148. löggjafarþing 2017–2018.
Þingskjal x — x. mál.
Stjórnarfrumvarp.

Frumvarp til laga

um persónuvernd og vinnslu persónuupplýsinga

Frá dómsmálaráðherra.

I. kafli. Markmið, skilgreiningar og gildissvið.

1.gr.
Markmið.

Með lögum þessum eru lögfest ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga, eins og hún var tekin upp í samninginn um Evrópska efnahagssvæðið, og sett frekari ákvæði til fyllingar og viðbótar reglugerðinni.

Markmið laganna er að stuðla að því að með persónuupplýsingar sé farið í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og að tryggja áreiðanleika og gæði slíkra upplýsinga og frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins. Sérstök stofnun, Persónuvernd, annast eftirlit með framkvæmd reglugerðarinnar, laga þessara og reglna sem settar verða samkvæmt þeim, sbr. nánar ákvæði VII. kafla laganna. Evrópsk eftirlitsstofnun samkvæmt VII. kafla reglugerðarinnar er Evrópska persónuverndarráðið.

2. gr.
Lögfesting.

Ákvæði reglugerðar 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 eins og hún var tekin upp í samninginn um Evrópska efnahagssvæðið skulu hafa lagagildi hér á landi með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar nr. xx frá 2018 og birtri í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. xx frá 2018.

Reglugerðin er birt sem fylgiskjal með lögum þessum.

3. gr.
Skilgreiningar.

Merking orða og hugtaka í lögum þessum er sem hér segir:

1. *Reglugerðin:* 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.

2. *Persónuupplýsingar*: Sérhverjar 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.

3. *Viðkvæmar persónuupplýsingar:*

a. Upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, heimspekilega sannfæringu 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 sem gefa upplýsingar um heilsufar hans 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.

f. 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, s.s. andlitsmyndir eða gögn um fingraför, enda sé unnið með upplýsingarnar í því skyni að persónugreina einstakling með einkvæmum hætti.

4. *Vinnsla:* Aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, s.s. 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.

5. *Skrá:* sérhvert skipulegt safn persónuupplýsinga sem er aðgengilegt samkvæmt tilteknum viðmiðunum, hvort heldur það er miðlægt, dreift eða skipt upp eftir notkun eða staðsetningu.

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

7. *Vinnsluaðili:* Einstaklingur eða lögaðili, stjórnvald eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila.

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

9. *Rafræn vöktun:* Vöktun sem er viðvarandi eða endurtekin reglulega og felur í sér eftirlit með einstaklingum með fjarstýrðum eða sjálfvirkum búnaði, og fer fram á almannafæri eða á svæði sem takmarkaður hópur fólks fer um að jafnaði. Hugtakið tekur til:

a. vöktunar sem leiðir, á að leiða eða getur leitt til vinnslu persónuupplýsinga, og
b. sjónvarpsvöktunar sem fer fram með notkun sjónvarpsmyndavéla, vefmyndavéla eða annars samsvarandi búnaðar, án þess að fram fari söfnun myndefnis eða aðrar aðgerðir sem jafngilda vinnslu persónuupplýsinga.

10. *Gerð persónusniðs:* hvers kyns sjálfvirk vinnsla persónuupplýsinga sem felst í því að nota persónuupplýsingar til að meta ákveðna þætti er varða hagi einstaklings, einkum að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsu, smekk, áhugamál, áreiðanleika, hegðun, staðsetningu eða hreyfanleika.

11. *Öryggisbrot við vinnslu persónuupplýsinga:* brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi.

4. gr.

Efnislegt gildissvið.

Lögin og reglugerðin gilda um vinnslu persónuupplýsinga sem er sjálfvirk að hluta eða í heild og um vinnslu með öðrum aðferðum en sjálfvirkum á persónuupplýsingum sem eru eða eiga að verða hluti af skrá.

Lögin og reglugerðin gilda ekki um meðferð einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða fjölskyldu hans eða eru einvörðungu ætlaðar til persónulegra nota.

Lögin og reglugerðin gilda um vinnslu persónuupplýsinga látinna einstaklinga í 10 ár frá andláti þeirra en lengur þegar um ræðir persónuupplýsingar sem sanngjarnt og eðlilegt má telja að leynt fari.

Lögin og reglugerðin gilda ekki um vinnslu persónuupplýsinga sem fer fram þegar dómstólar fara með dómsvald sitt.

Lögin og reglugerðin gilda ekki um vinnslu persónuupplýsinga sem fram fer í tengslum við lögbundin verkefni Alþingis.

Lögin og reglugerðin gilda ekki um vinnslu persónuupplýsinga af hálfu ríkisins í tengslum við það að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi.

Ákvæði laga þessara og reglugerðarinnar gilda án tillits til þess hvort málefni fellur undir gildissvið EES-samningsins, að undanskildum VII. kafla reglugerðarinnar.

5. gr.

Tengsl við önnur lög

Sérákvæði annarra laga um vinnslu persónuupplýsinga sem sett eru innan ramma reglugerðarinnar ganga framar ákvæðum laga þessara.

Lög þessi takmarka ekki þann rétt til aðgangs að gögnum sem mælt er fyrir um í upplýsingalögum og stjórnsýslulögum.

Ákvæði reglugerðarinnar ganga framar ákvæðum laga þessara.

6. gr.

Tengsl við tjáningarfrelsi.

Að því marki sem það er nauðsynlegt til að samræma sjónarmið um rétt til einkalífs annars vegar og tjáningarfrelsis hins vegar má víkja frá ákvæðum laganna og reglugerðarinnar í þágu fjölmiðlunar, lista eða bókmennta. Þegar persónuupplýsingar eru einvörðungu unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi gilda aðeins ákvæði a- og d-liðar, 1. mgr. 5. gr., 24., 26., 28., 29., 40. og 42. gr. og VI. og VIII. kafla reglugerðarinnar og VII. kafli laga þessara.

7. gr.

Landfræðilegt gildissvið.

Lögin gilda um vinnslu persónuupplýsinga í tengslum við starfsemi ábyrgðaraðila eða vinnsluaðila hér á landi, á Evrópska efnahagssvæðinu eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu óháð því hvort vinnslan sjálf fer fram þar.

Lögin gilda um vinnslu ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu hér á landi eða Evrópska efnahagssvæðinu eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu, á persónuupplýsingum um skráða einstaklinga innan Evrópska efnahagssvæðisins þegar vinnslustarfsemin tengist því að:

1. bjóða þessum skráðu einstaklingum á Evrópska efnahagssvæðinu vöru eða þjónustu, án tillits til þess hvort það er gert gegn greiðslu, eða
2. hafa eftirlit með hegðun þeirra að svo miklu leyti sem hegðun þeirra á sér stað innan þess svæðis.

Þegar svo hagar til sem greinir í 2. mgr. skal ábyrgðaraðili eða vinnsluaðili tilnefna fulltrúa sinn innan Evrópska efnahagssvæðisins eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu, með þeim undantekningum sem kveðið er á um í 27. gr. reglugerðarinnar. Gilda þá ákvæði laganna varðandi ábyrgðaraðila eða vinnsluaðila um þann fulltrúa samkvæmt nánari fyrirmælum 27. gr. reglugerðarinnar.

II. kafli. Almennar reglur um vinnslu.

8. gr.

Meginreglur um vinnslu persónuupplýsinga.

Við vinnslu persónuupplýsinga skal allra eftirfarandi þátta gætt eftir því sem nánar er lýst í 5. gr. reglugerðarinnar:

1. að þær séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart hinum skráða;
2. að þær séu fengnar í skýrt tilgreindum, lögmætum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Frekari vinnsla í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi telst ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt;
3. að þær séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar;
4. að þær séu áreiðanlegar og uppfærðar eftir þörfum; persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal eyða eða leiðrétta án tafar;
5. að þær séu varðveittar í því formi að ekki sé unnt að bera kennsl á skráða einstaklinga lengur en þörf krefur miðað við tilgang vinnslu; heimilt er að geyma persónuupplýsingar lengur að því tilskildu að vinnsla þeirra þjóni einungis skjalavistun í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi og að viðeigandi öryggis sé gætt.
6. að þær séu unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt,

Ábyrgðaraðili ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt ákvæði 1. mgr. og skal geta sýnt fram á það.

9. gr.

Almennar reglur um heimildir fyrir vinnslu persónuupplýsinga.

Vinnsla persónuupplýsinga er því aðeins heimil að einhver eftirfarandi þátta sé fyrir hendi eftir því sem nánar er lýst í 6. gr. reglugerðarinnar:

1. hinn skráði hafi gefið samþykki sitt fyrir vinnslu á persónuupplýsingum sínum í þágu eins eða fleiri tiltekinna markmiða;
2. vinnslan sé nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður;
3. vinnslan sé nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila;
4. vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings;
5. vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með;

6. vinnslan sé nauðsynleg vegna lögmætra hagsmuna sem ábyrgðaraðili, eða þriðji maður gætir nema hagsmunir eða grundvallarréttindi og frelsi hins skráða sem krefjast verndar persónuupplýsinga vegi þyngra, einkum þegar hinn skráði er barn.

10. gr.

Skilyrði fyrir samþykki.

Þegar vinnsla er byggð á samþykki skal ábyrgðaraðilinn geta sýnt fram á að skráður einstaklingur hafi samþykkt vinnslu persónuupplýsinga sinna samkvæmt nánari skilyrðum 7. og 8. gr. reglugerðarinnar.

Ef hinn skráði gefur samþykki sitt með skriflegri yfirlýsingu, sem einnig varðar önnur málefni, skal beiðnin um samþykki sett fram á þann hátt að hún sé auðgreinanleg frá hinum málefnunum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli.

Skráður einstaklingur á rétt á að draga samþykki sitt til baka hvenær sem er. Afturköllun samþykkis skal ekki hafa áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni.

Þegar metið er hvort samþykki sé gefið af fúsum og frjálsum vilja skal taka ítrasta tillit til þess hvort það sé skilyrði fyrir framkvæmd samnings, að samþykki sé gefið fyrir vinnslu persónuupplýsinga sem ekki er nauðsynleg vegna samningsins.

Þegar barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti og vinnsla persónuupplýsinga byggist á samþykki þess telst vinnslan því aðeins lögmæt ef barnið hefur náð 13 ára aldri. Sé barnið undir 13 ára aldri telst vinnslan aðeins lögmæt að því marki sem forsjáraðili þess heimilar samþykki. Ábyrgðaraðili skal gera það sem sanngjarnt má telja til að sannreyna í slíkum tilvikum að samþykkið sé gefið eða heimilað af hálfu forsjáraðila barnsins, að teknu tilliti til þeirrar tækni sem fyrir hendi er.

11. gr.

Sérstök skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga

Vinnsla viðkvæmra persónuupplýsinga skv. 3. tölul. 3. gr. laga þessara er óheimil nema uppfyllt sé eitthvert af skilyrðum 1. mgr. 10. gr. laga þessara og enn fremur eitthvert af eftirfarandi skilyrðum samkvæmt nánari fyrirmælum 9. gr. reglugerðarinnar:

1. hinn skráði hafi veitt afdráttarlaust samþykki sitt fyrir vinnslunni í þágu eins eða fleiri tiltekinna markmiða;
2. vinnslan sé nauðsynleg til þess að ábyrgðaraðili eða hinn skráði geti staðið við skuldbindingar sínar og nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf og löggjöf um almannatryggingar og félagslega vernd;
3. vinnslan sé nauðsynleg til að verja verulega hagsmuni hins skráða eða annars einstaklings sem ekki er sjálfur fær um að gefa samþykki sitt;
4. vinnslan fari fram sem liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila sem starfar ekki í hagnaðarskyni og hefur stjórnmálaleg, heimspekileg, trúarleg eða stéttarfélagsleg markmið, enda nái vinnslan einungis til meðlima eða fyrrum meðlima viðkomandi aðila eða einstaklinga sem eru í reglulegu sambandi við hann í tengslum við starfsemi hans, persónuupplýsingar séu ekki fengnar þriðja aðila í hendur án samþykkis hinna skráðu og gerðar séu viðeigandi verndarráðstafanir;
5. vinnslan taki einungis til upplýsinga sem hinn skráði hefur augljóslega sjálfur gert opinberar;
6. vinnslan sé nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur;
7. vinnslan sé nauðsynleg, af ástæðum sem varða verulega almannahagsmuni og fyrir henni sé sérstök lagaheimild;
8. vinnslan sé 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 sé hún framkvæmd af starfsmanni slíkrar þjónustu sem bundinn er þagnarskyldu;
9. vinnslan sé nauðsynleg af ástæðum er 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;
10. vinnslan sé nauðsynleg vegna tölfræði-, sagnfræði- eða vísindarannsókna, enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á í samræmi við lög þessi;
11. vinnslan sé nauðsynleg vegna skjalavistunar í þágu almannahagsmuna og fari fram á grundvelli laga sem kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða, einkum þagnarskyldu.

Persónuvernd leysir úr ágreiningi um hvort persónuupplýsingar skuli teljast viðkvæmar eða ekki.

12. gr.

Vinnsla upplýsinga um refsiverða háttsemi.

Stjórnvöld mega ekki vinna með upplýsingar um refsiverða háttsemi nema það sé nauðsynlegt í þágu lögbundinna verkefna þeirra.

Upplýsingum skv. 1. mgr. má ekki miðla nema því aðeins að:

1. hinn skráði hafi gefið ótvírætt samþykki sitt fyrir miðluninni;
2. miðlunin sé nauðsynleg í þágu lögmætra hagsmuna hins opinbera eða einkaaðila sem auðsjáanlega vega þyngra en þeir hagsmunir sem eru af leynd um upplýsingarnar, þ. á m. hagsmunir hins skráða;
3. miðlunin sé nauðsynleg í þágu lögbundinna verkefna viðkomandi stjórnvalds eða til að unnt sé að taka stjórnvaldsákvörðun; eða
4. miðlunin sé 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.

Upplýsingum skv. 3. mgr. má ekki miðla nema hinn skráði veiti til þess ótvírætt samþykki sitt. Þó má miðla upplýsingum án samþykkis sé það nauðsynlegt í þágu lögmætra hagsmuna hins opinbera eða einkaaðila sem auðsýnilega vega þyngra en þeir hagsmunir sem eru af leynd um upplýsingarnar, þ. á m. hagsmunir hins skráða.

Vinnsla samkvæmt þessari grein skal ávallt eiga stoð í einhverri af heimildum 1. mgr. 9. gr. laga þessara, sbr. 1. mgr. 6. gr. reglugerðarinnar.

13. gr.

Notkun kennitölu.

Notkun kennitölu er heimil eigi hún sér málefnalegan tilgang og sé nauðsynleg til að tryggja örugga persónugreiningu. Persónuvernd getur bannað eða fyrirskipað notkun kennitölu.

14. gr.

Rafræn vöktun.

Rafræn vöktun er ávallt háð því skilyrði að hún fari fram í málefnalegum tilgangi. Rafræn vöktun svæðis þar sem takmarkaður hópur fólks fer um að jafnaði er jafnframt háð því skilyrði að hennar sé sérstök þörf vegna eðlis þeirrar starfsemi sem þar fer fram.

Vinnsla persónuupplýsinga sem á sér stað í tengslum við rafræna vöktun skal uppfylla ákvæði laga þessara.

Heimilt er í tengslum við framkvæmd rafrænnar vöktunar, að safna efni sem verður til við vöktunina, svo sem hljóð- og myndefni, með viðkvæmum persónuupplýsingum ef eftirfarandi skilyrði eru uppfyllt:

1. vöktunin sé nauðsynleg og fari fram í öryggis- eða eignavörsluskyni;
2. það efni sem til verður við vöktunina verði ekki afhent öðrum eða unnið frekar nema með samþykki þess sem upptaka er af eða á grundvelli heimilda í reglum skv. 5. mgr.; heimilt er þó að afhenda lögreglu efni með upplýsingum um slys eða refsiverðan verknað en þá skal þess gætt að eyða öllum öðrum eintökum af efninu;
3. því efni sem safnast við vöktunina verði eytt þegar ekki er lengur málefnaleg ástæða til að varðveita það.

Þegar rafræn vöktun fer fram á vinnustað eða á almannafæri skal með merki eða á annan áberandi hátt gera glögglega viðvart um þá vöktun og hver sé ábyrgðaraðili.

Persónuvernd setur reglur og gefur fyrirmæli um rafræna vöktun og vinnslu efnis sem verður til við vöktunina, svo sem hljóð- og myndefnis, þar á meðal um öryggi þess, rétt hins skráða til að horfa eða hlusta á upptökur, varðveislutíma og eyðingu, varðveisluaðferð, afhendingu efnisins og notkun þess.

15. gr.

Vinnsla upplýsinga um fjárhagsmálefni og lánstraust.

Starfræksla fjárhagsupplýsingastofa og vinnsla upplýsinga sem varða fjárhagsmálefni og lánstraust einstaklinga og lögaðila, þ.m.t. vanskilaskráning og gerð lánshæfismats, í því skyni að miðla þeim til annarra, skal bundin leyfi Persónuverndar. Þegar um lögaðila er að ræða gilda eingöngu eftirfarandi ákvæði laganna: 17. gr. um upplýsingarétt hins skráða, 20. gr. um rétt til leiðréttingar og eyðingar gagna, 25. gr. um meðferð vinnsluaðila á upplýsingum, 31. gr. um leyfisskylda vinnslu, 32. gr. um forsendur leyfisveitingar, 33. gr. um

skilmála, 5. og. 6. tölul 1. mgr. 41. gr. um aðgang Persónuverndar að upplýsingum o.fl., 6. tölul. 42. gr. um stöðvun vinnslu o.fl., 45. gr. um dagsektir, 48. gr.um refsingar og 51. gr. um bætur.

Ráðherra skal setja reglugerð þar sem nánar er mælt fyrir um skilyrði fyrir vinnslu samkvæmt 1. mgr.

16. gr.

Miðlun persónuupplýsinga úr landi eða til alþjóðastofnana

Ákvarðanir framkvæmdastjórnarinnar um miðlun upplýsinga til þriðja lands eða alþjóðastofnunar samkvæmt 45. gr. reglugerðarinnar gilda hér á landi í samræmi við ákvörðun sameiginlegu EES nefndarinnar frá xx 2018 og skal Persónuvernd birta auglýsingu þar um í Stjórnartíðindum.

III. kafli. Réttindi hins skráða og takmarkanir á þeim.

17. gr.

Meginreglur um gagnsæi upplýsinga, rétt hins skráða til upplýsinga og aðgangs og undantekningar frá honum

Ábyrgðaraðili skal gera viðeigandi ráðstafanir til að tryggja gagnsæi upplýsinga og tilkynningar til skráðs einstaklings samkvæmt fyrirmælum 12. gr. reglugerðarinnar svo að hann geti neytt upplýsingaréttar síns og réttar til aðgangs.

Hinn skráði á rétt til upplýsinga um vinnslu, hvort sem persónuupplýsinga er aflað hjá honum sjálfum eða ekki, svo og rétt til aðgangs að persónuupplýsingum um sig samkvæmt fyrirmælum 13.-15. gr. reglugerðarinnar með þeim undantekningum sem greinir í 3. mgr.

Ákvæði 1.- 3. mgr. 13. gr. 1.-4. mgr. 14. gr. og 15. gr. reglugerðarinnar um réttindi hins skráða gilda ekki ef brýnir hagsmunir einstaklinga tengdir upplýsingunum, þar á meðal hins skráða sjálfs, vega þyngra.

Heimilt að víkja frá ákvæðum 13.-15. gr. reglugerðarinnar á grundvelli einhvers eftirtalinna atriða:

1. þjóðaröryggi;
2. landvarna;
3. almannaöryggis;
4. þess að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaöryggi;
5. annarra mikilvægra markmiða sem þjóna almannahagsmunum, einkum efnahagslegum eða fjárhagslegum þ.m.t. vegna gjaldeyrismála, fjárlaga og skattamála, lýðheilsu og almannatrygginga;
6. verndar skráðs einstaklings, brýnna almannahagsmuna eða grundvallarréttinda annarra;
7. þess að einkaréttarlegum kröfum sé fullnægt;
8. lagaákvæða um þagnarskyldu.

Upplýsingar í málum sem eru til meðferðar hjá stjórnvöldum má undanþiggja réttinum til aðgangs samkvæmt 1. mgr. 15. gr. reglugerðarinnar að sama marki og gildir um undantekningar á upplýsingarétti samkvæmt upplýsingalögum og stjórnsýslulögum.

Ákvæði 34. gr. reglugerðarinnar um skyldu til að tilkynna hinum skráða um öryggisbrot gildir ekki ef ákvæði 1. og 4. tölul. 2. mgr. eiga við.

18. gr.

Verndarráðstafanir og undanþágur varðandi vinnslu vegna rannsókna, tölfræði eða skjalavistunar í þágu almannahagsmuna.

Vinnsla vegna rannsókna á sviði vísinda eða sagnfræði, í tölfræðilegum tilgangi eða vegna skjalavistunar í þágu almannahagsmuna skal vera háð viðeigandi ráðstöfunum, þ. á m. tæknilegum og skipulagslegum, til verndar réttindum og frelsi skráðra einstaklinga í samræmi við 89. gr. reglugerðarinnar, einkum til þess að tryggja að farið sé að meginreglunni um lágmörkun gagna.

Ákvæði 15., 16., 18. og 21. gr. reglugerðarinnar um réttindi hins skráða gilda ekki þegar vinnsla persónuupplýsinga fer aðeins fram í þágu vísinda eða sagnfræði eða í tölfræðilegum tilgangi að svo miklu leyti sem telja má að þessi réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum.

Ákvæði 15., 16., 18., 19., 20. og 21. gr. reglugerðarinnar um réttindi hins skráða gilda ekki þegar vinnsla persónuupplýsinga fer aðeins fram vegna skjalavistunar í þágu almannahagsmuna að svo miklu leyti sem telja má þessi réttindi gera það ómögulegt eða hamla því verulega að unnt sé að ná viðkomandi markmiðum. Þó á hinn skráði rétt á að leggja fram yfirlýsingu til varðveislu í gögnum með persónuupplýsingum um hann.

19. gr.

Undantekning frá upplýsingaskyldu vegna vinnslu persónuupplýsinga hjá stjórnvöldum.

Upplýsingaskyldan samkvæmt 3. mgr. 13. gr. og 4. mgr. 14. gr. reglugerðarinnar gildir ekki þegar stjórnvald miðlar persónuupplýsingum til annars stjórnvalds í þágu lögbundins hlutverks við framkvæmd laga og upplýsingum er miðlað aðeins að því marki sem nauðsynlegt er til að rækja lagaskyldu stjórnvalds.

20. gr.

Réttur til leiðréttingar, eyðingar, flutnings eigin gagna o.fl.

Hinn skráði á rétt á að fá rangar, villandi eða ófullkomnar persónuupplýsingar um sig leiðréttar, þeim eytt (réttur til að gleymast) og til að takmarka vinnslu skv. 16.- 19. gr. reglugerðarinnar.

Skráður einstaklingur skal eiga rétt á að fá persónuupplýsingar um sig, sem hann hefur sjálfur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu sniði og jafnframt á að senda þessar upplýsingar til annars ábyrgðaraðila samkvæmt nánari skilyrðum 20. gr. reglugerðarinnar.

21. gr.

Um andmælarétt hins skráða og bannskrá Þjóðskrár Íslands.

Hinum skráða er heimilt að andmæla vinnslu persónuupplýsinga um sig sem byggist á e- eða f-lið 1. mgr. 6. gr. reglugerðarinnar, þ.m.t. gerð persónusniðs. Ábyrgðaraðili skal 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 hún sé nauðsynleg til að stofna, hafa uppi eða verja réttarkröfur samkvæmt nánari fyrirmælum 21. gr. reglugerðarinnar. Eigi andmælin rétt á sér er ábyrgðaraðila óheimil frekari vinnsla umræddra upplýsinga.

Þjóðskrá Íslands skal halda skrá yfir þá sem andmæla því að nöfn þeirra séu notuð í markaðssetningarstarfsemi. Ráðherra setur, í samráði við Persónuvernd, nánari reglur um gerð og notkun slíkrar skrár og hvaða upplýsingar skuli koma þar fram. Ábyrgðaraðilar sem starfa í beinni markaðssókn og þeir sem nota skrá með nöfnum, heimilisföngum, netföngum, símanúmerum og þess háttar eða miðla þeim til þriðja aðila í tengslum við slíka starfsemi skulu, áður en slík skrá er notuð í slíkum tilgangi, bera hana saman við skrá Þjóðskrár Íslands til að koma í veg fyrir að markpóstur verði sendur eða hringt verði til einstaklinga sem hafa andmælt slíku. Persónuvernd getur heimilað undanþágu frá þessari skyldu í sérstökum tilvikum.

Öll notkun bannskrár skv. 2. mgr. er óheimil í öðrum tilgangi en þar er lýst.

Skylt er að nafn ábyrgðaraðila komi fram á áberandi stað á útsendum markpósti og hvert þeir sem andmæla því að fá slíkan markpóst og marksímtöl geti snúið sér. Viðtakandi markpósts á rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja úthringingu eða útsendingu til grundvallar. Þetta gildir ekki um markaðssetningu ábyrgðaraðila á eigin vöru og þjónustu sem notar eigin viðskiptamannaskrár, enda beri útsent efni með sér hvaðan það kemur. Ef markpóstur er sendur með rafrænum hætti er skylt að fram komi á ótvíræðan hátt um leið og hann er móttekinn að um slíkan póst sé að ræða. Að öðru leyti fer um sendingu slíks markpósts skv. lögum um fjarskipti.

Ábyrgðaraðila er heimilt að afhenda félaga-, starfsmanna-, nemenda- eða viðskiptamannaskrár til nota í tengslum við markaðssetningarstarfsemi. Þetta á þó aðeins við ef:

1. ekki telst vera um afhendingu viðkvæmra persónuupplýsinga að ræða,
2. hinum skráðu hefur, áður en afhending fer fram, verið gefinn kostur á að andmæla því, hverjum fyrir sitt leyti, að upplýsingar um viðkomandi birtist á hinni afhentu skrá;
3. slíkt fer ekki gegn starfsreglum eða félagssamþykktum sem í gildi eru hjá viðkomandi ábyrgðaraðila;
4. ábyrgðaraðili kannar hvort einhver hinna skráðu hefur komið andmælum á framfæri við Þjóðskrá Íslands, sbr. 2. mgr., og eyðir upplýsingum um viðkomandi áður en hann lætur skrána af hendi ef svo reynist vera.

Ákvæði 5. mgr. gildir ekki ef afhending félaga-, starfsmanna- eða viðskiptamannaskrár til nota við dreifingu markpósts byggist á samþykki hins skráða, sbr. 1. tölul. 1. mgr. 9. gr. Ákvæði 2.–5. mgr. gilda, eftir því sem við á, einnig um markaðs-, neyslu- og skoðanakannanir.

22. gr.

Réttindi tengd einstaklingsmiðuðum ákvörðunum sem byggjast á sjálfvirkri gagnavinnslu.

Skráður einstaklingur skal eiga rétt á því að ekki sé tekin ákvörðun eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerðar persónusniðs, sem hefur réttaráhrif að því er hann sjálfan varðar eða snertir hann

á sambærilegan hátt að verulegu leyti samkvæmt nánari fyrirmælum 22. gr. reglugerðarinnar, með þeim undantekningum sem þar getur.

IV. kafli. Almennar reglur um skyldur ábyrgðaraðila og vinnsluaðila og öryggi persónuupplýsinga.

23. gr.

Ábyrgð ábyrgðaraðila.

Ábyrgðaraðili skal gera viðeigandi tæknilegar og skipulagslegar ráðstafanir sem taka mið af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu fyrir réttindi og frelsi skráðra einstaklinga til að tryggja og sýna fram á að vinnsla persónuupplýsinga uppfylli kröfur reglugerðarinnar samkvæmt nánari fyrirmælum 24. og 25. gr. reglugerðarinnar. Þegar tveir eða fleiri eru sameiginlegir ábyrgðaraðilar fer um skyldur þeirra eftir 26. gr. reglugerðarinnar.

24. gr.

Innbyggð og sjálfgefin persónuvernd.

Ábyrgðaraðili skal, bæði þegar ákveðnar eru aðferðir við vinnsluna og þegar vinnslan sjálf fer fram, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, sem hannaðar eru til að framfylgja meginreglum um persónuvernd, og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur þessarar reglugerðar og vernda réttindi skráðra einstaklinga samkvæmt nánari fyrirmælum 1. mgr. 25. gr. reglugerðarinnar

Ábyrgðaraðili skal gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að sjálfgefið sé að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar hverju sinni samkvæmt nánari fyrirmælum 2. mgr. 25. gr. reglugerðarinnar.

25. gr.

Almennar reglur um vinnsluaðila.

Þegar öðrum er falin vinnsla persónuupplýsinga fyrir hönd ábyrgðaraðila skal ábyrgðaraðili einungis leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnslan uppfylli kröfur reglugerðarinnar og réttindi skráðra einstaklinga séu tryggð.

Vinnsluaðili skal ekki ráða annan vinnsluaðila nema hafa til þess sértæka eða almenna skriflega heimild ábyrgðaraðila. Ef um er að ræða almenna skriflega heimild skal vinnsluaðilinn tilkynna ábyrgðaraðilanum um allar fyrirhugaðar breytingar sem fela í sér að bætt er við vinnsluaðilum eða þeim skipt út og gefa þannig ábyrgðaraðilanum færi á að andmæla slíkum breytingum.

Vinnsla af hálfu vinnsluaðila skal byggjast á samningi eða annarri réttargerð samkvæmt lögum sem skuldbindur vinnsluaðila gagnvart ábyrgðaraðilanum og tilgreinir viðfangsefni og tímalengd vinnslunnar, eðli hennar og tilgang, tegund persónuupplýsinga, flokka skráðra einstaklinga og skyldur og réttindi ábyrgðaraðilans eftir nánari fyrirmælum 28. gr. reglugerðarinnar.

26. gr.

Skrár yfir vinnslustarfsemi.

Sérhver ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúi þeirra, skal halda skrá yfir vinnslustarfsemi sína. Um upplýsingar sem skrá yfir vinnslustarfsemi skal innihalda, form skrár, aðgengileika o.fl. gilda fyrirmæli 30. gr. reglugerðarinnar.

27. gr.

Öryggi persónuupplýsinga og tilkynningar um öryggisbrot.

Ábyrgðaraðili og vinnsluaðili skulu gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja viðunandi öryggi persónuupplýsinga með hliðsjón af nýjustu tækni, kostnaði við framkvæmd, eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga, samkvæmt nánari fyrirmælum 32. gr. reglugerðarinnar

Ef um öryggisbrot við meðferð persónuupplýsinga er að ræða skal ábyrgðaraðili, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brotsins var tilkynna það til Persónuverndar nema ólíklegt þyki að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga. Sé Persónuvernd ekki tilkynnt um brotið innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni. Þá skal vinnsluaðili tilkynna ábyrgðaraðila um það án ótilhlýðilegrar tafar ef hann verður var við öryggisbrot við meðferð persónuupplýsinga. Um efni tilkynningar til Persónuverndar gilda fyrirmæli 33. gr. reglugerðarinnar.

Ef líklegt er að öryggisbrot við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðili tilkynna skráðum einstaklingi um brotið án ótilhlýðilegrar tafar. Um efni slíkrar tilkynningar og undanþágur frá tilkynningarskyldu gilda fyrirmæli 34. gr. reglugerðarinnar.

28. gr.

Samvinna við Persónuvernd.

Ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúar þeirra skulu, að fenginni beiðni Persónuverndar, hafa samvinnu við stofnunina við framkvæmd verkefna hennar**.**

V. kafli. Mat á áhrifum á persónuvernd, leyfisskylda o.fl.

29. gr.

Mat á áhrifum á persónuvernd.

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 samkvæmt nánari fyrirmælum 35. gr. reglugerðarinnar. Eitt og sama mat getur tekið til nokkurra svipaðra vinnsluaðgerða sem geta haft í för með sér svipaða áhættuþætti.

Persónuvernd birtir skrá yfir þær tegundir vinnsluaðgerða þar sem krafist er mats á áhrifum á persónuvernd skv. 1. mgr.

Persónuvernd getur einnig ákveðið að birta skrá yfir þær tegundir vinnsluaðgerða þar sem ekki er krafist mats á áhrifum á persónuvernd.

30. gr.

Fyrirframsamráð.

Ef mat á áhrifum á persónuvernd gefur til kynna að vinnsla myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðili grípi til ráðstafana til að draga úr henni, skal hann hafa samráð við Persónuvernd áður en vinnslan hefst, samkvæmt nánari fyrirmælum 36. gr. reglugerðarinnar.

Telji Persónuvernd að fyrirhuguð vinnsla, sem um getur í 1. mgr., myndi brjóta í bága við þessa reglugerð, 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 notað til þess allar þær valdheimildir sínar sem um getur í 41 – 43. gr. laganna. Lengja má frestinn 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 viðtöku beiðni um samráð, ásamt ástæðunum fyrir töfinni. Þessa fresti má framlengja þar til Persónuvernd hefur fengið þær upplýsingar sem hún óskar eftir vegna samráðsins.

31. gr.

Leyfisskyld vinnsla.

Sé um að ræða vinnslu persónuupplýsinga vegna verkefnis í þágu almannahagsmuna sem getur falið í sér sérstaka hættu á að farið verði í bága við réttindi og frelsi skráðra einstaklinga getur Persónuvernd ákveðið að vinnslan megi ekki hefjast fyrr en hún hefur verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar. Persónuvernd getur ákveðið að slík leyfisskylda falli brott þegar settar hafa verið almennar reglur og öryggisstaðlar sem fylgja skuli við slíka vinnslu.

Persónuvernd setur reglur um leyfisskyldu skv. 1. mgr.

32. gr.

Forsendur leyfisveitingar o.fl.

Ábyrgðaraðila má aðeins veita leyfi skv. 31. gr. laga þessara, eða einstakar aðrar heimildir samkvæmt lögunum, ef líklegt er að hann geti fullnægt skyldum sínum samkvæmt lögunum eða fyrirmælum Persónuverndar.

Við afgreiðslu leyfa skv. 31. gr. sem tengjast vinnslu viðkvæmra persónuupplýsinga skal Persónuvernd meta hvort vinnslan geti valdið hinum skráða slíku óhagræði að ekki verði úr því bætt með forsvaranlegum hætti með skilyrðum sem sett eru skv. 35. gr. laganna. Ef slíkt óhagræði getur orðið skal Persónuvernd meta hvort hagsmunir sem mæla með vinnslunni vegi þyngra en hagsmunir hins skráða.

33. gr.

Skilmálar Persónuverndar um vinnslu persónuupplýsinga.

Þegar ábyrgðaraðila er veitt leyfi skv. 34. gr. laga þessara skal Persónuvernd binda það þeim skilyrðum sem hún metur nauðsynleg hverju sinni til að draga úr eða koma í veg fyrir hugsanlegt óhagræði hins skráða af vinnslunni.

Við mat á því hvaða skilyrði skal setja fyrir vinnslu skal Persónuvernd m.a. athuga:

1. hvort tryggt sé að hinn skráði geti nýtt réttindi sín samkvæmt lögunum, þar á meðal til að afturkalla samþykki og eftir atvikum fá eytt skráðum persónuupplýsingum, svo og til að fá fræðslu um réttindi sín og beitingu þeirra;
2. hvort persónuupplýsingar verði nægjanlega öruggar, áreiðanlegar og uppfærðar í samræmi við tilgang vinnslunnar;
3. hvort með persónuupplýsingarnar verði farið af þeirri varúð sem reglur um þagnarskyldu og tilgangur vinnslunnar krefjast;
4. hvort skipulagt hafi verið hvernig hinum skráða verði veittar upplýsingar og leiðbeiningar, innan þeirra marka sem sanngjarnt er að ætlast til miðað við umfang vinnslunnar og aðrar öryggisráðstafanir sem viðhafðar eru;
5. hvort stofnað hafi verið til öryggisráðstafana sem séu eðlilegar miðað við tilgang vinnslunnar;
6. hvort mat á áhrifum á persónuvernd fari fram áður en vinnsla hefjist.

Persónuvernd getur ákveðið að ábyrgðaraðili og vinnsluaðili, svo og starfsmenn á vegum þeirra, skuli undirrita yfirlýsingu um að þeir séu bundnir þagnarskyldu um persónuupplýsingar sem þeir fá vitneskju um við störf sín. Ábyrgðaraðili eða fulltrúi hans skal votta rétta undirskrift viðkomandi og dagsetningu slíkrar yfirlýsingar og koma til Persónuverndar innan tilskilins frests. Þagnarskyldan helst þótt látið sé af starfi.

34. gr.

Leyfi fyrir vísindarannsóknum á heilbrigðissviði.

Um leyfi fyrir vísindarannsóknum á heilbrigðissviði fer samkvæmt lögum um vísindarannsóknir á heilbrigðissviði.

VI. kafli. Persónuverndarfulltrúar og vottunaraðilar.

35. gr.

Persónuverndarfulltrúar.

Ábyrgðaraðili og vinnsluaðili skulu tilnefna persónuverndarfulltrúa í sérhverju tilviki þar sem:

1. vinnsla er í höndum stjórnvalds;
2. meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í vinnsluaðgerðum sem krefjast, sakir eðlis síns, umfangs eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum eða
3. meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í umfangsmikilli vinnslu viðkvæmra persónuupplýsinga og upplýsinga sem varða sakfellingar í refsimálum og refsiverð brot.

Fyrirtækjasamstæðu er heimilt að skipa einn persónuverndarfulltrúa að því tilskildu að sérhver starfsstöð hafi greiðan aðgang að honum. Einnig er fleira en einu stjórnvaldi heimilt að skipa sameiginlegan persónuverndarfulltrúa að teknu tilliti til stjórnskipulags þeirra og stærðar.

Um hæfni persónuverndarfulltrúa, stöðu hans og verkefni gilda að öðru leyti fyrirmæli 37.-39. gr. reglugerðarinnar.

36. gr.

Þagnarskylda persónuverndarfulltrúa.

Persónuverndarfulltrúa er er óheimilt að segja frá nokkru því sem hann hefur fengið vitneskju um í starfi sínu og leynt á að fara.

Þagnarskylda gildir þó ekki hafi hinn skráði veitt samþykki sitt til þess að leynd sé aflétt, svo og þegar nauðsyn krefur vegna framkvæmdar starfa persónuverndarfulltrúans.

37. gr.

Vottun og vottunaraðilar.

Faggildingarsvið Einkaleyfastofu, að fenginni umsögn Persónuverndar, hefur heimild til að faggilda vottunaraðila sem gefur út vottun skv. 42. reglugerðarinnar.

Um skilyrði faggildingar vottunaraðila, fyrirkomulag og efni vottunar gilda að öðru leyti fyrirmæli 42. og 43. gr. reglugerðarinnar.

VII. kafli. Eftirlit og viðurlög.

38. gr.

Skipulag Persónuverndar og stjórnsýsla.

Persónuvernd er sjálfstæð stofnun með sérstaka stjórn. Hún tekur ekki við fyrirmælum frá stjórnvöldum eða öðrum aðilum. Ákvörðunum Persónuverndar samkvæmt lögum þessum verður ekki skotið til annarra stjórnvalda, en aðilum máls er heimilt að að leggja ágreining sinn fyrir dómstóla með venjubundnum hætti.

Ráðherra sem fer með persónuverndarmálefni skipar fimm menn í stjórn Persónuverndar og jafnmarga til vara til fimm ára í senn. Ekki er heimilt að skipa stjórnarmenn lengur en í þrjú tímabil samfellt. Formann og varaformann stjórnarinnar skipar ráðherra án tilnefningar og skulu þeir vera lögfræðingar og fullnægja hæfisskilyrðum héraðsdómara. Ráðherra sem fer með málefni netöryggis og fjarskipta tilnefnir einn stjórnarmann og ráðherra sem fer með málefni heilbrigðisþjónustu tilnefnir einn stjórnarmann. Þá tilnefnir Skýrslutæknifélag Íslands einn stjórnarmann og skal hann vera sérfróður á sviði tölvu- og tæknimála. Stjórnarmenn og varamenn þeirra skulu hafa sérþekkingu á málefnum tengdum persónuvernd og menntun sem nýtist á því sviði.

Ráðherra ákveður laun stjórnarmanna.

Stjórnarmanni verður aðeins vikið úr stjórn vegna alvarlegra ávirðinga eða ef hann fullnægir ekki lengur þeim skilyrðum sem krafist er vegna starfs hans.

Þegar stjórnarmenn eru ekki sammála ræður meiri hluti niðurstöðu máls. Ef atkvæði eru jöfn ræður atkvæði formanns.

Ráðherra skipar forstjóra Persónuverndar til fimm ára í senn að fenginni tillögu stjórnar. Forstjóri skal hafa menntun á háskólastigi og búa yfir þekkingu og reynslu á málefnum tengdum persónuvernd.

Forstjóri situr fundi stjórnar með málfrelsi og tillögurétti.

Forstjóri Persónuverndar annast daglega stjórn og ræður annað starfsfólk Persónuverndar.

Forstjóri ber ábyrgð á fjárreiðum og starfsmannahaldi Persónuverndar. Stjórn Persónuverndar ákveður að öðru leyti skiptingu starfa á milli stjórnar og starfsmanna hennar.

39. gr.

Verkefni Persónuverndar.

Persónuvernd er eftirlitsstjórnvald skv. VI. kafla reglugerðarinnar og annast eftirlit með framkvæmd hennar, laga þessara, sérákvæða í lögum sem fjalla um vinnslu persónuupplýsinga og annarra reglna um efnið.

Sérhver skráður einstaklingur eða fulltrúi hans hefur rétt til að leggja fram kvörtun hjá Persónuvernd ef hann telur að vinnsla persónuupplýsinga um hann hér á landi eða samkvæmt sérreglum 7. gr. laganna brjóti í bága við reglugerðina eða ákvæði laga þessara. Þá geta stofnun, samtök eða félög samkvæmt 80. gr. reglugerðarinnar lagt fram kvörtun hjá Persónuvernd hafi þau ástæðu til að ætla að réttindi skráðs einstaklings hafi verið brotin. Persónuvernd úrskurðar um hvort brot hafi átt sér stað.

Persónuvernd getur fjallað um einstök mál og tekið í þeim ákvörðun að eigin frumkvæði eða samkvæmt erindi þess sem telur að ekki hafi verið unnið með persónuupplýsingar um sig í samræmi við lög þessi og reglur sem settar eru samkvæmt þeim eða einstökum fyrirmælum.

Önnur verkefni Persónuverndar eru m.a. að:

1. efla vitund og skilning almennings á áhættu, reglum, verndarráðstöfunum og réttindum í tengslum við vinnslu svo og vitund ábyrgðaraðila og vinnsluaðila um skyldur sínar;

2. veita Alþingi, stjórnvöldum og öðrum aðilum ráðgjöf á sviði lagasetningar og stjórnsýslu sem tengist vernd einstaklinga við vinnslu persónuupplýsinga;

3. veita, að fenginni beiðni, skráðum einstaklingi upplýsingar um það hvernig hann getur neytt réttinda sinna samkvæmt lögum þessum og reglugerðinni og, ef við á, starfa með eftirlitsyfirvöldum í öðrum aðildarríkjum í því skyni,

4. eiga samstarf við eftirlitsyfirvöld í öðrum aðildarríkjum, þ.m.t. með því að skiptast við þau á upplýsingum, og veita gagnkvæma aðstoð, með það fyrir augum að tryggja samkvæmni í beitingu og framkvæmd laga þessara og reglugerðarinnar;

5. fylgjast með framvindu á sviðum tengdum persónuupplýsingavernd, einkum þróun upplýsinga- og fjarskiptatækni og viðskiptahátta;,

6. samþykkja föst samningsákvæði eins og um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr. reglugerðarinnar.

7. útbúa og viðhalda skrá yfir þær tegundir vinnsluaðterða þar sem krafist er mats á áhrifum á persónuvernd skv. 4. mgr. 35. gr. reglugerðarinnar;

8. veita ráðgjöf um vinnsluaðgerðir eins og um getur í 2. mgr. 36. gr. reglugerðarinnar;

9. hvetja til þess að samdar verði hátternisreglur skv. 1. mgr. 40. gr. reglugerðarinnar og gefa álit á og samþykkja hátternisreglur sem tryggja fullnægjandi verndarráðstafanir skv. 5. mgr. 40. gr. hennar;

10. Samþykkja viðmiðanir um vottun skv. 5. mgr. 42. gr. reglugerðarinnar og eftir atvikum, láta fara fram reglubundna endurskoðun á vottunum sem eru gefnar út í samræmi við 7. mgr. 42. gr. hennar.

11. semja og birta drög að viðmiðunum um faggildingu aðila sem hafa eftirlit með framkvæmd hátternisreglna skv. 41. gr. reglugerðarinnar og vottunaraðila skv. 43. gr. hennar og annast faggildingu sömu aðila;

12. samþykkja ákvæði, þ. á m. í samningum, eins og um getur í 3. mgr. 46. gr. reglugerðarinnar;

13. samþykkja bindandi fyrirtækjareglur skv. 47. gr. reglugerðarinnar;

14. taka þátt í starfsemi Evrópska persónuverndarráðsins;

15. skrásetja brot á þessari reglugerð og ráðstafanir sem gerðar eru í samræmi við 2. mgr. 58. gr. hennar;

16. sinna öðrum störfum sem tengjast vernd persónuupplýsinga.

40. gr.

Gjaldtaka.

Persónuvernd getur ákveðið að ábyrgðaraðili skuli greiða þann kostnað sem hlýst af eftirliti með því að hann fullnægi skilyrðum laga þessara og reglna sem settar eru samkvæmt þeim eða einstökum fyrirmælum. Persónuvernd getur einnig ákveðið að ábyrgðaraðili greiði kostnað við úttekt á starfsemi við undirbúning útgáfu vinnsluleyfis og annarrar afgreiðslu.

Ráðherra setur gjaldskrá um gjaldtöku skv. 1. mgr.

41. gr.

Valdheimildir Persónuverndar við eftirlitsstörf.

Persónuvernd fer með valdheimildir samkvæmt 1. mgr. 58. gr. reglugerðarinnar við eftirlitsstörf sín, þ. á m.:

1. til að fyrirskipa að ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúi þeirra veiti hverjar þær upplýsingar sem hún þarfnast vegna framkvæmdar reglugerðarinnar;

2. til að gera úttektir á vinnslu persónuupplýsinga;

3. til að láta fara fram endurskoðun á vottunum sem eru gefnar út skv. 7. mgr. 42. gr. reglugerðarinnar;

4. til að tilkynna ábyrgðaraðila eða vinnsluaðila um meint brot á þessari reglugerð;

5. til að fá hjá ábyrgðaraðila og vinnsluaðila aðgang að öllum þeim gögnum, þ. á m. persónuupplýsingum sem nauðsynlegar eru við framkvæmd laganna;

6. til aðgangs að húsnæði þar sem vinnsla persónuupplýsinga fer fram eða gögn eru varðveitt, þ.m.t. hvers kyns gagnavinnslubúnaður Persónuvernd getur framkvæmt hverja þá prófun eða eftirlitsaðgerð sem hún telur nauðsynlega og krafist nauðsynlegrar aðstoðar starfsfólks á slíkum vettvangi til að framkvæma prófun eða eftirlit;

Persónuvernd getur óskað liðveislu lögreglu ef einhver leitast við að hindra hana í eftirlitsstörfum sínum.

Komi í ljós að vinnsla persónuupplýsinga fer fram sem brýtur í bága við ákvæði reglugerðarinnar, laga þessara eða reglna settar samkvæmt þeim er Persónuvernd heimilt að fela lögreglustjóra að stöðva til bráðabirgða starfsemi viðkomandi og innsigla starfsstöð hans þegar í stað.

Réttur Persónuverndar til að krefjast upplýsinga eða aðgangs að starfsstöðvum og tækjabúnaði verður ekki takmarkaður með vísan til reglna um þagnarskyldu.

42. gr.

Fyrirmæli Persónuverndar um ráðstafanir til úrbóta.

Persónuvernd getur mælt fyrir um ráðstafanir til úrbóta eftir því sem nánar er mælt fyrir um í 2. mgr. 58. gr. reglugerðarinnar, þ. á m.:

1. veitt ábyrgðaraðila eða vinnsluaðila viðvörun um að líklegt sé að fyrirhugaðar vinnsluaðgerðir brjóti í bága við ákvæði reglugerðarinnar;

2. veitt ábyrgðaraðila eða vinnsluaðila áminningu ef vinnsluaðgerðir hafa brotið í bága við reglugerðina;

3. gefið fyrirmæli um að ábyrgðaraðili eða vinnsluaðili fari að beiðnum hins skráða um að fá að neyta réttinda sinna samkvæmt reglugerðinni;

4. gefið fyrirmæli um að ábyrgðaraðili eða vinnsluaðili færi vinnsluaðgerðir til samræmis við ákvæði reglugerðarinnar, eftir því sem við á, með tilteknum hætti og innan tiltekins tíma;

5. gefið fyrirmæli um að ábyrgðaraðili tilkynni hinum skráða um öryggisbrot við meðferð persónuupplýsinga;

6. takmarkað eða bannað vinnslu tímabundið eða til frambúðar;

7. gefið fyrirmæli um leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu þeirra skv. 16., 17. og 18. gr. reglugerðarinnar og að slíkar aðgerðir verði tilkynntar viðtakendum sem fengið hafa persónuupplýsingarnar í hendur skv. 2. mgr. 17. gr. og 19. gr. hennar.

8. afturkallað vottun eða fyrirskipað að vottunaraðili afturkalli vottun sem gefin var út skv. 42. og 43. gr. reglugerðarinnar;

9. gefið fyrirmæli um tímabundna stöðvun gagnaflæðis til viðtakanda í þriðja landi eða til alþjóðastofnunar.

43. gr.

Leyfisveitingar og ráðgjöf Persónuverndar.

Persónuvernd hefur eftirtaldar heimildir tengdar leyfisveitingum og ráðgjöf:

1. til að veita ábyrgðaraðila ráðgjöf í samræmi við fyrirframsamráðsferlið sem um getur í 36. gr. reglugerðarinnar;

2. til að leggja, að eigin frumkvæði eða samkvæmt beiðni, álitsgerðir fyrir Alþingi eða stjórnvöld, eða aðra aðila um hvert það málefni sem tengist vernd persónuupplýsinga;

3. til að leyfa vinnslu þar sem fyrirframheimildar er krafist samkvæmt lögum;

4. til að gefa álit og samþykkja drög að hátternisreglum skv. 5. mgr. 40. gr. reglugerðarinnar;

5. til að faggilda vottunaraðila skv. 43. gr. reglugerðarinnar, gefa út vottanir og samþykkja viðmiðanir fyrir vottun í samræmi við 5. mgr. 42. gr. hennar;

6. til að samþykkja stöðluð ákvæði um persónuvernd eins og um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr. reglugerðarinnar;

7. til að leyfa samningsákvæði sem um getur í a-lið 3. mgr. 46. gr. reglugerðarinnar;

8. til að leyfa stjórnvaldsráðstafanir sem um getur í b-lið 3. mgr. 46. gr. reglugerðarinnar;

9. til að samþykkja bindandi fyrirtækjareglur skv. 47. gr. reglugerðarinnar;

44. gr.

Þagnarskylda

Starfsmönnum Persónuverndar og öðrum sem vinna verkefni á vegum stofnunarinnar er óheimilt að segja frá nokkru sem þeir hafa fengið vitneskju um í starfi sínu og leynt á að fara.

Ákvæði um þagnarskyldu standa því ekki í vegi að Persónuvernd veiti erlendum persónuverndarstofnunum upplýsingar þegar slíkt er nauðsynlegt til að hún eða hin erlenda persónuverndarstofnun geti ákveðið eða framkvæmt aðgerðir til að tryggja persónuvernd.

Við gerð skilmála skv. 33. gr. laganna getur Persónuvernd ákveðið að ábyrgðaraðili og vinnsluaðili, svo og starfsmenn á vegum þeirra, skuli undirrita yfirlýsingu um að þeir gangist undir þagnarskyldu um persónuupplýsingar sem þeir fá vitneskju um við vinnslu þeirra. Ábyrgðaraðili eða fulltrúi hans skal votta rétta undirskrift starfsmanns og dagsetningu slíkrar yfirlýsingar og koma til Persónuverndar innan tilskilins frests.

Þagnarskylda skv. 1. og 3. mgr. helst þótt látið sé af starfi.

45. gr.

Dagsektir.

Ef ekki er farið að fyrirmælum Persónuverndar skv. 6. 7. og 9. tölul. 42. gr. laga þessara getur hún, áður en hún ákveður stjórnvaldssekt skv. 46. gr. laganna, lagt dagsektir á þann sem fyrirmælin beinast að þar til úr hefur verið bætt að mati hennar. Sektir geta numið allt að 200.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælunum sé fylgt.

Ef ákvörðun Persónuverndar um dagsektir er skotið til dómstóla byrja dagsektir ekki að falla á fyrr en dómur er endanlegur. Dagsektir renna í ríkissjóð og má án undangengins dóms gera aðför til fullnustu þeirra.

46. gr.

Stjórnvaldssektir.

Persónuvernd getur lagt stjórnvaldssektir á hvern þann sem brýtur gegn einhverju þeirra ákvæða reglugerðinnar og laga þessara sem talin eru upp í 2. og 3. mgr.

Stjórnvaldssektir geta numið frá 100 þús. kr. til 1,2 milljarða kr. eða ef um er að ræða fyrirtæki allt að 2% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra þegar brotið hefur verið gegn eftirfarandi ákvæðum.

1. um skyldur ábyrgðaraðila og vinnsluaðila skv. 8. gr., 25.-39. gr., 42. og 43. gr. reglugerðarinnar;

2. um skyldur vottunaraðila skv. 42. og 43. gr. reglugerðarinnar;

3. um skyldur eftirlitsaðila, skv. 4. mgr. 41. gr. reglugerðarinnar;

Stjórnvaldssektir geta numið frá 100 þús. kr. til 2,4 milljarða kr. eða ef um er að ræða fyrirtæki allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra, þegar brotið hefur verið gegn eftirfarandi ákvæðum:

1. um grundvallarreglur um vinnslu, þ.m.t. skilyrði fyrir samþykki, skv. 5., 6., 7. og 9. gr. reglugerðarinnar;
2. um réttindi skráðra einstaklinga skv. 12.-22. gr. reglugerðarinnar;
3. um miðlun persónuupplýsinga til viðtakanda í þriðja landi eða alþjóðastofnunar skv. 44.-49. gr. reglugerðarinnar;
4. ef ekki er farið að skyldu til að veita Persónuvernd aðgang að öllum gögnum og húsnæði skv. 5. og 6. tölul. 41. gr. laganna;
5. ef ekki er farið að fyrirmælum Persónuverndar um takmörkun eða bann við vinnslu persónuupplýsinga, um leiðréttingu eða eyðingu þeirra, eða stöðvun gagnaflæðis skv. 6., 7. og 9. tölul 42. gr. laganna.

Heimilt er að leggja sektir á einstaklinga og lögaðila, þar á meðal stjórnvöld og stofnanir sem falla undir gildissvið stjórnsýslulaga.

Stjórnvaldssektum verður beitt óháð því hvort lögbrot eru framin af ásetningi eða gáleysi.

Ákvarðanir um stjórnvaldssektir skulu teknar af stjórn Persónuverndar og eru þær aðfararhæfar. Sektir renna í ríkissjóð að frádregnum kostnaði við innheimtuna. Séu stjórnvaldssektir ekki greiddar innan mánaðar frá ákvörðun Persónuverndar skal greiða dráttarvexti af fjárhæð sektarinnar. Um ákvörðun og útreikning dráttarvaxta fer eftir lögum um vexti og verðtryggingu.

Heimild Persónuverndar til að leggja á stjórnvaldssektir samkvæmt lögum þessum fellur niður þegar fimm ár eru liðin frá því að háttsemi lauk. Fyrningarfrestur rofnar þegar Persónuvernd tilkynnir aðila um upphaf rannsóknar á meintu broti. Rof frests hefur réttaráhrif gagnvart öllum sem staðið hafa að broti.

47. gr.

Atriði sem áhrif hafa á ákvörðun um stjórnvaldssekt.

Þegar ákveðið er hvort beita skuli stjórnvaldssekt og fjárhæð sektarinnar er ákveðin í hverju tilviki skal taka tilhlýðilegt tillit til eftirfarandi:

1. hvers eðlis, hversu alvarlegt og hversu langvarandi brotið er, með tilliti til eðlis, umfangs eða tilgangs vinnslunnar sem um er að ræða og fjölda skráðra einstaklinga sem urðu fyrir því og hversu alvarlegu tjóni þeir urðu fyrir;
2. hvort brotið var framið af ásetningi eða af gáleysi;
3. aðgerða sem ábyrgðaraðilinn eða vinnsluaðilinn hefur gripið til í því skyni að draga úr tjóni skráðra einstaklinga;
4. hversu mikla ábyrgð ábyrgðaraðili eða vinnsluaðili ber með tilliti til tæknilegra og skipulagslegra ráðstafana sem þeir hafa komið til framkvæmda skv. 25. og 32. gr. reglugerðarinnar;
5. fyrri brota ábyrgðaraðila eða vinnsluaðila sem máli skipta, ef einhver eru,
6. umfangs samvinnu við Persónuvernd til þess að bæta úr brotinu og draga úr mögulegum, skaðlegum áhrifum þess;
7. hvaða flokka persónuupplýsinga brotið hafði áhrif á;
8. með hvaða hætti eftirlitsyfirvaldinu var gert kunnugt um brotið, einkum hvort, og þá að hvaða leyti, ábyrgðaraðili eða vinnsluaðili tilkynnti um brotið;
9. fylgni við fyrirmæli Persónuverndar um ráðstafanir til úrbóta skv. 42. gr. laganna hafi fyrirmælum um slíkar ráðstafanir áður verið beint til hlutaðeigandi ábyrgðaraðila eða vinnsluaðila að því er varðar sama efni;
10. fylgni við viðurkenndar hátternisreglur skv. 40. gr. reglugerðarinnar eða viðurkennt vottunarfyrirkomulag skv. 42. gr. hennar;
11. annarra íþyngjandi eða mildandi þátta sem varða kringumstæður málsins, s.s. hagnaðar sem fékkst eða taps sem komist var hjá, með beinum eða óbeinum hætti, vegna brotsins.

Ef ábyrgðaraðili eða vinnsluaðili brýtur, af ásetningi eða gáleysi, gegn fleiri en einu ákvæði reglugerðarinnar og laganna við sömu eða tengdar vinnsluaðgerðir skal heildarfjárhæð sektarinnar ekki vera hærri en fjárhæðin sem er tilgreind fyrir alvarlegasta brotið.

48. gr.

Refsingar.

Ef brot einstaklings er stórfellt getur það varðað fangelsi allt að 3 árum. Brot telst stórfellt þegar það er framið af ásetningi og í hagnaðarskyni með sérstaklega vítaverðum hætti og persónuupplýsingar mikils

fjölda skráðra einstaklinga sem leynt eiga að fara samkvæmt lögum eða eðli máls komast í hendur þriðja aðila eða birtast opinberlega.

Hafi fyrirsvarsmaður lögaðila, starfsmaður hans eða annar á hans vegum framið brot skv. 1. mgr. í starfsemi lögaðilans má gera honum refsingu, samhliða stjórnvaldssekt sem lögaðilanum er gerð skv. 46. gr.

Brot einstaklings á þagnarskyldu skv. 36. og 44. gr. laganna varðar fangelsi allt að einu ári Hafi hann framið brotið til þess að afla sér eða öðrum óréttmæts ávinnings má beita fangelsi allt að 3 árum.

49. gr.

Kæra til lögreglu.

Persónuvernd metur hvort meint brot einstaklings samkvæmt 48. gr. skuli kært til lögreglu eða því lokið með stjórnvaldsákvörðun hjá stofnuninni. Með kæru Persónuverndar skulu fylgja afrit þeirra gagna sem grunur um brot er studdur við. Ákvæði IV.–VII. kafla stjórnsýslulaga gilda ekki um ákvörðun Persónuverndar um að kæra mál til lögreglu.

Persónuvernd er heimilt að láta lögreglu og ákæruvaldi í té upplýsingar og gögn sem stofnunin hefur aflað og tengjast þeim brotum sem tilgreind eru í 1. og 2. mgr. Persónuvernd er heimilt að taka þátt í aðgerðum lögreglu sem varða rannsókn þeirra brota

Lögreglu og ákæruvaldi er heimilt að láta Persónuvernd í té upplýsingar og gögn sem þau hafa aflað og tengjast þeim brotum sem tilgreind eru í 2. mgr. Lögreglu er heimilt að taka þátt í aðgerðum Persónuverndar sem varða rannsókn þeirra brota sem tilgreind eru í 1 og. 2. mgr.

Telji ákærandi að ekki séu efni til málshöfðunar vegna ætlaðrar refsiverðrar háttsemi sem jafnframt varðar stjórnsýsluviðurlögum getur hann endursent málið til Persónuverndar til meðferðar og ákvörðunar

50. gr.

Réttur manna til að fella ekki á sig sök.

Í máli sem beinist að einstaklingi og lokið getur með álagningu stjórnvaldssekta eða kæru til lögreglu skv. 49. gr., hefur maður sem rökstuddur grunur leikur á að hafi gerst sekur um brot á lögunum, rétt til að neita að svara spurningum eða afhenda gögn eða muni nema hægt sé að útiloka að það geti haft þýðingu fyrir ákvörðun um brot hans. Persónuvernd skal leiðbeina hinum grunaða um þennan rétt.

51. gr.

Bætur.

Hafi ábyrgðaraðili eða vinnsluaðili unnið með persónuupplýsingar í andstöðu við ákvæði reglugerðarinnar, laga þessara, reglna settra á grundvelli þeirra eða fyrirmæli Persónuverndar skal hann bæta hinum skráða það fjárhagslega tjón sem sá síðarnefndi hefur orðið fyrir af þeim völdum. Ábyrgðaraðila eða vinnsluaðila verður þó ekki gert að bæta tjón sem hann sannar að hvorki verður rakið til mistaka né vanrækslu af hans hálfu.

Vinnsluaðili skal þó aðeins bera ábyrgð á tjóni, sem hlýst af vinnslu, hafi hann ekki uppfyllt skyldur samkvæmt reglugerðinni og lögunum sem beinast sérstaklega að vinnsluaðilum, eða ef hann hefur ekki fylgt lögmætum fyrirmælum ábyrgðaraðilans eða farið gegn þeim.

VIII. kafli. Gildistaka o.fl.

52. gr.

Reglugerðir á grundvelli laganna.

Með reglugerð má mæla fyrir um meðferð persónuupplýsinga í tiltekinni starfsemi og hjá einstökum starfsstéttum.

53. gr.

Gildistaka.

Lög þessi öðlast þegar gildi. Við gildistöku þeirra falla úr gildi lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

Ákvæði til bráðabirgða.

Ráðherra skipar stjórn Persónuverndar í samræmi við 38. gr. laganna þegar skipunartími sitjandi stjórnar rennur út.

Leyfi sem Persónuvernd hefur gefið út skulu halda gildi, enda fari þau ekki í bága við lög þessi og reglugerðina.

Greinargerð.

1. Inngangur.

Hinn 21. nóvember 2017 skipaði dómsmálaráðherra fimm manna starfshóp sem falið var að semja frumvarp til innleiðingar á 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 eins og hún hefur verið aðlöguð að samningnum um Evrópska efnahagssvæðið (*Regulation* (EU) *2016/679* of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC). Reglugerðin kemur til framkvæmda innan ESB 25. maí 2018 og mun leysa af hólmi tilskipun Evrópusambandsins og ráðsins 95/46/EB frá 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga.

Formaður starfshópsins og aðalhöfundur frumvarpsins var Björg Thorarensen, prófessor við Lagadeild Háskóla Íslands og formaður stjórnar Persónuverndar. Aðrir í starfshópnum voru Rósa Dögg Flosadóttir frá dómsmálaráðuneyti, Vigdís Eva Líndal og Þórður Sveinsson, frá Persónuvernd og Baldur Már Bragason frá rekstrarfélagi Stjórnarráðsins.

Núgildandi lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 voru sett til að tryggja að ákvæði íslenskra laga fullnægðu kröfum fyrrgreindrar tilskipunar ESB frá 1995 og var jafnframt tekið mið af því hvernig aðrar þjóðir á Norðurlöndunum leiddu ákvæði hennar inn í landsrétt. Við gerð laganna var einkum tekið mið af löggjöf Norðmanna um efnið í ljósi þess að bæði ríkin standa ein Norðurlandanna utan Evrópusambandsins sem aðilar að samningnum um Evrópska efnahagssvæðið. Líkt og tilskipunin, er reglugerðin tekin upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar frá **xx 2018**. Í frumvarpsvinnu þessari hefur m.a. verið litið til norska, danska, sænska og þýska frumvarpsins um sama efni en í öllum þessum ríkjum var ákveðið að setja ný heildarlög um vinnslu persónuupplýsinga.

Þótt flest kjarnaatriði tilskipunar ESB frá 1995, t.d. meginreglur um vinnslu persónuupplýsinga, réttindi hins skráða og skyldur ábyrgðaraðila standi áfram óbreytt í reglugerðinni eru þar ráðgerðar ýmsar grundvallarbreytingar og viðbætur við gildandi reglur. Einnig er ljóst að þar sem hinar nýju reglur eru settar með reglugerð ESB en ekki tilskipun, verður sú krafa leidd af 7. gr. EES-samningsins að leiða skal texta reglugerðarinnar sem slíkan inn í landsrétt, en íslensk stjórnvöld hafa ekki val um form eða aðferð við innleiðingu slíkra gerað svo sem með umritun. Engu að síður er ráðgert í reglugerðinni að í allmörgum atriðum geti aðildarríki útfært einstaka ákvæði og hafi svigrúm til að setja efnisreglur eða víkja frá ákvæðum reglugerðarinnar. Í ljósi umfangs þeirra breytinga og sérreglna sem setja þarf á grundvelli reglugerðarinnar er sú leið farin hér að gera frumvarp til nýrra heildarlaga um persónuvernd og vinnslu persónuupplýsinga sem leysi af hólmi lög nr. 77/2000. Samhliða því eru lögfest í heild sinni ákvæði reglugerðarinnar eins og hún var tekin upp í EES-samninginn og birtist hún sem fylgiskjal með frumvarpinu. Er þetta sami háttur og hafður er á í Noregi, Danmörku og Svíþjóð, en nánar verður fjallað um aðferð við innleiðingu reglugerðarinnar í 7. kafla hér á eftir.

Starfshópurinn skilaði frumdrögum að frumvarpi til dómsmálaráðherra til kynningar 26. janúar og fullbúnu frumvarpi xx. mars 2018. Auk þess er stefnt að því að dómsmálaráðherra leggi fram frumvarp til laga um breytingar á ýmsum sérlögum þar sem taka þarf mið af ákvæðum reglugerðarinnar.

Þess má geta að á vettvangi Evrópusambandsins hefur einnig verið samþykkt sérstök tilskipun Evrópuþingsins og ráðsins nr. 2016/680 frá 27. apríl 2016 um vinnslu persónuupplýsinga á sviði lögreglumála (Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA). Þar er um að ræða þýðingarmikið sérsvið um vinnslu persónuupplýsinga sem íslenskum stjórnvöldum ber einnig að innleiða Schengen-samstarfsins en það er ekki viðfangsefni frumvarps þessa. Þá er í undirbúningi hjá ESB ný reglugerð um vinnslu persónuupplýsinga og vernd einkalífs á sviði rafrænna fjarskipta sem ætlað er að leysa af hólmi tilskipun Evrópuþingsins og ráðsins 2002/58/EB frá 12. júlí 2002 um sama efni. Af þessu sést að umfangsmiklar breytingar eiga sér nú stað innan Evrópu á sviði reglna um vinnslu persónuupplýsinga og persónuvernd í átt til aukinnar samræmingar á þessu réttarsviði sem Ísland tekur virkan þátt í með aðild sinni að EES-samningnum.

2. Íslenskar réttarreglur um persónuvernd og þróun þeirra

Íslenskar réttarreglur líkt og alþjóðlegar skuldbindingar og Evrópureglur um persónuvernd byggjast á þeirri forsendu að persónuupplýsingar séu þáttur í friðhelgi einkalífs hvers einstaklings sem telst til grundvallarmannréttinda. Eru réttindi þessi fest í 71. gr. stjórnarskrárinnar og 8. gr. mannréttindasáttmála Evrópu. Með stjskl. 97/1995 var hugtakinu friðhelgi einkalífs bætt í 71. gr. stjórnarskrárinnar en fyrir þann tíma laut vernd samkvæmt texta stjórnarskrárinnar aðeins að friðhelgi heimilis. Markmiðið með hinni auknu vernd sem núgildandi stjórnarskrárákvæði veitir var einkum að færa efni þess og gildissvið til samræmis við 8. gr. mannréttindasáttmála Evrópu sem lögfestur var hér á landi með lögum nr. 62/1994 svo og 17. gr. alþjóðasamnings Sameinuðu þjóðanna frá 1966 um borgaraleg og stjórnmálaleg réttindi. Í greinargerð með stjskl. nr. 97/1995 eru rakin tengsl ákvæðisins við þessi alþjóðlegu samningsákvæði og lýst inntaki einkalífshugtaksins sem er afar víðtækt. Um það segir m.a. að í friðhelgi einkalífsins felist fyrst og fremst réttur manns til að ráða yfir lífi sínu og líkama og til að njóta friðar um lífshætti sína og einkahagi. Jafnframt er bent á að raunhæft dæmi um svið, þar sem álitaefni vaknar um hvort brotið er gegn friðhelgi einkalífs, sé skráning persónuupplýsinga um einstaklinga, en í því sambandi reynir á hversu langt megi ganga í skipulagðri skráningu á lífsháttum manns og högum og við meðferð slíkra upplýsinga.

Stjórnarskrárákvæðið um friðhelgi einkalífs gerir ráð fyrir því að skylda hvíli á ríkinu til að forðast afskipti af einkalífi manna þar með talið hvað varðar persónuupplýsingar þeirra. Það nægir þó ekki til þess að menn fái í reynd notið friðhelgi einkalífs og því ber ríkinu skylda til að setja reglur í löggjöf til verndar einstaklingunum í innbyrðis samskiptum þeirra. Auk þeirrar kröfu að þessum mannréttindum sé veitt refsivernd svo sem m.a. má sjá í XXV. kafla almennra hegningarlaga nr. 19/1940 um brot gegn friðhelgi einkalífs, leiðir af stjórnarskránni að binda þarf í löggjöf skýrar reglur um öflun, skráningu og meðferð persónuupplýsinga hvort sem um er að ræða meðferð stjórnvalda eða einkaaðila á upplýsingunum og um að einstaklingur eigi rétt til aðgangs að upplýsingum um sjálfan sig.

Setning réttarreglna um meðferð persónuupplýsinga er þannig einn mikilvægasti þátturinn í viðleitni ríkisvaldsins til þess að sinna þeirri skyldu sem stjórnarskráin leggur á hinn almenna löggjafa í þessum efnum. Þannig hefur mótast sjálfstætt og umfangsmikið réttarsvið hér á landi líkt og í öðrum vestrænum ríkjum, persónuverndarréttur (e. *Data Protection Law*) með ítarlegu regluverki sem stefnir í átt til æ meiri samræmingar í ljósi þess að vinnsla persónuupplýsinga með þeirri tækni sem er til staðar fylgir engum landamærum og því þarf að samræma eftirlit með framkvæmd laganna.

Hugmyndafræðilegur grundvöllur frumvarps þessa og lagareglna almennt um vinnslu persónuupplýsinga hvílir á þeirri forsendu að með persónuupplýsingar sé farið í samræmi við grundvallarsjónarmið um friðhelgi einkalífs eins og fyrr var lýst en einnig að tryggja áreiðanleika og gæði slíkra upplýsinga og frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins, og að því verði ekki settar of strangar skorður.

Íslensk réttarþróun um þetta efni hefur fylgt þróun í öðrum Evrópuríkjum samhliða byltingu í tölvu- og upplýsingatækni á fáum áratugum sem gerir bæði stjórnvöldum og einkaaðilum kleift að safna og miðla miklu magni persónuupplýsinga um einstaklinga með tiltölulega einföldum hætti, og jafnframt er vinnsla persónuupplýsinga órjúfanlegur þáttur í starfsemi opinberra aðila og fyrirtækja, stórra sem smárra. Þá hefur aðild Íslands að EES-samningnum leitt af sér skuldbindingu til að innleiða Evrópugerðir um efnið en eitt helsta markmið ESB-reglugerðarinnar sem frumvarpinu er ætlað að innleiða er einmitt að samræma enn frekar reglur um persónuvernd í öllum aðildarríkjum ESB.

Fyrstu lög sem sett voru hér á landi til verndar einstaklingum í þessum efnum voru lög nr. 63/1981 um kerfisbundna skráningu á upplýsingum er varða einkamálefni. Markmið þeirra var fyrst og fremst að fjalla um meðferð upplýsinga í tölvum og um vernd gegn misnotkun slíks efnis. Þau mæltu jafnframt fyrir um stofnun sérstakrar nefndar, tölvunefndar, sem var falið almennt eftirlit með framkvæmd laganna Höfðu þau fyrir fram afmarkaðan gildistíma og féllu úr gildi 31. desember 1985. Þann 1. janúar 1986 tóku gildi ný lög um sama efni, nr. 39/1985. Höfðu þau einnig fyrir fram afmarkaðan gildistíma og féllu úr gildi 31. desember 1989. Ástæða þess að fyrstu lög sem sett voru um efnið höfðu afmarkaðan gildistíma var sú að tölvutækni var í örri þróun og þótti nauðsynlegt að endurskoða lögin með reglulegu millibili til að tryggja að þau væru á hverjum tíma í samræmi við hinn tæknilega veruleika. Þá tóku gildi þann 1. janúar 1990 lög nr. 121/1989, um skráningu og meðferð persónuupplýsinga. Lög í flestum vestrænum ríkjum sem sett voru um meðferð persónuupplýsinga á árunum 1970-1990 höfðu í meginatriðum að geyma tvenns konar reglur sem settar voru til að sporna við hættum samfara tölvutækni. Annars vegar voru efnisreglur um söfnun, skráningu, meðferð, notkun og miðlun persónuupplýsinga. Gildissvið slíkra reglna var í upphafi víða takmarkað við þá meðferð eina þar sem tölvutækni var beitt. Þó voru nokkur ríki sem ekki gerðu neinn greinarmun á því í þessu sambandi hvort meðferðin var vélræn eða handunnin. Í þeirra hópi var Ísland og er enn í dag, enda hefur þróun reglna í Evrópusamvinnu verið á sama veg. Til að handvirk vinnsla falli undir þær er þó skilyrði að

upplýsingarnar séu eða eigi að verða hluti af skrá. Álitamál um vinnslu persónuupplýsinga eru hins vegar nú á tímum að langmestu leyti tengd rafrænni (sjálfvirkri) vinnslu.

Í núgildandi lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga sem frumvarpi þessu er ætlað að leysa af hólmi voru gerðar grundvallarbreytingar á íslensku lagaumhverfi og eftirliti með framkvæmd laganna. Sem fyrr segir var eitt helsta markmið þeirra að tryggja að ákvæði íslenskra laga fullnægðu kröfum tilskipunar ESB frá 1995 um efnið sem lagði grunn að nýskipan á þessu réttarsviði. Þannig komu inn í lögin skilgreiningar á helstu hugtökum sem enn er stuðst við á réttarsviðinu og gildissvið reglna afmarkað með skýrum hætti, meginreglur um vinnslu og vinnsluheimildir komu inn í lög, auk ítarlegri reglna um aukin réttindi hins skráða og skyldur ábyrgðaraðila og vinnsluaðila. Í stað tölvunefndar var sett á fót sérstök stofnun, Persónuvernd. Í lögunum er henni tryggt sérstakt sjálfstæði og valdheimildir til að sinna eftirlitshlutverki sínu með framkvæmd laganna, enda er lögð á það sérstök áhersla í tilskipuninni að ríki skuli tryggja að sjálfstæð stjórnvöld fari með slíkt eftirlit. Frá setningu laganna hafa ýmsar breytingar verið gerðar á þeim m.a. til að víkka út þá vernd sem þau veita. Með lögum nr. 90/2001 var m.a. fylgt eftir 25. gr. tilskipunarinnar þess efnis að framkvæmdastjórn EB gæti ákveðið að þriðja land teldist tryggja nægilega vernd í krafti laga sinna eða alþjóðaskuldbindinga um vernd friðhelgi einkalífs og var Persónuvernd veitt heimild til að auglýsa gildi slíkra ákvarðana hér á landi. Einnig voru með sömu lögum sett inn ítarlegri ákvæði um öryggi við vinnslu persónuupplýsinga til að endurspegla tiltekin ákvæði tilskipunarinnar þar að lútandi. Þá má nefna að með lögum nr. 81/2002 og 46/2003 voru gerðar breytingar á ákvæðum um rafræna vöktun, þar á meðal sjónvarpsvöktun, fræðsluskyldu ábyrgðaraðila og önnur skilyrði hennar, eyðingu efnis sem safnast við vöktun o.fl. Þá voru breytingar gerðar á aðkomu Persónuverndar að leyfisveitingum tengdum vísindarannsóknum á heilbrigðissviði með lögum nr. 44/2014.

3. Reglur um persónuvernd í samvinnu Evrópuríkja og áhrif á íslenskan rétt.

3.1. Almennt.

Frá seinni hluta 20. aldar óx verulega þörf á úrræðum til að vernda friðhelgi einkalífs í tæknivæddu nútímaþjóðfélagi, einkum vegna framfara á sviði tölvutækni þar sem möguleikar á öflun og skráningu persónuupplýsinga, bæði af hálfu stjórnvalda og einkaaðila hafa stöðugt aukist. Til þess að bregðast við hættum sem af þessu stafa fyrir friðhelgi einkalífs fór alþjóðlegt samstarf á sviði persónuverndar vaxandi eftir 1980 og ýmis fjölþjóðleg samtök hafa sinnt persónuverndarmálum í auknum mæli. Ein fyrsta fjölþjóðasamþykktin um efnið var ályktun á vettvangi Efnahags- og framfarastofnunarinnar, OECD, um leiðbeiningar varðandi verndun einkalífs við flutning persónuupplýsinga yfir landamæri frá 23. september 1980 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). Ekki er um bindandi samning að ræða en leiðbeiningarnar hafa þýðingu fyrir ríki sem ekki hafa sérstaka löggjöf um meðferð og verndun persónuupplýsinga

Ísland hefur tekið virkan þátt í alþjóðlegu samstarfi um vernd persónuupplýsinga innan Evrópuráðsins og á vegum evrópskra og norrænna persónuverndarstofnana. Í stórum dráttum má segja að alþjóðlegar reglur á þessu réttarsviði greinist í tvennt. Annars vegar eru alþjóðasamningar og sáttmálar sem eru þjóðréttarlega skuldbindandi fyrir Ísland. Í þann flokk falla samningur Evrópuráðsins frá 1981, tilskipun ESB, svo og reglugerðin sem frumvarpi þessu er ætlað að innleiða. Hins vegar eru tilmæli eða yfirlýsingar sem ekki eru þjóðréttarlega skuldbindandi en geta haft þýðingu við skýringu bindandi þjóðréttarreglna og mögulega íslenskra laga einnig. Í þann flokk falla m.a. fyrrnefndar leiðbeiningar OECD og leiðbeiningar, samþykktar af allsherjarþingi SÞ 14. desember 1990, um tölvufærðar persónuupplýsingaskrár (Guidelines Concerning Computerized Personal Data Files).

Hér á eftir verður gerð stuttlega grein fyrir Evrópureglum sem áhrif hafa á efni íslenskra réttarreglna um vernd persónuupplýsinga. Fyrst verður vikið að samningi Evrópuráðsins um vernd einstaklinga við vélræna vinnslu persónuupplýsinga frá árinu 1981 og öðrum samþykktum á sviði persónuverndarréttar hjá Evrópuráðinu. Í öðru lagi er fjallað um tilskipun ESB frá 24. október 1995 sem er grundvöllur núgildandi laga um persónuvernd og meðferð persónuupplýsinga. Þar á eftir verður lýst ástæðum og aðdraganda að setningu hinnar nýju ESB reglugerðar sem lagt er til að lögfest verði með frumvarpi þessu. Einnig verður vikið að frekari samþykktum á vettvangi ESB um efnið.

3.2. Samningur Evrópuráðsins og aðrar samþykktir á vegum ráðsins

Í samningi Evrópuráðsins um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga frá 28. janúar 1981 er lýst þeim tilgangi að tryggja einstaklingum virðingu fyrir réttindum þeirra og grundvallarfrelsi, einkum rétti til einkalífs að því er varðar vélræna vinnslu persónuupplýsinga um þá eða svokallaða persónuupplýsingavernd. Samningurinn var fullgiltur af Íslands hálfu 1991. Með honum var lagður mikilvægur grundvöllur að síðari reglusetningu hjá Evrópusambandsinu en helstu ákvæði hans voru leidd í

íslenskan rétt við gildistöku laga nr. 121/1989 um skráningu og meðferð persónuupplýsinga. Evrópuráðssamningurinn hefur að geyma lágmarksreglur, en í því felst að aðildarríkjum hans er heimilt að veita þeim er upplýsingarnar varðar víðtækari réttindi í löggjöf sinni. Árið 2001 var samþykktur viðauki við samninginn um eftirlitsstjórnvöld og flutning persónuupplýsinga á milli landa, en Ísland hefur ekki fullgilt hann.

Evrópuráðssamningurinn gildir að meginstefnu til um alla meðferð persónuupplýsinga þar sem tölvutækni er beitt við vinnsluna. Tilgangur samningsins er að tryggja sérhverjum manni á svæði hvers samningsaðila, hvert sem þjóðerni hans eða búseta er, virðingu fyrir réttindum hans og grundvallarfrelsi, einkum rétti hans til einkalífs að því er varðar vélræna vinnslu persónuupplýsinga sem hann varða.

Til fyllingar ákvæðum samningsins frá 1981 hafa ráðherranefnd og ráðgjafarþing Evrópuráðsins beint allmörgum tilmælum og ályktunum til aðildarríkja sinna um meðferð persónuupplýsinga á afmörkuðum sviðum. Tilmæli ráðherranefndarinnar eru nú 17 talsins., þar á meðal má nefna tilmæli um vernd mannréttinda í tengslum við samfélagsmiðla frá 4. apríl 2012, CM/Rec(2012)4 og tilmæli um vinnslu persónuupplýsinga í tengslum við atvinnu frá 1. apríl 2015 CM/Rec (2015)5. Réttarleg staða tilmæla ráðherranefndarinnar er önnur en samningsins þar sem þau eru ekki þjóðréttarlega skuldbindandi, en fela á hinn bóginn í sér ákveðna pólitíska skuldbindingu fyrir aðildarríkin. Sum tilmælin eru þess eðlis að efni þeirra á ekki beinlínis heima í ákvæðum almennra laga um vernd persónuupplýsinga. Þau geta hins vegar haft þýðingu við setningu sérlaga á þessu réttarsviði og í framkvæmd eftirlitsaðila þegar settir eru sérstakir skilmálar um vinnslu ákveðinna tegunda persónuupplýsinga.

3.3. Tilskipun Evrópusambandsins 95/46/EB

Markmiðið með samþykkt núgildandi tilskipunar frá 24. október 1995 var tvíþætt, annars vegar að vernda rétt manna til þess að njóta friðhelgi um einkalíf sitt í tengslum við meðferð persónuupplýsinga og hins vegar að tryggja frjálst flæði persónuupplýsinga milli aðildarríkja ESB. Hún byggist á sömu grundvallarsjónarmiðum og Evrópuráðssamningurinn frá 1981. Innan þess ramma sem hún setur hefur einstökum aðildarríkjum verið heimilt að setja strangari reglur sem tryggja meiri vernd en leiðir af ákvæðum hennar, en ýmsar sérreglur af þeim toga er að finna í lögum nr. 77/2000.

Það meginmarkmið tilskipunarinnar að tryggja samræmdar reglur og samræmda persónuvernd í öllum aðildarríkjum ESB, hvíldi ekki síst á markaðssjónarmiðum því að samræmdar reglur um persónuvernd eru taldar nauðsynlegar þess að frjáls og opinn markaður fái þrifist. Ljóst var að löggjöf aðildarríkjanna á persónuverndarsviðinu var afar mismunandi. Það stóð í vegi fyrir frjálsu flæði persónuupplýsinga milli aðildarríkjanna og skapaði vandkvæði í efnahagslegu samstarfi þeirra.

Tilskipunin festi í sessi mjög rúma skilgreiningu persónuupplýsingahugtaksins sem tekur til allra upplýsinga sem rekjanlegar eru til einstaklinga og setti fram ítarlegar skilgreiningar á nokkrum lykilhugtökum. Þá setti hún fram með skýrum hætti meginreglur um gæði og vinnslu gagna, lögmæta vinnslu almennra persónuupplýsinga, og sérstök skilyrði fyrir vinnslu persónuupplýsinga sem skilgreindar eru sem viðkvæmar. Loks setti tilskipunin fram ítarleg ákvæði um réttindi hins skráða og þær skyldur sem lagðar eru á ábyrgðaraðila vinnslu. Þar á meðal er skylda ábyrgðaraðila til að tilkynna viðkomandi persónuverndarstofnun um fyrirhugaða vinnslu tiltekinna persónuupplýsinga. Ýmsar undantekningar eru þó frá þessu þannig að um ákveðnar tegundir vinnslu gilda vægari tilkynningarreglur eða þær eru með öllu undanþegnar tilkynningarskyldunni auk þess sem um aðrar tegundir vinnslu gilda í sumum tilvikum strangari reglur, þ.e. leyfisskylda í stað tilkynningarskyldu.

Tilskipunin leiddi inn ýmis nýmæli varðandi upplýsingarétt hins skráða m.a. að þegar ákveðnar tegundir ákvarðana sem hann varða byggjast einungis á rafrænni vinnslu persónuupplýsinga á hann rétt á hann rétt á að fá vitneskju um fyrirkomulag þeirrar vinnslu. Þá hefur hver og einn rétt til þess að fá handunna endurskoðun umræddum ákvörðunum.

Samkvæmt tilskipuninni er aðildarríkjunum skylt að setja á laggirnar stofnanir til þess að hafa eftirlit með því að ákvæðum hennar sé fylgt innan landamæra viðkomandi ríkis. Skulu slíkar stofnanir njóta fullkomins sjálfstæðis í störfum sínum og m.a. hafa vald til þess að framkvæma rannsóknir, veita leyfi, stöðva ólöglega starfsemi o.fl. Sem fyrr segir voru þessi fyrirmæli leidd inn í íslenskan rétt með stofnun Persónuverndar sem tók til starfa 2001 og er verkefnum hennar og valdheimildum nánar lýst í VII. kafla laga nr. 77/2000.

Í 29. gr. tilskipunarinnar er mælt fyrir um stofnun starfshóps sem sinnir ráðgjafarhlutverki um persónuverndarmálefni. Í starfshópnum sitja fulltrúar persónuverndarstofnana aðildarríkja ESB en auk þeirra fulltrúar framkvæmdastjórnar ESB og Evrópsku persónuverndarstofnunarinnar (European Data Protection Supervisor). Persónunverndarstofnanir EFTA-ríkjanna Noregs, Lichtenstein og Íslands hafa áheyrnaraðild að hópnum, sem gengur undir nafninu 29. gr. starfshópurinn. Hann hefur gegnt mikilvægu hlutverki við útgáfu leiðbeininga og álita um túlkun ýmissa lykilákvæða tilskipunarinnar. Hefur framlag 29. gr.

starfshópsins til framkvæmdar tilskipunarinnar í aðildarríkjum verið mikilvægt og er gjarnan vísað til álita hans þegar reynir á úrlausn álitamála um túlkun tilskipunarinnar og landslaga. Starfshópurinn hefur þegar gefið út nokkrar leiðbeiningar um afmörkuð atriði reglugerðarinnar og fleiri eru í undirbúningi, sem tengjast innleiðingu nýju ESB-reglugerðarinnar og verður nánar vísað til þeirra í umfjöllun um tiltekin ákvæði frumvarpsins hér á eftir eftir því sem við á.

3.4. Aðrar tilskipanir og ákvarðanir ESB sem þýðingu hafa fyrir vernd persónuupplýsinga

Ýmsar aðrar tilskipanir og ályktanir stofnana ESB hafa haft þýðingu fyrir vernd persónuupplýsinga að íslenskum rétti fyrir milligöngu EES-samningsins eða samningsins um þátttöku Íslands í Schengen-samstarfsins. Þannig hefur vinnsla persónuupplýsinga sem fer fram vegna löggæslu og þjóðaröryggishagsmuna fallið utan gildissviðs tilskipunarinnar. Um slíka vinnslu hefur gilt rammaákvörðun ráðsins nr. 2008/977/DIM, um vernd persónuupplýsinga sem unnar eru innan ramma lögreglu- og dómsmálasamstarfs í sakamálum (Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters). Persónuverndarstofnanir í Evrópu hafa haft með sér samstarf á þessu sviði og hefur Ísland komið að þeirri vinnu vegna aðildar sinnar að Schengen-samstarfinu. Eins og fyrr var lýst verður sú ákvörðun leyst af hólmi með tilskipun Evrópuþingsins og ráðsins nr. 2016/680 frá 27. apríl 2016 um vinnslu persónuupplýsinga á sviði lögreglumála. Í undirbúningi er að innleiða tilskipunina hér á landi en hún mun fyrirsjáanlega hafa margþætt áhrif.

Þá má nefna tilskipun Evrópuþingsins og ráðsins nr. 2011/83/ESB frá 25. október 2011 um réttindi neytenda en hún leysti af hólmi tilskipun 97/7 um neytendavernd og fjarsölu. Gildissvið hennar nær til samninga um vöru og þjónustu sem gerðir eru af hálfu neytenda og seljenda með fjarsölu, þ.e. samninga sem alfarið komast á með milligöngu „fjarmiðla".

Loks má geta tilskipunar Evrópuþingsins og ráðsins nr. 2002/58/EB um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta sem innleidd var með fjarskiptalögum nr. 81/2003. Sú tilskipun sætir nú endurskoðun og fyrir liggur tillaga að nýrri reglugerð Evrópuþingsins og ráðsins um einkalífsvernd og rafræn fjarskipti, sem einnig mun fyrirsjáanlega hafa áhrif á vernd persónuupplýsinga hér á landi.

4. Reglugerð Evrópuþingsins og ráðsins nr. 2016/679 frá 27. apríl 2016.

4.1. Aðdragandi breytinga

Í kjölfar breytinga á stofnsamþykktum Evrópusambandsins með Lissabon-sáttmálanum frá 13. desember 2007 sem tók gildi 1. desember 2009 hófst undirbúningur innan Evrópusambandsins að endurskoðun regluverks á sviði persónuverndar. Grundvöllurinn var lagður með nýjum ákvæðum um efnið í 16. og 114. gr. sáttmálans um starfshætti ESB. Samkvæmt 16. gr. sáttmálans eiga allir rétt á því að persónuupplýsingar um þá njóti verndar og mælt er fyrir um að Evrópuþingið og ráðið skuli setja reglur um vernd einstaklinga með hliðsjón af vinnslu persónuupplýsinga á vegum stofnana og aðila á vegum Sambandsins og á vegum aðildarríkjanna vegna starfsemi sem fellur undir lög sambandsins, svo og reglur um frjálsa miðlun slíkra upplýsinga. Þá er kveðið á um að óháð yfirvöld skuli hafa eftirlit með því að slíkum reglum sé fylgt. Í 114. gr. er fjallað um almennar aðgerðir Evrópuþingsins og ráðsins til að vinna að samræmingu á þeim ákvæðum laga og stjórnsýslufyrirmæli í aðildarríkjum sem beinast að stofnun og starfsemi innri markaðarins

Þá birtist hugmyndafræðileg undirstaða evrópsku persónuverndarlöggjafarinnar í Sáttmála ESB um grundvallarréttindi sem settur var í stofnlög sambandsins með Lissabon- sáttmálanum. Þar er 8. gr. helguð rétti til verndar persónuupplýsinga sem er þannig skilinn frá hefðbundnu ákvæði sem stendur í 7. gr. um friðhelgi einkalífs. Í 8. gr. er fyrst lýst yfir rétti manns til verndar eigin persónuupplýsinga og settar fram nokkrar meginreglur persónuverndarréttar, svo sem að vinnsla persónuupplýsinga skuli fara fram með sanngjörnum hætti í yfirlýstum tilgangi og með samþykki hlutaðeigandi eða á einhverjum öðrum réttmætum grundvelli sem mælt er fyrir um í lögum. Lýst er rétti einstaklings til aðgangs að upplýsingum sem teknar hafa verið saman um hann og rétti til að fá þær leiðréttar. Loks er mælt fyrir um að óháð stjórnvald skuli hafa eftirlit með því að þessum reglum sé fylgt.

Fyrstu tillögur um heildarendurskoðun á persónuverndarlöggjöfinni í almennu lagasetningarferli innan ESB komu fram árið 2012. Markmið endurskoðunarinnar var að laga löggjöfina að þeirri byltingu sem orðið hafði í upplýsingatækni frá því að tilskipunin var sett, styrkja persónuvernd, stuðla að samræmdari framkvæmd innan ESB og efla virkni hins stafræna innri markaðar. Þing ESB samþykkti afstöðu sína til reglugerðarinnar þann 12. mars 2014 og ráðið 15. júní 2015. Þann 14. apríl 2016 var síðan samþykkt hin nýja reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB sem ætlað er að koma til

framkvæmda innan ESB 25. maí 2018. Þá var á sama tíma samþykkt tilskipun Evrópuþingsins og ráðsins (ESB) 2016/680 um vernd einstaklinga að því er varðar vinnslu lögbærra yfirvalda á persónuupplýsingum í tengslum við að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum og frjálsa miðlun slíkra upplýsinga og um niðurfellingu rammaákvörðun ráðsins 2008/977/DIM (löggæslutilskipunin).

4.2. Markmið reglugerðarinnar

Um ástæður þess að endurskoða þurfti persónuverndarlöggjöf ESB er m.a. fjallað í 9. lið formála reglugerðarinnar. Þar er tekið fram að þrátt fyrir að markmið og meginreglur tilskipunar 95/46/EB standi enn fyrir sínu hafi hún ekki náð að sporna við sundurlausri framkvæmd persónuverndar innan Sambandsins, réttaróvissu og þeim útbreiddu hugmyndum meðal almennings að fyrir hendi sé veruleg áhætta fyrir vernd einstaklinga, einkum í tengslum við netnotkun. Bent er á að rétturinn til verndar persónuupplýsinga sé mismikil í aðildarríkjunum í tengslum við vinnslu persónuupplýsinga og geti það hindrað frjálst flæði persónuupplýsinga um Sambandið. Þessi munur geti því orðið hindrun í vegi ýmiss konar atvinnustarfsemi á vettvangi Sambandsins, raskað samkeppni og komið í veg fyrir að yfirvöld sinni skyldustörfum sínum samkvæmt lögum Sambandsins. Þennan mun á vernd megi rekja til þess mismunar sem er á framkvæmd og beitingu tilskipunar 95/46/EB, en ljóst er að aðildarríki hafa haft talsvert svigrúm til að koma markmiðum tilskipunarinnar í framkvæmd.

Þá er tekið fram í 10. lið formálans að til þess að tryggja einstaklingum samræmda og öfluga vernd og ryðja úr vegi hindrunum á flæði persónuupplýsinga innan Sambandsins þurfi vernd réttinda og frelsis einstaklinga í tengslum við vinnslu slíkra upplýsinga að vera sambærileg í öllum aðildarríkjunum. Tryggja verði alls staðar í Sambandinu samræmda og einsleita beitingu reglna um vernd grundvallarréttinda og frelsis einstaklinga í tengslum við vinnslu persónuupplýsinga. Að því er varðar vinnslu persónuupplýsinga til þess að fullnægja lagaskyldu sé aðildarríkjunum þó heimilt, vegna framkvæmdar á verkefni sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, að viðhalda eða innleiða ný ákvæði í landslög til að tilgreina nánar hvernig þessari reglugerð skuli beitt. Auk almennrar og láréttrar löggjafar um persónuvernd, sem sett er til framkvæmdar tilskipun 95/46/EB, hafa aðildarríkin ýmsa geirabundna löggjöf á sviðum þar sem þörf er á sértækari ákvæðum. Tekið er fram að reglugerðin veiti aðildarríkjunum ákveðið svigrúm til að skilgreina reglur sínar, m.a. varðandi vinnslu sérstakra flokka persónuupplýsinga („viðkvæmra persónuupplýsinga“).

Af þessum inngangsorðum reglugerðarinnar sést að meginmarkmið hennar eru tvíþætt, annað er réttindamiðað og hitt byggist á þörfum hins stafræna innri markaðar og nauðsyn á samræmdri framkvæmd. Áherslan á aukna persónuvernd í þágu einstaklinga birtist einkum í ákvæðum sem veita þeim meiri stjórn á eigin persónuupplýsingum. Meðal annars er einstaklingum tryggður ríkari aðgangur að upplýsingum og vitneskju um hvað verði um þær eftir að þeir ákveða að deila þeim með öðrum. Einnig á að tryggja aukinn rétt til að fá upplýsingum eytt af Netinu og rétt til að gleymast en sá réttur felur t.d. í sér að geta farið fram á það við netþjónustuaðila að þeir fjarlægi, án tafa, persónuupplýsingar sem þeir hafa safnað um viðkomandi. Þá munu ný réttindi, réttur til gagnaflutnings auðvelda mönnum að fá upplýsingar um sig fluttar frá einum aðila til annars, t.d. frá einum samfélagsmiðli til annars. Til að ná þessu fram eru ýmsar nýjar skyldur lagðar á ábyrgðaraðila, m.a. til að auka gagnsæi um vinnslu persónuupplýsinga, veita fræðslu á skýru og skiljanlegu máli, að tryggja öryggi vinnslunnar, nota kerfi með innbyggðu og sjálfvirka persónuvernd og að halda sérstakar vinnsluskrár. Þá verður dregið úr heimildum til vinnslu persónuupplýsinga í þágu sjálfvirkrar ákvarðanatöku, þ.m.t. notkunar persónusniða til að greina manngerð viðkomandi, frammistöðu í starfi, lánshæfi, heilsuhagi, smekk o.s.frv. Ábyrgðaraðilum verður auk þess gert skylt að tilkynna, bæði Persónuvernd og hinum skráðu, um öryggisbrot og í vissum tilvikum verður þeim gert skylt að tilnefna persónuverndarfulltrúa. Loks verður einstaklingum gert kleift að kvarta beint til persónuverndarstofnunar í sínu heimalandi jafnvel þótt ábyrgðaraðilinn hafi staðfestu annars staðar.

Hitt meginmarkmið reglugerðarinnar er sem fyrr segir að greiða fyrir virkni hins innri stafræna markaðar. Til þess þarf samræmdar reglur og kerfi sem tryggir samstillta túlkun og framkvæmd, til að fyrirbyggja að misræmi komi upp sem geti truflað flæði upplýsinga yfir landamæri og torveldað ýmis viðskipti. Þá er leitast við að draga úr hættu á að einstök ríki kjósi að haga lögum sínum og reglum á þann hátt að til þeirra laðist fyrirtæki sem sækja í sem mest svigrúm og sem minnst eftirlit. Eyða á lagalegri óvissu í slíkum málum og koma á svokölluðu samræmingarkerfi. Það felur t.d. í sér að ábyrgðaraðili með dótturfélög í nokkrum ríkjum þarf aðeins að hafa samskipti við eftirlitsstjórnvald í því ríki þar sem hann hefur sínar höfuðstöðvar og mun hún taka eftirlitsákvarðanir í hans málum. Við slíka ákvarðanatöku geta eftirlitsstjórnvöld þurft að hafa samráð hvert við annað. Komi þá upp ágreiningur mun ný stofnun, Evrópska persónuverndarráðið, skera úr honum. Ætlunin er að framangreindar ráðstafanir muni draga úr kostnaði ábyrgðaraðila af því að uppfylla

lagaskyldur sínar. Þá á að auka samvinnu persónuverndarstofnana í aðildarríkjunum með það fyrir augum að auðvelda fyrirtækjum, einkum litlum og meðalstórum, að ná sem mestu úr þessum markaði, auk þess sem draga á úr kostnaði þeirra með því að heimila þeim að skilgreina áhættustig á grundvelli áhættumats og innleiða ráðstafanir í samræmi við það.

Reglugerðin er talsvert viðameiri en Evróputilskipunin um sama efni. Það skýrist að hluta til af því að formálsorð hennar eru óvenju löng eða 173 töluliðir í stað 72 liða í formála tilskipunarinnar. Formálinn er mikilvægur til fyllingar og skýringar efnisákvæðum reglugerðarinnar, en þar er m.a. útskýrt nánar inntak hugtaka og fjallað um leiðir sem mælt er með að aðildarríki fari til að ná markmiðum hennar. Þá eru efnisákvæði reglugerðarinnar 99 greinar í stað 33 greina í tilskipuninni. Um fjórðungur þeirra eru ákvæði sem lúta að nýju stofnana- og eftirlitskerfi sem reglugerðin setur á fót, samræmingarkerfinu og samstarfi eftirlitsstofnana í einstökum aðildarríkjum, svo og verkefnum Evrópska persónuverndarráðsins. Þá eru allmörg ákvæði með nýjum efnisreglum auk ítarlegri útfærslu á ýmsu sem kveðið er á um í tilskipuninni.

5. Tilefni og nauðsyn lagasetningar

5.1. Almennt

Markmið lagasetningarinnar er annars vegar að stuðla að því að vinnsla persónuupplýsinga sé í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og tryggja áreiðanleika og gæði slíkra upplýsinga og frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins. Hins vegar er markmiðið að lögfesta ákvæði ESB-reglugerðar um persónuvernd eins og hún var tekin upp í EES-samninginn og setja ýmsar sérreglur til fyllingar og viðbótar reglugerðinni eins og heimilt er samkvæmt nokkrum ákvæðum hennar

Það leiðir af EES-samstarfinu að taka ber reglugerðina upp í EES-samninginn, en skv. 7. gr. hans skal leiða texta reglugerðarinnar sem slíkan inn í landsrétt og íslensk stjórnvöld hafa ekki val um form eða aðferð við innleiðingu t.d. með umritun slíkra gerða. Reglugerðina verður því að lögfesta í heild sinni og ekki er sama svigrúm til staðar og þegar núgildandi lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 innleiddu efni tilskipunar ESB frá 1995. Við setningu laganna frá 2000 var sem fyrr segir að miklu leyti sótt fyrirmynd til norskra persónuverndarlaga um innleiðingu tilskipunarinnar eins og hún var tekin upp í EES-samninginn enda eru þessi tvö ríki í sömu stöðu sem aðilar að honum.

Persónuverndarreglugerð ESB hefur hins vegar þá sérstöðu, umfram reglugerðir ESB almennt, að hún veitir aðildarríkjum talsvert svigrúm til að setja sérreglur um tiltekin atriði, útfæra sum ákvæði hennar eða víkja frá þeim og í sumum tilvikum er skylt að festa ákveðin atriði í landslög. Í kafla 5.4. verður gerð nánari greining á því hvaða sérreglur reglugerðin gerir ráð fyrir að sett verði í landslög.

5.2. Þingsályktun um reglugerðina.

Þingsályktunartillaga til að heimila ríkisstjórninni að staðfesta fyrir Íslands hönd fyrirhugaða ákvörðun sameiginlegu EES-nefndarinnar var lögð fyrir Alþingi xx 2018**.** Alþingi samþykkti tillöguna xx 2018.

Með þingsályktuninni var ríkisstjórninni heimilað að staðfesta breytingar á xx. viðauka með aðlögun gerðarinnar. Þann xx 2018 tók sameiginlega EES-nefndin ákvörðun um upptöku gerðanna í EES-samninginn, þ.e. með ákvörðunum nr. xx/2018.

5.3. Þátttaka Íslands í Evrópska persónuverndarráðinu og aðlögun að EES-samningnum.

Samkvæmt 68. gr. reglugerðarinnar er sem fyrr segir nýrri stofnun komið á fót, Evrópska persónuverndarráðinu. Í því skulu eiga sæti yfirmenn eins eftirstjórnvalds hvers aðildarríkis og Evrópsku persónuverndarstofnunarinnar eða fulltrúar þeirra.

Fjallað er um verkefni ráðsins í 70. gr. reglugerðarinnar, en meginhlutverk þess er að tryggja samræmi í beitingu hennar. Persónuverndarráðið leysir af hólmi og tekur við þeim verkefnum starfshópsins samkvæmt 29. gr. tilskipunarinnar sem lýst var að framan, þ.e. útgáfu leiðbeininga og álita um túlkun ákvæða reglugerðarinnar. Til viðbótar fær ráðið allmörg önnur verkefni og valdheimildir, þar á meðal vald til þess að taka bindandi ákvarðanir gagnvart innlendum eftirlitsstofnunum í ákveðnum tilvikum. Í því tilliti hafa helst vaknað álitaefni um aðlögun fyrir EES-samninginn vegna ákvæða 63. – 67. gr. reglugerðarinnar um framkvæmd þess svokallaða samræmingarkerfis sem lýst var að framan. Kerfinu er komið á fót til að stuðla að samræmdri beitingu reglugerðarinnar í öllu Sambandinu. Við upptöku gerðarinnar EES-samninginn er gengið út frá því að kerfið hafi í för með sér aukna samvinnu á milli eftirlitsstofnana innan Evrópska efnahagssvæðisins. Af Íslands hálfu reynir þá á aðkomu Persónuverndar, sem er lögbært eftirlitsstjórnvald hér á landi samkvæmt ákvæðum reglugerðarinnar.

Til þess að tryggja rétta og samræmda beitingu reglugerðarinnar í hverju einstöku tilviki skal persónuverndarráðið samkvæmt 65. gr. hennar samþykkja bindandi ákvörðun í tengslum við lausn deilumála

milli eftirlitsstjórnvalda í samræmingarkerfinu. Við upptöku gerðarinnar voru ýmsir kostir skoðaðir í tengslum við aðlögun að stofnanakerfi hennar og hvernig mætti samræma það EES-samningnum. Ekki náðist samkomulag í samningaviðræðum milli EFTA-ríkjanna annars vegar og Evrópusambandsins hins vegar um að ná fram aðlögun gerðarinnar fyrir EFTA-ríkin sem byggðist á tveggja stoða kerfi EES-samningsins. Úr varð að velja þá leið sem kennd er við „fulla aðkomu Evrópska persónuverndarráðsins“. Í því felst að ráðið mun taka bindandi ákvarðanir gagnvart eftirlitsstjórnvaldi EFTA-ríkis innan EES. Þannig munu fulltrúar persónuverndarstofnana EFTA-ríkjanna innan EES sitja í Evrópska persónuverndarráðinu, án atkvæðisréttar, en með fullan tillögu- og málfrelsisrétt og afstaða fulltrúa EFTA ríkjanna verður skráð sérstaklega. Í þessu sambandi hefur verið vísað til fyrri fordæma varðandi þátttöku fulltrúa EFTA-ríkjanna innan EES í stjórnum stofnana ESB af svipuðu tagi. Þar má benda á þáttöku EFTA-ríkjanna í Evrópsku vinnuverndarstofnuninni og lyfjastofnuninni, þar sem þau hafa aðeins áheyrnaraðild en taka ekki þátt í atkvæðagreiðslu. Því mun Evrópska persónuverndarráðið taka bindandi ákvarðanir gagnvart eftirlitsstofnunum EFTA-ríkjanna, Persónuvernd hér á landi án þess að EFTA-ríkin sjálf hafi beina aðkomu að þeirri ákvörðun, nema með þátttöku í umræðum um hana á vettvangi ráðsins. Þá munu fulltrúar EFTA-ríkjanna hafa fulla aðkomu að rannsókn mála sem varða vinnslu persónuupplýsinga yfir landamæri.

Nánar verður fjallað um stjórnskipuleg álitaefni tengd framsali ríkisvalds í 8. kafla hér á eftir.

5.4. Setning sérreglna, takmarkana eða útfærslna á ákvæðum reglugerðarinnar.

Sem fyrr greinir hefur persónuverndarreglugerðin þá sérstöðu að hún veitir aðildarríkjum talsvert svigrúm til að setja sérreglur um tiltekin atriði, útfæra sum ákvæði hennar eða víkja frá þeim og í sumum tilvikum er skylt að festa ákveðin atriði sérstaklega í landslög. Í stórum dráttum má skipta þessum heimildum og skyldum til setningar sérreglna í landslögum í eftirfarandi fjóra flokka og jafnframt eru vísað til viðeigandi ákvæða reglugerðarinnar.

1) Heimild til nánari útfærslu á efni tiltekinna reglugerðarákvæða.

Í þennan flokk falla tiltekin ákvæði reglugerðarinnar þar sem kveðið er á um heimildir aðildarríkja til að útfæra nánari reglur innan ramma hennar. Ríkjum er hins vegar ekki skylt að setja slíkar reglur. Helstu ákvæði um þetta eru eftirfarandi: 2. og 3. mgr. 6. gr. um ítarlegri kröfur sem aðildarríki geta sett varðandi lögmæti vinnslu, 2.-4. mgr. 9. gr. um sérreglur tengdar vinnslu viðkvæmra persónuupplýsinga, 87. gr. um heimild til að útfæra reglur um kennitölur, 88. gr. um vinnslu í atvinnutengdu samhengi og 90. gr. um útfærslur á setningu reglna um þagnarskyldu ábyrgðar- eða vinnsluaðila.

2) Valkostir um að setja efnisreglur á tilteknum sviðum.

Í reglugerðinni eru víða settir fram valkostir fyrir aðildarríki um að setja efnisreglur um tiltekin atriði en innan ramma hennar, sem þau ráða hvort þau nýta eða ekki. Þannig er gert ráð fyrir því í 27. lið formálans að þótt gildissvið reglugerðarinnar nái til lifandi einstaklinga geti aðildarríki ákveðið að hún gildi einnig um persónuupplýsingar látinna manna. Samkvæmt 8. gr. geta aðildarríki ákveðið hvort þau hafa lægra aldursmark en 16 ára í tengslum við samþykki barns fyrir þjónustu í upplýsingasamfélaginu, en þó ekki lægra en 13 ár. Í 5. mgr. 36. gr. er ráðgert að aðildarríki geti sett áskilnað um að ábyrgðaraðilar þurfi leyfi eftirlitsstjórnvalds fyrir vinnslu tiltekinna upplýsinga. Samkvæmt 4. mgr. 37. gr. er heimilt að setja frekari ákvæði í lög um skyldur til að fyrirtæki hafi persónuverndarfulltrúa. Samkvæmt 5. mgr. 49. gr. geta lög aðildarríkis takmarkað miðlun sérstakra flokka persónuupplýsinga til þriðja lands eða alþjóðastofnunar á grundvelli mikilvægra almannahagsmuna. Samkvæmt 6. mgr. 58. gr. geta aðildarríki kveðið á um að eftirlitsstjórnvöld hafa fleiri valdheimilir en þær sem reglugerðin áskilur. Samkvæmt 1. og 2. mgr. 80. gr. geta lög aðildarríkis kveðið á um að einstaklingur veiti stofnunum eða samtökum umboð til að leggja fram kvörtun fyrir hans hönd til eftirlitsstjórnvalds og einnig um almennt fyrirsvar stofnana og samtaka fyrir hinn skráða. Þá er valkvætt samkvæmt 7. mgr. 58. gr. hvort aðildarríki heimili álagningu stjórnvaldssekta á stjórnvöld.

3) Svigrúm ríkja til að setja lög sem víkja frá ákvæðum reglugerðarinnar.

Reglugerðin veitir á nokkrum stöðum svigrúm til þess að vikið sé frá ýmsum grundvallarréttinum hins skráða. Þó eru sett ákveðin skilyrði fyrir því í hvaða tilgangi þessar undantekningar eru gerðar og hvað atriðum beri að hafa hliðsjón af í lagaákvæðum um efnið.

Samkvæmt 23. gr. reglugerðarinnar er heimilt í lögum aðildarríkis, sem ábyrgðaraðili eða vinnsluaðili persónuupplýsinga heyrir undir, að takmarka gildissvið þeirra skyldna og réttinda, sem um getur í 12.–22. gr. (um réttindi skráðs einstaklings) og í 34. gr. (tilkynningaskylda um öryggisbrot), og einnig í 5. gr. (meginreglur um vinnslu persónuupplýsinga) að nánari skilyrðum uppfylltum. Þá er í 89. gr. gert ráð fyrir því að aðildarríki geti kveðið á um undanþágur frá ýmsum réttindum hins skráða þegar vinnsla persónuupplýsinga fer fram vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi.

4) Skyldur sem hvíla á ríki til að setja sérstök atriði í lög eða reglur.
Fjórði flokkurinn lýtur að atriðum sem aðildarríkjum er skylt að innleiða með lögum. Hér vísast m.a. til 5. mgr. 38. gr. um þagnarskyldu persónuverndarfulltrúa, 1. mgr. 43. gr. um faggildingu vottunaraðila og allmargra atriða sem tengjast skipulagi, sjálfstæði og valdheimildum stjórnvalds sem ber ábyrgð á eftirliti og framkvæmd reglugerðarinnar og rakin eru í 51. – 54. gr. og 58. gr. reglugerðarinnar. Þá er í 84. gr. fjallað um skyldur aðildarríkja í tengslum við önnur viðurlög en stjórnvaldssektir og í 85. gr. er mælt fyrir um að setja skuli í lög ákvæði til að samræma vernd persónuupplýsinga og réttinn til tjáningar- og upplýsingafrelsis.

Um það hvernig sérreglur þessar birtast í ákvæðum frumvarpsins verður nánar fjallað í skýringum við einstaka greinar frumvarpsins.

6. Helstu breytingar sem frumvarpið hefur í för með sér

Þar sem frumvarpið mælir fyrir um að reglugerðin eins og hún var tekin upp í EES-samninginn, verði að landslögum verður hér gerð samantekt um helstu breytingar sem hún hefur í för með sér auk helstu sérreglna sem lagðar eru til í frumvarpinu að öðru leyti. Þótt ýmis kjarnaatriði tilskipunarinnar s.s. meginreglur um vinnslu persónuupplýsinga, réttindi hins skráða og skyldur ábyrgðaraðila standi áfram óbreytt í reglugerðinni eru þar ráðgerðar ýmsar grundvallarbreytingar og viðbætur við gildandi reglur. Hér á eftir er lýst helstu nýmælum og áherslum reglugerðarinnar sem lúta að réttindum einstaklinga sem m.a. birtist í auknum skyldum þeirra sem vinna með persónuupplýsingar gagnvart skráðum einstaklingum, og er ákvæðis reglugerðarinnar getið innan sviga.

* Fyrst má nefna nýmæli um landfræðilegt gildissvið reglugerðarinnar, en hún mun gilda um vinnslu allra fyrirtækja sem vinna með persónuupplýsingar skráðra einstaklinga á Evrópska efnahagssvæðinu. Þannig nær hún til allra fyrirtækja sem bjóða vöru og þjónustu til einstaklinga á hinum innri markaði án tillits til þess hvort vinnslan fer fram innan svæðisins eða ekki. Sem dæmi má nefna að hið samræmda regluverk mun ekki aðeins ná til evrópskra netþjónustufyrirtækja heldur einnig til annarra fyrirtækja utan Evrópu þegar þau vinna með persónuupplýsingar um einstaklinga sem staðsettir eru innan EES og um er að ræða boð um vörur eða þjónustu eða eftirlit með hegðun þeirra. Þannig er vernd allra einstaklinga á svæðinu aukin. (3. gr.)

* Almennt má segja að reglugerðin leggi mun ríkari skyldur en tilskipunin á ábyrgðaraðila og vinnsluaðila við vinnslu persónuupplýsinga, svokallaðar ábyrgðarskyldur, einkum um ráðstafanir til að tryggja öryggi við vinnslu persónuupplýsinga.

* Ný meginregla svokölluð öryggisregla, bætist við þær fimm meginreglur sem tilskipunin hefur byggst á, þ.e. lögmætis-, tilgangs-, meðalhófs-, áreiðanleika- og varðveislureglunar. **(**f-liður, 1. mgr. 5. gr.)

* Önnur ný meginregla sem endurspeglast skýrt víða í ákvæðum reglugerðarinnar er aukin ábyrgðarskylda. Í því felst ekki aðeins að ábyrgðaraðili beri frumábyrgð á því að farið sé að reglunum eins og á við samkvæmt núgildandi reglum heldur þarf hann jafnframt að geta sýnt fram á það. (2. mgr. 5. gr.)

* Skilyrði fyrir samþykki einstaklinga fyrir vinnslu persónuupplýsinga eru gerð strangari og fyrirtækjum er skylt að gera skilmála fyrir samþykki gagnsærri, aðgengilegri og á að hafa þá á skiljanlegu máli. (7. gr.)

* Börnum er veitt sérstök vernd þar sem afla þarf samþykkis foreldra áður en börn undir 16 ára aldri skrá sig í þjónustu í upplýsingasamfélaginu. Þó er heimilt að kveða á um lægra aldursmark í landslögum, en þó ekki lægra en 13 ár. (8. gr.)

* Réttur einstaklinga til aðgangs að persónuupplýsingum er viðbót við réttindi hins skráða. Auk þess er ábyrgðaraðila gert skylt að afhenda hinum skráða afrit upplýsinga um hann á rafrænu formi sé þess óskað. (15. gr.)

* Rétturinn til að gleymast er orðaður sérstaklega, en hann tryggir rétt hins skráða til að upplýsingar um hann verði afmáðar þegar þær eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun þeirra. Frá þessum rétti eru þó undantekningar, þar á meðal á grundvelli almannahagsmuna. (17. gr.)

* Skráðum einstaklingi er tryggður réttur til að fá persónuupplýsingar um sig sjálfan afhentar á aðgengilegu formi frá ábyrgðaraðila og til að láta flytja þær til annars ábyrgðaraðila. (20. gr.)

* Lögð er sú skylda á ábyrgðaraðila að tryggja bæði innbyggða og sjálfgefna persónuvernd með tæknilegum ráðstöfunum sem m.a. miða að því að sjálfgefið sé að einungis þær upplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar. (25. gr.)

* Öllum ábyrgðaraðilum er skylt að halda skrá yfir vinnslustarfsemi sem fer fram á ábyrgð þeirra sem geymi upplýsingar sem nánar eru taldar upp í reglugerðinni. (30. gr.)

* Ábyrgðaraðila er skylt að tilkynna til Persónuverndar ef öryggisbrot á sér stað við vinnslu persónuupplýsinga án ótilhlýðilegrar tafar og eigi síðar en 72 klst. eftir að hann verður brotsins var, nema ólíklegt þyki að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga. (33. gr.)

* Ef líklegt er að tiltekin tegund vinnslu hafi í för með sér mikla áhættu fyrir réttindi skráðra einstaklinga skal ábyrgðaraðilinn láta fara fram sérstakt mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga.(35. gr.)

* Stjórnvöldum svo og tilteknum fyrirtækjum sem vinna með ákveðna flokka persónuupplýsinga og umfangsmikið magn er skylt að tilnefna persónuverndarfulltrúa. Reglugerðin setur fram nánari skilyrði um stöðu, hlutverk og hæfni slíkra fulltrúa. (37. og 38. gr.)

***** Reglugerðin gerir ráð fyrir því að persónuverndarstofnanir í öllum ríkum verði efldar verulega, sjálfstæði tryggt og valdheimildir og eftirlitsúrræði stóraukin (57. og 58. gr.)

***** Mælt er fyrir um háar stjórnvaldssektir vegna brota á lögunum, allt að 20 millj. evra fyrir alvarlegustu brot (2,2 milljarðar kr.) eða 4% af heildarveltu fyrirtækis, hvort heldur er hærra. Persónuvernd sem er eftirlitsstjórnvald hér á landi leggur á stjórnvaldssektir. Heimilt verður að leggja stjórnvaldssektir á einstaklinga og lögaðila, þar með taldar opinberar stofnanir. (3. og 5. mgr. 83. gr.)

Allmörg ákvæði reglugerðarinnar endurspegla hitt meginmarkmiðið með setningu hennar, þ.e. að greiða fyrir frjálsu flæði persónuupplýsinga og virkni hins innri stafræna markaðar og tryggja samræmt eftirlit og framkvæmd. Í því skyni er komið á samræmda eftirlitskerfinu milli eftirlitsstofnana á svæðinu sem áður er getið. Samræmingarkerfið felur t.d. í sér að ábyrgðaraðili með dótturfélög í nokkrum ríkjum þarf aðeins að hafa samskipti við eftirlitsstofnun í því ríki þar sem hann hefur sínar höfuðstöðvar og mun hún taka eftirlitsákvarðanir í hans málum þótt vinnsla fari fram að einhverju leyti í öðrum ríkjum. (63.- 67.gr.)

Evrópska persónuverndarráðið er sett á fót með reglugerðinni. Í ráðinu sitja fulltrúar frá eftirlitsstofnun hvers aðildarríkis og fulltrúi Evrópsku persónuverndarstofnunarinnar. Persónuverndarráðinu er ætlað að tryggja samræmi í beitingu reglugerðarinnar, því er m.a. ætlað að gefa út viðmiðunarreglur, álit og tilmæli í tengslum við framkvæmd reglugerðarinnar. Þá getur ráðið skorið úr deilumálum sem kunna að rísa eftirlitsstjórnvalda í aðildarríkjunum með bindandi niðurstöðu. (68. -70. gr.)

7. Meginefni frumvarpsins og efnistök.

Með frumvarpinu er annars vegar stefnt að því að lögfesta ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 eins og hún var tekin upp í EES-samninginn og hins vegar að setja frekari ákvæði til fyllingar og viðbótar reglugerðinni þar sem hún heimilar eða mælir fyrir um að settar séu sérreglur í landslög. Samþykkt frumvarps þessa er forsenda fyrir þátttöku Íslands í samevrópsku regluverki um persónuvernd og vinnslu persónuupplýsinga

Þá hefur frumvarpið sem fyrr segir það efnislega markmið, eins og núgildandi lög um efnið að stuðla að því að með persónuupplýsingar sé farið í samræmi við grundvallarsjónarmið og reglur um persónuvernd og friðhelgi einkalífs og að tryggja áreiðanleika og gæði slíkra upplýsinga og frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins.

Við samningu frumvarpsins voru tveir valkostir uppi um efnistök í nýjum persónuverndarlögum. Fyrri valkosturinn var að setja, samhliða lögfestingu reglugerðarinnar, aðeins ákvæði í ný persónuverndarlög með þeim sérreglum, viðbótum og útfærslum sem mælt er fyrir um í reglugerðinni sjálfri og lýst var í kafla 5.4. að ofan. Seinni valkosturinn var að setja lög sem gæfu heildstæða mynd af reglum á réttarsviðinu og þá óhjákvæmilega með endurtekningum að einhverju marki á ákveðnum kjarnaákvæðum reglugerðarinnar og tilvísunum til ákvæða hennar.

Ljóst er að samkvæmt 7. gr. EES-samningsins ber ríkjum að leiða texta reglugerða inn í landslög í heild sinni og meginreglan er því að óheimilt sé að umorða eða breyta texta þeirra í innlendum lagatexta. Af skoðun á fyrirliggjandi frumvörpum um innleiðingu reglugerðarinnar í Noregi, Danmörku og Svíþjóð sést að þau miðast við fyrri valkostinn. Þótt frumvörpin séu misítarleg stefna þau aðeins að því að vera til viðbótar við eða fyllingar reglugerðinni sem verður þá meginréttarheimildin.

Það var mat starfshópsins við ákvörðun um efnistök og framsetningu frumvarpsins að ný persónuverndarlög yrðu bæði óaðgengileg og torskiljanleg almenningi ef þau geymdu aðeins sérreglur og undantekningar frá reglugerðinni. Til þess að gefa nýrri persónuverndarlöggjöf ákveðið heildaryfirbragð er sú leið því farin að setja inn í frumvarpið, auk sérreglna, undantekninga og viðbóta við reglugerðina, helstu hugtök og efni nokkurra kjarnaákvæða hennar. Jafnframt er leitast við að fylgja orðalagi hennar svo ekki komi upp misræmi og vísa jafnan til frekari reglna um efnið í ákvæðum reglugerðarinnar. Frumvarpið þjónar þannig bæði þeim tilgangi að lögfesta reglugerðina í heild sinni en einnig að setja heildarlög um efnið sem verði henni til fyllingar og viðbótar. Þá er mikilvægt að allar reglur um efnið verði aðgengilegar á einum stað og reglugerðin verði birt sem fylgiskjal með frumvarpinu.

Í þessu sambandi var sérstaklega haft í huga að hin nýja Evrópulöggjöf hefur víðtæk áhrif fyrir samfélagið allt en ekki t.d. sérhæfð svið í atvinnulífinu einvörðungu. Þá var tekið mið af 8. lið formála reglugerðarinnar. Þar segir að þegar kveðið sé á um það í reglugerðinni að setja megi fram í lögum aðildarríkja skýringar eða

takmarkanir á reglum hennar sé aðildarríkjum heimilt að fella inn í landslög sín þætti úr reglugerðinni að því marki sem nauðsynlegt sé vegna samræmis og til þess að gera ákvæði landslaga skiljanleg þeim sem þau eiga við um.

Þá má bæta við að í frumvarpinu er enn að finna ýmsar sérreglur um tiltekin svið sem þegar er að finna í núgildandi lögum nr. 77/2000. Þar á meðal eru ákvæði um rafræna vöktun, vinnslu upplýsinga um fjárhagsmálefni og lánstraust, bannskrá Þjóðskrár Íslands o.fl. Ætla má að sum þessara ákvæða ættu frekar heima í sérlögum, en ákveðið var að viðhalda þeim inni í lögum um persónuvernd á meðan ekki er ljóst hvort þau verði fest annars staðar í almenn lög, því ella skapast mögulega tímabundið lagalegt tómarúm og lakari réttarvernd.

Í texta reglugerðarinnar eru hugtök sem ætlað er að ná til aðstæðna og hugtaka í lagakerfum allra aðildarríkjanna. Við þýðingu ESB-gerða, þar með talinnar reglugerðarinnar um persónuvernd, hefur þýðingamiðstöð utanríkisráðuneytisins þannig notast við samræmdar og staðlaðar þýðingar hugtaka sem ætlað er að vera óháðar landsrétti einstaka ríkja. Við færslu hugtaka reglugerðarinnar inn í texta frumvarps þessa hefur sú leið verið valin að nota viðurkennd íslensk lagaheiti sem hefð er fyrir að nota um sömu efni og er þá í nokkrum tilvikum vikið frá opinberri þýðingu hennar. Sem dæmi má nefna að hugtakið „stjórnsýslusekt“ sem fram kemur í 83. gr. reglugerðarinnar og er þýðing á enska hugtakinu „administrative fine“, hefur samkvæmt langri hefð í íslensku lagamáli verið kallað „stjórnvaldssekt“. Sama er að segja um hugtakið „eftirlitsyfirvald“ sem kemur víða fyrir reglugerðinni og er þýðing á enska hugtakinu „supervisory authority“. Í íslensku lagamáli hefur skapast löng hefð fyrir því að nota orðið „eftirlitsstjórnvald“ í stað þess að vísa til „eftirlitsyfirvalds“ sem fyrirfinnst vart í íslenskum lögum. Þetta hefur m.a. verið gert í allmörgum lögum sem ætlað er að innleiða ESB-gerðir þar sem orðið eftirlitsyfirvald er notað í opinberri þýðingu á frumtexta gerða. Dæmi um slíka orðnotkun má sjá í lögum um fjármálafyrirtæki nr. 161/2002 þar sem ávallt er rætt um Fjármálaeftirlitið hér á landi og sambærilegar stofnanir á Evrópska efnahagssvæðinu sem „eftirlitsstjórnvöld“. Af þessari ástæðu er í frumvarpi þessu notað orðið „eftirlitsstjórnvald“ um stofnunina Persónuvernd hér á landi og hliðstæðar stofnanir á Evrópska efnahagssvæðinu enda hefur það beina tilvísun til hugtaksins „stjórnvald“ í stjórnsýslulögum og lögformlega merkingu. Í skýringum við einstök ákvæði frumvarpsins verður nánar fjallað um þau tilvik þar sem orðnotkun kann að víkja frá þýðingu texta reglugerðarinnar vegna hefðar sem ákveðin hugtök hafa áunnið sér í íslensku lagamáli, en það þjónar einnig því markmiði að gera lögin skiljanleg og aðgengileg almenningi.

Frumvarpið skiptist í átta kafla sem eru eftirfarandi I. Markmið, skilgreiningar og gildissvið, II. Almennar reglur um vinnslu, III. Réttindi hins skráða og takmarkanir á þeim, IV. Almennar reglur um skyldur ábyrgðaraðila og vinnsluaðila og öryggi persónuupplýsinga. V. Mat á áhrifum á persónuvernd, leyfisskylda o.fl. VI. Persónuverndarfulltrúar og vottunaraðilar. VII. Eftirlit og viðurlög. VIII. Gildistaka o.fl. Er hér í meginatriðum tekið mið af efnislegri uppbyggingu reglugerðarinnar og lykilákvæðum hennar í hverjum kafla og þannig gefa lögin ákveðna heildarmynd af efni hennar. Ekki eru þó fest í lögin sérákvæði um samstarf og samræmingarhlutverk, verkefni og valdheimildir Evrópska persónuverndarráðsins samkvæmt VII. kafla reglugerðarinnar, en í því tilliti má minna á að ákvæði reglugerðarinnar sem slík verða að lögum samkvæmt frumvarpi þessu.

Í umfjöllum um einstök ákvæði hér á eftir verður nánar lýst efni ákvæða reglugerðarinnar og lagafrumvarpsins, þeim breytingum sem þau hafa í för með sér frá gildandi lögum og þeim sérreglum og undanþágum sem lagðar eru til á grundvelli heimilda í reglugerðinni. Við skýringu á ákvæðum reglugerðarinnar verður m.a. sérstaklega litið til formálsorða hennar sem geyma ítarlegar skýringar á hugtökum og einstökum greinum reglugerðarinnar.