PERSÓNU VERND

FRÆÐSLUEFNI FYRIR PERSÓNUVERNDAR-FULLTRÚA

Þetta rit var fjármagnað af Evrópusambandinu
- The European Union's Rights, Equality and Citizenship programme (2014-2020)

Efni þessa rits er unnið af Persónuvernd sem ber fulla ábyrgð á því. Framkvæmdastjórn Evrópusambandsins ber enga ábyrgð á notkun þeirra upplýsinga sem ritið hefur að geyma.

2. útgáfa, október 2018

Efnisyfirlit

Almennt

Um meðferð og vinnslu persónuupplýsinga gilda lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (pvl.) sem tóku gildi 15. júlí 2018 og leystu af hólmi eldri lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Þau lögfestu jafnframt reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (hér eftir persónuverndarreglugerðin, eða pvrg.), eins og hún var aðlöguð og tekin upp í EES-samninginn.

Persónuvernd hefur gefið út fjölda leiðbeininga sem nýst geta þeim sem vinna með persónuupplýsingar. Þá hefur Evrópska persónuverndarráðið (European Data Protection Board - EDPB) gefið út leiðbeiningar um ýmis málefni tengd persónuverndarlöggjöfinni. Ráðið hefur jafnframt staðfest tilteknar leiðbeiningar forvera síns, svokallaðs 29. gr. vinnuhóps ESB, er varða almennu persónuverndarreglugerðina.

Ein af þeim nýjungum, sem kynntar voru til sögunnar með persónuverndarreglugerð ESB, er skylda til að tilnefna persónuverndarfulltrúa hjá öllum stofnunum og sumum fyrirtækjum. Samkvæmt reglugerðinni er tilteknum aðilum skylt að tilnefna persónuverndarfulltrúa, t.d. stjórnvöldum og öðrum stofnunum. Þá er fyrirtækjum jafnframt gert að tilnefna persónuverndarfulltrúa ef meginstarfsemi þeirra felur í sér vinnsluaðgerðir sem krefjast, sakir eðlis síns, umfangs og/eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum.

Persónuverndarfulltrúi er sá aðili sem ber sérstaka ábyrgð á málefnum fyrirtækisins eða stofnunarinnar sem tengjast persónuvernd. Verkefni hans er einkum að tryggja að fyrirtækið eða stofnunin uppfylli kröfur persónuverndarlöggjafarinnar. Persónuverndarfulltrúar aðstoða fyrirtæki og stofnanir við að sinna innra eftirliti, upplýsa og ráðleggja vegna persónuverndarlöggjafarinnar, veita ráðgjöf við framkvæmd mats á áhrifum á persónuvernd og eru tengiliðir við einstaklinga og Persónuvernd. Persónuverndarfulltrúi skal tilnefndur á grundvelli faglegrar hæfni sinnar, einkum sérþekkingar á persónuverndarlögum og lagaframkvæmd á því sviði.

Í persónuverndarreglugerðinni er litið á persónuverndarfulltrúann sem lykilstarfsmann og mælir hún fyrir um skilyrði fyrir ráðningu hans, stöðu og verkefni. Markmiðið er að gefa hlutverki hans vægi í því skyni að tryggja að ábyrgðaraðilar og vinnsluaðilar fari að reglunum og styrkja jafnframt persónuverndarfulltrúann í störfum sínum. Eitt af hlutverkum persónuverndarfulltrúa er að upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt persónuverndarlöggjöfinni og veita þeim ráðgjöf þar að lútandi. Með vitundarvakningu og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi hefur persónuverndarfulltrúi eftirlit með því að gætt sé að vernd persónuupplýsinga.

Í þessu riti verður fjallað um helstu reglur persónuverndarlaganna og persónuverndarreglugerðarinnar, sem allir persónuverndarfulltrúar þurfa að kunna skil á. Um er að ræða yfirlitsrit sem nýtist þeim sem starfa sem persónuverndarfulltrúar, sem og þeim sem hafa hug á slíku starfi. Er ritinu ætlað að gefa persónuverndarfulltrúum yfirlit yfir hlutverk þeirra og verkefni samkvæmt löggjöfinni og jafnframt vera þeim til stuðnings við að rækja skyldur sínar í starfi, m.a. fræðslu til starfsmanna um grunnfræði persónuverndar. Til þess að unnið sé með persónuupplýsingar á viðhlítandi máta er lykilatriði að þeir starfsmenn sem vinna með þær hafi þekkingu og skilning á grunnhugtökum eins og hvað persónuupplýsingar eru, hver er munurinn á almennum og viðkvæmum persónuupplýsingum, hvað felst í vinnslu persónuupplýsinga, hverjar eru meginreglur persónuverndarlöggjafarinnar og hverjar eru heimildirnar til vinnslu persónuupplýsinga.

Ljóst er að ekki er hægt að setja fram tæmandi umfjöllun um efnið í riti af þessu tagi. Er því sérstaklega áréttað mikilvægi þess að persónuverndarfulltrúar kynni sér vandlega lögin, reglugerðina og annað fræðsluefni. Á vefsíðu Persónuverndar eru jafnframt reglulega birtar leiðbeiningar um ýmis álitamál tengd persónuvernd ásamt annarri fræðslu. Þá er að lokum vísað til lista yfir áhugavert lesefni, sem finna má aftast í þessu riti, en þar er að finna ýmsa gagnlega tengla á fróðleik um persónuvernd.

Tekið skal fram að persónuverndarlögin og persónuverndarreglugerðin eru jafnrétthá, þar sem reglugerðin hefur verið leidd í lög hérlendis. Reglugerðin var ekki tekin upp í persónuverndarlögin í heild sinni, heldur aðeins tiltekin ákvæði hennar (þ.e. helstu meginreglurnar, auk þeirra ákvæða sem Ísland hafði heimild til að útfæra sérstaklega í landslögum). Þar sem ákvæði reglugerðarinnar eru ekki útfærð sérstaklega í persónuverndarlögum gilda ákvæði reglugerðarinnar. Því er ávallt nauðsynlegt að beita lögunum og reglugerðinni saman. Lagatilvísanir í þessu riti eru því í mörgum tilvikum settar þannig fram að vísað er bæði í viðeigandi ákvæði laganna og reglugerðarinnar, þegar við á.

1. Helstu hugtök

Í 4. gr. pvrg. og 3. gr. pvl. er að finna orðskýringar á helstu hugtökum laganna, m.a. persónuupplýsingum, viðkvæmum persónuupplýsingum, vinnslu, skrá, ábyrgðaraðila, vinnsluaðila, samþykki o.fl.

Persónuupplýsingar:

> Upplýsingar um persónugreindan eða persónugreinanlegan einstakling („skráðan einstakling“); einstaklingur telst persónugreinanlegur ef unnt er að persónugreina hann, beint eða óbeint, svo sem með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, lífeðlisfræðilegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti.
> (1. tölul. 4. gr. pvrg. og 2. tölul. 3. gr. pvl.)

Upplýsingarnar verða að vera nægjanlega nákvæmar til að hægt sé að átta sig á því hvaða einstaklingi þær tilheyra. Af þessu leiðir að persónuupplýsingar eru upplýsingar um fólk, en ekki upplýsingar um fyrirtæki eða dýr, svo dæmi séu nefnd. Lög um persónuvernd og vinnslu persónuupplýsinga taka þó raunar að nokkru leyti til upplýsinga um fjárhagsmálefni og lánstraust lögaðila, þótt slíkar upplýsingar teljist ekki til persónuupplýsinga.

Viðkvæmar persónuupplýsingar:

> a. Upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, lífsskoðun eða aðild að stéttarfélagi.
> b. Heilsufarsupplýsingar, þ.e. persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings, þ.m.t. heilbrigðisþjónustu sem hann hefur fengið, og upplýsingar um lyfja-, áfengis- og vímuefnanotkun.
> c. Upplýsingar um kynlíf manna og kynhneigð.
> d. Erfðafræðilegar upplýsingar, þ.e. persónuupplýsingar sem varða arfgenga eða áunna erfðaeiginleika einstaklings sem gefa einkvæmar upplýsingar um lífeðlisfræði eða heilbrigði einstaklingsins og fást einkum með greiningu á líffræðilegu sýni frá viðkomandi einstaklingi.
> e. Lífkennaupplýsingar, þ.e. persónuupplýsingar sem fást með sérstakri tæknivinnslu og tengjast líkamlegum, lífeðlisfræðilegum eða atferlisfræðilegum eiginleikum einstaklings og gera það kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti, svo sem andlitsmyndir eða gögn um fingraför, enda sé unnið með upplýsingarnar í því skyni að persónugreina einstakling með einkvæmum hætti.
> (3. tölul. 3. gr. pvl. (sjá ítarlegri skilgreiningar í 13., 14. og 15. tölul. 4. gr. pvrg.))

Viðkvæmar persónuupplýsingar eru þær persónuupplýsingar sem skilgreindar hafa verið sem slíkar í lögum, sbr. upptalninguna hér að framan. Þær eru því tæmandi taldar í lögum. Um þær gilda strangari reglur en um almennar persónuupplýsingar.

Gera verður greinarmun á viðkvæmum persónuupplýsingum annars vegar, og hins vegar þeim upplýsingum sem ekki teljast viðkvæmar samkvæmt persónuverndarlögum en eru engu að síður

viðkvæms eðlis, t.d. upplýsingum um félagsleg vandamál og önnur einkalífsatriði. Þrátt fyrir að slíkar upplýsingar séu ekki viðkvæmar í skilningi laganna eru að sjálfsögðu gerðar ríkari kröfur til vinnslu þeirra en upplýsinga almenns eðlis, t.d. um nöfn og heimilisföng, enda verður ávallt að haga meðferð persónuupplýsinga í samræmi við mikilvægi þeirra.

Vinnsla:

> Aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, svo sem söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtenging eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging.
> (2. tölul. 4. gr. pvrg. og 4. tölul. 3. gr. pvl.)

Vinnsluhugtakið er vítt og tekur til hvers konar meðferðar á persónuupplýsingum, óháð þeirri aðferð sem er notuð og óháð því hvort gagnagrunnur er miðlægur eða dreifður. Með vinnslu er t.d. átt við söfnun og skráningu, flokkun, varðveislu, breytingu, miðlun, eða hverja þá aðferð sem má nota til að gera upplýsingar tiltækar. Sama á við um eyðingu og eyðileggingu upplýsinga.

Ábyrgðaraðili:

> Einstaklingur, lögaðili, stjórnvald eða annar aðili sem ákveður einn eða í samvinnu við aðra tilgang og aðferðir við vinnslu persónuupplýsinga.
> (7. tölul. 4. gr. pvrg. og 6. tölul. 3. gr. pvl.)

Ábyrgðaraðili er sá sem ákveður tilgang og aðferðir við vinnslu persónuupplýsinga. Hann getur verið einstaklingur, fyrirtæki, stjórnvald eða annar aðili. Ábyrgðaraðili ber ábyrgð á því að sú vinnsla persónuupplýsinga, sem fer fram á hans vegum, samrýmist persónuverndarlögum, og hann þarf að geta sýnt fram á það.

Vinnsluaðili:

> Einstaklingur eða lögaðili, stjórnvald eða annar aðili sem vinnur með persónuupplýsingar á vegum ábyrgðaraðila.
> (8. tölul. 4. gr. pvrg. og 7. tölul. 3. gr. pvl.)

Vinnsluaðili er sá sem vinnur persónuupplýsingar fyrir hönd ábyrgðaraðila á grundvelli samnings þar að lútandi. Samningurinn nefnist vinnslusamningur og þarf að uppfylla tiltekin skilyrði sem sett eru í persónuverndarlögum. Vinnsluaðili getur verið einstaklingur, fyrirtæki, stjórnvald eða annar aðili.

Persónuvernd hefur gefið út ítarlegar leiðbeiningar fyrir vinnsluaðila. Þá hefur svonefndur 29. gr. vinnuhópur[1] útbúið leiðbeiningar með skýringum og skilgreiningum á ábyrgðaraðila og vinnsluaðila. Leiðbeiningarnar hafa ekki verið staðfestar af hálfu Evrópska persónuverndarráðsins eftir að nýja

[1] Ráðgefandi vinnuhópur fulltrúa persónuverndarstofnana í Evrópu) sem starfaði samkvæmt 29. gr. gildandi Evróputilskipunar nr. 95/46/EB, og var forveri Evrópska persónuverndarráðsins EDPB.

persónuverndarlöggjöfin tók gildi, en þær halda þó gildi sínu í meginatriðum og því getur verið gott að hafa þær til hliðsjónar.

Dæmi um mismunandi hlutverk vinnsluaðila og ábyrgðaraðila:
Fyrirtæki A veitir fyrirtæki B þá þjónustu að senda bréf í markaðssetningartilgangi þar sem byggt er á upplýsingum um viðskiptavini B.
A er vinnsluaðili fyrir B svo framarlega sem vinnsla umræddra viðskiptamannaupplýsinga B er nauðsynleg til að senda bréfin fyrir hönd fyrirtækis B eða samkvæmt fyrirmælum þess.
Fyrirtæki B er ábyrgðaraðili vegna vinnslu persónuupplýsinga um viðskiptamannahópinn með tilliti til markaðssetningarbréfsins. Hins vegar er fyrirtæki A ábyrgðaraðili að vinnslu persónuupplýsinga um eigin starfsmenn.

Samþykki:

Óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um sig.
(11. tölul. 4. gr. pvrg. og 8. tölul. 3. gr. pvl.)

Samþykki telst einungis hafa verið veitt ef hinn skráði hefur raunverulegt val um hvort hann samþykkir, eða hafnar, vinnslu persónuupplýsinga um sig. Það er hlutverk ábyrgðaraðila að meta hvort skilyrðum samþykkis hefur verið fullnægt.

Evrópska persónuverndarráðið (EDBP) hefur gefið út leiðbeiningar um samþykki. Þá hefur Persónuvernd einnig gefið út samskonar leiðbeiningar um samþykki. Einnig má lesa nánar um samþykki sem vinnsluheimild í kafla 6.8.

2. Heimildir til vinnslu persónuupplýsinga

Öll vinnsla persónuupplýsinga verður að byggjast á heimild í persónuverndarlögum. Það er ábyrgðaraðili sem ákveður tilgang og aðferðir við vinnslu persónuupplýsinga og þar af leiðandi hann sem tekur afstöðu til þess við hvaða heimild tiltekin vinnsla styðst. Það fer eftir tilgangi vinnslunnar hvort hún er leyfileg og þá hvaða heimild getur átt við í hvert sinn. Engin ein heimild er rétthærri, mikilvægari eða betri en önnur.

Til þess að vinnsla persónuupplýsinga sé lögmæt þarf hún jafnframt að vera í samræmi við meginreglur persónuverndarlaganna, en nánar verður fjallað um þær í kafla 4.

3.1 Almennar persónuupplýsingar

Öll vinnsla persónuupplýsinga verður að byggjast á einni af eftirfarandi sex heimildum, sem taldar eru upp í 1. mgr. 6. gr. pvrg., sbr. 9. gr. pvl., til þess að hún teljist fara fram á lögmætum grundvelli:

1. **Samþykki** þess sem persónuupplýsingarnar eru um (hins skráða) fyrir vinnslunni í þágu eins eða fleiri tiltekinna markmiða.
    - Hér er átt við samþykki samkvæmt 8. tölul. 3. gr. pvl., sbr. 11. tölul. 1. mgr. 4. gr. pvrg.

- Stjórnvöld geta sjaldnast byggt á samþykki, nema í undantekningartilvikum þegar samþykki hefur engin áhrif á veitingu þjónustu eða réttindi manna.
- Sjá kafla um auknar kröfur til samþykkis í kafla 6.8 í leiðbeiningum þessum.

2. Vinnslan er 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.
    - Gert er að skilyrði að samningurinn sé fullgildur og löglegur og skal þá litið til reglna samningaréttarins. Á sama hátt er ekki gert að skilyrði að samningurinn sé skriflegur þótt það sé betra.
    - Eingöngu er átt við samninga sem eru einkaréttarlegs eðlis, svo sem kaupsamninga, leigusamninga og ráðningarsamninga.
    - Sú krafa er almennt gerð að **hinn skráði sé aðili samningsins**.
    - Hvað varðar ráðstafanir áður en samningur er gerður er algjört skilyrði að þær séu að beiðni hins skráða. Hér er ekki endilega verið að tala um að uppfylla þurfi skilyrði samþykkis, skv. 1. tölul., fyrir ráðstöfunum sem gerðar eru til að undirbúa samningsgerðina heldur getur verið um vægari kröfur að ræða, jafnvel þannig að aðgerðaleysi geti nægt.
    - **Dæmi**: Einstaklingur sækir um lán og áður en samningur er gerður er gert greiðslumat eða áhættumat. Þá getur könnun á lánshæfi einnig farið fram á grundvelli beiðni hins skráða (hann þarf að hafa frumkvæði að því að veita tilteknar upplýsingar). Stundum getur þetta jafnvel verið á grundvelli fyrirmæla í lögum (eins og greiðslumat).

3. Vinnslan er nauðsynleg til að **fullnægja lagaskyldu** sem hvílir á þeim sem ákveður vinnsluna (ábyrgðaraðila).
    - Lagaskyldan verður að hvíla á ábyrgðaraðila sjálfum.
    - Skilyrðið um lagaskyldu felur í sér hvers konar skyldu sem leiðir af lagasetningu, hvort sem hana er að finna í lögum eða reglum leiddum af þeim. Dómar og stjórnvaldsúrskurðir geta haft þýðingu við túlkun þegar vafi leikur á hver þýðing tiltekins lagaákvæðis er.
    - Fyrir einkaaðila getur vinnsla persónuupplýsinga verið nauðsynleg til að tryggja gæði veittrar þjónustu og fyrir stjórnvöld til að hafa eftirlit. Þannig er til dæmis að finna ýmis ákvæði í skatta- og bókhaldslöggjöf, lögum um sjúkraskrár, lögum um ferðaþjónustu og lögum um fjármálaþjónustu sem gera ráð fyrir ýmiss konar vinnslu persónuupplýsinga og leggja bæði skyldur á einkaaðila (til að skrá upplýsingar) og stjórnvöld (til að fá upplýsingar).
    - Sérsjónarmið um ***stjórnvöld***:
        - Samkvæmt stjórnsýslurétti hafa stjórnvöld tiltekin lögboðin hlutverk. Til að geta sinnt þeim lögboðnum hlutverkum þurfa stjórnvöld oft að vinna með persónuupplýsingar.

- Ef vinnsla er ekki lögboðin þá verður að skoða hvort hún getur farið fram á grundvelli annars heimildarákvæðis í lögunum. Þetta getur t.d. átt við þegar hið opinbera veitir ýmiss konar þjónustu eða ráðgjöf.

4. Vinnslan er nauðsynleg til að **vernda brýna hagsmuni hins skráða eða annars einstaklings**.
    - Til þess að skilyrðið um brýna hagsmuni sé uppfyllt þarf að liggja fyrir að vinnslan sé svo áríðandi að hún geti ekki beðið. Þá verður vinnslan að tengjast hagsmunum sem hafa grundvallarþýðingu fyrir hinn skráða eða annan einstakling. Þetta getur til dæmis átt við þegar hinn skráði getur ekki, vegna sjúkdóms eða fjarveru, samþykkt vinnslu sem myndi forða honum frá verulegu fjárhagstjóni eða öðrum skaða.
    - Þessi heimild er almennt túlkuð mjög þröngt og litið svo á að ekki sé hægt að styðjast við hana nema í mjög afmörkuðum tilvikum.
    - Vinnsla persónuupplýsinga á grundvelli brýnna hagsmuna annars einstaklings ætti að meginreglu til aðeins að fara fram þegar greinilegt er að hún getur ekki byggst á öðrum lagagrundvelli.

5. Vinnslan er nauðsynleg vegna verks sem unnið er **í þágu almannahagsmuna** eða **við beitingu opinbers valds** sem ábyrgðaraðili fer með.
    - Almannahagsmunir:
        - Ákvæðið getur átt við þótt vinnsla fari ekki fram á vegum hins opinbera og einnig þótt hún eigi sér stað í fjárhagslegu augnamiði. Þá er almennt gert að skilyrði að vinnslan hafi þýðingu fyrir breiðan hóp manna. Ekki segir hversu breiður hann þurfi að vera eða hversu mikla þýðingu vinnslan verði að hafa fyrir hann.
        - Þessi heimild gæti t.d. átt við um vinnslu sem á sér stað í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi. Sama getur átt við um vinnslu sem á sér stað í upplýsingakerfi réttarkerfisins sem ætlað er að veita almenningi upplýsingar um löggjöf, dómaframkvæmd o.s.frv.
        - Þá á ákvæðið við um þá vinnslu persónuupplýsinga sem lýtur að innri málefnum ríkisins, þá vinnslu sem er nauðsynleg til að standa vörð um lögmæta ráðstöfun á almannafé og til að tryggja að með öruggum hætti sé haldið utan um gjörðir stjórnvalda.
    - Beiting opinbers valds:
        - Opinbert vald skiptist í þrennt: löggjafarvald, dómsvald og framkvæmdarvald. Lögmætisregla stjórnsýsluréttarins setur framkvæmdarvaldinu tilteknar skorður og leiðir af sér að stjórnvöld þurfa að hafa heimild að lögum til að athafna sig.
        - Ákveðin sérsjónarmið geta átt við um dómstóla.
        - Hjá stjórnvöldum kemur þessi heimild einkum til skoðunar við ýmiss konar vinnslu persónuupplýsinga í tengslum við beitingu opinbers valds, t.a.m. við töku stjórnvaldsákvarðana og þegar um er að ræða opinbera þjónustustarfsemi.

Þetta getur tekið til skráningar upplýsinga, miðlunar til gagnaðila í kærumálum, o.s.frv.

- Ef meðferð opinbers valds hefur verið falin þriðja manni með þjónustusamningi eða lögheimiluðu ytra valdframsali leiðir af ákvæðinu að hann getur viðhaft nauðsynlega vinnslu á upplýsingum við framkvæmd þeirrar stjórnsýslu.

6. Vinnslan er nauðsynleg vegna **lögmætra hagsmuna** sem ábyrgðaraðili eða einhver annar gætir, **nema hagsmunir eða grundvallarréttindi og frelsi hins skráða**, sem krefjast verndar persónuupplýsinga, **vegi þyngra**, einkum ef hinn skráði er barn.
    - Lögmætir hagsmunir þ.m.t. hagsmunir ábyrgðaraðila sem fá persónuupplýsingarnar í hendur, geta verið lagagrundvöllur fyrir vinnslu þeirra, að því tilskildu að hagsmunir eða grundvallarréttindi og frelsi hins skráða vegi ekki þyngra, að teknu tilliti til eðlilegra væntinga skráðra einstaklinga á grundvelli tengsla þeirra við ábyrgðaraðilann.
    - Ákvæðið á ekki við nema ábyrgðaraðili hafi viðhaft ákveðið mat á því hvort hagsmunir hins skráða af því að vinnslan fari ekki fram vegi þyngra en þeir hagsmunir sem mæla með vinnslunni. Í samræmi við ábyrgðarskylduna þarf hagsmunamatið að vera skjalfest og liggja fyrir áður en vinnslan hefst.
    - Lögmætir hagsmunir eru hins vegar ekki skilgreindir nánar í lögum eða frumvarpsathugasemdum en almennt má gera ráð fyrir að til þess að um lögmæta hagsmuni sé að ræða megi vinnslan ekki vera ólögmæt, ósanngjörn eða ómálefnaleg. Í þessu sambandi má gjarnan líta til meginreglna 10. gr. pvrg., sbr. 8. gr. pvl.
    - Í formálsorðum persónuverndarreglugerðarinnar segir að hvað sem öðru líði þurfi að meta af kostgæfni hvort um lögmæta hagsmuni sé að ræða, m.a. hvort skráður einstaklingur geti, þegar söfnun persónuupplýsinganna fer fram og í samhengi við hana, haft gilda ástæðu til að ætla að vinnsla muni fara fram í þeim tilgangi. Hagsmunir hins skráða og grundvallarréttindi hans geti einkum gengið framar hagsmunum ábyrgðaraðila þegar vinnsla persónuupplýsinga fari fram við aðstæður þar sem skráðir einstaklingar hafa ekki ástæðu til að ætla að um frekari vinnslu verði að ræða.
    - Í reglugerðinni segir einnig að vinnsla persónuupplýsinga, sem sé beinlínis nauðsynleg í þeim tilgangi að koma í veg fyrir svik, teljist einnig til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila.
    - Þá kveður reglugerðin á um að líta megi svo á að vinnsla persónuupplýsinga vegna *beinnar markaðssetningar* sé í þágu lögmætra hagsmuna. Hér þarf þó að athuga að sérreglur fjarskiptalaga geta gilt um markaðssetningu á Netinu (sjá nánar 46. gr. laga nr. 81/2003 um fjarskipti).
    - Í framkvæmd Persónuverndar hefur einnig verið litið svo á að rafræn vöktun á vinnustöðum, uppfylli hún önnur skilyrði persónuverndarlaga, geti farið fram á grundvelli lögmætra hagsmuna ábyrgðaraðilans. Í því samhengi reynir meðal annars á hvort tilgangur vöktunarinnar telst málefnalegur og hvort meðalhófs er gætt. Þá þarf að hafa í huga að ef um er að ræða kerfisbundið og umfangsmikið eftirlit með svæði

sem er aðgengilegt almenningi þarf að fara fram mat á áhrifum á persónuvernd, en um það er nánar fjallað í kafla 7.3.

- Stjórnvöld geta almennt ekki byggt á þessari heimild til vinnslu persónuupplýsinga, sbr. 1. mgr. 6. gr. pvrg.
    - Í persónuverndarreglugerðinni kemur fram um það efni: „Að því gefnu að það sé í höndum löggjafans að kveða á um lagagrundvöll vegna vinnslu opinberra yfirvalda á persónuupplýsingum ætti sá lagagrundvöllur [lögmætir hagsmunir] ekki að eiga við um vinnslu opinberra yfirvalda þegar þau sinna verkefnum sínum.“
    - Í sumum tilvikum þurfa stjórnvöld að sinna verkefnum sem ekki teljast til lögbundinna verkefna þeirra. Dæmi um slíkt er notkun eftirlitsmyndavéla á vinnustað. Er það sérstakt athugunarefni hvort líta megi svo á að í þeim tilvikum sé þeim heimilt að styðjast við lögmæta hagsmuni. Önnur heimild sem gæti komið til skoðunar er nauðsyn vegna almannahagsmuna, t.d. til að koma í veg fyrir rýrnun á eignum ríkisins.
- Í ákvæðinu segir að sérstakt tillit þurfi að taka til þess þegar hinn skráði er barn. Í athugasemdum við frumvarp það er varð að lögum nr. 90/2018 segir að með því birtist áherslur á að taka tillit til réttinda barna sem oftar en ekki séu ófær um að gefa samþykki eða nýta sér þau réttindi sem skráðir einstaklingar njóti samkvæmt persónuverndarreglugerðinni. Þannig þurfa hagsmunir af vinnslu að vera enn meiri þegar skráðir einstaklingar eru börn.
    - Í 38. lið formálsorða persónuverndarreglugerðarinnar er bent á að persónuupplýsingar barna eigi að njóta sérstakrar verndar þar sem þau kunna síður að vera meðvituð um áhættu, afleiðingar og viðkomandi verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga. Þessi sérstaka vernd ætti sérstaklega að eiga við um notkun persónuupplýsinga barna í markaðssetningarskyni, þegar búin eru til persónu- eða notendasnið og um söfnun persónuupplýsinga sem varða börn þegar þau nota þjónustu sem þeim er boðin beint.

Ef sú heimild sem byggt er á gerir kröfu um að vinnslan sé nauðsynleg þarf að gæta að því hvort unnt sé að ná sömu markmiðum án þess að vinna með persónuupplýsingar. Ef það er hægt þá er ekki lögmætur grundvöllur fyrir vinnslunni.

Ákveða þarf og skrá niður tilgang vinnslunnar og við hvaða heimild hún styðst áður en vinnsla hefst. Þessar upplýsingar eru skráðar í svokallaða vinnsluskrá (sjá nánar kafla 5.3).

Ekki má skipta um heimild eftir að vinnsla er hafin nema sérstaklega standi á. Ef tilgangur vinnslunnar breytist eftir að hún er hafin getur hún áfram verið lögmæt á grundvelli sömu heimildar ef nýr tilgangur samrýmist upphaflegum tilgangi. Þá þarf ávallt að ganga úr skugga um það fyrirfram. Þetta á ekki við ef heimildin er byggð á samþykki, þá getur þurft að afla nýs samþykkis

3.2 Viðkvæmar persónuupplýsingar

Viðkvæmar persónuupplýsingar eru upplýsingar sem varða kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, lífsskoðanir, aðild að stéttarfélagi, heilsufarsupplýsingar, upplýsingar um kynlíf manna og kynhneigð, erfðafræðilegar upplýsingar og lífkennaupplýsingar.

Til þess að heimilt sé að vinna viðkvæmar persónuupplýsingar þarf vinnslan að styðjast við einhverja af þeim sex heimildum sem þarf til að vinna almennar persónuupplýsingar, skv. 1. mgr. 6. gr. pvrg. og 9. gr. pvl., **og** auk þess að uppfylla að minnsta kosti eitt eftirfarandi skilyrða, sem talin eru upp í 11. gr. pvl.:

1. Sá sem persónuupplýsingarnar eru um (hinn skráði) hefur veitt **afdráttarlaust samþykki** sitt fyrir vinnslunni í þágu eins eða fleiri tiltekinna markmiða.
    - Samþykkið þarf að vera óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um sig.
    - Stjórnvöld geta sjaldnast byggt á samþykki, nema í undantekningartilvikum þegar samþykki hefur engin áhrif á veitingu þjónustu eða réttindi manna.
    - Við öflun samþykkis verður að uppfylla þær kröfur sem fram koma í skilgreiningu á samþykki, sbr. 8. tölul. 3. gr. pvl., sbr. 11. tölul. 1. mgr. 4. gr. pvrg., 10. gr. laganna um skilyrði fyrir samþykki, sbr. 7.-8. gr. pvrg., og jafnframt meginreglum 5. gr. pvrg., sbr. 8. gr. pvl.

2. Vinnslan er nauðsynleg til þess að ábyrgðaraðili eða hinn skráði geti staðið við **skuldbindingar** sínar og **nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf** og **löggjöf um almannatryggingar** eða **félagslega vernd**. Vinnslan þarf þá jafnframt að fara fram á grundvelli ákvæða laga eða kjarasamnings.
    - Hér er meðal annars átt við ráðningarsamninga og/eða heildarkjarasamninga.
    - Hér þarf að hafa í huga að því meiri sem íhlutun í einkalíf hins skráða sem vinnslan hefur í för með sér er þeim mun ótvíræðara verður slíkt ákvæði að vera.

3. Vinnslan er nauðsynleg **til að verja verulega hagsmuni** hins skráða eða annars einstaklings sem ekki er sjálfur fær um að gefa samþykki sitt.
    - Í athugasemdum við þetta ákvæði í frumvarpi til persónuverndarlaganna segir að hin ströngu skilyrði, með vísan til nauðsynjar og brýnna hagsmuna, gefi til kynna að ákvæðið beri að túlka þröngt. Átt sé við að hinn skráði sé ófær um að veita samþykki sitt af líkamlegum ástæðum eða í lagalegum skilningi, t.d. vegna lögræðissviptingar.

4. Vinnslan fer fram sem **liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila** sem starfar ekki í hagnaðarskyni og hefur stjórnmálaleg, heimspekileg, trúarleg eða stéttartfélagsleg markmið, enda nái vinnslan einungis til meðlima eða fyrrum meðlima viðkomandi aðila eða einstaklinga sem eru í reglulegu sambandi við hann í tengslum við

tilgang hans, persónuupplýsingar eru ekki fengnar þriðja aðila í hendur án samþykkis hinna skráðu og gerðar eru viðeigandi verndarráðstafanir.

- Hér er hægt að fella undir ýmiss konar samtök eins og t.d. samtök fólks með tiltekinn sjúkdóm, stéttarfélög, stjórnmálafélög, trúarfélög, menningar-, líknar- og hugsjónasamtök.
- Vinnslan getur eingöngu tekið til félagsmanna eða þeirra sem eru í reglubundnum tengslum við viðkomandi samtök, t.d. þeirra sem njóta þjónustu hjálparsamtaka.
- Það hvaða vinnsla er heimil hverju sinni samkvæmt ákvæðinu ræðst m.a. af eðli viðkomandi samtaka.

5. Vinnslan tekur einungis til upplýsinga sem hinn skráði hefur **augljóslega sjálfur gert opinberar**.
    - Varðandi hvað telst til þess að gera upplýsingar opinberar segir í frumvarpi til persónuverndarlaganna að átt sé við að þær hafi verið kunngjörðar ótilgreindum hópi manna, t.d. með ritun ævisögu eða í sjónvarpsviðtali. Þá segir jafnframt að vafi í þessum efnum yrði túlkaður hinum skráða í hag.
    - Þannig getur síðari vinnsla slíkra upplýsinga verið heimil á grundvelli þessa ákvæðis án sérstaks samþykkis hins skráða, en ávallt skal fara eftir meginreglum 5. gr. pvrg., sbr. 8. gr. pvl.

6. Vinnslan er nauðsynleg til að unnt sé að **stofna, hafa uppi eða verja réttarkröfur**.
    - Ekki er skilyrði að mál verði lagt fyrir dómstóla heldur nægir að vinnslan sé nauðsynleg til að styðja kröfu fullnægjandi rökum. Til dæmis getur vinnuveitanda verið nauðsynlegt að vinna upplýsingar um heilsufar starfsmanns til að geta sýnt fram á lögmætar forsendur fyrir uppsögn. Vinnsla viðkvæmra persónuupplýsinga í þessum tilgangi og á grundvelli þessarar heimildar telst hins vegar því aðeins vera lögleg að krafan verði hvorki afmörkuð né staðreynd með öðrum hætti.

7. Vinnslan er nauðsynleg af ástæðum sem varða verulega **almannahagsmuni** og fyrir henni er sérstök lagaheimild sem kveður á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða.
    - Ákvæðið á sér fyrirmynd í g-lið 2. mgr. 9. gr. reglugerðarinnar. Auk þess verður að skoða 7. tölul. 1. mgr. lagaákvæðisins í ljósi annarra ákvæða laganna og reglugerðarinnar. Þannig er til að mynda fjallað um leyfisskylda vinnslu í 31. gr. frumvarpsins, en þar er mælt fyrir um að ef vinnsla persónuupplýsinga fer fram vegna verkefnis í þágu almannahagsmuna sem getur falið í sér sérstaka hættu á að farið verði í bága við réttindi og frelsi skráðra einstaklinga geti Persónuvernd ákveðið að vinnslan megi ekki hefjast fyrr en hún hafi verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar. Um leyfisskylduna eru nánari fyrirmæli í reglum Persónuverndar, sem birtar eru á vefsíðu stofnunarinnar.
    - Í 52. lið formálsorða reglugerðarinnar er m.a. að finna dæmi um almannahagsmuni sem gætu fallið undir þetta ákvæði. Er þar m.a. bent á vinnslu persónuupplýsinga á

sviði vinnulöggjafar og löggjafar um félagslega vernd, t.d. lífeyri, og með hliðsjón af heilbrigðisöryggi, vöktun og viðvörunum, forvörnum og vörnum gegn smitsjúkdómum og annarri alvarlegri heilsufarsógn. Auk þess er mælt fyrir um að vinnslu megi heimila af heilbrigðisástæðum, svo sem vegna lýðheilsu og stjórnunar heilbrigðisþjónustu, einkum til að tryggja gæði og kostnaðarhagkvæmni þess verklags sem notað er við uppgjör á kröfum um bætur og þjónustu sjúkratryggingakerfisins, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi.

- Í 53. lið formálsorða reglugerðarinnar segir jafnframt að vinnsla viðkvæmra persónuupplýsinga, sem þurfa að njóta aukinnar verndar, ætti aðeins að fara fram í þágu heilsutengdra markmiða þegar það er nauðsynlegt til að ná þessum markmiðum í þágu einstaklinga og samfélagsins alls, einkum í tengslum við stjórnun heilbrigðis- eða félagsþjónustu og -kerfa. Í því sambandi er tilgreind vinnsla slíkra upplýsinga á vegum stjórnsýslunnar og miðlægra landsbundinna heilbrigðisyfirvalda í þágu gæðastýringar, gagnaumsýslu stjórnsýslunnar og almenns eftirlits með heilbrigðis- og félagsþjónustu á lands- og staðarvísu og til að tryggja samfellu í heilbrigðis- og félagsþjónustu og heilbrigðisþjónustu eða heilbrigðisöryggi yfir landamæri, vegna vöktunar og viðvörunar, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi.
- Ljóst er að vinnsla viðkvæmra persónuupplýsinga í þágu mikilvægra samfélagshagsmuna af þeim toga sem taldir eru upp í þessum liðum formálans er iðulega heimiluð í sérlögum.

8. Vinnslan er nauðsynleg til að unnt sé að **fyrirbyggja sjúkdóma eða vegna atvinnusjúkdómalækninga**, til að meta vinnufærni starfsmanns, greina sjúkdóma og veita umönnun eða meðferð á sviði heilbrigðis- eða félagsþjónustu, enda sé hún framkvæmd af starfsmanni slíkrar þjónustu sem bundinn er þagnarskyldu. Vinnsla sem fram fer á grundvelli þessarar heimildar þarf jafnframt að fara fram á grundvelli sérstakrar lagaheimildar.
    - Heimildin kemur einna helst til skoðunar í tengslum við vinnslu upplýsinga um sjúklinga innan heilbrigðiskerfisins, t.d. á grundvelli laga nr. 55/2009 um sjúkraskrár.
    - Þá getur heimildin einnig átt við um vinnslu upplýsinga um starfsmenn sem fer fram á vegum trúnaðarlækna á vinnustöðum.

9. Vinnslan er nauðsynleg af ástæðum sem varða **almannahagsmuni á sviði lýðheilsu**, svo sem til að verjast alvarlegum heilsufarsógnum sem ná yfir landamæri eða tryggja gæði og öryggi heilbrigðisþjónustu og lyfja eða lækningatækja. Vinnsla sem fram fer á grundvelli þessarar heimildar þarf jafnframt að fara fram á grundvelli laga.
    - Í formálsorðum persónuverndarreglugerðarinnar segir að túlka ætti hugtakið lýðheilsu eins og það er skilgreint í reglugerð Evrópuþingsins og ráðsins 1338/2008 frá 16. desember 2008 um hagskýrslur Bandalagsins um lýðheilsu og heilbrigði og öryggi á vinnustað. Þar segir að lýðheilsa feli í sér alla heilsufarstengda þætti, nánar tiltekið heilsufar, m.a. sjúkdómstilvik og fötlun, ákvarðandi þætti sem hafa áhrif á heilsufar,

þörf fyrir heilbrigðisþjónustu, fjármagn sem veitt er til heilbrigðisþjónustu, veitingu og almennan aðgang að heilbrigðisþjónustu og kostnað og fjármögnun heilbrigðisþjónustu, sem og dánarorsakir. Slík vinnsla heilsufarsupplýsinga í þágu almannahagsmuna ætti ekki að leiða til vinnslu persónuupplýsinga í öðrum tilgangi af hálfu þriðju aðila, s.s. vinnuveitenda eða tryggingafélaga og bankastofnana.

10. Vinnslan er nauðsynleg vegna **tölfræði-, sagnfræði- eða vísindarannsókna**, enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga, og fari fram á grundvelli laga.

- Tilteknar ráðstafanir geta falið í sér aðgerðir á borð við dulkóðun eða eyðingu persónuauðkenna, sem og aðrar nauðsynlegar öryggisráðstafanir.
- Hér ber að athuga að ýmsar sérreglur gilda um undanþágur varðandi vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, sjá nánar í 89. gr. pvrg., sbr. 18. gr. pvl.

11. Vinnslan er nauðsynleg vegna **skjalavistunar í þágu almannahagsmuna** og fer fram á grundvelli laga sem kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða, einkum þagnarskyldu.

- Ákvæðið skiptir fyrst og fremst máli í tengslum við Þjóðskjalasafn Íslands og önnur opinber skjalasöfn, sbr. lög nr. 77/2014 um opinber skjalasöfn.
- Hér ber að athuga að ýmsar sérreglur gilda um undanþágur varðandi vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, sjá nánar í 89. gr. pvrg., sbr. 18. gr. pvl.

Þess má að lokum geta að Persónuvernd leysir úr ágreiningi um hvort persónuupplýsingar skuli teljast viðkvæmar eða ekki.

3.3 Vinnsla upplýsinga um refsiverða háttsemi

Upplýsingar um refsiverða háttsemi einstaklinga lúta sérstökum reglum samkvæmt persónuverndarlögum. Þessar upplýsingar teljast ekki viðkvæmar í skilningi laganna, en engu að síður eru strangari kröfur gerðar til meðferðar þeirra en almennra persónuupplýsinga.

Gerður er greinarmunur á því hvort unnið sé með upplýsingar um refsiverða háttsemi á vegum stjórnvalda eða einkaaðila. Þannig eru gerðar mismunandi kröfur eftir því hvort ábyrgðaraðilinn er stjórnvald eða einkaaðili.

Stjórnvöld mega ekki vinna með upplýsingar um refsiverða háttsemi nema það sé nauðsynlegt í þágu lögbundinna verkefna þeirra, sbr. 12. gr. pvl. Þá mega stjórnvöld ekki miðla upplýsingum um refsiverða háttsemi nema að uppfylltu að minnsta kosti einu af eftirtöldum skilyrðum:

1. Hinn skráði hefur gefið afdráttarlaust samþykki sitt fyrir því.

2. Miðlunin er nauðsynleg í þágu lögmætra hagsmuna hins opinbera eða einkaaðila sem auðsjáanlega vega þyngra en hagsmunir af leynd um upplýsingarnar, þ. á m. hagsmunir hins skráða.

3. Miðlunin er nauðsynleg í þágu lögbundinna verkefna viðkomandi stjórnvalds eða til að unnt sé að taka stjórnvaldsákvörðun.

4. Miðlunin er nauðsynleg vegna verkefnis í þágu hins opinbera sem einkaaðila hefur verið falið á lögmætan hátt.

Einkaaðilar mega ekki vinna með upplýsingar um refsiverða háttsemi nema hinn skráði hafi veitt til þess *ótvírætt samþykki* sitt eða vinnslan sé nauðsynleg í þágu *lögmætra hagsmuna* sem auðsjáanlega vega þyngra en einkalífsréttur hins skráða. Þeim upplýsingum má ekki miðla nema hinn skráði veiti til þess afdráttarlaust samþykki sitt. Þó má miðla upplýsingum án samþykkis sé það nauðsynlegt í þágu lögmætra hagsmuna hins opinbera eða einkaaðila sem vega þyngra en þeir hagsmunir sem eru af leynd um upplýsingarnar, þar á meðal hagsmunir hins skráða.

Öll vinnsla upplýsinga um refsiverða háttsemi þarf jafnframt að byggja á einni af heimildunum sex (sbr. 1. mgr. 6. gr. pvrg. og 9. gr. pvl.) fyrir vinnslu almennra persónuupplýsinga

3. Heimildir stjórnvalda til vinnslu persónuupplýsinga

Stjórnvöld þurfa eins og aðrir að hafa einhverja af þeim heimildum sem persónuverndarlög gera kröfu um til vinnslu persónuupplýsinga. Stjórnvald þarf ávallt að uppfylla eitthvert af heimildarákvæðum 9. gr. laga nr. 90/2018 fyrir vinnslu almennra persónuupplýsinga, auk heimildar skv. 11. gr. sömu laga sé um að ræða viðkvæmar persónuupplýsingar. Þar að auki gilda meginreglur 8. gr. laganna um alla vinnslu persónuupplýsinga, m.a. að þær séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart hinum skráða og að þær séu nægilegar og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar. Nánar er fjallað um meginreglurnar í 4. kafla hér á eftir.

Ólíklegt er að stjórnvöld geti byggt heimild sína til vinnslu persónuupplýsinga á **samþykki** þegar þau starfa innan valdheimilda sinna, þar sem þar er til staðar valdaójafnvægi á milli ábyrgðaraðila og hins skráða. Af því leiðir að samþykkið getur ekki talist óþvingað og því er það ekki gilt. Þá segir í 1. mgr. 6. gr. persónuverndarreglugerðarinnar að ákvæði f-liðar 1. mgr. ákvæðisins, þar sem heimilað er að vinna með almennar persónuupplýsingar á grundvelli lögmætra hagsmuna, skuli ekki eiga við um vinnslu opinberra yfirvalda við störf sín.

Þrátt fyrir framangreint er ekki útilokað að stjórnvöld geti í einhverjum tilvikum byggt á samþykki eða lögmætum hagsmunum sem vinnsluheimild. Það gæti hins vegar aðeins átt við þegar um er að ræða vinnslu persónuupplýsinga sem ekki fer fram í beinum tengslum við lögbundin störf stjórnvalda.

Þær heimildir sem stjórnvöld byggja oftast sína vinnslu á eru annars vegar nauðsyn til að fullnægja **lagaskyldu** sem hvílir á stjórnvaldinu og hins vegar nauðsyn vegna verks sem unnið er í þágu **almannahagsmuna** eða við **beitingu opinbers valds** sem stjórnvaldið fer með. Þá koma aðrar heimildir einnig til greina eins og t.d. að vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að.

Persónuverndarlögin gera ráð fyrir því að ábyrgðaraðili, þ.e. hvert stjórnvald fyrir sig, gangi úr skugga um fullnægjandi heimildir standi til vinnslu persónuupplýsinga áður en vinnslan hefst.

4. Meginreglur um vinnslu persónuupplýsinga

Meginreglurnar sex eru oft kallaðar „gullnu reglurnar“ og þær eru taldar upp í 8. gr. persónuverndarlaganna. Meginreglurnar endurspeglast síðan í mörgum ákvæðum löggjafarinnar, t.d. um réttindi einstaklinga. Þegar unnið er með persónuupplýsingar þarf alltaf að hafa þessar meginreglur í huga og vinna með upplýsingarnar í samræmi við þær. Reglurnar eru:

Sanngirnisreglan (lögmætisreglan): að persónuupplýsingar séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart einstaklingnum.

- Þessi regla lýtur fyrst og fremst að réttindum einstaklinga, t.d. upplýsingarétti þeirra og aðgangsrétti. Þannig þarf ábyrgðaraðilinn að geta sýnt fram á að einstaklingar hafi fengið fullnægjandi fræðslu þegar það á við og hann þarf að veita einstaklingum aðgang að sínum persónuupplýsingum. Fara þarf yfir öll réttindin og kortleggja hvernig skuli veita þau.
- Sanngirnisreglan tekur líka til lögmætis vinnslunnar. Í því felst að ávallt þarf að vera til staðar heimild fyrir vinnslu persónuupplýsinga. Þá má vinnslan ekki ganga gegn öðrum lögum. Það er hluti af því að uppfylla ábyrgðarskylduna að kortleggja á hvaða heimild hver vinnslustarfsemi fyrir sig grundvallast.

Tilgangsreglan: að persónuupplýsingar séu unnar í skýrum, lögmætum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi.

- Tilgangsreglan lýtur fyrst og fremst að því hvenær skuli vinna persónuupplýsingar. Öll vinnsla verður að hafa skýran tilgang.
- Hér getur skrá yfir vinnslustarfsemi, sem í flestum tilvikum er skylt að halda, verið gagnlegt tæki til að sýna fram á að ábyrgðarskyldan sé uppfyllt en í henni skal gera grein fyrir tilgangi hverrar vinnslustarfsemi fyrir sig. Skráin rammar þannig inn tilgang vinnslu og auðveldar alla eftirfarandi vinnu. Einnig geta önnur tól, t.d. framkvæmd mats á áhrifum á persónuvernd (MÁP), hjálpað við mat á því hvort tilgangur vinnslunnar er lögmætur og málefnalegur.

Meðalhófsreglan: að persónuupplýsingar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilganginn með vinnslu þeirra.

- Meðalhófsreglan felur í sér að ekki á að vinna með meiri persónuupplýsingar en þörf er á. Hér geta tól á borð við skrá yfir vinnslustarfsemi og mat á áhrifum á persónuvernd (MÁP) hjálpað við mat á því hvort vinnslan er nægjanleg eða hvort verið er að safna upplýsingum sem ekki er þörf á að afla.
- Reglan felur einnig í sér að einungis er heimilt að vinna með upplýsingar sem eru viðeigandi í ljósi tilgangsins með vinnslunni. Þá getur þurft að gæta þess að unnið sé með nægilegar upplýsingar til þess að tilganginum verði náð.

- Oft er gagnlegt að átta sig á helstu tegundum persónuupplýsinga og flokkum þeirra einstaklinga sem vinna þarf með upplýsingar um og spyrja sig hvers vegna þurfi að vinna með upplýsingarnar. Þetta tengist líka tilgangsreglunni, þ.e. tilgangurinn þarf að vera skýr svo að hægt sé að átta sig á því hvaða upplýsingar ábyrgðaraðilanum er nauðsynlegt að vinna með.

Áreiðanleikareglan: að persónuupplýsingar séu áreiðanlegar og uppfærðar eftir þörfum; persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar skal eyða eða þær leiðréttar án tafar.

- Áreiðanleikareglan felur í sér að persónuupplýsingar skuli vera réttar. Til að geta sýnt fram á að farið hafi verið að henni getur verið nauðsynlegt að skjalfesta verklag um hvenær skuli uppfæra upplýsingar í upplýsingakerfum, til dæmis tengiliðaupplýsingar einstaklinga. Þetta getur verið sérstaklega mikilvægt þegar um er að ræða viðkvæmar persónuupplýsingar.
- Í tilviki stjórnvalda og þeirra sem falla undir reglur um skilaskyldu til skjalasafna er sjaldnast heimilt að eyða upplýsingum. Því er sérstaklega mikilvægt að skrá réttar upplýsingar strax í byrjun. Séu óáreiðanlegar eða ófullkomnar persónuupplýsingar skráðar hjá stjórnvöldum, sem ekki er heimilt að eyða, má bæta við lýsingu sem leiðréttir þær upplýsingar sem þegar hafa verið skráðar, þegar við á. Í þessu samhengi er einnig mikilvægt að hafa meðalhófsregluna í huga, enda er stjórnvöldum almennt ekki heimilt að eyða þeim upplýsingum sem hafa verið skráðar, jafnvel þótt þær séu of umfangsmiklar.

Varðveislureglan: að persónuupplýsingar séu varðveittar í því formi að ekki sé unnt að bera kennsl á einstaklinga lengur en þörf krefur miðað við tilganginn með vinnslu þeirra. Heimilt er að geyma persónuupplýsingar lengur að því tilskildu að vinnsla þeirra þjóni eingöngu skjalavistun í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi og að viðeigandi öryggis sé gætt.

- Varðveislureglan felur í sér að eyða á persónuupplýsingum þegar þeirra er ekki lengur þörf vegna tilgangsins. Í sumum tilvikum er jafnframt hægt að gera upplýsingarnar ópersónugreinanlegar í stað þess að eyða þeim.
- Best er að skjalfesta verkferla um hvenær skuli eyða tilteknum tegundum persónuupplýsinga.
- Hér getur skrá yfir vinnslustarfsemi einnig komið að gagni við að fá yfirlit yfir hvenær eyðing skuli fara fram.

Öryggisreglan: að persónuupplýsingar séu unnar með þeim hætti að viðeigandi öryggi þeirra sé tryggt.

- Öryggisreglan lýtur að því að tryggja öryggi persónuupplýsinga í hvívetna. Hún endurspeglast í mörgum ákvæðum persónuverndarlöggjafarinnar.
- Þannig þarf ábyrgðaraðilinn að skjalfesta áhættumat hvað varðar öryggi persónuupplýsinganna og ákveða öryggisráðstafanir út frá niðurstöðu áhættumatsins. Í þessu felst líka skjalfesting þess þegar mat á áhrifum á persónuvernd (MÁP) er framkvæmt og skjalfesting á verkferlum í tengslum við tilkynningu um öryggisbresti. Þá þarf ábyrgðaraðili einnig að halda skrá yfir alla öryggisbresti sem verða í starfseminni og geta sýnt Persónuvernd hana, sé þess óskað.

Persónuvernd hefur útbúið leiðbeiningar um öryggi persónuupplýsinga.

5. Skyldur þeirra sem vinna með persónuupplýsingar

5.1 Ábyrgðarskyldan

Ein þeirra nýju skyldna sem lagðar eru á þá sem vinna með persónuupplýsingar samkvæmt persónuverndarlöggjöfinni er svokölluð ábyrgðarskylda. Í henni felst einkum tvennt. Annars vegar að fyrirtæki, stofnanir, sveitarfélög og aðrir sem bera ábyrgð á vinnslu persónuupplýsinga (ábyrgðaraðilar) þurfa að fara að meginreglum löggjafarinnar, og hins vegar þurfa þeir að geta sýnt fram á það. Það að ábyrgðaraðilinn þurfi að sýna fram á hvernig hann fer að reglunum felur í sér að hann þarf að geta sannað það, t.d. með skjölum og verklagsreglum, og geta sýnt fram á skilvirkni ráðstafana sem hann hefur ákveðið að beita, t.d. með skráningu frávika o.fl. Í öllum tilvikum þarf að taka mið af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættunni fyrir réttindi og frelsi einstaklingsins.

Þannig þarf að gera mismunandi ráðstafanir eftir því hvort um er að ræða almennar eða viðkvæmar persónuupplýsingar, hvort unnið er með mikið magn upplýsinga eða lítið, og hvort ætlunin sé að búa til persónusnið eða láta fara fram sjálfvirka ákvarðanatöku, svo dæmi séu nefnd. Þá þarf að hugsa um hvaða áhrif vinnslan hefur á einstaklinginn.

Þegar unnið er með persónuupplýsingar þarf alltaf að hafa meginreglurnar sex í huga og vinna með upplýsingar í samræmi við þær. Reglurnar eru:

- **Sanngirnisreglan**
- **Tilgangsreglan**
- **Meðalhófsreglan**
- **Áreiðanleikareglan**
- **Varðveislureglan**
- **Öryggisreglan**

Til að uppfylla ábyrgðarskylduna þarf að skoða hverja meginreglu fyrir sig og meta hvaða kröfur persónuverndarlöggjöfin gerir til þess að þær séu uppfylltar. Þetta er hins vegar ekki tæmandi talning á þeim atriðum sem þarf að huga að, enda er það mjög háð eðli, umfangi, samhengi og tilgangi vinnslunnar hverju þarf að huga að og hversu mikið.

5.2 Fræðsluskyldan

Fræðsluskyldan (sbr. m.a. 13. og 14. gr. pvrg.) er einn þáttur í ábyrgðarskyldu fyrirtækja og stjórnvalda samkvæmt persónuverndarlögum og felur í sér að framangreindir aðilar veiti einstaklingum rétt til upplýsinga samkvæmt löggjöfinni. Þannig er alla jafna talað um upplýsingarétt einstaklinga og fræðsluskyldu fyrirtækja og stjórnvalda og er þá átt við sama hlutinn.

Hvers kyns vinnsla persónuupplýsinga á að vera lögmæt og sanngjörn. Það ætti því að vera einstaklingum ljóst þegar persónuupplýsingum um þá er safnað, þær notaðar, skoðaðar eða unnar á annan hátt og að hvaða marki persónuupplýsingar eru eða munu verða unnar.

Þegar fræðslan er veitt ætti einstaklingum að vera gerð grein fyrir áhættu, reglum, verndarráðstöfunum og réttindum í tengslum við vinnslu persónuupplýsinga og hvernig þeir geta neytt réttar síns í tengslum

við slíka vinnslu. Einkum ætti tilgangurinn með vinnslu persónuupplýsinganna að vera skýr og liggja fyrir við söfnun þeirra.

Meginreglan um gagnsæi krefst þess að hvers kyns upplýsingar og samskipti, sem tengjast vinnslu þessara persónuupplýsinga, séu auðveldlega aðgengileg og á skýru og einföldu máli. Sú meginregla á einkum við um upplýsingar til skráðra einstaklinga um það hver ábyrgðaraðilinn er og um tilganginn með vinnslunni, frekari upplýsingar til að tryggja sanngjarna og gagnsæja vinnslu gagnvart viðkomandi einstaklingum og um rétt þeirra til að fá staðfestingu og tilkynningu um vinnslu á persónuupplýsingum um sig.

5.2.1 Hvaða fræðslu á að veita?

Hvað þarf að upplýsa um?	Upplýsinga er aflað frá hinum skráða	Upplýsinga er aflað frá öðrum
Heiti og samskiptaupplýsingar ábyrgðaraðila og persónuverndarfulltrúa	X	X
Tilgang vinnslu og heimild til vinnslu	X	X
Lögmæta hagsmuni (ef vinnsla byggir á þeirri heimild)	X	X
Tegundir persónuupplýsinga		X
Viðtakendur	X	X
Miðlun til þriðju landa og verndarráðstafanir	X	X
Varðveislutíma	X	X
Upplýsingar um réttindi einstaklinga	X	X
Afturköllun samþykkis, ef við á	X	X
Rétt til að leggja fram kvörtun hjá Persónuvernd	X	X
Hvaðan upplýsingar koma		X
Skyldu til að veita upplýsingar skv. lögum eða samningi	X	
Sjálfvirka ákvarðanatöku	X	X
Tímamörk	Við söfnun upplýsinga	Í síðasta lagi mánuði eftir að upplýsinga er aflað, þegar fyrst er haft samband eða þegar upplýsingar eru sendar öðrum í fyrsta sinn

Þessa fræðslu á að veita þegar upplýsinganna er aflað, sbr. 13. gr. pvrg. Ef upplýsinganna er aflað hjá öðrum en hinum skráða þarf að veita fræðsluna innan mánaðar, sbr. 3. tölul. 14. gr. pvrg. Þetta má til að mynda gera í persónuverndarstefnu fyrirtækisins eða stjórnvaldsins sem í hlut á.

5.2.2 Hvernig á að veita fræðslu?

Hægt er að veita fræðslu á ýmsan hátt. Sérstaklega er hvatt til þess að fyrirtæki og stofnanir nýti sér þá tækni sem fyrir hendi er til að koma upplýsingum á framfæri. Fyrst og fremst er lögð áhersla á að fræðslan skuli vera á gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi.

Það er ekki skylda fyrir þá sem vinna með persónuupplýsingar að gera persónuverndarstefnu en hún getur verið hentugt tæki til þess að sinna fræðsluskyldunni.

Fræðslan skal vera á skýru og einföldu máli. Hún þarf líka að vera aðskilin frá öðrum atriðum, t.d. almennum samningsskilmálum. Þá þarf einnig að gæta þess að tilkynningum um uppfærslur á fræðslu, t.d. í persónuverndarstefnu, sé ekki blandað saman við önnur atriði, t.d. tilboð á vörum, þegar sendur er tölvupóstur.

Þetta er sérstaklega mikilvægt þegar um er að ræða upplýsingar sem beint er sérstaklega til barns.

Upplýsingarnar skulu veittar skriflega eða á annan hátt, þ.m.t., eftir því sem við á, á rafrænu formi. Þá skulu upplýsingarnar veittar hinum skráða að kostnaðarlausu.

Skrá yfir vinnslustarfsemi (vinnsluskrá) getur hér gefið ábyrgðaraðilanum yfirsýn yfir hvaða fræðslu þarf að veita með tilliti til þess hvaða persónuupplýsingar er verið að vinna með og á hvaða máta.

5.2.3 Undantekningar frá fræðsluskyldunni

Almennt séð verða fyrirtæki og stjórnvöld að veita einstaklingum fræðslu þegar unnið er með persónuupplýsingar um þá, en í tilteknum tilvikum þurfa þau þess þó ekki. Rétt er þó að taka fram að þessum undantekningum er eingöngu heimilt að beita í þröngt afmörkuðum tilvikum. Þessi tilvik eru:

- ef einstaklingurinn hefur þegar fengið upplýsingarnar og þær eru óbreyttar
- ef ekki er hægt að veita upplýsingarnar, eða það myndi kosta óhóflega fyrirhöfn
- þegar persónuupplýsingar eru bundnar trúnaði

Þegar upplýsinga er aflað frá öðrum en einstaklingnum sjálfum þarf ekki að veita fræðslu ef skýrt er mælt fyrir um öflun eða miðlun upplýsinganna í lögum.

5.3 Vinnsluskrá

Sérhver ábyrgðaraðili og vinnsluaðili og, eftir atvikum fulltrúi þeirra, skal halda skrá yfir vinnslustarfsemi sína og bera þeir ábyrgð á að halda slíka skrá. Þeir geta hins vegar falið persónuverndarfulltrúa að halda slíka skrá á þeirra ábyrgð.

Fyrirtæki og stofnanir sem hafa færri en 250 starfsmenn eru undanþegin skyldunni til að halda vinnsluskrár að því er varðar ákveðnar vinnslur. Undanþágan er aftur á móti mjög þröng og því er sjaldgæft að hún eigi við að öllu leyti um fyrirtæki eða stofnun.

Þannig þurfa fyrirtæki og stofnanir með færri en 250 starfsmenn að halda slíka skrá ef vinnslan er:

- líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga,
- ekki tilfallandi, eða
- taki til sérstakra flokka upplýsinga, eins og um getur í 1. mgr. 9. gr. pvrg., eða persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot sem um getur í 10. gr. pvrg.

Sem dæmi má nefna að vinnsla persónuupplýsinga í tengslum við launagreiðslur til starfsmanna telst almennt ekki vera tilfallandi. Fyrirtæki sem greiða starfsmönnum sínum laun þurfa því að halda vinnsluskrá.

Í framkvæmd og nær án undantekninga skulu því öll fyrirtæki og stofnanir halda skrár yfir vinnslustarfsemi sína.

Fyrirtækjum og stofnunum mun í öllum tilvikum gagnast að kortleggja þá vinnslu persónuupplýsinga sem þar fer fram, sem þátt í innra utanumhaldi og skjölun. Megintilgangur skrárinnar er að fá yfirsýn yfir þá vinnslu persónuupplýsinga sem fram fer í starfseminni, en ekki endilega hverja einustu vinnsluaðgerð sem framkvæmd er.

Um upplýsingar sem skráin skal innihalda, form skrár, aðgengileika o.fl. gilda fyrirmæli 30. gr. persónuverndarreglugerðarinnar. Persónuvernd hefur jafnframt gefið út ítarlegar leiðbeiningar fyrir skrá yfir vinnslustarfsemi ásamt sniðmátum af vinnsluskrám sem nálgast má á vefsíðu stofnunarinnar.

5.4 Öryggi persónuupplýsinga

Ein meginskylda þeirra sem vinna með persónuupplýsingar er að tryggja öryggi þeirra. Ef vinnslan er umfangsmikil eða unnið er með mikið magn viðkvæmra persónuupplýsinga getur þurft að setja upp flókin öryggiskerfi og jafnvel fá vottun á það upplýsingaöryggiskerfi sem sett er upp.

Hvaða skyldur hvíla á þeim sem geyma eða vinna með persónuupplýsingar?

- Ekki sé hætta á að óviðkomandi aðilar komist í þær
- Að þær skaðist ekki eða glatist
- Að þeir sem hafa gilda ástæðu til, komist í upplýsingarnar
- Öryggisráðstafanir skulu taka mið af umfangi og viðkvæmni gagnanna

5.4.1 Öryggisbrestur

Öryggisbrestur felur í sér brest á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi.

Mikilvægt er að ábyrgðaraðili meti allar hugsanlegar afleiðingar öryggisbrestsins, en það fer eftir aðstæðum hvort nauðsynlegt er að tilkynna um hann til Persónuverndar og upplýsa hina skráðu. Sé nauðsynlegt að tilkynna um hann til Persónuverndar skal það **gert innan 72 klst. frá því að brestsins verður vart**. Sé Persónuvernd ekki tilkynnt um brestinn innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni. Vinnsluaðili sem verður var við öryggisbrest skal láta ábyrgðaraðila vita eins fljótt og unnt er. Ef bresturinn getur valdið einstaklingi skaða á einhvern hátt skal láta hann vita tafarlaust.

Persónuvernd hefur gefið út ítarlegar leiðbeiningar um öryggisbrest. Á vefsíðu Persónuverndar má nálgast eyðublað vegna tilkynningar um öryggisbrest.

6. Helstu réttindi og úrræði hins skráða

6.1 Upplýsingaréttur (fræðsluskylda)

17. gr. pvl. og 13.-14. gr. pvrg.

Fræðsluskylda er einn þáttur í ábyrgðarskyldu fyrirtækja og stjórnvalda samkvæmt persónuverndarlögum og felur í sér að framangreindir aðilar veiti einstaklingum tilteknar upplýsingar samkvæmt löggjöfinni. Þannig er alla jafna talað um upplýsingarétt einstaklinga og fræðsluskyldu fyrirtækja og stjórnvalda og er þá átt við sama hlutinn.

Áður en vinnsla hefst og upplýsinga er aflað frá hinum skráða á hann rétt á að fyrirtækið eða stjórnvaldið sem óskar upplýsinga veiti m.a. fræðslu um eftirfarandi (ekki tæmandi talning):

- hvers vegna er verið að vinna með upplýsingarnar
- hver lagagrundvöllur vinnslunnar er
- hvaða tegundir upplýsinga eru notaðar
- hvaðan upplýsingarnar eru fengnar, ef þær koma frá öðrum en hinum skráða
- hversu lengi á að varðveita upplýsingarnar
- hvort miðla eigi upplýsingunum til þriðja aðila og þá til hvers og hvers vegna
- hvort flytja eigi upplýsingarnar úr landi, og þá hvert og hvað eigi að gera við þær
- hvort nota eigi upplýsingarnar við gerð persónusniðs
- rétt hins skráða til að kvarta til Persónuverndar

Þegar upplýsinga er aflað frá öðrum en hinum skráða sjálfum þarf ekki að veita fræðslu ef skýrt er mælt fyrir um öflun eða miðlun upplýsinganna í lögum.

Sjá nánar undir kafla 5.2 „Fræðsluskyldan“.

6.2 Aðgangsréttur

17. gr. pvl. og 15. gr. pvrg.

Einstaklingar eiga rétt á að fá upplýsingar um það hvort fyrirtæki eða stjórnvald, eða annar aðili sem vinnur með persónuupplýsingar, vinnur með persónuupplýsingar um þá. Þessi réttur nefnist rétturinn til aðgangs, eða aðgangsréttur. Í honum felst réttur til þess að fá:

- staðfestingu á því að unnið sé með persónuupplýsingar einstaklings,
- afrit af þeim persónuupplýsingum um einstaklinginn sem unnið er með, og
- aðrar upplýsingar um vinnsluna.
    - Með öðrum upplýsingum um vinnsluna er átt við upplýsingar um:
      a. tilgang vinnslunnar,

b. viðkomandi flokka persónuupplýsinga,
c. viðtakendur eða flokka viðtakenda sem hafa fengið eða munu fá persónuupplýsingarnar í hendur,
d. ef mögulegt er, hversu lengi er fyrirhugað að varðveita persónuupplýsingarnar eða, ef það reynist ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,
e. að fyrir liggi réttur til að fara fram á leiðréttingu persónuupplýsinganna, eyðingu þeirra eða takmörkun vinnslu þeirra hvað hinn skráða varðar, eða til að andmæla slíkri vinnslu,
f. réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi (Persónuvernd),
g. ef persónuupplýsinganna er ekki aflað hjá hinum skráða, allar fyrirliggjandi upplýsingar um uppruna þeirra, og
h. hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr. persónuverndarreglugerðarinnar, og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.

Hvenær ber að svara aðgangsbeiðni?

Aðgangsbeiðnum á að svara án ótilhlýðilegrar tafar og eigi síðar en innan mánaðar frá því að beiðnin barst fyrirtækinu/stjórnvaldinu. Þennan frest má þó lengja um tvo mánuði til viðbótar ef þörf er á, með hliðsjón af fjölda beiðna sem bíða afgreiðslu og því hversu flóknar þær eru. Ef þessi heimild til framlengingar er nýtt ber fyrirtækinu/stjórnvaldinu að tilkynna einstaklingnum um það innan mánaðar frá því að beiðnin barst, og greina jafnframt frá ástæðunum fyrir töfinni. Ef ekki er orðið við aðgangsbeiðninni skal fyrirtækið/stjórnvaldið, án tafar og í síðasta lagi innan mánaðar frá viðtöku beiðninnar, tilkynna einstaklingnum um ástæðurnar fyrir því að það var ekki gert og um möguleikann á að leggja fram kvörtun hjá Persónuvernd. Þegar beiðni um aðgang að persónuupplýsingum er beint að fjárhagsupplýsingastofu getur í sumum tilvikum verið skylt að veita svar innan tveggja vikna.

Ef einstaklingur er ósáttur við það hvernig fyrirtæki eða stjórnvald hefur brugðist við beiðni um aðgang, og frekari samskipti við fyrirtækið/stjórnvaldið hafa engar úrbætur í för með sér, getur hann sent Persónuvernd formlega kvörtun.

Einstaklingur getur óskað eftir aðgangi að persónuupplýsingunum sínum oftar en einu sinni. Þó skal tekið fram að fyrirtækið/stjórnvaldið sem um ræðir getur í vissum tilvikum neitað að verða við beiðni um aðgang að persónuupplýsingum, en það á t.d. við þegar beiðnin er augljóslega tilefnislaus eða óhófleg, einkum vegna endurtekningar. Þegar svo háttar til er jafnframt heimilt að setja upp sanngjarnt gjald með tilliti til stjórnsýslukostnaðar við upplýsingagjöfina.

Á hvaða formi ber að afhenda gögn?

Fyrirtæki eða stjórnvald, sem fær í hendur beiðni frá einstaklingi um aðgang að persónuupplýsingum sínum, á að láta í té afrit af þeim persónuupplýsingum sem unnið er með. Ef aðgangsbeiðnin er sett fram rafrænt skulu upplýsingarnar látnar í té með rafrænu sniði sem almennt er notað, nema einstaklingurinn fari fram á annað. Ef upplýsingarnar eru veittar rafrænt, sbr. framangreint, eru því ekki aðrar kröfur gerðar til fyrirtækisins/stjórnvaldsins en þær að notast sé við rafrænt snið sem er

„almennt notað“. Einstaklingurinn getur hins vegar óskað eftir öðrum afhendingarmáta, svo sem að fá gögn afhent á pappírsformi eða að upplýsingar séu veittar munnlega, þegar slíkt er mögulegt.

Ef verulegur vafi leikur á því hver sá einstaklingur er, sem leggur fram beiðni um aðgang að persónuupplýsingum, er hægt að fara fram á að veittar séu nauðsynlegar viðbótarupplýsingar til þess að staðfesta deili á honum. Fyrirtæki og stjórnvöld þurfa þó ávallt að hafa meginreglu persónuverndarlaganna um meðalhóf í huga og biðja ekki um ítarlegri eða meiri upplýsingar en þörf er á í framangreindum tilgangi.

6.3 Réttur til að krefjast takmörkunar á vinnslu

20. gr. pvl. og 18. gr. pvrg.

Einstaklingur getur krafist þess að ábyrgðaraðili takmarki vinnslu þegar eitt af eftirfarandi á við:

a) hinn skráði vefengir að persónuupplýsingar séu réttar, þangað til ábyrgðaraðilinn hefur fengið tækifæri til að staðfesta að þær séu réttar.
b) vinnslan er ólögmæt og hinn skráði andmælir því að persónuupplýsingunum sé eytt og fer fram á takmarkaða notkun þeirra í staðinn.
c) ábyrgðaraðilinn þarf ekki lengur á persónuupplýsingunum að halda fyrir vinnsluna en skráði einstaklingurinn þarfnast þeirra til þess að stofna, hafa uppi eða verja réttarkröfur.
d) skráði einstaklingurinn hefur andmælt vinnslunni skv. 1. mgr. 21. gr. pvl. á meðan beðið er sannprófunar á því hvort hagsmunir ábyrgðaraðila gangi framar lögmætum hagsmunum hins skráða.

Þegar vinnsla hefur verið takmörkuð skal ábyrgðaraðili einungis vinna slíkar persónuupplýsingar, að varðveislu undanskilinni, með samþykki hins skráða eða til að stofna, hafa uppi eða verja réttarkröfur eða til að vernda réttindi annars einstaklings eða lögaðila eða með skírskotun til brýnna almannahagsmuna Sambandsins eða aðildarríkis.

Ábyrgðaraðili skal tilkynna skráðum einstaklingi, sem fengið hefur fram takmörkun á vinnslu, um það áður en takmörkuninni á vinnslunni er aflétt.

6.4 Réttur til leiðréttingar

20. gr. pvl. og 16. gr. pvrg.

Einstaklingur á rétt á að fá óáreiðanlegar persónuupplýsingar sem varða hann sjálfan leiðréttar án ótilhlýðlegar tafar. Hinn skráði á einnig rétt á því, að teknu tilliti til tilgangs vinnslunnar, að láta fullgera ófullkomnar persónuupplýsingar, þ.m.t. með því að leggja fram yfirlýsingu til viðbótar við þær. Við vinnslu persónuupplýsinga ber að gæta að því að þær séu áreiðanlegar og uppfærðar eftir þörfum. Persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal eyða eða leiðrétta án tafar.

Tekið skal fram að stjórnvöldum er almennt ekki heimilt að eyða gögnum að hluta eða í heild. Hið sama á við um sveitarfélög, dómstóla og aðra aðila sem taldir eru upp í 14. gr. laga nr. 77/2014 um opinber skjalasöfn. Ástæðan er sú að á þeim hvílir skylda til að varðveita þau gögn sem verða til í tengslum við starfsemina og afhenda þau opinberu skjalasafni, í samræmi við ákvæði laganna.

6.5 Réttur til eyðingar – rétturinn til að gleymast

20. gr. pvl. og 17. gr. pvrg.

Ábyrgðaraðilum ber í vissum aðstæðum að eyða upplýsingum um einstaklinga. Meta þarf í hverju tilviki fyrir sig hvort skilyrði séu fyrir því að persónuupplýsingum um mann verði eytt. Ef einhver eftirtalinna ástæðna á við er ábyrgðaraðila skylt að eyða persónuupplýsingum án ótilhlýðlegar tafar:

- Persónuupplýsingarnar eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun þeirra eða annarri vinnslu þeirra.
- Vinnsla persónuupplýsinga er byggð á samþykki einstaklingsins og hann dregur samþykki sitt til baka, og ekki er annar lagagrundvöllur fyrir vinnslunni.
- Einstaklingurinn andmælir vinnslunni og ekki eru fyrir hendi lögmætar ástæður fyrir henni sem ganga framar.
- Vinnsla persónuupplýsinganna var ólögmæt.
- Eyða þarf persónuupplýsingunum til að uppfylla lagaskyldu.
- Persónuupplýsingunum var safnað saman í tengslum við það þegar barni var boðin þjónusta í upplýsingasamfélaginu.

Skylda ábyrgðaraðila til eyðingar persónuupplýsinga **gildir ekki** að því marki sem vinnsla er nauðsynleg:

- til að neyta réttarins til tjáningar- og upplýsingafrelsis.
- til að uppfylla lagaskyldu, eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðilinn fer með.
- vegna almannahagsmuna á sviði lýðheilsu.
- vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi.
- til að stofna, hafa uppi eða verja réttarkröfur.

Tekið skal fram að rétturinn til eyðingar persónuupplýsinga á almennt ekki við um þær persónuupplýsingar sem stjórnvöld vinna með. Hið sama á við um sveitarfélög, dómstóla og aðra aðila sem taldir eru upp í 14. gr. laga nr. 77/2014 um opinber skjalasöfn. Ástæðan er sú að á þeim hvílir skylda til að varðveita þau gögn sem verða til í tengslum við starfsemina og afhenda þau opinberu skjalasafni, í samræmi við ákvæði laganna.

Tilkynningarskylda varðandi leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu (19. gr. pvrg.)

- Ábyrgðaraðili skal tilkynna sérhverjum viðtakanda, sem fengið hefur persónuupplýsingar í hendur, um hvers kyns leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu sem á sér stað í samræmi við 16. gr., 1. mgr. 17. gr. og 18. gr. pvrg. , nema það sé ekki unnt eða feli í sér óhóflega fyrirhöfn. Ábyrgðaraðilinn skal tilkynna hinum skráða um þessa viðtakendur fari hann fram á það.

6.6 Flutningsréttur

20. gr. pvl. og 20. gr. pvrg.

Flutningsréttur á við þegar einstaklingur hefur sjálfur afhent ábyrgðaraðila persónuupplýsingar um sig á rafrænu formi, nánar tiltekið á skipulegu, algengu, tölvulesanlegu sniði. Í réttinum felst að ábyrgðaraðila ber að verða við ósk einstaklingsins um að fá persónuupplýsingarnar í hendur. Þá felst í réttinum að einstaklingurinn á að geta sent upplýsingarnar öðrum ábyrgðaraðila án þess að fyrri ábyrgðaraðilinn hindri það, en slíkt gæti til dæmis átt við þegar upplýsingar hafa verið skráðar í prófil einstaklings á samfélagsmiðli og hann vill flytja þær til annars slíks miðils.

Eftirfarandi eru skilyrði þess að rétturinn eigi við:

- Vinnsla upplýsinganna byggist á samþykki hins skráða einstaklings eða samningi.
- Vinnslan sé sjálfvirk.
- Flutningur upplýsinganna sé tæknilega framkvæmanlegur.

Af þessu leiðir meðal annars að flutningsrétturinn er ekki til staðar þegar vinnslan styðst við aðrar heimildir en samþykki eða samning. Til dæmis má nefna þau tilvik þegar vinnsla persónuupplýsinganna styðst við lagaheimild eða nauðsyn vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds, svo sem algengt er þegar stjórnvöld eru ábyrgðaraðilar.

Það að neyta réttarins til flutnings eigin gagna hefur ekki áhrif á réttinn til eyðingar (réttinn til að gleymast). Sá réttur skal ekki gilda um vinnslu sem er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með.

Rétturinn til að flytja eigin gögn skal ekki skerða réttindi og frelsi annarra.

Evrópska persónuverndarráðið (EDBP) hefur staðfest leiðbeiningar 29. gr. vinnuhópsins um flutningsrétt.

Til hvaða gagna nær flutningsrétturinn?

Stundum er auðvelt að rekja hvaða upplýsingar hinn skráði hefur veitt ábyrgðaraðilanum, t.d. nafn, tölvupóstfang, notandanafn o.fl. Rétturinn er þó ekki einskorðaður við þær upplýsingar. Hann nær einnig til persónuupplýsinga sem fylgja notkun einstaklingsins, s.s. þegar tæki eða þjónusta er notuð. Nánar tiltekið er þá átt við hráar, óunnar upplýsingar sem stafa frá hinum skráða sjálfum, svo sem:

- vefnotkunar- og leitarsögu.
- staðsetningar- og ferðagögn.
- upplýsingar um hinn skráða sem skrást við notkun stafræns búnaðar sem hinn skráði ber á sér (t.d. heilsuúrs).

Flutningsrétturinn tekur hins vegar ekki til afleiddra gagna sem ábyrgðaraðilinn gæti hafa útbúið á grundvelli þeirra upplýsinga sem stafa frá einstaklingnum sjálfum, en sem dæmi um slík afleidd gögn má til dæmis nefna skýrslur um lánshæfi sem skylt er að gera á grundvelli löggjafar um neytendalán og áhættumat sem áskilið er í löggjöf um aðgerðir gegn peningaþvætti.

Hafa ber í huga að ef umrædd, afleidd gögn hafa að geyma persónuupplýsingar falla þær undir reglur um aðgangsrétt viðkomandi einstaklings ef hann leggur inn beiðni um aðgang.

6.7 Andmælaréttur

21. gr. pvl. og 21. gr. pvrg.

Hinum skráða er almennt heimilt að andmæla vinnslu persónuupplýsinga er varða hann sjálfan þegar vinnsla byggist á almannahagsmunum eða beitingu opinbers valds, eða lögmætum hagsmunum sem ábyrgðaraðili eða þriðji aðili gætir. Má þá ekki vinna upplýsingarnar frekar nema sýnt sé fram á mikilvægar lögmætar ástæður fyrir vinnslunni.

Ábyrgðaraðili má í þeim tilfellum ekki vinna persónuupplýsingarnar frekar nema hann geti sýnt fram á mikilvægar lögmætar ástæður fyrir vinnslunni sem ganga framar hagsmunum, réttindum og frelsi hins skráða, eða vinnslan sé nauðsynleg til að stofna, hafa uppi eða verja réttarkröfur.

Það er ávallt á hendi ábyrgðaraðila að sýna fram á að mikilvægir lögmætir hagsmunir gangi framar hagsmunum eða grundvallarréttindum og frelsi hins skráða í tengslum við andmælarétt hins síðarnefnda.

6.8 Auknar kröfur til samþykkis

Samþykki er áfram ein af þeim heimildum sem byggja má vinnslu persónuupplýsinga á samkvæmt nýrri löggjöf. 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. Hér verður fjallað um helstu þætti samþykkis en Persónuvernd hefur gefið út ítarlegar leiðbeiningar um samþykki. Evrópska persónuverndarráðið (EDBP) hefur jafnframt gefið út leiðbeiningar um samþykki.

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.

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, en það getur leitt til þess að samþykkið teljist ekki gilt.

Sértækt samþykki

Til að samþykki teljist vera fullnægjandi í skilningi persónuverndarlaganna og 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.

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
- 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:

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.

Upplýst samþykki

Persónuverndarreglugerðin 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.

Ótvírætt samþykki

Í persónuverndarreglugerðinni og persónuverndarlögunum 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. Samþykki verður þannig að vera veitt með einhvers konar aðgerð af hálfu hins skráða.

Heimilt er að veita yfirlýsinguna munnlega, skriflega eða með rafrænum hætti. Aðgerðaleysi, svo sem box sem þegar hefur verið hakað í, fullnægir hins vegar ekki skilyrðum laganna 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 laganna.

Samþykki er ekki hægt að veita samhliða undirritun samnings eða viðurkenningu á almennum skilmálum. Slíkt telst ekki uppfylla skilyrði laganna til ótvíræðs samþykkis fyrir vinnslu persónuupplýsinga.

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

Þrátt fyrir að ekki sé kveðið á um það berum orðum í persónuverndarreglugerðinni að afla þurfi samþykkis áður en hafist er handa við vinnslu persónuupplýsinga, þá segir í 1. tölul. 1. mgr. 6. gr. pvrg. og 1. tölul. 9. gr. pvl. 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.

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 eða rafræn skilríki.

Aðrar kröfur varðandi samþykki

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 það hafi verið veitt, hvernig og hvenær. 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.

Afturköllun samþykkis: Í persónuverndarreglugerðinni er lögð aukin áhersla á afturköllun samþykkis. 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.

Dæmi:

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 ekki sambærilegur við að þurfa að hringja símtal á tilteknum tíma.

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.

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.

6.9 Börnum veitt sérstök vernd

Persónuupplýsingar barna njóta sérstakrar verndar, þar sem þau kunna að vera síður meðvituð um áhættu, afleiðingar og réttindi sín í tengslum við vinnslu persónuupplýsinga. Er þetta sérstaklega áréttað í formálsorðum persónuverndarreglugerðarinnar. Það er því mikilvægt að hlúa vel að persónuvernd barna. Þá skiptir miklu máli að fylgja ávallt meginreglum persónuverndarlaganna, og skal sanngirni til dæmis höfð að leiðarljósi við alla vinnslu. Þá ættu hvers kyns upplýsingar og tilkynningar, þegar vinnsla beinist að barni, að vera á skýru og einföldu máli sem barnið getur auðveldlega skilið.

Foreldrar og forráðamenn sjá yfirleitt um að samþykkja vinnslu persónuupplýsinga um börn sín. Áður en börn undir 13 ára aldri skrá sig í þjónustu í upplýsingasamfélaginu þarf að afla samþykkis foreldra eða forráðamanna. Börn sem hafa náð 13 ára aldri þurfa hins vegar ekki samþykki forráðamanna. Samþykki foreldra eða forráðamanna er auk þess ekki nauðsynlegt þegar um er að ræða forvarnar- eða ráðgjafarþjónustu sem barni er boðin beint.

Réttur til eyðingar persónuupplýsinga kann að vera sérstaklega mikilvægur í þeim tilvikum þegar einstaklingurinn var barn þegar hann gaf samþykki sitt fyrir vinnslunni.

7. Persónuverndarfulltrúar

7.1 Almennt

Persónuverndarfulltrúi er sá aðili sem ber sérstaka ábyrgð á málefnum fyrirtækisins eða stofnunarinnar sem tengjast persónuvernd. Persónuverndarfulltrúar aðstoða fyrirtæki og stofnanir við að sinna innra eftirliti, upplýsa og ráðleggja vegna persónuverndarlöggjafarinnar, veita ráðgjöf við framkvæmd mats á áhrifum á persónuvernd, og eru tengiliðir við einstaklinga og Persónuvernd.

Í persónuverndarreglugerðinni er litið á persónuverndarfulltrúann sem lykilstarfsmann og mælir hún fyrir um skilyrði fyrir ráðningu hans, stöðu og verkefni. Markmiðið er að gefa hlutverki hans vægi í því skyni að tryggja að ábyrgðaraðilar og vinnsluaðilar fari að reglunum og styrkja jafnframt persónuverndarfulltrúann í störfum sínum.

Í 35.-36. gr. pvl. og 37.-39. gr. pvrg. er fjallað um persónuverndarfulltrúa.

7.2 Tilnefning og staða persónuverndarfulltrúa

Persónuverndarfulltrúi skal tilnefndur á grundvelli faglegrar hæfni sinnar, einkum sérþekkingar á persónuverndarlögum og lagaframkvæmd á því sviði, auk getu sinnar til að vinna þau verkefni sem honum eru falin í reglugerðinni.

Við mat á því hvaða kröfur þarf að gera til sérþekkingar persónuverndarfulltrúans þarf að hafa hliðsjón af þeirri vinnslu persónuupplýsinga sem fram fer og þeim kröfum sem gerðar eru til verndar þeirra persónuupplýsinga sem vinnslan lýtur að. Þegar vinnsla persónuupplýsinga er mjög flókin eða þegar um er að ræða umfangsmikla vinnslu viðkvæmra upplýsinga þarf að gera ríkari kröfur til sérþekkingar persónuverndarfulltrúans og þess stuðnings sem hann getur þarfnast. Ef um stjórnvöld er að ræða ætti persónuverndarfulltrúinn að hafa þekkingu á stjórnsýslulögum svo og þeim lögum er varða umrædda starfsemi.

Rétt er að taka fram að persónuverndarfulltrúar þurfa ekki að hafa sérstaka vottun sem persónuverndarfulltrúar til að geta gegnt umræddu starfi, þó svo að vissulega geti slík vottun verið til marks um að viðkomandi hafi a.m.k. einhverja þekkingu á persónuverndarlöggjöf. Þá er ekki gert að skilyrði að persónuverndarfulltrúinn sé lögfræðingur, en viðkomandi þarf engu að síður að hafa greinargóða þekkingu á persónuverndarreglugerðinni og öðrum lögum sem starfsemina varða.

Skylt er að **tilnefna persónuverndarfulltrúa** þegar:

- vinnsla fer fram hjá stjórnvaldi (óháð því hvaða persónuupplýsingar eru unnar). Þetta á við um opinberar stofnanir og sveitarfélög.
- meginstarfsemi ábyrgðaraðila eða vinnsluaðila lýtur að vinnsluaðgerðum, sem fela í sér umfangsmikið, reglubundið og kerfisbundið eftirlit með einstaklingum.
- meginstarfsemi ábyrgðaraðila eða vinnsluaðila er umfangsmikil vinnsla viðkvæmra persónuupplýsinga eða persónuupplýsinga er varða sakfellingar í refsimálum og refsiverð brot.

Æskilegt er að fyrirtæki, sem sinna verkefnum sem innt eru af hendi í þágu almannahagsmuna, tilnefni persónuverndarfulltrúa þó þau teljist ekki til stjórnvalda. Nefna má sem dæmi þá sem sinna

almenningssamgöngum, vegaframkvæmdum eða fjölmiðlun, orkuveitur, hússnæðisstofnanir eða opinbera eftirlitsaðila tiltekinna starfsstétta. Einnig er æskilegt að fyrirtæki sem eru að meirihluta í eigu opinberra aðila tilnefni slíka fulltrúa.

Fyrirtækjum sem ekki sinna þessari starfsemi er engu að síður frjálst að tilnefna persónuverndarfulltrúa, þótt þeim sé það ekki skylt, en hafa þarf í huga að þá þarf að gera sömu kröfur og gerðar eru þegar skylt er að tilnefna fulltrúann.

Benda má á að þegar um umfangsmikla starfsemi persónuupplýsinga er að ræða getur þurft að skipa teymi persónuverndarfulltrúa (í teyminu eru þá persónuverndarfulltrúi og starfsmenn hans). Í slíkum tilvikum þarf skipulag teymisins og verkefni hvers og eins að vera skýrt skilgreint.

Ábyrgðaraðila eða vinnsluaðila sem hefur tilnefnt persónuverndarfulltrúa er skylt að birta samskiptaupplýsingar hans og tilkynna hann til Persónuverndar, sbr. 7. mgr. 37. gr. pvrg.

Nánari upplýsingar um tilnefningu og stöðu persónuverndarfulltrúa er að finna í leiðbeiningum Persónuverndar um persónuverndarfulltrúa. Þá hefur Evrópska persónuverndarráðið (EDPB) gefið út leiðbeiningar um persónuverndarfulltrúa.

7.2.1 Sjálfstæði persónuverndarfulltrúa

Persónuverndarfulltrúi getur sinnt starfi sínu samhliða öðrum verkefnum en þau mega ekki valda hagsmunaárekstrum. Það þýðir að persónuverndarfulltrúinn getur ekki verið í þannig stöðu að hann ákveði tilgang og aðferð við vinnslu persónuupplýsinga. Þetta þarf að skoða í hverju tilviki fyrir sig, með tilliti til sérstöðu og stjórnskipulags hverrar stofnunar/fyrirtækis.

Nokkur ákvæði í persónuverndarlöggjöfinni eiga að tryggja að persónuverndarfulltrúinn geti starfað sjálfstætt:

- Hann má ekki fá fyrirmæli frá ábyrgðaraðila eða vinnsluaðila um hvernig hann á að sinna starfi sínu.
- Ekki má reka hann eða refsa honum fyrir störf sín sem persónuverndarfulltrúi.
- Hann á ekki að lenda í því að hagsmunir vegna annarra verkefna og starfa geti skarast við starf hans sem persónuverndarfulltrúi.

Hér þarf líka sérstaklega að gæta að því að við ákvarðanatöku um hvernig skuli haga ákveðinni vinnslu að ekki er hægt að leggja þá ábyrgð á persónuverndarfulltrúann, þó svo að það geti verið freistandi, enda væri hann þá farinn að taka ákvarðanir um vinnslu persónuupplýsinga sem aftur myndi valda hagsmunaárekstrum.

Almenna reglan er sú að hagsmunaárekstrar geta orðið ef persónuverndarfulltrúi er millistjórnandi í stofnun/fyrirtæki (svo sem framkvæmdastjóri, rekstarstjóri, fjármálastjóri, markaðsstjóri, mannauðsstjóri, tæknistjóri o.fl.) en einnig getur það átt við í tilviki annarra lægra settra starfsmanna ef störf þeirra fela í sér ákvarðanatöku um tilgang og aðferð við vinnslu persónuupplýsinga. Að auki geta hagsmunaárekstrar orðið ef utanaðkomandi persónuverndarfulltrúi er beðinn um að koma fram fyrir hönd fyrirtækis eða stofnunar fyrir dómi í máli er varðar vinnslu persónuupplýsinga hjá viðkomandi aðila.

Skrá yfir vinnslustarfsemi getur hjálpað við að leggja mat á hvort hugsanlegir hagsmunaárekstrar varðandi ákvarðanatöku séu til staðar.

Sjálfstæði persónuverndarfulltrúans þýðir ekki að hann hafi ákvörðunarvald umfram þau verkefni sem honum eru falin.

Persónuverndarfulltrúi á ekki að taka ákvarðanir um vinnslu persónuupplýsinga heldur veita ráðgjöf og sinna eftirliti.

Tryggja þarf að önnur verkefni eða skyldur sem falin eru persónuverndarfulltrúanum leiði ekki af sér hagsmunaárekstra.

7.3 Hlutverk og verkefni persónuverndarfulltrúa

Verkefni persónuverndarfulltrúa er einkum að tryggja að fyrirtækið eða stofnunin uppfylli kröfur persónuverndarlaganna. Persónuverndarfulltrúinn þarf að vera sjálfstæður, sérfræðingur í persónuverndarlöggjöfinni, hafa fullnægjandi aðstöðu og mannafla og hafa beinan aðgang að æðstu yfirstjórn. Þá er hlutverk hans einnig að veita ráðgjöf um persónuvernd og eiga samstarf við Persónuvernd og vera fulltrúi fyrirtækisins eða stofnunarinnar gagnvart eftirlitsstofnuninni.

Tryggja skal að persónuverndarfulltrúinn komi með viðeigandi hætti og tímanlega að öllum málum er tengjast vernd persónuupplýsinga. Honum skal m.a. boðið að funda með yfirstjórn reglulega, vera viðstaddur þegar ákvarðanir um aðgerðir vegna vinnslu persónuupplýsinga eru teknar og gefa þarf honum möguleika á að gefa viðeigandi ráð. Ef ekki er farið að ráðum persónuverndarfulltrúans þarf að skrásetja það sérstaklega. Persónuverndarfulltrúi getur annaðhvort verið starfsmaður eða utanaðkomandi sérfræðingur.

Í 39. gr. pvrg. segir að persónuverndarfulltrúi skuli sinna **a.m.k.** eftirfarandi verkefnum:

a) upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt reglugerðinni og öðrum ákvæðum Sambandsins eða aðildarríkis um persónuvernd og veita þeim ráðgjöf þar að lútandi,
b) fylgjast með því að farið sé að ákvæðum reglugerðarinnar, öðrum ákvæðum í lögum Sambandsins eða aðildarríkis um persónuvernd og stefnum ábyrgðaraðila eða vinnsluaðila varðandi vernd persónuupplýsinga, þ.m.t. úthlutun ábyrgðar, vitundarvakning og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi og tilheyrandi úttektir,
c) veita ráðgjöf, sé farið fram á það, varðandi mat á áhrifum á persónuvernd og fylgjast með framkvæmd þess skv. 35. gr.,
d) vinna með eftirlitsyfirvaldinu,
e) vera tengiliður fyrir eftirlitsyfirvaldið varðandi mál sem tengjast vinnslu, þ.m.t. fyrirframsamráðið sem um getur í 36. gr., og leita ráða, eftir því sem við á, varðandi önnur málefni.

Þá segir jafnframt að persónuverndarfulltrúi skuli við framkvæmd verkefna sinna taka tilhlýðilegt tillit til þeirrar áhættu sem fylgir vinnslustarfseminni, með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar.

a) Fræðsla og ráðgjöf

Persónuverndarfulltrúi á samkvæmt persónuverndarreglugerðinni að upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt reglugerðinni og öðrum ákvæðum í lögum Sambandsins eða aðildarríkis um persónuvernd og veita þeim ráðgjöf þar að lútandi.

Persónuverndarfulltrúi stuðlar þannig að vitundarvakningu, sinnir fræðslu og framkvæmir reglulegar úttektir.

Þannig getur persónuverndarfulltrúi séð til þess að vinnustaðarmenning innanhúss taki mið af persónuverndarlöggjöfinni og að starfsmenn séu meðvitaðir um skyldur sínar. Persónuverndarfulltrúi getur þannig séð um að veita starfsfólki í sínu fyrirtæki, eða sinni stofnun, fræðslu um persónuvernd og tryggt að starfsfólk sem hefur aðgang að persónuupplýsingum fái nauðsynlega fræðslu og þjálfun á því sviði sem við á. Þá er mikilvægt að hann fræði þá, sem vinna með persónuupplýsingar, um þær meginreglur sem ber að hafa að leiðarljósi við alla vinnslu persónuupplýsinga, ásamt heimildum til vinnslu.

Vitundarvakningu og fræðslu persónuverndarfulltrúa til starfsmanna lýkur ekki eftir að fræðsla hefur verið veitt í fyrsta sinn. Persónuverndarfulltrúinn þarf að gæta þess að áframhald sé á reglulegri fræðslu eftir því sem þörf krefur og jafnframt að gæta sérstaklega að fræðslu til nýrra starfsmanna.

b) Eftirlit með reglufylgni

Til að sinna eftirliti með reglufylgni og aðstoða ábyrgðaraðila og vinnsluaðila við að fylgja persónuverndarreglugerðinni þarf persónuverndarfulltrúinn sérstaklega að:

- safna upplýsingum til að greina vinnslustarfsemi,
- greina og fylgjast með reglufylgni í starfseminni,
- upplýsa, ráðleggja og koma á framfæri tillögum til ábyrgðaraðila eða vinnsluaðila.

c) Mat á áhrifum á persónuvernd (MÁP)

Ef líklegt er að tiltekin tegund vinnslu geti haft í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga, einkum þar sem beitt er nýrri tækni og með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar, skal ábyrgðaraðili láta fara fram mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan hefst (MÁP).

Hvað er MÁP?

MÁP er tól til að meta og lágmarka áhættu fyrir persónuvernd einstaklinga við framkvæmd nýrra verkefna. Matið er hluti af nýjum skyldum fyrirtækja og stofnana samkvæmt persónuverndarreglugerðinni og mikilvægur hluti af „innbyggðri og sjálfgefinni persónuvernd“ sem er eitt af grundvallaratriðunum í nýju löggjöfinni.

Mat á áhrifum á persónuvernd er kerfisbundið ferli sem hjálpar til við að greina, bera kennsl á og lágmarka persónuverndaráhættu verkefnis eða kerfis. Yfirleitt er ekki hægt að koma í veg fyrir alla áhættu en það ætti að vera hægt að lágmarka hana og ákveða hvort áhættan sé ásættanleg miðað við ávinning.

MÁP er ekki bara æfing. Það að framkvæma matið getur greint möguleg vandamál áður en þau verða, aukið traust og tiltrú þeirra sem verkefnið nær til og getur auk þess leitt til sparnaðar ef verkefnið er gert einfaldara og minna af persónuupplýsingum er safnað.

Að gera ekki mat á áhrifum á persónuvernd þar sem kringumstæður krefjast þess getur auk þess leitt til álagningar stjórnvaldssekta eða beitingar annarra valdheimilda Persónuverndar.

Persónuvernd hefur gefið út ítarlegar leiðbeiningar um mat á áhrifum á persónuvernd (MÁP) með athugunarlista vegna framkvæmdar MÁP. Þá hefur evrópska persónuverndarráðið (EDPB) gefið út leiðbeiningar um mat á áhrifum á persónuvernd.

Hvert er hlutverk persónuverndarfulltrúa í tengslum við MÁP?

Ábyrgðaraðili og vinnsluaðili skulu leita ráðgjafar hjá persónuverndarfulltrúa, sé hann til staðar, þegar matið er framkvæmt og er nauðsynlegt að skjalfesta í matinu þau ráð sem hann gefur. Ef ekki er farið að ráðum persónuverndarfulltrúans þarf ábyrgðaraðilinn að skrásetja ástæður þess.

Persónuverndarfulltrúi skal m.a. veita ráðgjöf um eftirfarandi þætti:

- hvort meta eigi áhrif á persónuvernd,
- hvaða aðferð eigi að beita við að matið,
- hvort matið eigi að fara fram innanhúss eða hvort útvista eigi verkefninu,
- hvaða tæknilegu og skipulagslegu öryggisráðstafanir þurfi að gera til að draga úr áhættu fyrir réttindi og frelsi hinna skráðu,
- hvort matið hafi farið fram með réttum hætti og hvort niðurstaða þess (að hefja umrædda vinnslu og hvaða öryggisráðstöfunum eigi að beita) sé í samræmi við kröfur um persónuvernd.

Hvenær á að framkvæma MÁP?

Persónuverndarreglugerðin tekur þrjú dæmi um vinnslu sem sjálfkrafa krefst mats á áhrifum á persónuvernd.

- Vinnsla sem felur í sér umfangsmikla söfnun persónuupplýsinga, gerð persónusniðs og notkun þess til ákvarðanatöku sem hefur lagalegar afleiðingar fyrir einstaklinga
- Umfangsmikil vinnsla viðkvæmra upplýsinga, svo sem um heilsufar, fjárhag, erfðaupplýsingar og fleira, eða upplýsinga um sakfellingar í refsimálum eða refsiverð brot
- Umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi

Hér ekki um tæmandi lista að ræða. Þannig getur verið um að ræða vinnsluaðgerðir sem fylgir mikil áhætta og eru ekki tilteknar í upptalningunni og þá þarf að framkvæma MÁP.

Við mat á því hvort MÁP þurfi að fara fram má líta til þess hvort vinnslan felur í sér eitthvað af eftirfarandi atriðum:

1. Mat á einstaklingum
2. Sjálfvirk ákvarðanataka sem hefur réttaráhrif að því er varðar einstaklinginn sjálfan eða snertir hann á sambærilegan hátt að verulegu leyti
3. Kerfisbundið eftirlit

4. Viðkvæmar persónuupplýsingar eða upplýsingar persónulegs eðlis
5. Umfangsmiklar vinnsluaðgerðir
6. Samkeyrsla
7. Persónuupplýsingar um viðkvæma hópa einstaklinga
8. Tækninýjungar eða nýstárlegar aðferðir við vinnslu persónuupplýsinga
9. Þegar komið er í veg fyrir að einstaklingar njóti réttinda sinna

Eftir því sem fleiri af þessum viðmiðum eiga við um þá vinnslu sem á sér stað, því líklegra er að vinnslan hafi í för með sér mikla áhættu fyrir réttindi og frelsi einstaklinga.

Í flestum tilvikum geta fyrirtæki og stofnanir metið sem svo að vinnsla sem fellur undir tvö fyrrgreindra viðmiða þarfnist MÁP. Í einhverjum tilvikum getur þó niðurstaðan verið sú að vinnsla sem tekur til eins af viðmiðunum þarfnist mats.

Nánari skýringar á hverju viðmiði fyrir sig ásamt viðmiðatöflu má finna í leiðbeiningum Persónuverndar um MÁP. Þá mun Persónuvernd á næstu mánuðum birta lista yfir þær vinnsluaðgerðir sem þurfa ávallt að fara í MÁP.

Hvernig á að framkvæma MÁP?

Mat á áhrifum á persónuvernd á að framkvæma áður en vinnslan hefst. Það er fyrst og fremst fyrirtækið sjálft eða stofnunin sem ber ábyrgð á að framkvæma matið, ekki þjónustuaðili eða persónuverndarfulltrúinn. Það er þó hægt að útvista matinu en ábyrgðin liggur áfram hjá ábyrgðaraðilanum.

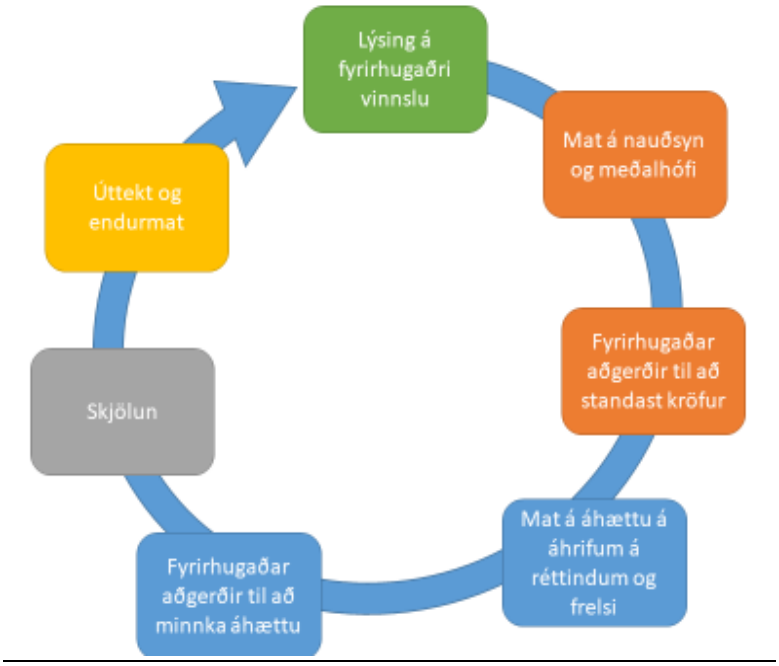
Öryggisstjórar og persónuverndarfulltrúar geta einnig lagt til að MÁP sé framkvæmt á tiltekinni vinnsluaðgerð. Þá ættu þessir aðilar einnig að aðstoða og hafa eftirlit með gerð matsins, þ. á m. til að meta gæði þess og hvort áhætta sem enn er til staðar sé viðunandi.

Ábyrgðaraðilar geta tileinkað sér mismunandi aðferðafræði við framkvæmd matsins, en viðmiðin eru þau hin sömu.

Reglugerðin tiltekur ákveðna lágmarksþætti sem matið þarf að geyma:

- Kerfisbundin lýsing á fyrirhugðum vinnsluaðgerðum og tilganginum með vinnslunni
- Mat á því hvort vinnsluaðgerðirnar eru nauðsynlegar og hóflegar
- Mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga
- Ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu og fyrirkomulag við að sýna fram á að farið sé að þessari reglugerð

Eftirfarandi skýringarmynd sýnir með myndrænum hætti það almenna ferli sem stöðugt þarf að viðhafa við framkvæmd MÁP:



Þær kröfur sem persónuverndarreglugerðin gerir til mats á áhrifum veita á vissan hátt breiðan og almennan ramma fyrir hönnun og framkvæmd matsins. Reglugerðin veitir ábyrgðaraðilum sveigjanleika til þess að ákveða hvernig þeir vilja nákvæmlega haga uppbyggingu og tegund mats á áhrifum á persónuvernd. Óháð því hvaða tegund eða gerð mats verður fyrir valinu, þá verður mat á áhrifum að vera raunverulegt mat á þeirri áhættu sem stafar af vinnsluaðgerð, svo ábyrgðaraðilar geti viðhaft viðeigandi ráðstafanir til þess að koma til móts við áhættuna.

Það er hlutverk ábyrgðaraðila að velja þá aðferðafræði sem notast er við við framkvæmd mats á áhrifum, en að lágmarki ber að fara eftir þeim viðmiðum sem Persónuvernd hefur sett fram.

d) Vinna með eftirlitsyfirvaldinu

Persónuverndarfulltrúi sinnir samskiptum við Persónuvernd og er tengiliður við stofnunina. Hann vinnur með Persónuvernd, t.d. vegna beiðni um fyrirframsamráð, og getur ávallt leitað til Persónuverndar til að fá ráðgjöf.

e) Fyrirframsamráð

Ef mat á áhrifum á persónuvernd skv. 35. gr. pvrg. gefur til kynna að vinnslan myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við eftirlitsyfirvaldið áður en vinnsla hefst.

Telji Persónuvernd að fyrirhuguð vinnsla muni brjóta í bága við reglugerðina, einkum ef ábyrgðaraðili hefur ekki greint eða dregið úr áhættunni með fullnægjandi hætti, skal stofnunin, innan átta vikna frá því að henni berst beiðni um samráð, veita ábyrgðaraðila og, eftir atvikum, vinnsluaðila skriflega ráðgjöf og getur hún notað til þess allar valdheimildir sínar sem um getur í 41.-43. gr. pvl. Frestinn má lengja um sex vikur með hliðsjón af því hversu flókin fyrirhuguð vinnsla er. Persónuvernd skal tilkynna ábyrgðaraðila og, eftir atvikum, vinnsluaðila, um slíkar framlengingar innan mánaðar frá því beiðni um samráð berst, ásamt ástæðunum fyrir töfinni. Þessa fresti má framlengja þar til Persónuvernd hefur fengið þær upplýsingar sem hún óskar eftir vegna samráðsins.

Persónuverndarfulltrúi skal, skv. e-lið 35. gr. pvrg., vera tengiliður fyrir eftirlitsyfirvaldið varðandi mál sem tengjast vinnslu, þ.m.t. fyrirframsamráð.

Þegar ábyrgðaraðili hefur samráð við eftirlitsyfirvaldið skal hann gefa því upp:

a) eftir atvikum, ábyrgðarsvið ábyrgðaraðila, sameiginlegra ábyrgðaraðila og vinnsluaðila, sem koma að vinnslunni, hvers um sig, einkum þegar um er að ræða vinnslu innan fyrirtækjasamstæðu,
b) tilgang fyrirhugaðrar vinnslu og aðferðir við hana,
c) ráðstafanir og verndarráðstafanir sem gerðar eru til að vernda réttindi og frelsi skráðra einstaklinga samkvæmt þessari reglugerð,
d) ef við á, samskiptaupplýsingar persónuverndarfulltrúa,
e) mat á áhrifum á persónuvernd sem kveðið er á um í 35. gr. pvrg., og
f) hverjar þær upplýsingar aðrar sem eftirlitsyfirvaldið fer fram á.

7.4 Önnur verkefni persónuverndarfulltrúa:

Verkefni persónuverndarfulltrúa eru ekki tæmandi talin í persónuverndarlöggjöfinni þar sem hún mælir fyrir um lágmarksverkefni hans. Persónuverndarlöggjöfin kemur því ekki í veg fyrir að persónuverndarfulltrúi sinni öðrum verkefnum en þeim sem honum eru falin í löggjöfinni, og raunar gerir reglugerðin ráð fyrir að hann geti það svo lengi sem tryggt er að önnur verkefni eða skyldur sem falin eru persónuverndarfulltrúanum **leiði ekki af sér hagsmunaárekstra** og að persónuverndarfulltrúinn **taki ekki ákvarðanir um vinnslu persónuupplýsinga**.

Í dæmaskyni eru hér talin upp nokkur verkefni sem persónuverndarfulltrúi gæti haft undir höndum. Hér er hvorki um tæmandi talningu að ræða né lögbundin verkefni persónuverndarfulltrúa.

Skrá yfir vinnslustarfsemi (vinnsluskrá)

Hvað varðar skrá yfir vinnslustarfsemi, þá er það ábyrgðaraðilinn eða vinnsluaðilinn, en ekki persónuverndarfulltrúinn, sem ber ábyrgð á að halda slíka skrá. Þeir geta hins vegar falið persónuverndarfulltrúa að halda slíka skrá á þeirra ábyrgð.

Með því að kortleggja þá vinnslu persónuupplýsinga sem fram fer hjá viðkomandi fyrirtæki eða stofnun, sem þátt í innra utanumhaldi og skjölun, fæst yfirsýn yfir þá vinnslu persónuupplýsinga sem fram fer í starfseminni. Þannig er litið á slíka skrá sem eina af þeim verkfærum sem persónuverndarfulltrúinn hefur til að sinna starfi sínu við vöktun vinnslu og að upplýsa og ráðleggja

ábyrgðar- eða vinnsluaðila. Vinnsluskrá er því mikilvægt verkfæri fyrir persónuverndarfulltrúa til þess að hann geti sinnt hlutverki sínu í tengslum við eftirlit með reglufylgni.

Tilkynning um öryggisbrest

Öryggisbrestur felur í sér brest á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi.

Það er á ábyrgð ábyrgðaraðila að tilkynna Persónuvernd **innan 72 klst.** um öryggisbrest sem hefur áhrif á einstaklinga.

Þegar ábyrgðaraðili tilkynnir um öryggisbrest til Persónuverndar skal í tilkynningunni a.m.k.:

- lýsa eðli öryggisbrestsins, þ.m.t. ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem hann varðar og flokkum og áætluðum fjölda skráninga persónuupplýsinga sem um er að ræða,
- gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar,
- lýsa líklegum afleiðingum öryggisbrests við meðferð persónuupplýsinga,
- lýsa þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna öryggisbrests við meðferð persónuupplýsinga, þ.m.t. eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif hans.

Það er því ekki óeðlilegt að það sé persónuverndarfulltrúinn sem sendir inn tilkynningu um öryggisbrest, verði því komið við, þar sem gert er ráð fyrir að hann geti verið tengiliður við Persónuvernd til að upplýsa stofnunina frekar sé þess óskað.

Stefna um persónuvernd (e. privacy policy)

Persónuverndarfulltrúi er sá aðili sem ber sérstaka ábyrgð á málefnum fyrirtækisins eða stofnunarinnar sem tengjast persónuvernd. Fræðsluskyldan er einn þáttur í ábyrgðarskyldu fyrirtækja og stjórnvalda samkvæmt persónuverndarlögum og felur í sér að framangreindir aðilar veiti einstaklingum tilteknar upplýsingar samkvæmt löggjöfinni.

Fyrirtæki geta sett sér stefnu um persónuvernd sem þátt í því að uppfylla fræðsluskyldu sína. Með stefnu um persónuvernd er átt við skráð skipulag og verkferla ábyrgðaraðila þegar kemur að vernd persónuupplýsinga, viðbrögðum við aðgangsbeiðnum, meðferð persónuupplýsinga og viðbrögðum við öryggisbrestum. Upplýsingar um hvernig fyrirtæki meðhöndlar persónuupplýsingar þurfa að vera á einföldu, aðgengilegu og auðskiljanlegu formi.

Athuga skal að stefna um persónuvernd er ekki það sama og persónuverndarstefna (e. privacy notice) sem hefur þann tilgang að uppfylla fræðsluskyldu gagnvart hinum skráða.

Verkferlar og áætlanir

Persónuverndarfulltrúar geta séð um að útbúa verkferla og áætlanir er varða persónuvernd. T.d. má útbúa verkferla sem grípa má til þegar tilkynna þarf brot á persónuverndarlöggjöfinni.

Þá er gott að þeir sem vinna með persónuupplýsingar séu búnir að gera áætlun um hvernig koma má til móts við flóknari kröfur, t.d. rétt fólks til að fá aðgang að upplýsingum, til að leiðrétta rangar upplýsingar, til að færa gögn á milli kerfa og til að eyða upplýsingum.

Samskipti við hinn skráða

Persónuverndarfulltrúi tekur á móti fyrirspurnum og beiðnum frá þeim einstaklingum sem verið er að vinna með upplýsingar um.

Samkvæmt 4. mgr. 38. gr. pvrg. geta skráðir einstaklingar haft samband við persónuverndarfulltrúann með öll mál sem tengjast vinnslu á persónuupplýsingum þeirra og því hvernig þeir geta neytt réttar síns samkvæmt reglugerðinni.

Til þess að einstaklingar, starfsmenn og Persónuvernd eigi auðvelt með að hafa samband við persónuverndarfulltrúann þarf að vera gott aðgengi að honum. Því má ná með því að birta upplýsingar um sérstakt netfang og/eða símanúmer sem hægt er að nota til að komast í samband við persónuverndarfulltrúann, til dæmis á vefsíðu fyrirtækisins eða stofnunarinnar.

Úrbætur og úttektir

Persónuverndarfulltrúi getur sett fram tillögur að úrbótum og má gera það á reglulegum fundum með æðstu yfirmönnum þess ábyrgðaraðila eða vinnsluaðila sem persónuverndarfulltrúinn starfar hjá.

Þá gæti persónufulltrúi farið í óundirbúnar heimsóknir og gert úttektir á starfsstöð sinni til að sinna hlutverki sínu um eftirlit með reglufylgni.

8. Áhugaverðir tenglar og lesefni

Evrópska persónuverndarráðið (European Data Protection Board - EDPB)
https://edpb.europa.eu/edpb_en

Leiðbeiningar EDPB
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Leiðbeiningar og álit 29. gr. vinnuhópsins
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

Handbók frá ESB um GDPR (Handbook on European data preotection law)
https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en/format-PDF/source-76364708

Handbók frá ESB um öryggi persónuupplýsinga (Handbook on Security of Personal Data Precessing)
https://publications.europa.eu/en/publication-detail/-/publication/eee277d3-d26f-4a18-825b-8e1fd80d2f0d/language-en/format-PDF/source-search

Breska persónuverndarstofnunin – ICO
https://ico.org.uk/

Norska persónuverndarstofnunin - Datatilsynet
https://www.datatilsynet.no/

Danska persónuverndarstofnunin - Datatilsynet
https://www.datatilsynet.dk/

Sænska persónuverndarstofnunin – Datainspektionen
https://www.datainspektionen.se/

The International Association of Privacy Professionals (IAPP)
https://iapp.org/