Þessi glærupakki er unninn upp úr fræðsluriti fyrir persónuverndarfulltrúa sem er útgefið af Persónuvernd árið 2018.

PERSÓNU VERND

Notkun kynningarefnisins

Glærurnar eru unnar upp úr fræðsluefni fyrir persónuverndarfulltrúa sem Persónuvernd hefur tekið saman og birt á vefsíðu sinni.

Notkun glæranna og kynningarefnisins í óbreyttri mynd er öllum heimil.

Óheimilt er að gera hvers kyns breytingar á glærunum, hvort sem er á efni þeirra eða útliti.

Persónuvernd ber enga ábyrgð á notkun þeirra upplýsinga sem kynningarefnið hefur að geyma.

PERSÓNU VERND

Ný evrópsk persónuverndarlöggjöf

Reglugerð Evrópuráðsins og þingsins (ESB) nr. 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 (GDPR)

Kom til framkvæmda 25. maí 2018 í Evrópu

- 99 lagagreinar, 173 formálsorð, 81 bls.

Víðtækt gildissvið – allur heimurinn undir

Helstu markmið

- Auka réttindi einstaklinga
  Hver vinnur upplýsingar um þá, **hvenær** og í **hvaða** tilgangi
- Þróun á hinum innri stafræna markaði
  Sparnaður og hagræðing fyrir fyrirtæki á evrópskum markaði – einnig auknar kröfur

- Í **apríl 2016** voru samþykktar í Evrópu **umfangsmestu breytingar** á evrópskri persónuverndarlöggjöf sem gerðar hafa verið í 20 ár. Þessar breytingar gera það að verkum að persónuverndarmálefni eru eitt af lykilatriðunum í rekstri hins opinbera og allra fyrirtækja landsins.

PERSÓNU VERND

Ný persónuverndarlög

- **Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga**
  - Tóku gildi 15. júlí 2018
  - Þau lögfestu reglugerð Evrópuþingsins og ráðsins (ESB) nr. 2016/679
- **Persónuverndarreglugerðin sem slík hefur lagagildi rétt eins og lög nr. 90/2018**
  - Ákvæði reglugerðarinnar ganga framar ákvæðum laganna
  - Þar sem ákvæði reglugerðarinnar eru ekki útfærð sérstaklega í persónuverndarlögum gilda ákvæði reglugerðarinnar.
    - **Ávallt nauðsynlegt að beita lögunum og reglugerðinni saman**

- 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.
- 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.

- **Ávallt er nauðsynlegt að beita lögunum og reglugerðinni saman**

PERSÓNU VERND

Nokkur mikilvæg hugtök

Persónuupplýsingar

- Hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling
- Allar upplýsingar sem hægt er að tengja við einstakling
  - Nafn, kennitala, raðnúmer snjalltækja, staðsetningargögn, IP-tölur, ljósmynd o.fl.
- Fjöldi breyta getur skipt máli
- Almennar persónuupplýsingar – viðkvæmar persónuupplýsingar
- Ópersónugreinanleg gögn falla utan persónuverndarlaga

- Í reglugerðinni eru 26 skilgreind hugtök. Sjá skilgreiningar í 4. gr. reglugerðarinnar.

PERSÓNU VERND

Nokkur mikilvæg hugtök

Persónuupplýsingar

- **Almennar persónuupplýsingar**
- **Viðkvæmar persónuupplýsingar**
  - Upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, lífsskoðun og aðild að stéttarfélagi
  - Heilsufarsupplýsingar
  - Upplýsingar um kynlíf manna og kynhneigð.
  - Erfðafræðilegar upplýsingar
  - Líkennaupplýsingar
- **Upplýsingar um refsiverða háttsemi**
  - Sérreglur um meðferð þeirra

- Í persónuverndarlögum er greint á milli almennra og viðkvæmra persónuupplýsinga. Þá gilda sérstakar reglur um vinnslu persónuupplýsinga um refsiverða háttsemi.
  - Almennar persónuupplýsingar eru t.d. nafn, kennitala, raðnúmer snjalltækja, IP-tölur o.fl.
  - Viðkvæmar persónuupplýsingar eru þær persónuupplýsingar sem skilgreindar hafa verið sem slíkar í 3. tölul. 2. gr. laga nr. 90/2018. Þær eru því tæmandi taldar í lögum og um þær gilda strangari reglur en um almennar persónuupplýsingar.
  - Hvað varðar upplýsingar um refsiverða háttsemi eru strangari kröfur gerðar við vinnslu þeirra heldur en á við um almennar persónuupplýsingar. Þær eru þó ekki settar í flokk með viðkvæmum persónuupplýsingum heldur eru sérstakar reglur settar fram um meðferð þeirra (sjá 12. gr. laga nr. 90/2018).

Nokkur mikilvæg hugtök

Vinnsla

- Sérhver aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnsla er sjálfvirk eða ekki.
- Dæmi:
  - 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.

- Vinnsluhugtakið er vítt og tekur til **hvers konar meðferðar á persónuupplýsingum**, óháð þeirri aðferð sem er notuð.

PERSÓNU VERND

Nokkur mikilvæg hugtök

Ábyrgðaraðili

- Einstaklingur, lögaðili, stjórnvald eða annar aðili sem ákveður einn eða í samvinnu við aðra tilgang og aðferðir við vinnslu persónuupplýsinga.
- 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.

- **Ábyrgðaraðili** er sá sem ákvarðar 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. Það er ávallt ábyrgðaraðili sem tekur ákvörðun um vinnslu persónuupplýsinga og hvaða heimildir standa til vinnslunnar.

PERSÓNU VERND

Nokkur mikilvæg hugtök

Vinnsluaðili

- Einstaklingur eða lögaðili, stjórnvald eða annar aðili sem vinnur með persónuupplýsingar á vegum ábyrgðaraðila.
- 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.
- Fyrirmynd að vinnslusamningi má nálgast á vefsíðu Persónuverndar.

- **Vinnsluaðili** er sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila á grundvelli samnings þar að lútandi. Samningurinn nefnist **vinnslusamningur** og þarf hann að uppfylla tiltekin skilyrði sem sett eru í persónuverndarlögum. Vinnsluaðili getur verið einstaklingur, fyrirtæki, stjórnvald eða annar aðili. Í flestum tilvikum er um að ræða utanaðkomandi þjónustuaðila. Sem dæmi um vinnsluaðila má nefna fyrirtæki sem heldur utan um upplýsingakerfi, hýsingaraðila, bókhaldsþjónustu, ráðningafyrirtæki og fleira.
- Starfsmenn innan fyrirtækis teljast almennt ekki vinnsluaðilar í skilningi laganna.

- Í eldri persónuverndarlögum var ábyrgð á vinnslu persónuupplýsinga nær alfarið lögð á ábyrgðaraðilann. Nýja persónuverndarreglugerðin breytti þessu og leggur jafnframt beinar skyldur á vinnsluaðila, samhliða þeirri ábyrgð sem er lögð á ábyrgðaraðilann.

- Persónuvernd hefur gefið út ítarlegar leiðbeiningar fyrir vinnsluaðila. Þá hefur svonefndur 29. gr. vinnuhópur útbúið leiðbeiningar með skýringum og skilgreiningum á ábyrgðaraðila og vinnsluaðila. Leiðbeiningarnar hafa ekki verið staðfestar af hálfu Evrópska persónuverndarráðsins eftir að nýja persónuverndarlöggjöfin tók gildi, en þær halda þó gildi sínu í meginatriðum og því getur verið gott að hafa þær til hliðsjónar.

PERSÓNU VERND

Nokkur mikilvæg hugtök

Samþykki

- **Óþvinguð**, **sértæk**, **upplýst** og **ótvíræð** viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um sig.

- 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 (EDPB) hefur gefið út leiðbeiningar um samþykki. Þá hefur Persónuvernd einnig gefið út samskonar leiðbeiningar um samþykki á íslensku.

Hvað breyttist ekki við gildistöku nýju löggjafarinnar?

Þarf áfram að fylgja ákveðnum kröfum:

- Hvaða heimild stendur til vinnslunnar?
  - —Lagaheimild/skylda - almannahagsmunir
  - —Samþykki
  - —Lögmætir hagsmunir
  - —Aðrar heimildir
- Er vinnslan lögmæt, gagnsæ, hófleg, áreiðanleg?
- Er tilgangur vinnslunnar skýrt tilgreindur, lögmætur og málefnalegur?
- Er öryggi upplýsinganna tryggt?
- Hvar eru upplýsingarnar vistaðar og hvar má vista þær? Innan eða utan EES?

- **Hvar eru upplýsingarnar vistaðar og hvar má vista þær**? Þetta er sérstaklega mikilvægt við notkun á tölvuskýjum og erlendum hugbúnaði á borð við Google Docs, Dropbox, Facebook og fleira. Í mörgum tilvikum eru persónuupplýsingar fluttar úr landi, stundum án þess að ábyrgðaraðilinn hafi gert sér grein fyrir því. Það að flytja upplýsingar erlendis er ekki endilega bannað – en það þarf bara að ganga úr skugga um að kröfum persónuverndarlöggjafar sér fylgt.
- Almennt má ganga út frá því að flutningur persónuupplýsinga sé heimill samkvæmt persónuverndarlögunum ef viðtökulandið er á lista yfir svokölluð örugg þriðju ríki (eða örugga staði). Til þeirra teljast m.a. ríki á Evrópska efnahagssvæðinu. Persónuvernd birtir lista yfir þessi ríki (og staði) í auglýsingu nr. 228/2010 um flutning persónuupplýsinga til annarra landa.
- Ef viðtökulandið er ekki á þessum lista þarf að huga sérstaklega að því að kröfur persónuverndarlaganna um flutning til slíkra landa séu uppfylltar. Þær kröfur lúta bæði að heimild til flutningsins og því að öryggi upplýsinganna sé tryggt.

PERSÓNU VERND

Heimildir til vinnslu persónuupplýsinga

- Öll vinnsla persónuupplýsinga verður að byggjast á heimild í persónuverndarlögum.
  - Almennar persónuupplýsingar: Heimild þarf í 9. gr. laganna
  - Viðkvæmar persónuupplýsingar: Heimild þarf í 9. gr. **og** í 11. gr. laganna
- Það fer eftir tilgangi vinnslunnar hvaða heimild getur átt við í hvert sinn.
- Engin ein heimild er rétthærri, mikilvægari eða betri en önnur.
- Ábyrgðaraðili ákveður á hvaða heimild vinnsla er byggð.

- Öll vinnsla persónuupplýsinga **verður að byggjast á einhverri heimild** í persónuverndarlögum. Það er ábyrgðaraðili sem ákveður tilgang og aðferðir við vinnslu persónuupplýsinga og þar af leiðandi hann sem tekur afstöðu til þess á hvaða heimild tiltekin vinnsla er byggð. Það fer eftir tilgangi vinnslunnar hvort hún er leyfileg og þá hvaða heimild getur átt við í hvert sinn.
- Taka þarf afstöðu til þess við hvaða heimild er stuðst áður en vinnslan hefst.
- Til þess að vinnsla persónuupplýsinga sé lögmæt þarf hún jafnframt að vera í samræmi við **meginreglur persónuverndarlaganna.** Sjá umfjöllun um meginreglurnar á glæru 17 og áfram.

Heimildir til vinnslu persónuupplýsinga

Almennar persónuupplýsingar

- **Samþykki** hins skráða fyrir vinnslu persónuupplýsinga í þágu tiltekinna markmiða
- Nauðsyn til að **efna samning** sem hinn skráði er aðili að
- Nauðsyn til að **fullnægja lagaskyldu** sem hvílir á ábyrgðaraðila
- Nauðsyn til að **vernda brýna hagsmuni hins skráða eða annars einstaklings**
- Nauðsyn vegna verks sem unnið er í þágu **almannahagsmuna** eða við **beitingu opinbers valds**
- Nauðsyn 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.
  - Stjórnvöld geta almennt ekki byggt á þessari heimild

- Öll vinnsla persónuupplýsinga verður að byggjast á einni af þeim 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
- Stjórnvöld geta almennt ekki byggt á nauðsyn vegna lögmætra hagsmuna þegar þau sinna lögbundnum verkefnum sínum.
  - Í sumum tilvikum þurfa stjórnvöld að vinna persónuupplýsingar í tengslum við verkefni sem ekki teljast til lögbundinna verkefna þeirra. Dæmi um slíkt er notkun eftirlitsmyndavéla á vinnustað. Í þeim tilvikum getur nauðsyn vegna lögmætra hagsmuna komið til greina sem heimild.
- Þegar stuðst er við nauðsyn vegna lögmætra hagsmuna sem heimild fyrir vinnslu persónuupplýsinga þarf að taka afstöðu til þess, áður en vinnslan hefst, hvort hagsmunirnir sem um ræðir vega þyngra en hagsmunir og grundvallarréttindi og frelsi hins skráða, sem krefjast verndar persónupplýsinga.

- Sjá nánari upplýsingar um heimildir til vinnslu persónuupplýsinga á bls. 7-11 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa.

Heimildir til vinnslu persónuupplýsinga

Viðkvæmar persónuupplýsingar

- **Afdráttarlaust samþykki** hins skráða fyrir vinnslu í þágu tiltekinna markmiða
- Vinnslan er nauðsynleg til þess að sá sem ákveður vinnsluna (ábyrgðaraðili) eða hinn skráði geti staðið við **skuldbindingar** sínar og **nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf** eða **löggjöf um almannatryggingar** eða **félagslega vernd**.
- Vinnslan er nauðsynleg **til að verja verulega hagsmuni** hins skráða eða annars einstaklings sem ekki er sjálfur fær um að gefa samþykki sitt.
- Vinnslan fer fram sem **liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila** sem starfar ekki í hagnaðarskyni og hefur stjórnmálaleg, heimspekileg, trúarleg eða stéttarfélagsleg markmið. Ekki má þá afhenda öðrum persónuupplýsingarnar án samþykkis hins skráða.
- Vinnslan tekur einungis til upplýsinga sem hinn skráði hefur augljóslega **sjálfur gert opinberar**.

- Til þess að heimilt sé að vinna viðkvæmar persónuupplýsingar þarf vinnslan að styðjast við einhverja af þeim sex heimildum sem þarf til að vinna megi almennar persónuupplýsingar, skv. 1. mgr. 6. gr. pvrg. og 9. gr. pvl., **og auk þess** að uppfylla að minnsta kosti eitt þeirra skilyrða, sem talin eru upp í 11. gr. pvl.
- Þegar talað er um „hinn skráða“ er átt við einstaklinginn sem upplýsingarnar varða hverju sinni.
- Sjá nánari upplýsingar um heimildir til vinnslu persónuupplýsinga á bls. 7-11 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa.

Heimildir til vinnslu persónuupplýsinga

Viðkvæmar persónuupplýsingar, frh.

- Vinnslan er nauðsynleg til að unnt sé að stofna, hafa uppi eða verja **réttarkröfur**.
- Vinnslan er nauðsynleg af ástæðum sem varða **verulega almannahagsmuni og fyrir henni er sérstök lagaheimild**.
- Vinnslan er nauðsynleg til að unnt sé að **fyrirbyggja sjúkdóma eða vegna atvinnulækninga**, til að meta vinnufærni starfsmanns, greina sjúkdóma og láta í té umönnun eða meðferð á sviði heilbrigðis- eða félagsþjónustu, enda er hún framkvæmd af starfsmanni slíkrar þjónustu sem bundinn er þagnarskyldu.
- 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.
- Vinnslan er nauðsynleg vegna **tölfræði-, sagnfræði- eða vísindarannsókna**, enda er persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga.
- 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 þína, einkum þagnarskyldu.

- Heimildirnar til vinnslu, bæði hvað varðar almennar og viðkvæmar persónuupplýsingar, eru tæmandi taldar í persónuverndarlögunum. Ef þær eiga ekki við þá er óheimilt að vinna með upplýsingarnar.

PERSÓNU VERND

Vinnsla upplýsinga um refsiverða háttsemi

- Upplýsingar um refsiverða háttsemi einstaklinga lúta sérstökum reglum samkvæmt persónuverndarlögum.
- Þær teljast ekki til viðkvæmra persónuupplýsinga í skilningi laganna.
- Þó eru gerðar strangari kröfur til meðferðar þeirra en almennra persónuupplýsinga.
- Gerðar eru 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

PERSÓNU VERND

Heimildir stjórnvalda til vinnslu persónuupplýsinga

- Öll vinnsla stjórnvalda á persónuupplýsingum verður að byggjast á heimild í persónuverndarlögum.
- Helstu heimildir stjórnvalda:
  - Lagaskylda
  - Nauðsyn vegna almannahagsmuna eða beitingar opinbers valds
  - Nauðsyn til að efna samning
- Heimildir sem stjórnvöld geta almennt ekki byggt á
  - Samþykki
  - Lögmætir hagsmunir

- Stjórnvöld þurfa, eins og aðrir, að styðja alla vinnslu sína á persónuupplýsingum við einhverja af þeim heimildum sem persónuverndarlög tilgreina.
- Stjórnvald þarf því 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. um 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. Umfjöllun um meginreglur laganna hefst á næstu glæru.
- Þær heimildir til vinnslu almennra persónuupplýsinga sem stjórnvöld byggja sína vinnslu á í flestum tilvikum 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, svo sem að vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að.
- 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.

- Persónuverndarlögin gera ráð fyrir því að ábyrgðaraðili, þ.e. hvert stjórnvald fyrir sig, gangi úr skugga um að fullnægjandi heimildir standi til vinnslu persónuupplýsinga áður en vinnslan hefst. Þetta á einnig við um aðra ábyrgðaraðila en stjórnvöld, svo sem fyrirtæki og félög sem vinna með persónuupplýsingar.

PERSÓNU VERND

Meginreglur um vinnslu persónuupplýsinga

- ***Sanngirnisreglan***: að persónuupplýsingar séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart einstaklingnum
- ***Tilgangsreglan***: að persónuupplýsingar séu unnar í skýrum, lögmætum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi.
- ***Meðalhófsreglan***: að persónuupplýsingar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilganginn með vinnslu þeirra.

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

PERSÓNU VERND

Meginreglur um vinnslu persónuupplýsinga

- ***Áreiðanleikareglan***: að persónuupplýsingar séu áreiðanlegar og uppfærðar eftir þörfum; persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar skal eyða eða þær leiðréttar án tafar.
- ***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.
- ***Öryggisreglan***: að persónuupplýsingar séu unnar með þeim hætti að viðeigandi öryggi þeirra sé tryggt.

Nánari umfjöllun um meginreglurnar er á bls. 17-18 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa.

PERSÓNU VERND

Skyldur þeirra sem vinna með persónuupplýsingar
Ábyrgðarskyldan

- Fyrirtæki, stofnanir, sveitarfélög og aðrir sem bera ábyrgð á vinnslu persónuupplýsinga (ábyrgðaraðilar) þurfa að fara að meginreglum löggjafarinnar, og þeir þurfa að geta sýnt fram á það.
  – Hvað felst í þessu?

- 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 hann þarf að 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.
- Svokölluð vinnsluskrá (eða skrá yfir vinnslustarfsemi) getur verið gagnlegt tæki í þessu samhengi, en um hana er fjallað í 30. gr. pvrg. Sjá hér glæru 23.
- 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.
  - **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.

PERSÓNU VERND

Skyldur þeirra sem vinna með persónuupplýsingar

Fræðsluskyldan

- Fræðsluskyldan er einn þáttur í ábyrgðarskyldu fyrirtækja og stjórnvalda.
- Hún felur í sér að þeir sem vinna með persónuupplýsingar veiti einstaklingum rétt til upplýsinga samkvæmt löggjöfinni.
- Talað er um upplýsingarétt einstaklinga og fræðsluskyldu fyrirtækja og stjórnvalda (ábyrgðaraðila), og er þá átt við sama hlutinn.
- Meginreglan um gagnsæi krefst þess að upplýsingar séu auðveldlega aðgengilegar og á skýru og einföldu máli.

- 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 allajafna 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 að gera einstaklingum 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.

PERSÓNU VERND

- **Hvað á að veita fræðslu um?**

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

- Þessa fræðslu á að veita þegar upplýsinganna er aflað frá hinum skráða, sbr. 13. gr. pvrg.
- Ef upplýsinganna er aflað hjá öðrum en hinum skráða þarf að veita fræðsluna innan hæfilegs tíma, þó í síðasta lagi innan mánaðar frá því að upplýsingarnar eru fengnar, sbr. 3. mgr. 14. gr. pvrg.
    - Ef nota á upplýsingarnar til samskipta við hinn skráða þarf að veita honum fræðsluna í síðasta lagi þegar fyrst er haft samband við hann.
    - Ef fyrirhugað er að fá öðrum viðtakanda persónuupplýsingarnar í hendur þá þarf að veita hinum skráða fræðsluna í síðasta lagi þegar það er gert í fyrsta sinn.
- Fræðsluna má til að mynda veita í persónuverndarstefnu fyrirtækisins eða stjórnvaldsins sem í hlut á.

PERSÓNU VERND

Skyldur þeirra sem vinna með persónuupplýsingar

Fræðsluskyldan, frh.

- **Hvernig á að veita fræðslu?**
  - Fræðslan skal vera á skýru og einföldu máli.
  - Áhersla er lögð á að fræðslan skuli vera á gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi.
  - Hún skal vera aðskilin frá öðrum atriðum, t.d. almennum samningsskilmálum.
  - Upplýsingarnar skulu veittar skriflega eða á annan hátt.
  - Upplýsingarnar skulu veittar hinum skráða að kostnaðarlausu.
- **Undantekningar frá 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 barna.
- 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.

- **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
- Þá er mikilvægt að hafa í huga að 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.

Skyldur þeirra sem vinna með persónuupplýsingar

Skrá yfir vinnslustarfsemi

- Yfirlit yfir alla vinnslu persónuupplýsinga hjá viðkomandi stofnun/fyrirtæki
  - Efni og form
- Bæði haldin hjá ábyrgðaraðila og vinnsluaðila
  - Ítarlegri skrá hjá ábyrgðaraðilum
- Sniðmát vinnsluskrár og leiðbeiningar á vefsíðu Persónuverndar
- Skráin er aðgengileg Persónuvernd
- Undantekning – ekki þarf að gera vinnsluskrá þar sem starfsmenn eru færri en 250, nema þegar vinnslan:
  - er líkleg til að leiða af sér áhættu fyrir réttindi og frelsi hins skráða
  - **er ekki tilfallandi**
  - tekur til viðkvæmra persónuupplýsinga
- ***Í framkvæmd og nær án undantekninga skulu því öll fyrirtæki og stofnanir halda skrá yfir vinnslustarfsemi sína, óháð starfsmannafjölda.***

- Persónuverndarlöggjöfin mælir fyrir um að ábyrgðaraðilar útbúi skrá yfir alla vinnslu persónuupplýsinga, þ.e. **alla vinnslustarfsemi**. Í því felst að hver ábyrgðaraðili fyrir sig þarf að útbúa sína vinnsluskrá.
- Ekki er til staðar nein formkrafa um hvernig vinnsluskráin skuli sett fram, eða hvaða aðferð skuli notuð við gerð hennar. Fyrirtæki og stofnanir ákveða því fyrirkomulag skrárinnar sjálf; hvort sem það er gert með því að hafa yfirlit í formi skriflegs skjals, Excel-skjals, eða með öðrum hætti. Hafa skal þó í huga að skylt er að fara að kröfum hvað varðar efni vinnsluskráa, og þarf því að gæta þess að þær séu uppfylltar óháð því formi sem notast er við.
- Gert er ráð fyrir að bæði ábyrgðaraðilar og vinnsluaðilar haldi vinnsluskrá. Skráin er þó almennt ekki jafn ítarleg hjá vinnsluaðilum.
- Skráin á að vera aðgengileg Persónuvernd ef hún óskar þess
- Það er gerð **undantekning** frá skyldunni til gerðar vinnsluskrár fyrir aðila með færri en 250 starfsmenn – en frá þeirri undanþágu eru gerðar undantekningar, sem eru þess valdandi að flestar stofnanir og fyrirtæki þurfa í raun að vera með vinnsluskrá, óháð starfsmannafjölda.
  - 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 skrá yfir vinnslustarfsemi sína.***
- Persónuvernd hefur, í dæmaskyni og til leiðbeiningar, útbúið form að vinnsluskrá fyrir ábyrgðaraðila annars vegar og vinnsluaðila hins vegar. Nýta má þau til að fá nauðsynlega yfirsýn. Verið getur að hver ábyrgðaraðili/vinnsluaðili þurfi að laga skrána

að aðstæðum hjá sér, enda getur starfsemi stjórnvalda og fyrirtækja verið mjög ólík að stærð og umfangi. Gott er að hafa í huga að megintilgangur skrárinnar er að fá yfirsýn yfir þá vinnslu persónuupplýsinga sem fram fer í starfseminni, en ekki endilega hverja einustu vinnsluaðgerð sem framkvæmd er.

- Leiðbeiningar og sniðmát af vinnsluskrá má finna á vefsíðu Persónuverndar.

Skyldur þeirra sem vinna með persónuupplýsingar

Skrá yfir vinnslustarfsemi, frh.

Hvaða upplýsingar eiga að koma fram í vinnsluskrá ábyrgðaraðila?

1. Heiti og samskiptaupplýsingar ábyrgðaraðila og, eftir atvikum, sameiginlegs ábyrgðaraðila, fulltrúa ábyrgðaraðila og persónuverndarfulltrúa.
2. Tilgangur vinnslunnar.
3. Lýsing á flokkum skráðra einstaklinga og flokkum persónuupplýsinga.
4. Flokkar viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, m.a. viðtakenda í þriðju löndum eða alþjóðastofnanir.
5. Ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1. mgr. 49. gr. pvrg., gögn um viðeigandi verndarráðstafanir.
6. Ef mögulegt er, fyrirhuguð tímamörk varðandi eyðingu mismunandi gagnaflokka.
7. Ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr. pvrg.

Sjá nánar umfjöllum um vinnsluskrár í leiðbeiningum Persónuverndar um skrá yfir vinnslustarfsemi.

Skyldur þeirra sem vinna með persónuupplýsingar

Skrá yfir vinnslustarfsemi, frh.

Hvaða upplýsingar skulu koma fram í vinnsluskrá vinnsluaðila?

1. Nafn og samskiptaupplýsingar vinnsluaðila, eins eða fleiri, og sérhvers ábyrgðaraðila sem vinnsluaðilinn starfar í umboði fyrir og eftir atvikum, fulltrúa ábyrgðaraðila eða vinnsluaðila og persónuverndarfulltrúa.
2. Flokkar vinnslu sem fer fram fyrir hönd hvers ábyrgðaraðila.
3. Ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1.mgr. 49. gr. pvrg., gögn um viðeigandi verndarráðstafanir.
4. Ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr. pvrg.

Sjá nánar umfjöllum um vinnsluskrár í leiðbeiningum Persónuverndar um skrá yfir vinnslustarfsemi.

PERSÓNU VERND

Öryggi persónuupplýsinga

- Þeir sem vinna með persónuupplýsingar þurfa að gera viðeigandi **tæknilegar og skipulagslegar ráðstafanir** til að tryggja öryggi þeirra
  - T.d. með dulkóðun, notkun gerviauðkenna, tryggja tiltækileika, álagsþol o.s.frv.
  - Skipulagðir ferlar nauðsynlegir
  - Innbyggð og sjálfgefin persónuvernd
- Hvaða skyldur hvíla á þeim sem geyma eða vinna með persónuupplýsingar?
  - Ekki sé hætta á að óviðkomandi aðilar komist í þær
  - Tryggja að þær skaðist ekki eða glatist
  - Tryggja að þeir, sem hafa gilda ástæðu til, komist í upplýsingarnar
  - Öryggisráðstafanir skulu taka mið af umfangi og viðkvæmni upplýsinganna

- Ein meginskylda þeirra sem vinna með persónuupplýsingar er að tryggja öryggi þeirra. Ef vinnslan er umfangsmikil eða ef unnið er með mikið af viðkvæmum persónuupplýsingum getur þurft að setja upp flókin öryggiskerfi og jafnvel fá vottun á það upplýsingaöryggiskerfi sem sett er upp.
- Aukin áhersla er lögð á að allar viðeigandi öryggisráðstafanir séu gerðar þegar unnið er með persónuupplýsingar, t.d. að dulkóða gögn, nota gerviauðkenni, tryggja tiltækileika, álagsþol o.s.frv. Hér er notkun verklagsreglna og skjala til að sýna fram á reglufylgni gríðarlega mikilvæg.
- Það er einnig mjög mikilvægt að fyrirmæli til vinnsluaðila séu skýr – hvað má og hvað má ekki.

PERSÓNU VERND

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.

- **Skylda til að tilkynna öryggisbrest**
  - Til Persónuverndar **innan 72 klst.**
  - Til einstaklingsins sjálfs ef áhættan er mikil
  - Vinnsluaðilar þurfa að tilkynna ábyrgðaraðila um öryggisbrestinn

- Ábyrgðaraðili þarf að tilkynna Persónuvernd innan 72 klst. um öryggisbrest sem hefur áhrif á einstaklinga.
- Sé Persónuvernd ekki tilkynnt um brestinn innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni.
- Ef bresturinn getur valdið einstaklingi skaða á einhvern hátt skal láta hann vita tafarlaust.
- Vinnsluaðilar þurfa einnig að tilkynna til ábyrgðaraðila um leið og þeir verða varir við að öryggisbrot hafi átt sér stað.

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

PERSÓNU VERND

Breytt eftirlit – sektarheimildir

- Þátttaka persónuverndarstofnana í samevrópsku umhverfi
  - Einn afgreiðslustaður og samræmingarkerfi
- Stórauknar sektarheimildir
  - Allt að 4% af árlegri heildarveltu eða 20 milljónum evra, hvort heldur er hærra
  - Allt að 2% af árlegri heildarveltu eða 10 milljónum evra, hvort heldur er hærra
  - Ná einnig til vinnsluaðila

- Í nýju persónuverndarlöggjöfinni er gert ráð fyrir auknu samstarfi persónuverndarstofnana á Evrópska efnahagssvæðinu með hjálp svokallaðs samræmingarkerfis. Tilgangurinn er að samræma framkvæmd löggjafarinnar á milli landa.
- Meðal nýjunga í löggjöfinni er reglan um einn afgreiðslustað, sem hefur það í för með sér að þegar ágreiningur rís um vinnslu eða meðferð persónuupplýsinga getur einstaklingurinn, sem í hlut á, haft samband við persónuverndarstofnun í heimalandi sínu, þar sem hann starfar eða þar sem meint brot átti sér stað, óháð því hvar í heiminum sá aðili er staddur sem kann að hafa brotið á viðkomandi einstaklingi. Reglan felur einnig í sér að fyrirtæki, sem starfa í fleiri en einu ríki á Evrópska efnahagssvæðinu, þurfa aðeins að leita til persónuverndaryfirvalda í því landi þar sem þau hafa höfuðstöðvar.
- Nýja löggjöfin gerir ráð fyrir því að Persónuvernd, sem og persónuverndarstofnanir annarra ríkja á Evrópska efnahagssvæðinu, geti lagt á stjórnvaldssektir vegna brota gegn löggjöfinni.
  - Í reglugerðinni er tiltekinn fjöldi atriða sem ber að hafa í huga þegar sekt er lögð á, s.s. við ákvörðun sektarfjárhæðar. Meðal annars skal líta til þess hvort um ítrekuð brot er að ræða, hvað hefur verið gert til að draga úr tjóni skráðra einstaklinga, með hvaða hætti Persónuvernd var gert kunnugt um brotið og umfangs samvinnu við Persónuvernd til þess að bæta úr broti og draga úr mögulegum skaðlegum áhrifum þess.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

- Með nýrri löggjöf er einstaklingum veitt betri vernd og aukinn ákvörðunarréttur yfir persónuupplýsingunum sínum.
- Er verið að vinna persónuupplýsingar um einstakling? Þá á hann rétt á að vita:
  - **Hver** vinnur þær
  - **Hvenær** þær eru unnar
  - Í **hvaða tilgangi**

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Upplýsingaréttur (fræðsluskyldan)

- **Einstaklingar eiga rétt á að sá aðili, sem vinnur með persónuupplýsingar um þá, veiti m.a. fræðslu um eftirfarandi:**
  - 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

- Sjá hér einnig glærur 20-22, 17. gr. pvl. og 13.-14. gr. pvrg.
- Fræðsluskylda er einn þáttur í ábyrgðarskyldu fyrirtækja, stjórnvalda og annarra sem vinna með persónuupplýsingar samkvæmt persónuverndarlögum og felur í sér að framangreindir aðilar veiti einstaklingum tilteknar upplýsingar um vinnsluna. Þannig er alla jafna talað um upplýsingarétt einstaklinga og fræðsluskyldu fyrirtækja og stjórnvalda og er þá átt við sama hlutinn.
- Einstaklingar eiga rétt á að sá aðili, sem vinnur með persónuupplýsingar um þá, veiti m.a. fræðslu um þau atriði, sem talin eru upp á glærunni.
- **Athugið að upptalningin á glærunni er ekki tæmandi.**
- 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.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Aðgangsréttur

- 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 einstaklingsins,
  - afrit af þeim persónuupplýsingum um einstaklinginn sem unnið er með, og
  - aðrar upplýsingar um vinnsluna.

- Sjá einnig 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.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Aðgangsréttur

- **Hvenær ber að svara aðgangsbeiðni?**
  - 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.
  - Ef ekki er orðið við aðgangsbeiðni skal, í síðasta lagi innan mánaðar frá viðtöku beiðninnar, tilkynna einstaklingnum um ástæðurnar fyrir því og um möguleikann á að leggja fram kvörtun hjá Persónuvernd.
- **Á hvaða formi ber að afhenda gögn?**
  - Ef aðgangsbeiðnin er sett fram rafrænt skulu upplýsingarnar látnar í té með rafrænu sniði sem almennt er notað, nema einstaklingurinn fari fram á annað, t.d. að fá gögn afhent á pappírsformi eða að upplýsingar séu veittar munnlega.

- 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.

Helstu réttindi og úrræði hins skráða

Réttur til takmörkunar á vinnslu

- **Einstaklingur getur krafist þess að ábyrgðaraðili takmarki vinnslu persónuupplýsinga um hann þegar eitt af eftirfarandi á við:**
  - hinn skráði vefengir að persónuupplýsingar séu réttar, þangað til ábyrgðaraðilinn hefur fengið tækifæri til að staðfesta að þær séu réttar.
  - vinnslan er ólögmæt og hinn skráði andmælir því að persónuupplýsingunum sé eytt og fer fram á takmarkaða notkun þeirra í staðinn.
  - ábyrgðaraðilinn þarf ekki lengur á persónuupplýsingunum að halda fyrir vinnsluna en skráði einstaklingurinn þarfnast þeirra til þess að stofna, hafa uppi eða verja réttarkröfur.
  - 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.

- Sjá hér 20. gr. pvl. og 18. gr. pvrg.
- 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.
- Ábyrgðaraðili skal tilkynna skráðum einstaklingi, sem fengið hefur fram takmörkun á vinnslu, um það áður en takmörkuninni á vinnslunni er aflétt.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Réttur til leiðréttingar

- 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.
- **Stjórnvöldum er almennt ekki heimilt að eyða gögnum að hluta eða í heild.**
  - **Þeim mun mikilvægara er að passa upphaflega skráningu, hvað þarf nauðsynlega að skrá og hvað þarf ekki að skrá!**

- Sjá hér 20. gr. pvl. og 16. og 19. 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. Þeim mun mikilvægara er því að þessir aðilar passi upphaflega skráningu, hvað þarf nauðsynlega að skrá og hvað þarf ekki að skrá.
- 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.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Réttur til eyðingar – rétturinn til að gleymast

- **Skráðir einstaklingar eiga í vissum aðstæðum rétt á að ábyrgðaraðilar eyði persónuupplýsingum um þá**
- **Ef einhver eftirtalinna ástæðna á við er ábyrgðaraðila skylt að eyða persónuupplýsingum án ótilhlýðilegar 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

- 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 einstakling verði eytt. Ef einhver þeirra ástæðna, sem taldar eru á glærunni, á við er ábyrgðaraðila skylt að eyða persónuupplýsingum án ótilhlýðlegar tafar.

Helstu réttindi og úrræði hins skráða

Réttur til eyðingar – rétturinn til að gleymast

- 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.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Réttur til eyðingar – rétturinn til að gleymast

- **Stjórnvöldum er almennt ekki heimilt að eyða gögnum – hvorki að hluta né í heild**
  - 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 laga um opinber skjalasöfn
  - **Þeim mun mikilvægara er því að passa upphaflega skráningu, hvað þarf nauðsynlega að skrá og hvað þarf ekki að skrá**

- 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. (Sjá 19. gr. pvrg. Um tilkynningarskyldu varðandi leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu)

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

Flutningsréttur

- Flutningsréttur á við þegar einstaklingur hefur sjálfur afhent ábyrgðaraðila persónuupplýsingar um sig
- Einstaklingurinn á þá rétt á að fá persónuupplýsingar sem varða hann sjálfan á skipulegu, algengu, tölvulesanlegu sniði
- Ábyrgðaraðila ber að verða við ósk einstaklingsins um að fá persónuupplýsingarnar í hendur. Einstaklingurinn á að geta sent upplýsingarnar öðrum ábyrgðaraðila án þess að fyrri ábyrgðaraðilinn hindri það.
  - Hann á einnig rétt á að láta senda upplýsingarnar beint frá einum ábyrgðaraðila til annars, ef það er tæknilega framkvæmanlegt
- **Skilyrði þess að rétturinn eigi við**:
  - Vinnsla upplýsinganna byggist á samþykki hins skráða einstaklings eða samningi.
  - Vinnslan sé sjálfvirk.
- Flutningsrétturinn er ekki til staðar þegar vinnslan styðst við aðrar heimildir en samþykki eða samning.

- 20. gr. pvl. og 20. gr. pvrg.
- 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.
- *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 einstakling sem skrást við notkun stafræns búnaðar sem hann 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.

Helstu réttindi og úrræði hins skráða

Andmælaréttur

- Einstaklingum er almennt heimilt að andmæla vinnslu um sig sjálfa þegar vinnslan byggist á:
  - **nauðsyn vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds,** eða
  - **nauðsyn vegna lögmætra hagsmuna.**
- Má þá ekki vinna upplýsingarnar frekar nema sýnt sé fram á mikilvægar lögmætar ástæður fyrir vinnslunni, sem ganga framar hagsmunum, réttindum og frelsi hins skráða
  - Einnig undanþága ef vinnslan er nauðsynleg til að stofna, hafa uppi eða verja réttarkröfur

- 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 hlutverk ábyrgðaraðila að sýna fram á að mikilvægir lögmætir hagsmunir gangi framar hagsmunum eða grundvallarréttindum og frelsi hins skráða í tengslum við andmælarétt hins síðarnefnda.

PERSÓNU VERND

Auknar kröfur til samþykkis

- Samþykki telst einungis hafa verið veitt ef hinn skráði hefur raunverulegt val um hvort hann samþykkir eða hafnar vinnslu persónuupplýsinga um sig
- Samþykki felur í sér ***óþvingaða***, ***sértæka***, ***upplýsta*** og ***ótvíræða*** viljayfirlýsingu hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan
- Það er hlutverk ábyrgðaraðila að meta hvort skilyrðum samþykkis hefur verið fullnægt

- Persónuvernd hefur gefið út ítarlegar leiðbeiningar um samþykki. Evrópska persónuverndarráðið (EDBP) hefur jafnframt gefið út leiðbeiningar um samþykki sem nálgast má á vefsíðu Persónuverndar.
- Sjá nánar um auknar kröfur til samþykkis í leiðbeiningum Persónuverndar og á bls. 28-31 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa.

PERSÓNU VERND

Auknar kröfur til samþykkis

- **Óþvingað**
  - Samþykkið þarf að vera veitt af fúsum og frjálsum vilja.
- **Sértækt**
  - Hinn skráði verður að vera upplýstur um hvaða persónuupplýsingar á að vinna með og í hvaða tilgangi. Hann á að hafa val um hvaða tilgang hann samþykkir og hvaða tilgang hann samþykkir ekki.
- **Upplýst**
  - Upplýsingagjöf af hálfu ábyrgðaraðila um vinnsluna, 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.
- **Ótvírætt**
  - Samþykki verður einungis veitt með skýrri staðfestingu sem felur ávallt í sér einhvers konar aðgerð eða yfirlýsingu af hálfu hins skráða.

Í þessu felst meðal annars að samþykki er ekki hægt að veita með aðgerðaleysi, heldur þarf það að vera veitt með aðgerð eða yfirlýsingu. Það er því ekki nóg að tilkynna að vinnsla fari fram ef því verði ekki sérstaklega andmælt, svo dæmi sé tekið.

PERSÓNU VERND

Helstu réttindi og úrræði hins skráða

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
- Mikilvægt er að hlúa vel að persónuvernd barna
  - fylgja ávallt meginreglum persónuverndarlaganna, og skal sanngirni til dæmis höfð að leiðarljósi við alla vinnslu.
- Sérstaklega áréttað í formálsorðum reglugerðarinnar
- Foreldrar og forráðamenn sjá yfirleitt um að samþykkja vinnslu persónuupplýsinga um börn sín.
  - Þjónusta í upplýsingasamfélaginu: börn yfir 13 ára þurfa ekki samþykki foreldra.

- 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 við þessar aðstæður. 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.

Persónuverndarfulltrúar

Almennt

- Persónuverndarfulltrúi er sá aðili sem ber sérstaka ábyrgð á málefnum fyrirtækisins eða stofnunarinnar sem tengjast persónuvernd.
- Í persónuverndarreglugerðinni er litið á persónuverndarfulltrúann sem **lykilstarfsmann** og mælir hún fyrir um skilyrði fyrir ráðningu hans, stöðu og verkefni.

Persónuverndarfulltrúar

Almennt

- 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.
- Með vitundarvakningu og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi hefur persónuverndarfulltrúi eftirlit með því að gætt sé að vernd persónuupplýsinga.

- 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 35.-36. gr. pvl. og 37.-39. gr. pvrg. er fjallað um persónuverndarfulltrúa.
- Persónuvernd hefur gefið út ítarlegt fræðslurit fyrir persónuverndarfulltrúa sem nálgast má á vefsíðu stofnunarinnar.

Persónuverndarfulltrúar

Tilnefning og staða

- 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.
- Persónuverndarfulltrúar þurfa ekki að hafa sérstaka vottun sem persónuverndarfulltrúar til að geta gegnt umræddu starfi

- 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.

Persónuverndarfulltrúar

Tilnefning og staða

- **Hvenær er skylt að tilnefna persónuverndarfulltrúa?**
  - Þegar vinnsla persónuupplýsinga fer fram hjá stjórnvaldi. Þetta á m.a. við um opinberar stofnanir og sveitarfélög.
  - Þegar meginstarfsemi ábyrgðaraðila eða vinnsluaðila lýtur að vinnsluaðgerðum, sem fela í sér **umfangsmikið**, **reglubundið** og **kerfisbundið eftirlit** með einstaklingum.
  - Þegar 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 þótt þau teljist ekki til stjórnvalda.
- 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.

Hlutverk persónuverndarfulltrúa

Fræðsla og ráðgjöf

- Persónuverndarfulltrúi á að upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt persónuverndarlöggjöfinni og veita þeim ráðgjöf þar að lútandi.
  - Hann tryggir þannig að starfsfólk sem hefur aðgang að persónuupplýsingum fái nauðsynlega fræðslu og þjálfun á því sviði sem við á.
- Persónuverndarfulltrúi stuðlar að vitundarvakningu, sinnir fræðslu og framkvæmir reglulegar úttektir.

- 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.

Hlutverk persónuverndarfulltrúa

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.

Hlutverk persónuverndarfulltrúa

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).
- Ábyrgðaraðili og vinnsluaðili **skulu leita ráðgjafar hjá persónuverndarfulltrúanum**, 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.

- 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.
- Sjá nánar um MÁP á bls. 35-38 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa, m.a. um það hvenær og hvernig á að framkvæma MÁP.

Hlutverk persónuverndarfulltrúa

Mat á áhrifum á persónuvernd (MÁP)

- **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.

Hlutverk persónuverndarfulltrúa

Vinna með eftirlitsvaldinu

- 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.

Hlutverk persónuverndarfulltrúa

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

Sbr. 36. gr. pvrg.
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.

Persónuverndarfulltrúar

Önnur verkefni

- Verkefni persónuverndarfulltrúa eru ekki tæmandi talin í persónuverndarlöggjöfinni þar sem hún mælir fyrir um lágmarksverkefni hans.
- Löggjöfin kemur ekki í veg fyrir að persónuverndarfulltrúi sinni öðrum verkefnum
  - Engu að síður þarf að tryggja að önnur verkefni eða skyldur sem falin eru persónuverndarfulltrúanum **leiði ekki af sér hagsmunaárekstra** og að persónuverndarfulltrúinn **taki ekki ákvarðanir um vinnslu persónuupplýsinga**.

Persónuverndarfulltrúar

Önnur verkefni

- Nokkur dæmi um verkefni sem persónuverndarfulltrúi gæti haft undir höndum (hér er hvorki um tæmandi talningu að ræða né lögbundin verkefni persónuverndarfulltrúa):
  - **Skrá yfir vinnslustarfsemi (vinnsluskrá)**
  - **Tilkynning um öryggisbrest**
  - **Stefna um persónuvernd (e. privacy policy)**
  - **Verkferlar og áætlanir**
  - **Samskipti við hinn skráða**
  - **Úrbætur og úttektir**

Sjá nánar dæmi um önnur verkefni persónuverndarfulltrúa á bls. 39-41 í fræðsluriti Persónuverndar fyrir persónuverndarfulltrúa.

PERSÓNU VERND

Frekari upplýsingar

- Ný og endurbætt vefsíða Persónuverndar
  - Spurt og svarað
  - Leiðbeiningar Persónuverndar
    - Leiðbeiningar og fræðsluefni fyrir persónuverndarfulltrúa
    - Leiðbeiningar um öryggisbresti
    - Leiðbeiningar fyrir vinnsluaðila
    - Sniðmát af vinnsluskrá
    - O.fl.
  - Bæklingar
  - Annað fræðsluefni

- Að mörgu er að huga varðandi nýja persónuverndarlöggjöf en mikilvægt að hafa í huga að sums staðar er ekki um svo stórar breytingar að ræða í raun og veru. Fyrst og fremst þarf að svara því hvort um persónuupplýsingar er að ræða og sé því svarað játandi þarf að skoða hvort, og þá hvaða heimild standi til vinnslunnar, hvort hún samrýmist meginreglum laganna og svo framvegis.

- Að lokum er bent á nýja vefsíðu Persónuverndar en þar má finna mikinn fróðleik og almennar upplýsingar um fjölda persónuverndartengdra málefna.

PERSÓNU VERND

Gagnlegir tenglar - ítarefni

- **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
- **Vefsíða Evrópuráðsins um persónuvernd:**
- https://www.coe.int/en/web/data-protection/home
- **Handbók um evrópska persónuverndarlöggjöf (Handbook on European data protection law)**
- https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en/format-PDF/source-76364708
- **Handbók ENISA um öryggi persónuupplýsinga (Handbook on Security of Personal Data Processing)**
- https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

PERSÓNU VERND

Gagnlegir tenglar - ítarefni

- **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/

PERSÓNU VERND

Þetta kynningarefni er styrkt af Evrópusambandinu - The European Union's Rights, Equality and Citizenship Programme (2014-2020).