en honum er ekki heimilt að skipta á milli vinnsluheimilda eftir að vinnsla hefst. Ábyrgðaraðila er því t.d. ekki heimilt að byggja vinnslu persónuupplýsinga á lögmætum hagsmunum, sbr. f-lið 1. mgr. 6. gr. pvrg., eftir að upp kemur að skilyrðum samþykkis fyrir vinnslu persónuupplýsinga var ekki fullnægt. Þá er einnig vakin athygli á að skv. c-lið 1. mgr. 13. gr. pvrg. ber ábyrgðaraðila að fræða hinn skráða um lagagrundvöll vinnslunnar.

7. Önnur atriði

7.1 Samþykki barna

Persónuupplýsingar barna njóta sérstakar verndar samkvæmt reglugerðinni og í 8. gr. hennar er að finna sérstakt ákvæði um samþykki barna í tengslum við þjónustu í upplýsingasamfélaginu. Í ákvæðinu kemur fram að þegar vinnsla er byggð á samþykki, í tengslum við það þegar barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti, skuli slík vinnsla teljast lögmæt ef barn hefur náð a.m.k. 16 ára aldri. Hafi barn ekki náð 16 ára aldri skal vinnslan einungis teljast lögmæt ef, og að því marki sem, forsjáraðili barnsins gefur eða heimilar samþykkið. Aðildarríki geta kveðið á um lægri aldur í lögum en þó ekki lægri en 13 ára.[4]

Ástæða þess að börnum er veitt aukin vernd er sú að þau kunna að vera síður meðvituð um áhættu, afleiðingar, verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga. Þessi sérstaka vernd á einkum við um notkun persónuupplýsinga barna í markaðssetningarskyni, þegar búin eru til persónu- eða notendasnið og um söfnun persónuupplýsinga um börn þegar þau nota þjónustu sem þeim er boðin beint. Samþykki forsjáraðila er þó ekki nauðsynlegt þegar um er að ræða forvarnar- eða ráðgjafarþjónustu sem barni er boðin beint.

Ákvæði 8. gr. pvrg. eiga því einungis við þegar:

- barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti, og
- vinnslan fer fram á grundvelli samþykkis.

Með þjónustu í upplýsingasamfélaginu er átt við samninga og aðra þjónustu sem veitt er á Netinu. Ef um að ræða tvær aðgerðir, s.s. kaup og sölu á Netinu annars vegar og afhendingu vörunnar hins vegar, myndi sú fyrrnefnda teljast til þjónustu í upplýsingasamfélaginu en ekki sú síðarnefnda. Eins og áður segir verður þjónustan að vera boðin barni með beinum hætti. Í því felst að ef ábyrgðaraðili undanskilur börn undir 18 ára aldri frá þjónustunni, svo sem með efni síðunnar eða markaðssetningu, verður ekki talið að þjónustan sé boðin barni með beinum hætti.

Ábyrgðaraðili verður að grípa til eðlilegra ráðstafana til að ganga úr skugga um að notandi hafi náð lágmarksaldri samkvæmt lögum til að geta veitt samþykki sitt. Þær ráðstafanir skulu taka mið af eðli þeirra persónuupplýsinga sem er safnað og umfangi vinnslunnar. Athygli er vakin á því að ef vinnsla persónuupplýsinga fer fram á grundvelli samþykkis barns, sem hefur ekki náð þeim aldri sem krafist er í reglugerðinni eða landslögum, er ekki um að ræða fullnægjandi vinnsluheimild.

[4] Athuga skal að drög að frumvarpi til nýrra persónuverndarlaga gera ráð fyrir 13 ára aldursmarki á Íslandi. Þetta getur verið mismunandi eftir löndum innan Evrópu. Fyrirtæki sem er í starfsemi sem þessari geta því þurft að kanna innlenda löggjöf á hverjum þeim stað þar sem þjónustan er boðin.

Reglugerðin mælir ekki fyrir um hvernig afla á samþykkis eða staðfestingar frá forsjáraðila. Við öflun slíks samþykkis eða staðfestingar þarf að gæta meðalhófs og því mælir 29. gr. vinnuhópurinn með því að leggja áherslu á að safna eingöngu nauðsynlegum upplýsingum, s.s. tengiliðaupplýsingum foreldris eða forsjáraðila. Þá þarf einnig að meta umfang upplýsingasöfnunarinnar út frá eðli þeirra persónuupplýsinga sem unnið er með og umfangi vinnslunnar. Ef áhættan er lítil getur verið fullnægjandi að óska eftir tölvupóstfangi hjá forsjáraðila til að afla samþykkis hans.

Dæmi 17

Vettvangur fyrir tölvuleiki á Netinu (ábyrgðaraðili) vill sjá til þess að vinnsla persónuupplýsinga um ólögráða einstaklinga fari eingöngu fram á grundvelli samþykkis foreldra eða forsjáraðila. Ábyrgðaraðilinn tekur eftirfarandi skref:

1. Hann óskar eftir staðfestingu viðkomandi spilara á því að hann sé eldri en 16 ára (miðað er við þann aldur sem tilgreindur er í 8. gr. pvrg.)

2. Hann tilkynnir börnum að foreldri eða forsjáraðili þurfi að samþykkja vinnsluna og óskar eftir netfangi foreldris/forsjáraðila.

3. Ábyrgðaraðilinn hefur samband við foreldri eða forsjáraðila til að fá samþykki hans með tölvupósti og gerir eðlilegar ráðstafanir til að tryggja að viðkomandi fari með forsjá yfir barninu.

4. Ef ábyrgðaraðila berst kvörtun skal hann framkvæma frekari ráðstafanir til að tryggja að viðkomandi fari með forsjá yfir barninu.

Samþykki foreldra rennur út þegar hinn skráði nær þeim aldri sem tiltekinn er í 8. gr., en þá þarf að afla samþykkis viðkomandi fyrir vinnslunni.

7.2 Vísindarannsóknir

Oft er ekki hægt að greina tilgang með vinnslu persónuupplýsinga í þágu vísindarannsókna að fullu þegar upplýsingunum er safnað. Því ættu skráðir einstaklingar að geta gefið samþykki sitt fyrir vinnslu á tilteknum sviðum vísindarannsókna þegar þær samrýmast viðurkenndum, siðferðislegum viðmiðunum fyrir vísindarannsóknir. Skráðir einstaklingar ættu að hafa tækifæri til að veita samþykki sitt einungis á tilteknum sviðum rannsókna eða fyrir hlutum rannsóknarverkefna, að því marki sem fyrirhugaður tilgangur leyfir, sbr. formálsorð 33.

Með þessu er þó ekki verið að afnema skilyrðið um að samþykki sé sértækt, en þegar tilgangur vísindarannsókna er óljós í upphafi getur verið vandkvæðum bundið að uppfylla skilyrði samþykkis samkvæmt pvrg. Í þeim tilvikum veita því formálsorð 33 ákveðna undanþágu fyrir ábyrgðaraðila vísindarannsókna til að orða upplýsingar um tilgang vinnslunnar á almennari hátt. Hér verður þó, eins og í hvívetna, að meta skýrleikann með hliðsjón af eðli og umfangi vinnslunnar, en gera verður kröfur til aukins skýrleika ef vinna á með t.d. viðkvæmar persónuupplýsingar.

Ef ábyrgðaraðili vísindarannsókna getur ekki að fullu tilgreint tilgang rannsóknarinnar þarf hann að leita annarra leiða til að tryggja að grundvallarmarkmiði með samþykki hinna skráðu sé náð, til að mynda með því að óska eftir almennu samþykki og fyrir tiltekin stig rannsóknarinnar. Eftir því sem rannsókninni vindur fram er síðan hægt að afla sérstaks samþykkis áður en hvert stig hennar hefst. Slíkt samþykki skal þó ávallt vera í samræmi við siðareglur um vísindarannsóknir. Einnig geta önnur atriði á borð við skýra rannsóknaráætlun með rannsóknarspurningu, gagnsæi, dulkóðun og lágmörkun gagna lagt lóð á vogarskálarnar þegar það er vandkvæðum bundið að setja fram skýrar

upplýsingar um tilgang vinnslunnar. Að lokum þarf að hafa í huga að hinir skráðu eiga ávallt rétt á því að draga samþykki sitt til baka.

7.3 Réttindi hins skráða

Það að vinnsla persónuupplýsinga fari fram á grundvelli samþykkis ræður nokkru um það hvaða réttindi hinn skráði á samkvæmt reglugerðinni. Þannig á hinn skráði þá rétt á að flytja gögn sín á milli ábyrgðaraðila eða fá þau flutt til sín samkvæmt 20. gr. pvrg. en að sama skapi á hann ekki rétt á að andmæla vinnslu persónuupplýsinga um sig, byggist vinnslan á samþykki hans.

7.4 Samþykki veitt fyrir gildistöku persónuverndarreglugerðarinnar

Þeir ábyrgðaraðilar sem byggja vinnslu persónuupplýsinga á samþykki í samræmi við lög nr. 77/2000 eru ekki sjálfkrafa skyldugir til að endurnýja öll samþykki áður en reglugerðin kemur til framkvæmda. Samþykki sem veitt var áður en reglugerðin kemur til framkvæmda þann 25. maí 2018 heldur gildi sínu, að því gefnu að það uppfylli kröfur reglugerðarinnar.

Þannig þurfa ábyrgðaraðilar að endurskoða verkferla sína og skrár til að ganga úr skugga um að samþykki sem þegar hafa verið veitt uppfylli kröfur reglugerðarinnar (sjá nánar í formálsorðum 171). Ef ábyrgðaraðili kemst að þeirri niðurstöðu að samþykki, sem veitt var áður en reglugerðin kemur til framkvæmda, uppfylli ekki kröfur hennar þarf hann meta hvort vinnslan geti byggst á annarri heimild til vinnslu persónuupplýsinga í reglugerðinni. Þetta þarf að gerast áður en reglugerðin kemur til framkvæmda og hér þarf að hafa í huga að eftir það tímamark er ábyrgðaraðila ekki heimilt að skipta á milli þeirra ákvæða sem heimila vinnslu persónuupplýsinga.

Ábyrgðaraðila er óheimilt að halda áfram vinnslu persónuupplýsinga ef hann getur ekki endurnýjað samþykki hins skráða, þannig að það uppfylli kröfur reglugerðarinnar og ef hann getur ekki byggt á annarri heimild til vinnslu persónuupplýsinga á sama tíma og að hann tryggir að vinnslan sé sanngjörn og málefnaleg.