

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 og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) eins og hún var tekin upp í samninginn um Evrópska efnahagssvæðið. Þá eru með lögnum sett frekari ákvæði til fyllingar og viðbótar reglugerðinni og sérreglur um persónuvernd.

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 (almenna persónuverndarreglugerðin) eins og hún er tekin upp í samninginn um Evrópska efnahagssvæðið skulu hafa lagagildi hér á landi með þeim aðlögunum sem leiðir af ákvörðun sameiginlegu EES-nefndarinnar um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 (sem inniheldur skrána sem kveðið er á um í 101. gr.) við EES-samninginn

Reglugerðin og drög að ákvörðun sameiginlegu EES-nefndarinnar eru birt sem fylgiskjöl 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 tilvisun 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. Lífkennuupplýsingar, 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 með persónuupplýsingar á vegum ábyrgðaraðila.
8. *Samþykki*: Öpvinguð, 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 ólögmatrar 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 5 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 dómssvald 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 refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoðryggi.

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., 32., 40.-43. og 82. gr. reglugerðarinnar og 48. og 51. gr. laga þessara.

7. gr.

Landfræðilegt gildissvið.

Lögin og reglugerðin gilda um vinnslu persónuupplýsinga í tengslum við starfsemi ábyrgðaraðila eða vinnsluaðila með staðfestu hér á landi óháð því hvort vinnslan sjálf fer fram á Evrópska efnahagssvæðinu eða ekki.

Lögin og reglugerðin gilda um vinnslu persónuupplýsinga um skráðra einstaklinga sem eru hér á landi og fer fram í starfsemi ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu á Evrópska efnahagssvæðinu, eða 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 skjálavistun 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 málefnum, 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 stjórnmalaleg, 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 afdráttarlaust 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 afdráttarlaust samþykki sitt eða vinnslan sé nauðsynleg í þágu lögmætra hagsmuna sem auðsjáanlega vega þyngra en grundvallarréttindi og frelsi hins skráða.

Upplýsingum skv. 3. mgr. má ekki miðla nema hinn skráði veiti til þess afdráttarlaust samþykki sitt. Þó má miðla upplýsingum án samþykkis sé það nauðsynlegt í þágu lögmætra hagsmuna hins opinbera eða einkaaðila sem vega þyngra en þeir hagsmunir sem eru af leynd um upplýsingarnar, 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 leyfis skylda 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. Skal ráðherra staðfesta slíkar ákvarðanir og 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. almannaoöryggis;
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 almannaoöryggi;
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, tölfraði eða skjalavistunar í þágu almannahagsmuna.

Vinnsla vegna rannsókna á sviði vísinda eða sagnfræði, í tölfraðilegum 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 tölfraðilegum 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.

Heimilt er að afhenda opinberu skjalasafni upplýsingar sem falla undir lög þessi í samræmi við ákvæði laga um opinber skjalasöfn.

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 framur 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 skrá 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.

Skýlt 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 skýlt að fram komi á ótvíræðan hátt um leið og hann er móttakinn 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 Þjóðskrár 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 á 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.

Skyldur til að halda skrá yfir vinnslustarfsemi skulu ekki eiga við um fyrirtæki eða stofnun sem hefur færri en 250 starfsmenn nema vinnslan, sem innt er þar af hendi, sé líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, vinnslan sé ekki tilfallandi eða taki til viðkvæmra persónuupplýsinga skv. 1. mgr. 11. gr. laganna eða persónuupplýsinga er varða sakfellingar í refsímálum og refsiverð eins og um getur í 12. gr. laganna.

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, leyfis skylda 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 reglugerðina, einkum ef ábyrgðaraðili hefur ekki greint eða dregið úr áhættunni með fullnægjandi hætti, skal stofnunin, innan átta vikna frá því að henni berst beiðni um samráð, veita ábyrgðaraðila og, eftir atvikum, vinnsluaðila skriflega ráðgjöf og getur 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.

Leyfis skylda 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 leyfis skylda falli brott þegar settar hafa verið almennar reglur og öryggisstaðlar sem fylgja skuli við slíka vinnslu.

Persónuvernd setur reglur um leyfis skyldu skv. 1. mgr.

32. gr.

Forsendur leyfisveitingar o.fl.

Ábyrgðaraðila má aðeins veita leyfi skv. 31. gr. laga þessara ef líklegt er að hann geti fullnægt skyldum sínum samkvæmt reglugerðinni og lögnum 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. 33. 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. 31. 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 lögnum, 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.

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 **eða** upplýsinga sem varða sakfellingar í refsimálum og refsiverð brot.

Fyrirtækjamstæðu er heimilt að tilnefna 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.

Pagnarskylda persónuverndarfulltrúa.

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

Pagnarskylda 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 stjórnarsýsla.

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 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 þekkingu á málefnum tengdum persónuvernd og menntun sem nýtist á því sviði. Ráðherra ákveður laun stjórnarmanna.

Hlutverk stjórnar er að móta áherslur í starfi í samráði við forstjóra og fylgjast með starfsemi og rekstri Persónuverndar. Þá tekur stjórn meiriháttar efnislegar eða stefnumótandi ákvarðanir í málum sem stofnunin hefur til meðferðar, þar á meðal um álagningu dagsekta og stjórnvaldssekta. Stjórn Persónuverndar setur nánari reglur um skiptingu starfa á milli stjórnar og skrifstofu stofnunarinnar og framkvæmd þeirra.

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 ber ábyrgð á og annast daglega stjórnun á starfsemi, fjárreiðum og rekstri stofnunarinnar og ræður starfsmenn 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 vinnsluaðgerða 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 háttarnisreglur skv. 1. mgr. 40. gr. reglugerðarinnar og gefa álit á og samþykkja háttarnisreglur 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 háttarnisreglna 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. birta árlega skýrslu um starfsemi sína;

17. 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 laga þessara og 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 viðvörðun 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, álitserðir fyrir Alþingi eða stjórnvöld, eða aðra aðila um hvert það málefni sem tengist vernd persónuupplýsinga;
 3. til að leyfa vinnslu þar sem fyrirframheimildir er krafist samkvæmt lögum;
 4. til að gefa álit og samþykkja drög að háttarnisreglum skv. 5. mgr. 40. gr. reglugerðarinnar;
 5. til að veita umsagnir vegna faggildingar vottunaraðila skv. 43. gr. reglugerðarinnar 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

Stjórnarmönnum og starfsmönnum Persónuverndar, svo 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 liða 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 ábyrgðaraðila eða vinnsluaðila 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 eftirlitsfyrvaldinu 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 háttisreglur 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 **sektum** eða 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.

Um upptöku ávinnings af broti og hluta sem notaðir eru til að fremja brot fer eftir ákvæðum VII. kafla A almennra hegningarlaga.

49. gr.

Kæra til lögreglu.

Persónuvernd metur hvort meint brot einstaklings samkvæmt 48. gr. skuli kært til lögreglu eða hvort hjá stofnuninni fari fram á því rannsókn sem lykti með stjórnvaldsákvörðun. 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 ákærvaldi í té upplýsingar og gögn sem stofnunin hefur aflað og tengjast brotum skv. 48. gr. Persónuvernd er heimilt að taka þátt í aðgerðum lögreglu sem varða rannsókn þeirra brota

Lögreglu og ákærvaldi er heimilt að láta Persónuvernd í té upplýsingar og gögn sem þau hafa aflað og tengjast brotum skv. 48. gr. Lögreglu er einnig heimilt að taka þátt í aðgerðum Persónuverndar sem varða rannsókn þeirra brota sem tilgreind eru í 46. gr. laganna.

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 stjórnvaldssektar eða kærur 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. Ábyrgðaraðili eða vinnsluaðili 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 vinnslu persónuupplýsinga og öryggisráðstafanir í tiltekinni starfsemi eða 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.

I.

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

II.

Reglugerðir svo og reglur, fyrirmæli og leyfi sem Persónuvernd eða ráðherra hafa gefið út á grundvelli laga nr. 77/2000 skulu halda gildi, enda fari þau ekki í bága við lög þessi og reglugerðina.

III.

Þrátt fyrir 6. mgr. 4. gr. laga þessara gilda 2. mgr. 1. gr., 3. gr., 1.–5. og 7. mgr. 4. gr., 5. gr., 1. mgr. 7. gr., 8.–13. gr., 1. og 2. mgr. 14. gr., 1. og 3. tölul. 3. mgr. sömu greinar, 22. gr., 23.

gr., 25. gr., 27.–33. gr., VI. kafli, 38.–45. gr., 48. gr. og 51.–53. gr. laganna um vinnslu persónuupplýsinga, sem varða almannaöryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu, þar til tilskipun (ESB) 2016/680 hefur verið innleidd í íslenskan rétt. Um framangreinda vinnslu, og fram að sama tímamarki, gilda einnig fyrirmæli 1. mgr. 20. gr. í lögum þessum um rétt hins skráða til að fá rangar, villandi eða ófullkomnar persónuupplýsingar um sig leiðréttar .

Fylgiskjal I

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 (almenna persónuverndarreglugerðin)

EVROPUÞINGIÐ OG RÁÐ EVRÓPUSAMBANDBSINS HAFAR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins, einkum 16. gr.,

með hliðsjón af tillögu framkvæmdastjórnar Evrópusambandsins,

eftir að hafa lagt drög að lagagerð fyrir þjóðþingin,

með hliðsjón af álitum efnahags- og félagsmálanefndar Evrópusambandsins ⁽¹⁾,

með hliðsjón af álitum svæðanefndarinnar ⁽²⁾,

í samræmi við almenna lagasetningarmeðferð ⁽³⁾,

og að teknu tilliti til eftirfarandi:

1) Vernd einstaklinga í tengslum við vinnslu persónuupplýsinga telst til grundvallarréttinda. Í 1. mgr. 8. gr. sáttmála Evrópusambandsins um grundvallarréttindi („sáttmálanum um grundvallarréttindi“) og í 1. mgr. 16. gr. sáttmálans um starfshætti Evrópusambandsins er kveðið á um að sérhver einstaklingur eigi rétt á að persónuupplýsingar um hann njóti verndar.

2) Meginreglur og reglur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga þeirra ættu að virða grundvallarréttindi og frelsi einstaklinga án tillits til ríkisfangs þeirra eða búsetu, einkum rétt þeirra til verndar persónuupplýsingum. Reglugerð þessari er ætlað að stuðla að því að koma á svæði frelsis, öryggis og réttlætis og efnahagsbandalagi, að efnahagslegri og félagslegri þróun, að styrkingu og aukinni samleitni efnahagskerfa sem mynda innri markaðinn og að velferð einstaklinga.

⁽¹⁾ Stjóð. ESB C 229, 31.7.2012, bls. 90.

⁽²⁾ Stjóð. ESB C 391, 18.12.2012, bls. 127.

⁽³⁾ Afstaða Evrópuþingsins frá 12. mars 2014 (hefur enn ekki verið birt í Stjórnartíðindunum) og afstaða ráðsins eftir fyrstu umræðu frá 8. apríl 2016 (hefur enn ekki verið birt í Stjórnartíðindunum). Afstaða Evrópuþingsins frá 14. apríl 2016.

- 3) Í tilskipun Evrópuþingsins og ráðsins 95/46/EB ⁽⁴⁾ er leitast við að samræma vernd grundvallarréttinda og frelsis einstaklinga í tengslum við vinnslustarfsemi og tryggja frjálst flæði persónuupplýsinga milli aðildarríkja.
- 4) Vinnsla persónuupplýsinga ætti að hafa það að markmiði að þjóna mannkyninu. Rétturinn til verndar persónuupplýsingum er ekki ófrávikjanlegur, hann þarf að ígrunda í tengslum við hlutverk hans í samfélaginu og vega hann og meta gagnvart öðrum grundvallarréttindum í samræmi við meðalhöfsregluna. Í þessari reglugerð eru öll grundvallarréttindi og mannfrelsi virt og þeim meginreglum fylgt sem eru viðurkenndar í sáttmálanum um grundvallarréttindi eins og þær koma fram í sáttmálunum, einkum varðandi friðhelgi einkalífs og fjölskyldu, heimilis og samskipta, vernd persónuupplýsinga, hugsana-, samvisku- og trúfrelsi, tjáningar- og upplýsingafrelsi, frelsi til atvinnurekstrar, rétt til skilvirks úrræðis til að leita réttar síns og réttlátrar málsmeðferðar fyrir dómi og fjölbreytni menningar, trúarbragða og tungumála.
- 5) Með þeirri efnahagslegu og félagslegu aðlögun, sem fylgir starfsemi innri markaðarins, hefur flæði persónuupplýsinga yfir landamæri aukist verulega. Skipti á persónuupplýsingum milli opinberra aðila og einkaaðila, þ.m.t. einstaklinga, samtaka og fyrirtækja í Sambandinu, hafa farið vaxandi. Samkvæmt lögum Sambandsins ber yfirvöldum í aðildarríkjunum að starfa saman og skiptast á persónuupplýsingum til að þau geti rækt skyldur sínar og framkvæmt verkefni fyrir hönd yfirvalda í öðru aðildarríki.
- 6) Hröð tækniþróun og hnattvæðing hafa leitt til nýrra viðfangsefna varðandi vernd persónuupplýsinga. Umfang söfnunar og miðlunar persónuupplýsinga hefur aukist verulega. Tæknin gerir jafnt einkafyrirtækjum sem opinberum yfirvöldum kleift að nýta persónuupplýsingar við starfsemi sína í áður óþekktum mæli. Einstaklingar gera í auknum mæli persónuupplýsingar aðgengilegar öllum og á alþjóðavísu. Tæknin hefur breytt bæði efnahagskerfinu og félagslífi fólks og ætti að greiða enn frekar fyrir frjálsu flæði persónuupplýsinga innan Sambandsins og miðlun þeirra til þriðju landa og alþjóðastofnana, jafnframt því að tryggja öfluga vernd upplýsinganna.
- 7) Þessi þróun kallar á að komið verði á fót öflugum og heildstæðari ramma um persónuvernd í Sambandinu og honum fylgt kröftuglega eftir, með hliðsjón af mikilvægi þess að skapa traust sem gerir hinu stafræna hagkerfi kleift að þróast á öllum innri markaðnum. Einstaklingar ættu að stjórna eigin persónuupplýsingum. Efla ætti réttarvissu og fyrirsjáanleika gagnvart einstaklingum, rekstraraðilum og opinberum yfirvöldum.
- 8) Þegar kveðið er á um það í þessari reglugerð að setja megi fram í lögum aðildarríkja skýringar eða takmarkanir á reglum hennar er aðildarríkjum heimilt að fella inn í landslög sín þætti úr þessari reglugerð að því marki sem nauðsynlegt er vegna samræmis og til þess að gera ákvæði landslaga skiljanleg þeim sem þau eiga við um.
- 9) Markmið og meginreglur tilskipunar 95/46/EB standa enn fyrir sínu en hún hefur ekki náð að sporna gegn sundurlausri framkvæmd persónuverndar innan Sambandsins, réttaróvissu eða þeim útbreiddu hugmyndum meðal almennings að fyrir hendi sé veruleg áhætta fyrir vernd einstaklinga, einkum í tengslum við Netnotkun. Réttindi og frelsi einstaklinga, einkum rétturinn til verndar persónuupplýsingum, njóta mismikillar verndar í aðildarríkjunum í tengslum við vinnslu persónuupplýsinga og getur það hindrað frjálst flæði persónuupplýsinga um Sambandið. Þessi munur getur 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 má rekja til þess mismunar sem er á framkvæmd og beitingu tilskipunar 95/46/EB.
- 10) Til þess að tryggja einstaklingum samræmda og öfluga vernd og ryðja úr vegi hindrunum á flæði persónuupplýsinga innan Sambandsins ætti vernd réttinda og frelsis einstaklinga í tengslum við vinnslu slíkra upplýsinga að vera sambærileg í öllum aðildarríkjunum. Tryggja ætti alls staðar í Sambandinu samræmda og einsleita beitingu reglna um vernd grundvallarréttinda og frelsis einstaklinga í tengslum við

⁽⁴⁾ Tilskipun Evrópuþingsins og ráðsins 95/46/EB frá 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga (Stjóð. EB L 281, 23.11.1995, bls. 31).

vinnslu persónuupplýsinga. Að því er varðar vinnslu persónuupplýsinga til þess að fullnægja lagaskyldu ætti aðildarríkjunum að vera 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 láréttar 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. Þessi reglugerð veitir aðildarríkjunum einnig ákveðið svigrúm til að skilgreina reglur sínar, m.a. varðandi vinnslu sérstakra flokka persónuupplýsinga („viðkvæmra upplýsinga“). Hvað þetta varðar útilokar þessi reglugerð ekki að í lögum aðildarríkjanna sé mælt fyrir um aðstæður sem réttlæta sérstaka vinnslu, þar sem m.a. er skilgreint nánar með hvaða skilyrðum vinnsla persónuupplýsinga sé lögmæt.

- 11) Til að tryggja skilvirka vernd persónuupplýsinga alls staðar í Sambandinu þarf að styrkja og setja fram með ítarlegum hætti réttindi skráðra einstaklinga og skyldur þeirra sem vinna persónuupplýsingar og taka ákvarðanir um vinnslu þeirra, svo og samsvarandi heimildir til að hafa eftirlit með og tryggja að farið sé að reglum um vernd persónuupplýsinga, og setja fram sambærileg viðurlög vegna brota í aðildarríkjunum.
- 12) Í 2. mgr. 16. gr. sáttmálans um starfshætti Evrópusambandsins er Evrópuþinginu og ráðinu veitt heimild til að mæla fyrir um reglur er varða vernd einstaklinga með tilliti til vinnslu persónuupplýsinga og um reglur er varða frjálsa miðlun slíkra upplýsinga.
- 13) Til að tryggja samræmda vernd einstaklinga alls staðar í Sambandinu og koma í veg fyrir að misræmi hamli frjálsri miðlun persónuupplýsinga á innri markaðnum er þörf á reglugerð sem skapar réttarvissu og gagnsæi gagnvart rekstraraðilum, þ.m.t. örfyrirtækjum, litlum og meðalstórum fyrirtækjum, tryggir einstaklingum í öllum aðildarríkjum sömu lagalega framfylgjanlegu réttindi og skyldur og leggur samsvarandi ábyrgð á herðar ábyrgðaraðilum og vinnsluaðilum, og tryggir samræmt eftirlit með vinnslu persónuupplýsinga og sambærileg viðurlög í öllum aðildarríkjum, sem og skilvirkt samstarf milli eftirlitsyfirvalda einstakra aðildarríkja. Eðlileg starfsemi innri markaðarins krefst þess að ekki séu settar takmarkanir eða lagt bann við frjálsri miðlun persónuupplýsinga innan Sambandsins af ástæðum sem varða vernd einstaklinga í tengslum við vinnslu persónuupplýsinga. Með hliðsjón af sérstökum aðstæðum örfyrirtækja, lítilla og meðalstórra fyrirtækja er sett fram undanþága í þessari reglugerð varðandi skráahald fyrirtækja með færri en 250 starfsmenn. Enn fremur eru stofnanir og aðilar Sambandsins og aðildarríkin og eftirlitsyfirvöld þeirra hvött til að taka tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja við beitingu þessarar reglugerðar. Hugtökin örfyrirtæki, lítið og meðalstórt fyrirtæki ættu að byggjast á 2. gr. viðaukans við tilmæli framkvæmdastjórnarinnar 2003/361/EB ⁽⁵⁾.
- 14) Sú vernd, sem þessi reglugerð veitir í tengslum við vinnslu persónuupplýsinga, ætti að gilda um einstaklinga án tillits til ríkisfangs eða búsetu. Þessi reglugerð nær ekki yfir vinnslu persónuupplýsinga er varða lögaðila, einkum fyrirtæki sem stofnuð eru sem lögaðilar, þ.m.t. upplýsinga um heiti lögaðila, rekstrarform hans og samskiptaupplýsingar.
- 15) Til að komast hjá því að fram komi alvarleg hætta á að reglur verði sniðgengnar ætti vernd einstaklinga að vera tæknilega hlutlaus og ekki háð þeim aðferðum sem notaðar eru. Vernd einstaklinga ætti að eiga við um sjálfvirka jafnt sem handvirka vinnslu persónuupplýsinga ef upplýsingarnar eru varðveittar eða ráðgert er að varðveita þær í skráningarkerfi. Skrár eða skráasöfn, sem og forsiður þeirra, sem eru ekki skipulögð samkvæmt tilteknum viðmiðunum, ættu ekki að falla undir gildissvið þessarar reglugerðar.
- 16) Þessi reglugerð á ekki við um vernd grundvallarréttinda og mannfrelsis eða frjálst flæði persónuupplýsinga í tengslum við starfsemi sem fellur utan gildissviðs laga Sambandsins, s.s. starfsemi er varðar þjóðaröryggi. Þessi reglugerð á ekki við um vinnslu aðildarríkjanna á persónuupplýsingum vegna starfsemi í tengslum við sameiginlega stefnu Sambandsins í utanríkis- og öryggismálum.

⁽⁵⁾ Tilmæli framkvæmdastjórnarinnar frá 6. maí 2003 um skilgreininguna á örfyrirtækjum, litlum fyrirtækjum og meðalstórum fyrirtækjum (Sjtið. ESB L 124, 20.5.2003, bls. 36).

17) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 45/2001 ⁽⁶⁾ gildir um vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins á persónuupplýsingum. Laga ætti reglugerð (EB) nr. 45/2001 og aðrar réttargerðir Sambandsins, sem eiga við um slíka vinnslu persónuupplýsinga, að þeim meginreglum og reglum sem komið er á með þessari reglugerð og beitt er í ljósi þessarar reglugerðar. Í því skyni að setja öflugan og samræmdan ramma um persónuvernd í Sambandinu ættu nauðsynlegar aðlaganir á reglugerð (EB) nr. 45/2001 að fylgja í kjölfar samþykktar þessarar reglugerðar til þess að þær geti komið til framkvæmda á sama tíma og hún.

18) Þessi reglugerð á ekki við um vinnslu einstaklings á persónuupplýsingum ef hún er einungis í þágu hans sjálfs eða fjölskyldu hans og hefur þannig engin tengsl við atvinnu- eða viðskiptastarfsemi. Vinnsla, sem er einungis í þágu einstaklings eða fjölskyldu hans, getur t.d. tekið til bréfaskrifta og þess að halda skrár yfir heimilisföng, notkunar samfélagsmiðla og Netnotkunar sem fram fer í tengslum við slíka vinnslu. Hins vegar á þessi reglugerð við um ábyrgðaraðila eða vinnsluaðila sem setja fram leiðir til að vinna persónuupplýsingar í þágu einstaklings eða fjölskyldu hans.

19) Vernd einstaklinga að því er varðar vinnslu lögbærra yfirvalda á persónuupplýsingum í þeim tilgangi að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoðryggi og frjálsa miðlun slíkra gagna, er efni í sérstaka réttargerð Sambandsins. Þessi reglugerð ætti því ekki að gilda um vinnslustarfsemi í þessum tilgangi. Persónuupplýsingar, sem opinber yfirvöld taka til vinnslu samkvæmt þessari reglugerð, ættu hins vegar að heyra undir sértækari réttargerð Sambandsins þegar þær eru notaðar í þessum tilgangi, þ.e. tilskipun Evrópuþingsins og ráðsins (ESB) 2016/680 ⁽⁷⁾. Aðildarríkin geta falið lögbærum yfirvöldum í skilningi tilskipunar (ESB) 2016/680 verkefni, sem ekki eru endilega unnin í þeim tilgangi að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoðryggi, þannig að vinnsla persónuupplýsinga í þessum öðrum tilgangi falli, að svo miklu leyti sem hún fellur undir lög Sambandsins, innan gildissviðs þessarar reglugerðar.

Að því er varðar vinnslu þessara lögbæru yfirvalda á persónuupplýsingum í þeim tilgangi sem fellur innan gildissviðs þessarar reglugerðar ætti aðildarríkjunum að vera heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglna þessarar reglugerðar. Í slíkum ákvæðum mætti tilgreina nánar sértækar kröfur um vinnslu þessara lögbæru yfirvalda á persónuupplýsingum í þessum öðrum tilgangi, með hliðsjón af stjórnskipan, stjórnskipulagi og skipulagi stjórnsýslu í viðkomandi aðildarríki. Þegar vinnsla einkaaðila á persónuupplýsingum fellur innan gildissviðs þessarar reglugerðar ætti hún að veita aðildarríkjunum kost á að takmarka að lögum, við sérstakar aðstæður, tiltekna skyldur og réttindi þegar slík takmörkun telst nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi til að standa vörð um tiltekna mikilvæga hagsmuni, m.a. almannaoðryggi, og koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoðryggi. Þetta á m.a. við innan ramma baráttu gegn peningaþvætti eða í starfsemi réttarrannsóknarstofa.

20) Enda þótt þessi reglugerð gildi m.a. um starfsemi dómstóla og annarra dómsyfirvalda mætti í lögum Sambandsins eða lögum aðildarríkis tilgreina vinnsluáðgerðir og verklagsreglur í tengslum við vinnslu dómstóla og annarra dómsyfirvalda á persónuupplýsingum. Til að standa vörð um sjálfstæði dómskerfisins við framkvæmd verkefna þess á sviði dómsmála, m.a. ákvarðanatöku, ætti valdsvið eftirlitsyfirvalda ekki að ná til vinnslu dómstóla á persónuupplýsingum þegar þeir fara með dómssvald sitt. Mögulegt ætti að vera að fela eftirlit með slíkri gagnavinnslu sérstökum aðilum innan dómskerfis aðildarríkisins sem ættu einkum að tryggja að farið sé að reglum þessarar reglugerðar, efla vitund dómara um skyldur sínar samkvæmt henni og annast meðferð kvartana í tengslum við slíka gagnavinnslu.

⁽⁶⁾ Reglugerð Evrópuþingsins og ráðsins (EB) nr. 45/2001 frá 18. desember 2000 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem stofnanir og aðilar Bandalagsins hafa unnið, og um frjálsa miðlun slíkra upplýsinga (Stjóð. EB L 8, 12.1.2001, bls. 1).

⁽⁷⁾ Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/680 frá 27. apríl 2016 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 refsivíðurlögum og frjálsa miðlun slíkra upplýsinga og um miðurfellingu rammaákvæðunar ráðsins 2008/977/DIM (Stjóð. ESB L 119, 4.5.2016, bls. 89).

- 21) Þessi reglugerð hefur ekki áhrif á beitingu tilskipunar Evrópuþingsins og ráðsins 2000/31/EB⁽⁸⁾, einkum reglur í 12.-15. gr. hennar um bótaábyrgð þjónustuveitenda sem eru milliliðir. Með þeirri tilskipun er leitast við að stuðla að eðlilegri starfsemi innri markaðarins með því að tryggja frjálsa þjónustustarfsemi milli aðildarríkjana á sviði upplýsingasamfélagsins.
- 22) Hvers kyns vinnsla persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu ætti að fara fram í samræmi við þessa reglugerð, án tillits til þess hvort vinnslan sjálf fer fram í Sambandinu. Með staðfestu er átt við virka og raunverulega starfsemi með föstu fyrirkomulagi. Lögakveðið rekstrarform slíks fyrirkomulags, hvort sem um er að ræða útibú eða dótturfélag með réttarstöðu lögaðila, ræður ekki úrslitum að því er þetta varðar.
- 23) Til að tryggja að einstaklingar séu ekki sviptir þeirri vernd, sem þeir eiga rétt á samkvæmt þessari reglugerð, ætti vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga, sem eru í Sambandinu, að heyra undir þessa reglugerð ef vinnslustarfsemin tengist því að bjóða hinum skráðu vörur eða þjónustu, án tillits til þess hvort það er gegn greiðslu. Til að ákvarða hvort slíkur ábyrgðaraðili eða vinnsluaðili bjóði skráðum einstaklingum í Sambandinu vörur og þjónustu ætti að ganga úr skugga um hvort ljóst sé að ábyrgðaraðilinn eða vinnsluaðilinn hafi í hyggju að bjóða skráðum einstaklingum þjónustu í einu eða fleiri aðildarríkjum Sambandsins. Enda þótt aðgangurinn einn og sér að vefsetri ábyrgðaraðila, vinnsluaðila eða milliliðar í Sambandinu, netfangi hans eða öðrum upplýsingum um hvernig megi nálgast viðkomandi, eða notkun tungumáls, sem almennt er notað í þriðja landinu þar sem ábyrgðaraðili hefur staðfestu, nægi ekki til að staðfesta að um slíka fyrirtælan sé að ræða, geta þættir eins og að nota tungumál eða gjaldmiðil, sem er almennt notaður í einu eða fleiri aðildarríkjum og möguleikinn á að panta vörur og þjónustu á því tungumáli eða að nefna viðskiptavinum eða notendum í Sambandinu gert það ljóst að ábyrgðaraðili hefur í hyggju að bjóða skráðum einstaklingum í Sambandinu vörur eða þjónustu.
- 24) Vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga, sem eru í Sambandinu, ætti einnig að falla undir þessa reglugerð ef hún tengist því að vakta hegðun hinna skráðu, að því marki sem slík hegðun á sér stað innan Sambandsins. Til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga ætti að ganga úr skugga um hvort slóð einstaklinga sé rakin á Netinu, m.a. hvort í kjölfarið séu notaðar vinnsluáðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf.
- 25) Þegar lög aðildarríkis gilda í krafti þjóðaréttar ætti þessi reglugerð einnig að gilda um ábyrgðaraðila sem hefur ekki staðfestu í Sambandinu, s.s. í sendiskrifstofu eða ræðisstofnun aðildarríkis.
- 26) Meginreglur um persónuvernd ættu að gilda um hvers kyns upplýsingar varðandi persónugreindan eða persónugreinanlegan einstakling. Persónuupplýsingar sem hafa verið færðar undir gerviauðkenni, sem kann að vera hægt að rekja til einstaklings með notkun viðbótarupplýsinga, skulu teljast upplýsingar um persónugreinanlegan einstakling. Til þess að ákvarða hvort einstaklingur er persónugreinanlegur ætti að taka mið af öllum þeim aðferðum sem ástæða er til að ætla að annaðhvort ábyrgðaraðili eða annar aðili geti beitt til að bera kennsl á viðkomandi einstakling með beinum eða óbeinum hætti. Til að ganga úr skugga um hvort fremur líklegt megi telja að aðferðum verði beitt til að bera kennsl á einstakling ætti að taka tillit til allra hlutlægra þátta, s.s. kostnaðar við það og þess tíma sem það tæki, að teknu tilliti til þeirrar tækni sem fyrir hendi er þegar vinnslan fer fram og til tækniþróunar. Meginreglur um persónuvernd ættu því ekki að eiga við um nafnlausar upplýsingar, þ.e. upplýsingar sem tengjast ekki persónugreindum eða persónugreinanlegum einstaklingi, eða persónuupplýsingar sem hafa verið aftengdar persónuauðkennum þannig að ekki er lengur unnt að persónugreina hinn skráða. Þessi reglugerð varðar því ekki vinnslu slíkra nafnlausra upplýsinga, s.s. í tölfærðilegum tilgangi eða vegna rannsókna.

(8) Tilskipun Evrópuþingsins og ráðsins 2000/31/EB frá 8. júní 2000 um tiltekna lagalega þætti þjónustu, einkum rafræna viðskipta, í tengslum við upplýsingasamfélagið á innri markaðnum (tilskipun um rafræn viðskipti) (Stjóð. EB L 178, 17.7.2000, bls. 1).

- 27) Þessi reglugerð á ekki við um persónuupplýsingar látinna einstaklinga. Aðildarríkjunum er heimilt að kveða á um reglur um vinnslu persónuupplýsinga látinna einstaklinga.
- 28) Notkun gerviauðkenna fyrir persónuupplýsingar getur dregið úr áhættu viðkomandi skráðra einstaklinga og auðveldað ábyrgðaraðilum og vinnsluaðilum að uppfylla persónuverndarskyldur sínar. Sérstakri innleiðingu á „notkun gerviauðkenna“ í þessari reglugerð er ekki ætlað að útiloka aðrar persónuverndarráðstafanir.
- 29) Til þess að skapa hvata til notkunar gerviauðkenna við vinnslu persónuupplýsinga ættu ráðstafanir vegna gerviauðkennanotkunar, sem leyfa jafnframt almenna greiningu, að vera mögulegar hjá sama ábyrgðaraðila þegar hann hefur gert nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að tryggja, vegna viðkomandi vinnslu, að þessari reglugerð sé komið til framkvæmda og að viðbótarupplýsingum, sem gera það kleift að rekja persónuupplýsingarnar til tiltekins skráðs einstaklings, sé haldið aðgreindum. Ábyrgðaraðili, sem vinnur persónuupplýsingarnar, ætti að gefa upp hvaða aðilar í starfsemi hans hafa tilskildar heimildir.
- 30) Tæki og töl, forrit og samskiptareglur, sem einstaklingar nota, geta tengt Netauðkenni við þá, s.s. IP-tölur (e. internet protocol addresses), smygildauðkenni (e. cookie identifiers) eða önnur auðkenni, s.s. fjarskiptatíðniauðkenningar. Þetta getur skilið eftir spor sem hægt er að nota til að útbúa persónusnið um einstaklinga og bera kennsl á þá, einkum þegar sporunum er bætt við einkvæm auðkenni og aðrar upplýsingar sem berast netþjónum.
- 31) Ekki ætti að líta á opinber yfirvöld, sem fá í hendur persónuupplýsingar á grundvelli lagaskyldu í tengslum við opinber störf sín, s.s. skatta- og töllyfirvöld, einingar sem fara með rannsóknir á sviði fjármála, sjálfstæð stjórnsýsluyfirvöld eða yfirvöld fjármálamarkaða, sem bera ábyrgð á reglusetningu og eftirliti með verðbréfamörkuðum, sem viðtakendur ef þau fá í hendur persónuupplýsingar sem eru nauðsynlegur þáttur í tiltekinni fyrirspurn í þágu almennra hagsmuna, í samræmi við lög Sambandsins eða lög aðildarríkis. Beiðnir opinberra yfirvalda um afhendingu upplýsinga ættu ætíð að vera skriflegar, rökstuddar og tilvikabundnar og ættu ekki að varða skráningarkerfi í heild eða leiða til samtengingar á milli skráningarkerfa. Vinnsla þessara opinberu yfirvalda á persónuupplýsingum ætti að samrýmast gildandi reglum um persónuvernd samkvæmt tilgangi vinnslunnar.
- 32) Veita ætti samþykki með skýrri staðfestingu, s.s. skriflegri yfirlýsingu, þ.m.t. með rafrænum hætti, eða munnlegri yfirlýsingu, á því að fyrir liggi óþvinguð, afmörkuð, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki vinnslu persónuupplýsinga sem varða hann sjálfan. Þetta gæti falið í sér að haka við reit þegar farið er inn á vefsetur á Netinu, velja tæknilegar stillingar fyrir þjónustu í upplýsingasamfélaginu eða aðra yfirlýsingu eða athöfn sem gefur skýrt til kynna í þessu samhengi að skráður einstaklingur samþykki fyrirhugaða vinnslu á persónuupplýsingum um sig. Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi ættu því ekki að fela í sér samþykki. Samþykki ætti að ná til allrar vinnslustarfsemi sem fram fer í sama tilgangi, einum eða fleiri. Þegar vinnslan er í margvíslegum tilgangi ætti að gefa samþykki fyrir hverjum og einum þeirra. Ef hinn skráði á að veita samþykki sitt við rafrænni beiðni verður beiðnin að vera skýr og skilmerkileg og ekki raska óþarflega notkun þjónustunnar sem það er veitt fyrir.
- 33) Oft er ekki hægt að greina tilgang með vinnslu persónuupplýsinga í þágu vísindarannsókna að fullu þegar upplýsingunum er safnað. Því ættu skráðir einstaklingar að geta gefið samþykki sitt fyrir tilteknum sviðum vísindarannsókna þegar þær samrýmast viðurkenndum, siðferðislegum viðmiðunum fyrir vísindarannsóknir. Skráðir einstaklingar ættu að hafa tækifæri til að veita samþykki sitt einungis á tilteknum sviðum rannsókna eða fyrir hlutum rannsóknarverkefna, að því marki sem fyrirhugaður tilgangur leyfir.

- 34) Skilgreina ætti erfðafræðilegar upplýsingar sem persónuupplýsingar sem varða arfgenga eða áunna erfðaeiginleika einstaklings, sem fást með greiningu á líffræðilegu sýni frá viðkomandi einstaklingi, einkum litningagreiningu, greiningu á deoxýríbósakjarnsýru (DNA) eða ríbósakjarnsýru (RNA), eða með greiningu á öðrum þætti sem gerir kleift að fá fram jafngildar upplýsingar.
- 35) Persónuupplýsingar sem varða heilsufar ættu að taka til allra gagna tengdra heilsufari skráðs einstaklings og veita upplýsingar um líkamlegt eða andlegt heilsufar hans í fortíð, nútíð eða framtíð. Þar á meðal eru upplýsingar um einstaklinginn sem safnað er við skráningu hans vegna heilbrigðisþjónustu eða við veitingu hennar, eins og um getur í tilskipun Evrópuþingsins og ráðsins 2011/24/ESB ⁽⁹⁾; númer, tákn eða atriði sem einstaklingi er úthlutað til að auðkenna hann með einkvæmum hætti í tengslum við heilsufar; upplýsingar sem má rekja til prófunar eða rannsóknar á líkamshluta eða líkamsefni, þ.m.t. erfðafræðilegar upplýsingar og líffræðileg sýni; og hvers kyns upplýsingar um t.d. sjúkdóm, fötlun, hættu á sjúkdómi, heilsufarssögu, klíniska meðferð eða lífeðlisfræðilegt eða líf- og læknisfræðilegt ástand hins skráða, án tillits til uppruna þeirra, s.s. hvort sem þær koma frá lækni eða öðrum heilbrigðisstarfsmanni, sjúkrahúsi, úr lækningatæki eða með greiningarprófun í glasi.
- 36) Höfuðstöðvar ábyrgðaraðila í Sambandinu ættu að vera sá staður þar sem hann hefur yfirstjórn sína í Sambandinu nema ákvarðanir um tilgang með og aðferðir við vinnslu persónuupplýsinga séu teknar í annarri starfsstöð ábyrgðaraðila í Sambandinu en í því tilviki ætti síðarnefnda starfsstöðin að teljast vera höfuðstöðvar. Ákvarða ætti hverjar höfuðstöðvar ábyrgðaraðila eru í Sambandinu í samræmi við hlutlægar viðmiðanir og ætti þar að fara fram virk og raunveruleg stjórnun með föstu fyrirkomulagi þar sem helstu ákvarðanir eru teknar um tilgang og aðferðir við vinnsluna. Sú viðmiðun ætti ekki að velta á því hvort vinnsla persónuupplýsinga fer fram á þeim stað. Tilvist og notkun nauðsynlegra tæknilegra aðferða og tækni við vinnslu persónuupplýsinga eða vinnslustarfsemi jafngildir ekki höfuðstöðvum í sjálfu sér og er því ekki ákvarðandi viðmiðun um hvað telst vera höfuðstöðvar. Höfuðstöðvar vinnsluaðila ættu að vera sá staður þar sem hann hefur yfirstjórn sína í Sambandinu eða, hafi hann enga yfirstjórn í Sambandinu, sá staður þar sem helsta vinnslustarfsemi fer fram í Sambandinu. Í tilvikum þar sem bæði ábyrgðaraðili og vinnsluaðili koma við sögu ætti leiðandi lögbært eftirlitsyfirvald áfram að vera eftirlitsyfirvald aðildarríkisins þar sem ábyrgðaraðili hefur höfuðstöðvar sínar en eftirlitsyfirvald vinnsluaðila ætti að teljast hlutaðeigandi eftirlitsyfirvald og það eftirlitsyfirvald ætti að taka þátt í samstarfsferlinu sem kveðið er á um í þessari reglugerð. Þó ættu eftirlitsyfirvöld aðildarríkis eða aðildarríkja þar sem vinnsluaðili hefur eina starfsstöð eða fleiri aldrei að teljast hlutaðeigandi eftirlitsyfirvöld ef drög að ákvörðun varða einungis ábyrgðaraðilann. Ef fyrirtækjasamstæða annast vinnsluna ættu höfuðstöðvar ráðandi fyrirtækis að teljast höfuðstöðvar samstæðunnar nema ákvarðanataka um tilgang og aðferðir við vinnslu persónuupplýsinganna sé á hendi annars fyrirtækis.
- 37) Fyrirtækjasamstæða ætti að taka til ráðandi fyrirtækis og undirfyrirtækja þess þar sem ráðandi fyrirtækið ætti að vera það fyrirtæki sem hefur ráðandi áhrif á hin fyrirtækin, s.s. í krafti eignarhalds, fjárhagslegrar þátttöku eða reglna sem gilda um fyrirtækið eða valds til að koma reglum um vernd persónuupplýsinga til framkvæmda. Fyrirtæki, sem stjórnar vinnslu persónuupplýsinga í fyrirtækjum sem eru í eignartengslum við það, ætti, ásamt þeim fyrirtækjum, að teljast fyrirtækjasamstæða.
- 38) Persónuupplýsingar barna ættu að njóta sérstakrar verndar þar sem þau kunna að vera síður meðvituð um áhættu, afleiðingar og viðkomandi verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga. Þessi sérstaka vernd ætti einkum að eiga við um notkun persónuupplýsinga barna í markaðssetningarskyni eða þegar búin eru til persónu- eða notendasnið og um söfnun persónuupplýsinga er varða börn þegar þau nota þjónustu sem börnum eru boðin beint. Samþykki forsjáraðila ætti ekki að vera nauðsynlegt þegar um er að ræða forvarnar- eða ráðgjafarþjónustu sem barni er boðin beint.

⁽⁹⁾ Tilskipun Evrópuþingsins og ráðsins 2011/24/ESB frá 9. mars 2011 um réttindi sjúklinga varðandi heilbrigðisþjónustu yfir landamæri (Stjóð. ESB L 88, 4.4.2011, bls. 45).

- 39) Hvers kyns vinnsla persónuupplýsinga ætti að vera lögmæt og sanngjörn. Það ætti að vera einstaklingum ljóst þegar persónuupplýsingum um þá er safnað, þær eru notaðar, skoðaðar eða unnar á annan hátt og að hvaða marki persónuupplýsingar eru eða munu verða unnar. Meginreglan um gagnsæi krefst þess að hvers kyns upplýsingar og samskipti, sem tengjast vinnslu þessara persónuupplýsinga, séu auðveldlega aðgengileg og auðskiljanleg og á skýru og einföldu máli. Sú meginregla á einkum við um upplýsingar til skráðra einstaklinga um það hver ábyrgðaraðilinn er og tilganginn með vinnslunni og frekari upplýsingar til að tryggja sanngjarna og gagnsæja vinnslu gagnvart viðkomandi einstaklingum og rétt þeirra til að fá staðfestingu og tilkynningu um vinnslu á persónuupplýsingum um þá. Gera ætti einstaklingum ljósa áhættu, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga og hvernig þeir geta neytt réttar síns í tengslum við slíka vinnslu. Einkum ætti tilgangurinn með vinnslu persónuupplýsinganna að vera skýr og lögmæt og liggja fyrir við söfnun þeirra. Persónuupplýsingarnar ættu að vera nægilegar, viðeigandi og takmarkaðar við það sem nauðsynlegt er miðað við tilganginn með vinnslunni. Þetta krefst þess einkum að geymslutími persónuupplýsinganna sé takmarkaður við algjört lágmark. Því aðeins ætti að vinna persónuupplýsingar að ekki sé unnt að ná tilganginum með vinnslunni á annan aðgengilegan hátt. Til að tryggja að persónuupplýsingar séu ekki varðveittar lengur en nauðsynlegt er ætti ábyrgðaraðilinn að setja tímafresti varðandi eyðingu eða reglulega endurskoðun þeirra. Gera verður hóflegar ráðstafanir til að tryggja að óáreiðanlegar persónuupplýsingar verði leiðréttar eða þeim eytt. Vinnsla persónuupplýsinga ætti að vera með þeim hætti að viðeigandi öryggi og trúnaður um upplýsingarnar sé tryggt, m.a. að komið sé í veg fyrir óheimilan aðgang eða notkun á persónuupplýsingum og þeim búnaði sem notaður er við vinnsluna.
- 40) Til að vinnsla persónuupplýsinga teljist lögmæt ætti hún að fara fram með samþykki hlutaðeigandi skráðs einstaklings eða á einhverjum öðrum lögmætum grundvelli, sem mælt er fyrir um í lögum, annaðhvort í þessari reglugerð eða í öðrum lögum Sambandsins eða lögum aðildarríkis, eins og um getur í þessari reglugerð, þ. á m. þegar hún er nauðsynleg til að fara að ákvæðum um lagaskyldu sem hvílir á ábyrgðaraðilanum eða vegna framkvæmdar samnings sem hinn skráði á aðild að eða með hliðsjón af ráðstöfunum sem eru gerðar að beiðni hans áður en samningur er gerður.
- 41) Þegar vísað er til lagagrundvallar eða löggjafarráðstöfunar í þessari reglugerð er ekki endilega gerð sú krafa að þing samþykki lagagerð, með fyrirvara um kröfur samkvæmt stjórnskipan hlutaðeigandi aðildarríkis. Slíkur lagagrundvöllur eða löggjafarráðstöfun ætti þó að vera skýr og nákvæm og beitingin fyrirsjáanleg þeim sem falla þar undir, eins og krafist er í dómaframkvæmd Evrópudómstólsins („Dómstólsins“) og Mannréttindadómstóls Evrópu.
- 42) Þegar vinnsla er byggð á samþykki skráðs einstaklings ætti ábyrgðaraðilinn að geta sýnt fram á að hinn skráði hafi samþykkt vinnsluáðgerðina. Verndarráðstafanir ættu að tryggja, einkum í tengslum við skriflega yfirlýsingu um annað málefni, að hinum skráða sé kunnugt um að samþykki hafi verið veitt og að hvaða marki. Í samræmi við tilskipun ráðsins 93/13/EB⁽¹⁰⁾ ætti ábyrgðaraðilinn að setja fram yfirlýsingu um samþykki á skiljanlegu og aðgengilegu formi og á skýru og einföldu máli sem ætti ekki að fela í sér óréttmæta skilmála. Til þess að samþykki teljist upplýst ætti skráður einstaklingur að vita deili á a.m.k. ábyrgðaraðilanum og vera kunnugt um tilgang þeirrar vinnslu sem persónuupplýsingunum er ætlað að þjóna. Ekki ætti að telja að samþykki hafi verið veitt af fúsum og frjálsum vilja ef hinn skráði hefur ekki raunverulegt eða frjálst val eða getur ekki neitað eða dregið til baka samþykki án þess að verða fyrir tjóni.
- 43) Til þess að tryggja að samþykki sé veitt af fúsum og frjálsum vilja ætti það ekki að teljast gildur lagagrundvöllur fyrir vinnslu persónuupplýsinga í tilteknu tilviki þar sem skýr aðstöðumunur er milli hins skráða og ábyrgðaraðilans, einkum þegar ábyrgðaraðilinn er opinbert yfirvald og því ólíklegt að samþykki hafi verið veitt af fúsum og frjálsum vilja við allar aðstæður í því tiltekna tilviki. Samþykki telst ekki veitt

(10) Tilskipun ráðsins 93/13/EBE frá 5. apríl 1993 um óréttmæta skilmála í neytendasamningum (Stjtið. EB L 95, 21.4.1993, bls. 29).

af fúsum og frjálsum vilja ef ekki er hægt að veita sérstakt samþykki fyrir aðskildum aðgerðum við vinnslu persónuupplýsinga, þótt slíkt ætti við í því einstaka tilviki, eða ef framkvæmd samnings, m.a. veiting þjónustu, er komin undir samþykkinu þótt samþykkið sé ekki nauðsynlegt vegna framkvæmdar samningsins.

44) Vinnsla ætti að teljast lögmæt þegar hún er nauðsynleg í tengslum við samning eða fyrirætlun um að gera samning.

45) Þegar vinnsla fer fram í samræmi við lagaskyldu sem hvílir á ábyrgðaraðilanum eða er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds ætti vinnslan að byggjast á lögum Sambandsins eða lögum aðildarríkis. Þess er ekki krafist í þessari reglugerð að sett verði sérstök lög um hverja einstaka vinnslu. Það kann að vera nægilegt að hafa lög sem grundvöll fyrir ýmsum vinnsluaðgerðum, sem byggjast á lagaskyldu sem hvílir á ábyrgðaraðilanum, eða þegar vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds. Einnig ættu lög Sambandsins eða lög aðildarríkis að ákvarða tilgang vinnslunnar. Í þeim lögum mætti enn fremur tilgreina almenn skilyrði þessarar reglugerðar um lögmæta vinnslu persónuupplýsinga og hvernig skuli ákvarða hver ábyrgðaraðilinn er, hvaða tegund persónuupplýsinga unnið verður með, þá skráðu einstaklinga sem í hlut eiga, hvaða aðilar mega fá persónuupplýsingarnar, hvaða takmarkanir eiga við vegna tilgangs, varðveislutímabil og aðrar ráðstafanir til að tryggja að vinnslan fari fram á lögmætan og sanngjarnan hátt. Einnig ætti að ákvarða í lögum Sambandsins eða lögum aðildarríkis hvort ábyrgðaraðili, sem annast framkvæmd verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds, ætti að vera opinbert yfirvald eða annar einstaklingur eða lögaðili sem fellur undir opinberan rétt eða, þegar slíkt er í þágu almannahagsmuna, m.a. heilbrigðismála á borð við lýðheilsu og félagslega vernd og við stjórnun heilbrigðisþjónustu, undir einkarétt, s.s. fagfélag.

46) Einnig verður að telja vinnslu persónuupplýsinga lögmæta ef hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir líf skráðs einstaklings eða annars einstaklings. Vinnsla persónuupplýsinga á grundvelli brýnna hagsmuna annars einstaklings ætti að meginreglu til aðeins að fara fram þegar greinilegt er að hún getur ekki byggst á öðrum lagagrundvelli. Sumar tegundir vinnslu geta bæði þjónað mikilvægum almannahagsmunum og brýnum hagsmunum skráðs einstaklings, t.d. þegar vinnsla er nauðsynleg í mannúðarskyni, s.s. við að fylgjast með farsóttum og útbreiðslu þeirra eða við neyðarástand sem kallar á mannúðaraðstoð, einkum þegar um er að ræða náttúruhamfarir eða stóráföll af mannavöldum.

47) Lögmætir hagsmunir ábyrgðaraðila, þ.m.t. hagsmunir ábyrgðaraðila sem fá persónuupplýsingarnar í hendur, eða þriðja aðila geta verið lagagrundvöllur fyrir vinnslu þeirra, að því tilskildu að hagsmunir eða grundvallarréttindi og frelsi hins skráða vegi ekki þyngra, að teknu tilliti til eðlilegra væntinga skráðra einstaklinga á grundvelli tengsla þeirra við ábyrgðaraðilann. Um lögmæta hagsmuni gæti m.a. verið að ræða þegar viðeigandi tengsl sem máli skipta eru milli skráða einstaklingsins og ábyrgðaraðilans, t.d. í tilvikum þar sem hinn skráði er viðskiptavinur ábyrgðaraðilans eða í þjónustu hans. Hvað sem öðru líður þyrfti að meta af kostgæfni hvort um lögmæta hagsmuni er að ræða, m.a. hvort skráður einstaklingur getur, þegar söfnun persónuupplýsinganna fer fram og í samhengi við hana, haft gilda ástæðu til að ætla að vinnsla muni fara fram í þeim tilgangi. Hagsmunir hins skráða og grundvallarréttindi hans gætu einkum gengið fram hagsmunum ábyrgðaraðila gagna þegar vinnsla persónuupplýsinga fer fram við aðstæður þar sem skráðir einstaklingar hafa ekki ástæðu til að ætla að um frekari vinnslu verði að ræða. Að því gefnu að það sé í höndum löggjafans að kveða á um lagagrundvöll vegna vinnslu opinberra yfirvalda á persónuupplýsingum ætti sá lagagrundvöllur ekki að eiga við um vinnslu opinberra yfirvalda þegar þau sinna verkefnum sínum. Vinnsla persónuupplýsinga, sem er beinlínis nauðsynleg í þeim tilgangi að koma í veg fyrir svik, telst einnig til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna. Líta má svo á að vinnsla persónuupplýsinga vegna beinnar markaðssetningar sé í þágu lögmætra hagsmuna.

- 48) Ábyrgðaraðilar, sem eru hluti af fyrirtækjasamstæðu eða stofnunum sem tengjast miðlægri stofnun, geta haft lögmæta hagsmuni af því að miðla persónuupplýsingum innan fyrirtækjasamstæðunnar í þágu innri stjórnunar, m.a. vegna vinnslu persónuupplýsinga um viðskiptavinum eða starfsmenn. Þetta hefur engin áhrif á almennar meginreglur um miðlun persónuupplýsinga, innan fyrirtækjasamstæðu, til fyrirtækis sem er staðsett í þriðja landi.
- 49) Vinnsla persónuupplýsinga, að því marki sem hún er beinlínis nauðsynleg og hófleg til að tryggja net- og upplýsingaöryggi, þ.e. getu nets eða upplýsingakerfis til að standast, á tilteknu öryggisstigi, atburði sem verða fyrir slysi eða aðgerðir sem eru ólögmætar eða skaðlegar og stofna í hættu aðgengileika, sannvottuðum uppruna, heilleika og leynd vistaðra eða sendra persónuupplýsinga, og öryggi tengdrar þjónustu sem boðin er eða er aðgengileg um þessi net og kerfi, af hálfu opinberra yfirvalda, viðbragðsteymis vegna neyðartilvika er varða tölvuöryggi (CERT), viðbragðsteymis vegna váatvika er varða tölvuöryggi (CSIRT), þeirra sem reka rafræn fjarskiptanet og -þjónustu og þeirra sem útvega öryggistækni og -þjónustu, telst til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna. Þetta gæti t.d. falið í sér að komið sé í veg fyrir óheimilan aðgang að rafrænum fjarskiptanetum og dreifingu spilliforrita og til að stöðvaðar séu atlgör að þjónustumiðlun (e. „denial of service“ attacks) og skemmdir á tölvum og rafrænum fjarskiptakerfum.
- 50) Heimila ætti vinnsla persónuupplýsinga í öðrum tilgangi en þeim sem var upphaflega markmiðið með söfnun þeirra því aðeins að vinnslan samrýmist þeim tilgangi sem var forsenda söfnunarinnar í upphafi. Í því tilviki er ekki krafist annars lagagrundvallar en þess sem heimilaði söfnun persónuupplýsinganna. Ef vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds, sem ábyrgðaraðili fer með, má í lögum Sambandsins eða lögum aðildarríkis ákvarða og tilgreina hvenær frekari vinnsla telst samrýmanleg og lögmæt með tilliti til tiltekinnar verkefna og tilgangs. Frekari vinnsla vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi ætti að teljast til samrýmanlegra, lögmætra vinnsluáðgerða. Lagagrundvöllur samkvæmt lögum Sambandsins eða lögum aðildarríkis vegna vinnslu persónuupplýsinga getur einnig verið lagagrundvöllur frekari vinnslu. Til þess að ganga úr skugga um hvort tilgangur með frekari vinnslu samrýmist þeim tilgangi sem var forsenda söfnunarinnar í upphafi ætti ábyrgðaraðilinn, þegar hann hefur fullnægt öllum kröfum um lögmæti vinnslunnar í upphafi, að taka tillit til m.a.: hvers kyns tengsla milli þessa tilgangs og tilgangs með fyrirhugaðri frekari vinnslu, þess í hvaða samhengi persónuupplýsingunum var safnað, einkum eðlilegra væntinga skráðra einstaklinga um frekari notkun þeirra á grundvelli tengsla þeirra við ábyrgðaraðilann, eðlis persónuupplýsinganna, afleiðinga fyrirhugaðrar frekari vinnslu þeirra fyrir skráða einstaklinga og hvort viðeigandi verndarráðstafanir hafi verið eða séu gerðar, bæði í upphaflegu vinnsluáðgerðunum og fyrirhuguðum frekari áðgerðum.
- Þegar skráður einstaklingur hefur veitt samþykki sitt eða vinnslan byggist á lögum Sambandsins eða lögum aðildarríkis, sem fela í sér nauðsynlega og hóflega ráðstöfun í lýðræðisþjóðfélagi og sem er einkum ætlað að standa vörð um mikilvæg markmið sem þjóna almannahagsmunum, ætti ábyrgðaraðilinn að vera heimil frekari vinnslu persónuupplýsinganna án tillits til þess hvort tilgangurinn telst samrýmanlegur. Hvað sem öðru líður ætti að tryggja beitingu meginreglnanna sem settar eru fram í þessari reglugerð, einkum um að upplýsa hinn skráða um þennan viðbótartilgang og réttindi hans, m.a. andmælaréttinn. Ef ábyrgðaraðilinn bendir á mögulega refsiverða háttsemi eða ógnanir við almannaoöryggi og sendir lögbæru yfirvaldi viðeigandi persónuupplýsingar í stökum eða fleiri tilvikum, sem snerta sama refsiverða verknað eða ógnanir við almannaoöryggi, ætti að telja slíkt í þágu lögmætra hagsmuna ábyrgðaraðilans. Þó ætti að banna slíka sendingu í þágu lögmætra hagsmuna ábyrgðaraðilans eða vegna frekari vinnslu persónuupplýsinga ef vinnslan samrýmist ekki lagalegri, faglegri eða annars konar bindandi þagnarskyldu.
- 51) Persónuupplýsingar, sem eru í eðli sínu sérlega viðkvæmar að því er varðar grundvallarréttindi og mannfrelsi, eiga að njóta sérstakrar verndar þar sem vinnsla þeirra gæti haft í för með sér umtalsverða áhættu fyrir grundvallarréttindi og mannfrelsi. Til þessara persónuupplýsinga ætti að telja upplýsingar um kynþátt eða þjóðernislegan uppruna, en ekki ber að skilja notkun hugtaksins „kynþáttur“ í þessari

reglugerð sem viðurkenningu Sambandsins á kenningum sem reyna að sanna tilvist mismunandi kynþátta manna. Ekki ætti kerfisbundið að telja vinnslu ljósmynda til vinnslu sérstakra flokka persónuupplýsinga þar sem þær falla eingöngu undir skilgreiningu á lífkennaupplýsingum þegar vinnsla þeirra fer fram með sérstakri tæknilegri aðferð sem gerir kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti. Vinnsla slíkra persónuupplýsinga ætti ekki að fara fram nema hún sé heimiluð í sérstökum tilvikum, eins og sett er fram í þessari reglugerð, að teknu tilliti til þess að í lögum aðildarríkjanna er heimilt að mæla fyrir um sértæk ákvæði um persónuvernd til þess að aðlaga beitingu reglna þessarar reglugerðar svo að þær samrýmist lagaskyldu eða vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Almennar meginreglur og aðrar reglur þessarar reglugerðar ættu að gilda, auk hinna sértæku krafna vegna slíkrar vinnslu, einkum að því er varðar skilyrði fyrir lögmætti vinnslunnar. Veita ætti með skýrum hætti undanþágur frá almennu banni við vinnslu slíkra sérstakra flokka persónuupplýsinga, t.d. þegar hinn skráði gefur ótvírætt samþykki sitt eða, að því er varðar sérstakar þarfar, einkum þegar vinnslan fer fram sem hluti af lögmætri starfsemi tiltekinna samtaka eða stofnana sem hafa það að markmiði að tryggja mannfrelsi.

52) Einnig ætti að heimila undanþágu frá banni við vinnslu sérstakra flokka persónuupplýsinga ef kveðið er á um það í lögum Sambandsins eða lögum aðildarríkis og með fyrirvara um viðeigandi verndarráðstafanir, svo að vernda megi persónuupplýsingar og önnur grundvallarréttindi, þegar það þjónar almannahagsmunum, einkum vinnslu persónuupplýsinga á sviði vinnulöggjafar, löggjafar um félagslega vernd, m.a. lífeyri, og með hliðsjón af heilbrigðisöryggi, vöktun og viðvörðunum, forvörðum og vörðum gegn smitsjúkdómum og annarri alvarlegri heilsufarsógn. Heimilt er að veita slíka undanþágu af heilbrigðisástæðum, s.s. vegna lýðheilsu og stjórnunar heilbrigðisþjónustu, einkum til að tryggja gæði og kostnaðarhagkvæmni þeirra verklagsreglna sem notaðar eru við uppgjör á kröfum um bætur og þjónustu sjúkratryggingakerfisins, eða vegna skjalavistunar í þágu almannahagsmuna, rannsóknar á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Með undanþágu ætti líka að vera heimilt að vinna slíkar persónuupplýsingar þegar það er nauðsynlegt til að unnt sé að stofna, hafa uppi eða verja réttarkröfur, hvort heldur er fyrir dómstól eða við stjórnsýslumeðferð eða málsmeðferð utan réttar.

53) Vinnsla sérstakra flokka persónuupplýsinga, sem þurfa að njóta aukinnar verndar, ætti aðeins að fara fram í þágu heilsutengdra markmiða þegar það er nauðsynlegt til að ná þessum markmiðum í þágu einstaklinga og samfélagsins alls, einkum í tengslum við stjórnun heilbrigðis- eða félagsþjónustu og -kerfa, þ.m.t. vinnslu slíkra upplýsinga á vegum stjórnsýslunnar og miðlægra landsbundinna heilbrigðisyfirvalda í þágu gæðastýringar, gagnaumsýslu stjórnsýslunnar og almenns eftirlits með heilbrigðis- og félagsþjónustu á lands- og staðarvísu og til að tryggja samfellu í heilbrigðis- og félagsþjónustu og heilbrigðisþjónustu eða heilbrigðisöryggi yfir landamæri, vegna vöktunar og viðvörðunar, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi, á grundvelli laga Sambandsins eða laga aðildarríkis, sem verða að þjóna hagsmunum almennings, sem og vegna rannsókna sem fara fram í þágu almannahagsmuna á sviði lýðheilsu. Þessi reglugerð ætti því að kveða á um samræmd skilyrði fyrir vinnslu sérstakra flokka persónuupplýsinga sem verða heilbrigðismál, með hliðsjón af sérstökum þörfum, einkum þegar vinnsla slíkra upplýsinga fer fram í þágu tiltekinna heilsutengdra markmiða af hálfu aðila sem falla undir þagnarskyldu samkvæmt lögum. Lög Sambandsins eða lög aðildarríkis ættu að kveða á um sértækar og viðeigandi ráðstafanir til að vernda grundvallarréttindi og persónuupplýsingar einstaklinga. Aðildarríkjum ætti að vera heimilt að viðhalda eða setja frekari skilyrði, m.a. takmarkanir, að því er varðar vinnslu erfðafræðilegra upplýsinga, lífkennaupplýsinga eða heilsufarsupplýsinga. Þetta ætti þó ekki að standa í vegi fyrir frjálsu flæði persónuupplýsinga innan Sambandsins þegar þessi skilyrði eiga við um vinnslu slíkra upplýsinga yfir landamæri.

54) Vinnsla sérstakra flokka persónuupplýsinga kann að vera nauðsynleg vegna almannahagsmuna á sviði lýðheilsu án samþykkis skráða einstaklingsins. Slík vinnsla ætti að vera með fyrirvara um viðeigandi og sértækar ráðstafanir til að standa vörð um réttindi og frelsi einstaklinga. Í þessu samhengi ætti að túlka hugtakið „lýðheilsa“ eins og það er skilgreint í reglugerð Evrópuþingsins og ráðsins (EB) nr. 1338/2008⁽¹¹⁾, þ.e. allir heilsufarstengdir þættir, nánar tiltekið heilsufar, m.a. sjúkdómstilvik og fötlun,

(11) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1338/2008 frá 16. desember 2008 um hagskýrslur Bandalagsins um lýðheilsu og heilbrigði og öryggi á vinnustað (Stjótið. ESB L 354, 31.12.2008, bls. 70).

ákvarðandi þættir sem hafa áhrif á heilsufar, þörf fyrir heilbrigðisþjónustu, fjármagn sem veitt er til heilbrigðisþjónustu, veiting og almennur aðgangur að heilbrigðisþjónustu og kostnaður og fjármögnun heilbrigðisþjónustu, sem og dánarorsakir. Slík vinnsla heilsufarsupplýsinga í þágu almannahagsmuna ætti ekki að leiða til vinnslu persónuupplýsinga í öðrum tilgangi af hálfu þriðju aðila, s.s. vinnuveitenda eða tryggingafélaga og bankastofnana.

55) Vinnsla persónuupplýsinga af hálfu opinberra yfirvalda í þeim tilgangi að vinna að markmiðum opinberlega viðurkenndra trúarsamtaka, eins og mælt er fyrir um í stjórnskipunarlögum eða samkvæmt þjóðarétti, fer einnig fram með vísan til almannahagsmuna.

56) Þegar nauðsynlegt reynist fyrir starfsemi lýðræðislegs stjórnkerfis í aðildarríki, í tengslum við kosningar, að stjórn málaflókkar taki saman persónuupplýsingar um stjórn mála skoðanir fólks má heimila vinnslu slíkra upplýsinga í þágu almannahagsmuna, að því tilskildu að gerðar séu viðeigandi verndarráðstafanir.

57) Ef persónuupplýsingar sem ábyrgðaraðili vinnur gera honum ekki kleift að persónugreina einstakling ætti honum ekki að vera skylt að afla viðbótarupplýsinga til að greina skráðan einstakling eingöngu í þeim tilgangi að uppfylla eitthvert ákvæðanna í þessari reglugerð. Þó ætti ábyrgðaraðili ekki að neita að taka við viðbótarupplýsingum sem hinn skráði lætur í té til þess að ná fram rétti sínum. Í persónugreiningu ætti að felast stafræn auðkenning á skráðum einstaklingi, m.a. með hjálp sannvottunaraðferðar á borð við sömu skilríki og hann notar við innskráningu á þjónustu á vegum ábyrgðaraðila gagna á Netinu.

58) Meginreglan um gagnsæi krefst þess að hvers kyns upplýsingar, sem ætlaðar eru almenningi eða skráðum einstaklingi, séu gagnorðar, aðgengilegar og auðskiljanlegar, að þær séu á skýru og einföldu máli og að auki að sjónrænum aðferðum sé beitt, eftir því sem við á. Veita mætti slíkar upplýsingar á rafrænu formi, t.d. á vefsetri, þegar þær eru ætlaðar almenningi. Þetta á einkum við í tilvikum þar sem erfitt er fyrir skráðan einstakling að vita og skilja, vegna hins mikla fjölda aðila sem koma að máli og flókinna tækni sem notuð er, hvort, af hverjum og í hvaða tilgangi upplýsingum er safnað um hann, s.s. þegar um er að ræða auglýsingar á Netinu. Þar sem börn þurfa að njóta sérstakrar verndar ættu hvers kyns upplýsingar og tilkynningar, þegar vinnsla beinist að barni, að vera á skýru og einföldu máli sem barnið getur auðveldlega skilið.

59) Koma ætti á nánari reglum til að greiða fyrir því að skráður einstaklingur geti neytt réttar síns samkvæmt þessari reglugerð, m.a. ráðstöfunum sem gera honum kleift að fara fram á og, ef við á, fá því endurgjaldslaust framgengt að honum sé veittur aðgangur að persónuupplýsingum, þær séu leiðréttar eða þeim eytt, sem og að hann geti neytt andmælaréttar síns. Ábyrgðaraðili ætti einnig að sjá til þess að hægt sé að leggja fram beiðnir rafrænt, einkum þegar vinnsla persónuupplýsinga fer fram með rafrænum hætti. Ábyrgðaraðila ætti að vera skylt að svara beiðnum skráðs einstaklings án ótilhlýðilegrar tafar og innan eins mánaðar hið mesta og færa fram rök ef hann hyggst ekki taka slíkar beiðnir til greina.

60) Meginreglurnar um sanngirni og gagnsæi við vinnslu krefjast þess að skráðum einstaklingi sé tilkynnt um að vinnsluáðgerð standi yfir og hver sé tilgangur hennar. Ábyrgðaraðili ætti að veita hinum skráða frekari upplýsingar sem nauðsynlegar eru til að tryggja að gætt sé sanngirni og gagnsæi við vinnslu persónuupplýsinga með tilliti til þeirra sérstöku aðstæðna og samhengis sem eiga við vinnslu þeirra. Enn fremur ætti að upplýsa hinn skráða um að gert hafi verið persónusnið og um afleiðingar þess. Þegar persónuupplýsingar eru fengnar hjá skráðum einstaklingi ætti einnig að upplýsa hann um hvort honum sé skylt að láta persónuupplýsingarnar í té og um það hvaða afleiðingar það hefur að veita þær ekki. Hægt er að láta staðlaðar táknmyndir fylgja þessum upplýsingum til að veita greinargott yfirlit yfir fyrirhugaða vinnslu á auðsýnilegan, skiljanlegan og auðlæsilegan hátt. Táknmyndirnar ættu að vera á tölvulesanlegu sniði þegar þær eru settar fram rafrænt.

- 61) Veita ætti skráðum einstaklingi upplýsingar í tengslum við vinnslu persónuupplýsinga um hann á þeim tíma þegar upplýsinganna er aflað hjá honum eða, þegar persónuupplýsinganna er aflað frá öðrum heimildum, innan hæfilegs tíma, með hliðsjón af aðstæðum í hverju tilviki fyrir sig. Ef fá má öðrum viðtakanda persónuupplýsingar í hendur með lögmætum hætti ætti að tilkynna það hinum skráða þegar viðtakandinn fær persónuupplýsingarnar í fyrsta sinn. Ef ábyrgðaraðili hyggst vinna persónuupplýsingarnar í öðrum tilgangi en þeim sem er að baki söfnun þeirra ætti hann að láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum nauðsynlegum upplýsingum. Ef ekki er hægt að skýra hinum skráða frá uppruna persónuupplýsinganna vegna þess að þær koma frá mismunandi heimildum ætti að veita almennar upplýsingar.
- 62) Þó er ekki nauðsynlegt að setja fram skyldu til að veita upplýsingar ef skráður einstaklingur hefur þær þegar undir höndum, ef sérstaklega er mælt fyrir um skráningu eða birtingu persónuupplýsinganna í lögum, ef ómögulegt reynist að veita hinum skráða upplýsingar eða það hefði í för með sér óhóflega fyrirhöfn. Það síðasttalda gæti einkum átt við þegar vinnslan fer fram vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Í því sambandi ætti að taka tillit til fjölda skráðra einstaklinga, þess hversu gamlar upplýsingarnar eru og viðeigandi verndarráðstafana sem gerðar hafa verið.
- 63) Skráður einstaklingur ætti að hafa rétt til aðgangs að persónuupplýsingum sem hefur verið safnað um hann og til að neyta þessa réttar með auðveldum hætti og hæfilegum hléum til þess að hann geti gert sér grein fyrir því hvort vinnslan fari fram með lögmætum hætti og sannreynt það. Þetta felur í sér rétt skráðra einstaklinga til aðgangs að upplýsingum sem varða heilsufar þeirra, t.d. upplýsingum í sjúkraskrá á borð við sjúkdómsgreiningu, niðurstöður rannsókna, mat meðhöndlandi lækna og hvers kyns meðferðir eða inn grip. Sérhver skráður einstaklingur ætti því einkum að hafa rétt til að fá vitneskju og tilkynningu um tilganginn með vinnslu persónuupplýsinganna, vinnslutímabil upplýsinganna ef unnt er, viðtakendur þeirra, hvaða rök liggja að baki sjálfvirkri vinnslu persónuupplýsinga og afleiðingar slíkrar vinnslu, einkum þegar hún er byggð á gerð persónusniðs. Ábyrgðaraðilinn ætti, ef mögulegt er, að vera fær um að veita hinum skráða fjaraðgang að öruggu kerfi sem myndi veita honum beinan aðgang að persónuupplýsingum um sig. Sá réttur ætti ekki að hafa neikvæð áhrif á réttindi eða frelsi annarra, þ.m.t. viðskiptaleyndarmál eða hugverkaréttindi og þá einkum höfundarrétt til verndar hugbúnaðinum. Niðurstaða þessara atriða ætti þó ekki að vera sú að skráðum einstaklingi sé neitað um allar upplýsingar. Þegar ábyrgðaraðili vinnur með mikið magn upplýsinga sem varða skráðan einstakling ætti hann að geta óskað eftir því að hinn skráði tilgreini nánar um hvaða upplýsingar eða vinnsluáðgerðir beiðnin snýst, áður en upplýsingarnar eru veittar.
- 64) Ábyrgðaraðilinn ætti að gera allar eðlilegar ráðstafanir til að sannreyna deili á skráðum einstaklingi sem óskar eftir aðgangi, einkum í tengslum við þjónustu á Netinu og netauðkenni. Ábyrgðaraðili ætti ekki að halda eftir persónuupplýsingum í þeim tilgangi einum að geta brugðist við hugsanlegum beiðnum.
- 65) Skráður einstaklingur ætti að hafa rétt til leiðréttingar á persónuupplýsingum er varða hann sjálfan og „rétt til að gleymast“ ef varðveisla slíkra upplýsinga brýtur í bága við þessa reglugerð, lög Sambandsins eða lög aðildarríkis sem ábyrgðaraðilinn fellur undir. Skráður einstaklingur ætti einkum að hafa rétt til þess að fá persónuupplýsingum er varða hann sjálfan eytt og að vinnslu með þær sé hætt ef upplýsingarnar eru ekki lengur nauðsynlegar í tengslum við tilganginn með söfnun eða vinnslu þeirra að öðru leyti, ef hann hefur afturkallað samþykki sitt eða andmælir vinnslu persónuupplýsinga um sig eða ef vinnsla persónuupplýsinga um hann samrýmist ekki þessari reglugerð að öðru leyti. Þessi réttur á einkum við þegar hinn skráði hefur veitt samþykki sitt sem barn og gerir sér ekki fulla grein fyrir áhættunni sem vinnslan felur í sér og óskar eftir því síðar að persónuupplýsingunum verði eytt, einkum á Netinu. Skráður einstaklingur ætti að geta neytt þessa réttar þrátt fyrir að hann sé ekki lengur barn. Þó ætti frekari varðveisla persónuupplýsinganna að vera lögmæt, ef nauðsyn krefur, til að neyta réttar til tjáningar- og upplýsingafrelsis, til að uppfylla lagaskyldu, vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, í þágu almannahagsmuna á sviði lýðheilsu, vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum

tilgangi eða til að unnt sé að stofna, hafa uppi eða verja réttarkröfur.

- 66) Til að efla megi réttinn til að gleymast í netumhverfinu ætti einnig að víkka réttinn til eyðingar þannig að ábyrgðaraðila, sem gerði persónuupplýsingarnar opinberar, sé skylt að upplýsa þá ábyrgðaraðila sem vinna slíkar upplýsingar um að afmá beri alla tengla á þessar persónuupplýsingar eða afrit af þeim eða endurgerðir þeirra. Í því sambandi ætti viðkomandi ábyrgðaraðili að gera eðlilegar ráðstafanir með tilliti til þeirrar tækni sem er fyrir hendi og aðferða sem honum eru aðgengilegar, þ.m.t. tæknilegar ráðstafanir til að upplýsa ábyrgðaraðilana, sem vinna persónuupplýsingar um hinn skráða, um beiðni hans.
- 67) Aðferðir til að takmarka vinnslu persónuupplýsinga gætu m.a. falið í sér að færa valdar upplýsingar tímabundið í annað vinnslukerfi, gera valdar persónuupplýsingar óaðgengilegar notendum eða fjarlægja birtar upplýsingar tímabundið af vefsetri. Í sjálfvirkum skráningarkerfum ætti að jafnaði að tryggja takmörkun vinnslunnar með tæknilegum aðferðum á þann hátt að ekki verði um frekari vinnslu persónuupplýsinganna að ræða og ekki sé hægt að breyta þeim. Tilgreina ætti með skýrum hætti í kerfinu að vinnsla persónuupplýsinga sé takmörkuð.
- 68) Til að styrkja enn frekar stjórn skráðs einstaklings á upplýsingum er varða hann sjálfan þegar vinnsla persónuupplýsinga fer fram með sjálfvirkum aðferðum ætti hann einnig að hafa rétt til að fá persónuupplýsingar er varða hann sjálfan, sem hann hefur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu og samvirkandi sniði og senda þær öðrum ábyrgðaraðila. Hvetja ætti ábyrgðaraðila gagna til að þróa samvirkandi snið sem gera það mögulegt að flytja eigin gögn. Þessi réttur ætti að gilda þegar hinn skráði lét persónuupplýsingarnar í té á grundvelli eigin samþykkis eða ef vinnslan er nauðsynleg vegna framkvæmdar samnings. Hann ætti ekki að eiga við þegar vinnslan byggist á öðrum lagagrundvelli en samþykki eða samningi. Eðli málsins samkvæmt ætti ekki að beita þessum rétti gagnvart ábyrgðaraðilum sem vinna persónuupplýsingar við opinber skyldustörf sín. Hann ætti því ekki að gilda þegar vinnsla persónuupplýsinga er nauðsynleg til að framfylgja lagaskyldu sem hvílir á ábyrgðaraðilanum eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Réttur skráðs einstaklings til að senda eða taka á móti persónuupplýsingum er varða hann sjálfan ætti ekki að verða til þess að ábyrgðaraðilum sé skylt að taka upp eða viðhalda vinnslukerfum sem eru tæknilega samhæfð. Ef tiltekið mengi persónuupplýsinga varðar fleiri en einn skráðan einstakling ætti réttur þeirra til að fá persónuupplýsingarnar að vera með fyrirvara um réttindi og frelsi annarra skráðra einstaklinga í samræmi við þessa reglugerð. Þessi réttur ætti enn fremur ekki að hafa áhrif á rétt skráðs einstaklings til að láta eyða persónuupplýsingum og takmarkanir á þeim rétti eins og sett er fram í þessari reglugerð, einkum ætti hann ekki að gefa til kynna að persónuupplýsingum, sem varða hinn skráða, sem hann hefur látið af hendi vegna efndar á samningi, verði eytt, að því marki og svo lengi sem persónuupplýsingarnar eru nauðsynlegar til að efna samninginn. Ef það er tæknilega gerlegt ætti skráður einstaklingur að hafa rétt til að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars.
- 69) Þegar vinnsla persónuupplýsinga gæti verið lögmæt vegna þess að hún er nauðsynleg vegna verkefnis, sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með eða vegna lögmætra hagsmuna ábyrgðaraðila eða þriðja aðila, ætti skráður einstaklingur engu að síður að hafa rétt til að andmæla vinnslu persónuupplýsinga sem varða hans tilteknu aðstæður. Það ætti að vera á hendi ábyrgðaraðila að sýna fram á að mikilvægir lögmætir hagsmunir hans gangi framár hagsmunum eða grundvallarréttindum og frelsi hins skráða.
- 70) Þegar persónuupplýsingar eru unnar í þágu beinnar markaðssetningar ætti skráður einstaklingur að hafa rétt til að andmæla slíkri vinnslu, m.a. gerð persónusniðs, að því marki sem hún tengist slíkri beinni markaðssetningu, hvort sem um er að ræða upphaflega eða frekari vinnslu eða ekki, hvenær sem er og endurgjaldslaut. Gera ætti hinum skráða sérstaklega grein fyrir þessum rétti með skýrum hætti og aðgreint frá öðrum upplýsingum.
- 71) Skráður einstaklingur ætti að eiga rétt á því að sæta ekki ákvörðun sem kann að fela í sér ráðstöfun þar sem

persónulegir þættir hans eru metnir eingöngu á grundvelli sjálfvirkar gagnavinnslu og hefur réttaráhrif gagnvart honum sjálfum eða veruleg sambærileg áhrif, s.s. sjálfvirka höfnun lánsúmsóknar á Netinu eða rafrænt ráðningarferli án mannlegrar ihlutunar. Til slíkrar vinnslu telst „gerð persónusniðs“ sem felur í sér hvers kyns sjálfvirka vinnslu persónuupplýsinga til að meta persónulega þætti er varða hagi einstaklings, einkum að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsufar, smekk, áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika, þegar hún hefur réttaráhrif hvað hann sjálfan varðar eða veruleg sambærileg áhrif. Ákvarðanatöku, sem byggist á slíkri vinnslu, þ.m.t. gerð persónusniðs, ætti að vera leyfileg samkvæmt sérstakri heimild í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðilinn fellur undir, m.a. í þeim tilgangi að fylgjast með og koma í veg fyrir svindl og skattsvik í samræmi við reglur, staðla og tilmæli stofnana Sambandsins eða landsbundinna eftirlitsaðila og til að tryggja öryggi og áreiðanleika þjónustu sem ábyrgðaraðili veitir eða, þegar nauðsyn krefur, vegna gerðar eða framkvæmdar samnings milli skráðs einstaklings og ábyrgðaraðila eða þegar hinn skráði hefur veitt ótvírætt samþykki sitt. Hvað sem öðru líður ætti slík vinnsla að falla undir viðeigandi verndarráðstafanir, þ. á m. að veita hinum skráða skilmerkilegar upplýsingar og rétt hans til mannlegrar ihlutunar, að láta skoðun sína í ljós, fá útskýringar á ákvörðun sem tekin er að loknu slíku mati og vefengja ákvörðunina. Slík ráðstöfun ætti ekki að varða barn.

Til að tryggja að vinnslan sé sanngjörn og gagnsæ gagnvart skráðum einstaklingi, að teknu tilliti til sérstakra aðstæðna og samhengis við vinnslu persónuupplýsinganna, ætti ábyrgðaraðilinn að nota viðeigandi stærðfræðilegar eða tölfræðilegar aðferðir við gerð persónusniðs, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, einkum til að tryggja að þættir sem gera persónuupplýsingar óáreiðanlegar séu leiðréttir og dregið sé úr hættu á mistökum, að tryggja öryggi persónuupplýsinga þannig að tekið sé tillit til mögulegrar áhættu fyrir hagsmuni og réttindi hins skráða og m.a. komið í veg fyrir að einstaklingum sé mismunað á grundvelli kynþáttar eða þjóðernislegs uppruna, stjórnmálaskoðana, trúarbragða eða trúar, þátttöku í stéttarfélagi, erfðaeiginleika eða heilsuhaga eða kynhneigðar, eða að gerðar verði ráðstafanir sem hafa samsvarandi áhrif. Sjálfvirka ákvarðanatöku og gerð persónusniðs, sem byggist á sérstökum flokkum persónuupplýsinga, ætti einungis að heimila með sérstökum skilyrðum.

72) Gerð persónusniðs fellur undir reglurnar um vinnslu persónuupplýsinga í þessari reglugerð, m.a. hvað varðar lagagrundvöll vinnslunnar eða meginreglur um persónuvernd. Evrópska persónuverndarráðið, sem komið er á fót með þessari reglugerð („persónuverndarráðið“), ætti að geta gefið út leiðbeiningar í því tilliti.

73) Lög Sambandsins eða lög aðildarríkis geta kveðið á um að takmarka megi sértækar meginreglur og rétt á upplýsingum, aðgang að persónuupplýsingum og leiðréttingu á þeim eða eyðingu þeirra, rétt til að flytja eigin gögn, rétt til andmæla, ákvarðanir sem byggjast á gerð persónusniðs, ásamt tilkynningum til skráðs einstaklings um öryggisbrot við meðferð persónuupplýsinga og tilteknar tengdar skyldur ábyrgðaraðila, að því marki sem nauðsynlegt er og hóflegt í lýðræðisþjóðfélagi til að vernda almannaoöryggi, þ.m.t. mannslíf, einkum vegna viðbragða við náttúruhamförum og hamförum af mannavöldum, vegna forvarna, rannsóknar og saksóknar í refsímálum eða fullnustu refsiviðurlaga, m.a. til að vernda gegn og koma í veg fyrir ógnir við almannaoöryggi eða brot á siðareglum í lögvernduðum atvinnugreinum, vegna annarra mikilvægra markmiða sem þjóna almannahagsmunum Sambandsins eða aðildarríkis, einkum mikilvægum efnahagslegum eða fjárhagslegum hagsmunum Sambandsins eða aðildarríkis, vegna halds opinberra skráa í þágu almannahagsmuna, frekari vinnslu persónuupplýsinga í skjalasöfnum til að ná fram sérstökum upplýsingum um stjórnmálahegðun undir stjórnnum fyrrverandi einræðisríkja eða til að vernda skráða einstaklinginn eða réttindi og frelsi annarra, m.a. í þágu félagslegrar verndar, lýðheilsu og mannúðar. Þessar takmarkanir ættu að vera í samræmi við kröfurnar sem settar eru fram í sáttmálanum um grundvallarréttindi og Evrópusáttmálanum um verndun mannréttinda og mannfrelsis.

74) Setja ætti reglur um ábyrgð og bótaábyrgð ábyrgðaraðila vegna vinnslu persónuupplýsinga af hans hálfu eða fyrir hans hönd. Ábyrgðaraðilanum ætti einkum að vera skylt að gera viðeigandi og skilvirkar ráðstafanir og hann ætti að vera fær um að sýna fram á að vinnslan fari fram í samræmi við þessa reglugerð, þ.m.t. að því er varðar skilvirkni ráðstafananna. Ráðstafanirnar ættu að taka mið af eðli,

umfangi, samhengi og tilgangi vinnslunnar og áhættu fyrir réttindi og frelsi einstaklinga.

- 75) Vinnsla persónuupplýsinga kann að leiða til misjafnlegra líklegar og alvarlegrar áhættu fyrir réttindi og frelsi einstaklinga sem getur leitt af sér efnislegt tjón, eignatjón og óefnislegt tjón, einkum þegar vinnslan getur haft í för með sér mismunun, auðkennisþjófnað eða svik, fjárhagstjón, skaða á orðstír, tapaðan trúnað um persónuupplýsingar sem njóta verndar á grundvelli þagnarskyldu, að notkun gerviauðkenna sé aflétt í leyfisleysi eða annað umtalsvert efnahagslegt eða félagslegt óhagræði, þegar skráðir einstaklingar gætu misst réttindi sín og frelsi eða verið hindraðir í að stjórna eigin persónuupplýsingum, þegar persónuupplýsingar eru unnar sem leiða í ljós kynþátt eða þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð eða heimspekilega sannfæringu, þátttöku í stéttarfélagi og vinnsla erfðafræðilegra upplýsinga, upplýsinga sem varða heilsu eða upplýsinga um kynlíf eða sakfellingu í refsímálum og refsiverð brot eða tengdar öryggisráðstafanir, þegar lagt er mat á persónulega þætti, einkum við að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsuhagi, smekk eða áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika, til þess að gera eða nota persónusnið, þegar persónuupplýsingar berskjaldaðra einstaklinga, einkum barna, eru unnar eða þegar vinnsla tekur til mikils magns persónuupplýsinga og hefur áhrif á marga skráða einstaklinga.
- 76) Ákvarða ætti hversu líkleg og alvarleg áhættan er fyrir réttindi og frelsi skráða einstaklingsins með vísun til eðlis, umfangs, samhengis og tilgangs vinnslunnar. Meta ætti áhættu út frá hlutlægu mati þar sem leitt er í ljós hvort aðgerðir við vinnslu persónuupplýsinga feli í sér áhættu eða mikla áhættu.
- 77) Veita mætti ábyrgðaraðila eða vinnsluaðila leiðbeiningar um framkvæmd viðeigandi ráðstafana og um það hvernig sýna skuli fram á fylgni við reglur, einkum að því er varðar greiningu á áhættu í tengslum við vinnsluna, mat þeirra að því er varðar orsök áhættunnar, eðli hennar, hversu líkleg og alvarleg hún er og við að greina bestu starfsvenjur til að draga úr henni, einkum með því að nota viðurkenndar háttarnisreglur, viðurkennda vottun, viðmiðunarreglur frá persónuverndarráðinu eða ábendingar frá persónuverndarfulltrúa. Persónuverndarráðið getur einnig gefið út viðmiðunarreglur um vinnsluaðgerðir sem ólíklegt er að leiði af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga og benda á ráðstafanir sem geta verið nægilegar í slíkum tilvikum til að bregðast við slíkri áhættu.
- 78) Til að vernda réttindi og frelsi einstaklinga að því er varðar vinnslu persónuupplýsinga er nauðsynlegt að gerðar séu viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að kröfum þessarar reglugerðar sé fullnægt. Til að geta sýnt fram á farið sé að þessari reglugerð ætti ábyrgðaraðilinn að setja sér innri stefnu og innleiða ráðstafanir sem fylgja einkum meginreglunum um innbyggða persónuvernd og sjálfgefna persónuvernd. Slíkar ráðstafanir gætu m.a. falið það í sér að draga sem mest úr vinnslu persónuupplýsinga, færa persónuupplýsingar undir gerviauðkenni eins skjótt og unnt er, gagnsæi að því er varðar eiginleika persónuupplýsinga og vinnslu þeirra, gera skráðum einstaklingi kleift að fylgjast með vinnslu upplýsinganna, gera ábyrgðaraðila kleift að taka upp og bæta öryggisþætti. Þegar framleiðendur vöru, þjónustu og hugbúnaðar þróa, hanna, velja og nota hugbúnað, vöru og þjónustu, sem er byggð á vinnslu persónuupplýsinga, eða vinna persónuupplýsingar í störfum sínum ætti að hvetja þá til að taka tillit til réttarins til persónuverndar við þróun og hönnun á slíkum vörum, þjónustu og hugbúnaði og ganga úr skugga um, að teknu tilhlýðilegu tilliti til nýjustu tækniþekkingar, að ábyrgðaraðilar og vinnsluaðilar geti uppfyllt skyldur sínar um persónuvernd. Einnig ætti að taka tillit til meginreglnanna um innbyggða og sjálfgefna persónuvernd í tengslum við opinber útboð.
- 79) Vernd réttinda og frelsis skráðra einstaklinga, ásamt ábyrgð og bótaábyrgð ábyrgðaraðila og vinnsluaðila, einnig að því er varðar eftirlit og aðgerðir eftirlitsyfirla, krefst þess að skipting ábyrgðarsviða samkvæmt þessari reglugerð sé skýr, m.a. þegar ábyrgðaraðili ákvarðar, ásamt öðrum ábyrgðaraðilum, tilgang og aðferðir við vinnslu eða þegar vinnsluaðgerð er framkvæmd fyrir hönd ábyrgðaraðila.
- 80) Ef ábyrgðaraðili eða vinnsluaðili, sem ekki hefur staðfestu í Sambandinu, vinnur persónuupplýsingar um

skráða einstaklinga sem eru í Sambandinu og vinnslustarfsemi hans tengist því að bjóða slíkum skráðum einstaklingum í Sambandinu vöru eða þjónustu, án tillits til þess hvort þeir verði krafðir um greiðslu, eða hafa eftirlit með hegðun þeirra, að svo miklu leyti sem hegðunin á sér stað innan Sambandsins, ætti ábyrgðaraðilinn eða vinnsluaðilinn að tilnefna fulltrúa nema því aðeins að vinnslan sé tilfallandi, feli ekki í sér stórfellda vinnslu sérstakra flokka persónuupplýsinga eða vinnslu persónuupplýsinga er varða sakfellingu í refsímálum og refsiverð brot, og ólíklegt teljist að hún leiði af sér áhættu fyrir réttindi og frelsi einstaklinga, með tilliti til eðlis, samhengis, umfangs og tilgangs vinnslunnar eða ef ábyrgðaraðilinn er opinbert yfirvald eða stofnun. Fulltrúinn ætti að koma fram fyrir hönd ábyrgðaraðilans eða vinnsluaðilans og getur hvaða eftirlitsyfirvald sem er haft samband við hann. Ábyrgðaraðilinn eða vinnsluaðilinn ætti að tilnefna fulltrúann sérstaklega með skriflegu umboði til að koma fram fyrir sína hönd með tilliti til skuldbindinga hans samkvæmt þessari reglugerð. Tilnefning slíks fulltrúa hefur ekki áhrif á ábyrgð eða bótaábyrgð ábyrgðaraðilans eða vinnsluaðilans samkvæmt þessari reglugerð. Slíkur fulltrúi ætti að inna verk sín af hendi í samræmi við fengið umboð frá ábyrgðaraðilanum eða vinnsluaðilanum, þ.m.t. starfa með lögbærum eftirlitsyfirvöldum með tilliti til hvers konar aðgerða sem gripið er til í því skyni að tryggja að farið sé að þessari reglugerð. Tilnefndur fulltrúi ætti að sæta fullnustumeðferð hafi ábyrgðaraðili eða vinnsluaðili ekki farið að reglugerðinni.

81) Til að tryggja að farið sé að kröfum þessarar reglugerðar að því er varðar þá vinnslu, sem vinnsluaðilinn á að annast fyrir hönd ábyrgðaraðilans, ætti ábyrgðaraðilinn, þegar hann felur vinnsluaðila vinnsluaðgerðir, einungis að nota vinnsluaðila sem veita fullnægjandi tryggingar, einkum með tilliti til sérþekkingar, áreiðanleika og úrræða, fyrir því að koma til framkvæmda tæknilegum ráðstöfunum og skipulagsráðstöfunum sem samrýmast kröfum þessarar reglugerðar, m.a. að því er varðar öryggi vinnslunnar. Ef vinnsluaðili fylgir samþykktum háttænisreglum eða samþykktu vottunarfyrirkomulagi má nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar. Ákvæði um að vinnsla sé í höndum vinnsluaðila ætti að setja fram í samningi eða annarri réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis, sem skuldbindur vinnsluaðilann gagnvart ábyrgðaraðilanum og tilgreinir viðfangsefni og lengd vinnslunnar, eðli og tilgang hennar, tegund persónuupplýsinga og flokka skráðra einstaklinga, með tilliti til sérstakra verkefna og ábyrgðar vinnsluaðilans í tengslum við vinnsluna sem á að fara fram og áhættu sem skapast varðandi réttindi og frelsi hins skráða. Ábyrgðaraðilinn og vinnsluaðilinn geta valið að nota stakan samning eða föst samningsákvæði sem annaðhvort framkvæmdastjórnin samþykkir beint eða eftirlitsyfirvald samþykkir í samræmi við samræmingarkerfið og framkvæmdastjórnin samþykkir síðan. Þegar vinnslu á vegum ábyrgðaraðilans er lokið ætti vinnsluaðilinn, eftir því sem ábyrgðaraðilinn ákveður, að skila eða eyða persónuupplýsingunum nema fyrir liggi krafa um varðveislu persónuupplýsinganna samkvæmt lögum Sambandsins eða lögum aðildarríkis sem vinnsluaðilanum ber að hlíta.

82) Til þess að sýna fram á að farið sé að þessari reglugerð ætti ábyrgðaraðilinn eða vinnsluaðilinn að halda skrár um vinnsluaðgerðir sem eru á hans ábyrgð. Hverjum ábyrgðaraðila og vinnsluaðila ætti að vera skylt að vinna með eftirlitsyfirvaldi og gera þessar skrár, að fenginni beiðni, aðgengilegar eftirlitsyfirvaldinu svo að nýta megir þær í þágu eftirlits með þessum vinnsluaðgerðum.

83) Til þess að viðhalda öryggi og koma í veg fyrir vinnslu, sem brýtur í bága við þessa reglugerð, ætti ábyrgðaraðili eða vinnsluaðili að meta þá áhættu sem fylgir vinnslunni og gera ráðstafanir til að draga úr slíkri áhættu, s.s. með dulkóðun. Þessar ráðstafanir ættu að tryggja viðeigandi öryggisstig, þ.m.t. trúnað, með tilliti til nýjustu tækni og kostnaðar við framkvæmd í tengslum við áhættu og eðli persónuupplýsinganna sem á að vernda. Við mat á áhættu fyrir gagnaöryggi ætti að líta til þeirrar áhættu sem fylgir vinnslu persónuupplýsinga, s.s. óviljandi eða ólögð mætrar eyðingar persónuupplýsinga þegar þær eru sendar, geymdar eða unnar á annan hátt, s.s. að þær glattist, breytist, verði birtar eða aðgangur

veittur að þeim í leyfisleysi, sem kann einkum að leiða til efnislegs tjóns, eignatjóns eða óefnislegs tjóns.

- 84) Til að stuðla að því að farið sé að þessari reglugerð þegar líklegt er að vinnsluaðgerðir leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga ætti ábyrgðaraðilinn að vera ábyrgur fyrir að gert sé mat á áhrifum á persónuvernd, einkum til að meta uppruna, eðli, sérkenni og alvarleika þeirrar áhættu. Taka ætti tillit til niðurstöðu matsins þegar ákvarðaðar eru viðeigandi ráðstafanir sem gripa skal til þannig að hægt sé að sýna fram á að vinnsla persónuupplýsinga sé í samræmi við þessa reglugerð. Þegar mat á áhrifum á persónuvernd gefur til kynna að vinnsluaðgerðir feli í sér mikla áhættu, sem ábyrgðaraðilinn getur ekki dregið úr með viðeigandi ráðstöfunum með hliðsjón af tiltækri tækni og kostnaði við framkvæmd, ætti að hafa samráð við eftirlitsyfirvaldið áður en vinnslan hefst.
- 85) Öryggisbrot við meðferð persónuupplýsinga getur, ef ekki er brugðist við því á réttan hátt og tímanlega, valdið einstaklingum efnislegu tjóni, eignatjóni eða óefnislegu tjóni, s.s. missi yfirráða yfir persónuupplýsingum um þá eða takmörkun réttinda þeirra, mismunun, auðkennisþjófnaði eða svikum, fjárhagstjóni, að notkun gerviauðkenna sé aflétt í leyfisleysi, skaða á orðstír, töpuðum trúnaði um persónuupplýsingar sem njóta verndar samkvæmt þagnarskyldu eða öðru umtalsverðu efnahagslegu eða félagslegu óhagræði fyrir viðkomandi einstakling. Af þeim sökum ætti ábyrgðaraðilinn, um leið og hann verður þess áskynja að öryggisbrot hafi orðið við meðferð persónuupplýsinga, að tilkynna það eftirlitsyfirvaldinu án ótilhlýðilegrar tafar og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brotsins var nema ábyrgðaraðilinn geti sýnt fram á, í samræmi við meginregluna um ábyrgðarskyldu, að ekki sé líklegt að viðkomandi brot leiði af sér áhættu fyrir réttindi og frelsi einstaklinga. Ef ekki er hægt að tilkynna slíkt innan 72 klst. ættu ástæður tafarinnar að fylgja tilkynningunni og veita má upplýsingar í áföngum án frekari ástæðulausrar tafar.
- 86) Ábyrgðaraðilinn ætti að tilkynna skráðum einstaklingi um öryggisbrot við meðferð persónuupplýsinga án ótilhlýðilegrar tafar ef líklegt má telja að brotið leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklingsins og gefa viðkomandi þannig færi á að gera nauðsynlegar varúðarráðstafanir. Í tilkynningunni ætti að koma fram eðli öryggisbrotsins við meðferð persónuupplýsinga, auk tilmæla til viðkomandi einstaklings um að draga úr mögulegum skaðlegum áhrifum. Slíkar tilkynningar til skráðra einstaklinga ætti að senda eins fljótt og mögulegt er og í nánú samstarfi við eftirlitsyfirvaldið, í samræmi við leiðbeiningar frá því sjálfu eða öðrum viðeigandi yfirvöldum, s.s. löggæsluyfirvöldum. Þörf á að draga úr bráðri hættu á tjóni kallar eftir skjóttum samskiptum við skráða einstaklinga en þörf á að gripa til viðeigandi ráðstafana gagnvart áframhaldandi eða sambærilegum öryggisbrotum við meðferð persónuupplýsinga kann að réttlæta að meiri tími fari í samskipti.
- 87) Ganga ætti úr skugga um hvort allar viðeigandi tæknilegar verndarráðstafanir og skipulagsráðstafanir hafi verið gerðar til að staðfesta tafarlaust hvort öryggisbrot við meðferð persónuupplýsinga hafi átt sér stað og að upplýsa eftirlitsyfirvaldið og skráða einstaklinginn þegar í stað um það. Ganga ætti úr skugga um að tilkynningin hafi verið send án ótilhlýðilegrar tafar, einkum með tilliti til eðlis og alvarleika öryggisbrots við meðferð persónuupplýsinga, afleiðinga þess og skaðlegra áhrifa þess fyrir hinn skráða. Slík tilkynning getur leitt til inngripa af hálfu eftirlitsyfirvaldsins í samræmi við verkefni þess og valdsvið sem mælt er fyrir um í þessari reglugerð.
- 88) Þegar settar eru ítarlegar reglur um viðeigandi framsetningu og verklag við tilkynningu öryggisbrots við meðferð persónuupplýsinga ætti að taka tilhlýðilegt tillit til aðstæðna þegar viðkomandi brot átti sér stað, m.a. hvort persónuupplýsingar hafi verið varðar með viðeigandi tæknilegum ráðstöfunum sem takmarka í reynd líkur á auðkennasvikum eða annars konar misnotkun. Enn fremur ættu slíkar reglur og málsmeðferð að taka tillit til lögmætra hagsmuna löggæsluyfirvalda þegar upplýsingagjöf snemma í ferlinu kann að ástæðulausu að standa í vegi fyrir rannsókn á aðstæðum þegar öryggisbrot við meðferð persónuupplýsinga átti sér stað.
- 89) Í tilskipun 95/46/EB er kveðið á um almenna skyldu til að tilkynna eftirlitsyfirvöldum um vinnslu persónuupplýsinga. Þótt sú skylda leiði til stjórnsýslulegrar og fjárhagslegrar byrði leiddi hún ekki í öllum tilvikum til bættrar verndar persónuupplýsinga. Af þeim sökum ætti að afnema slíka tilviljanakennda almenna tilkynningaskyldu og þess í stað ættu að koma skilvirkar verklagsreglur og aðferðir sem leggja í staðinn áherslu á þær tegundir vinnsluaðgerða sem líklegt er að leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga vegna eðlis þeirra, umfangs, samhengis og tilgangs. Slíkar tegundir vinnsluaðgerða

geta verið þær sem fela einkum í sér notkun nýrrar tækni eða eru nýrrar gerðar og þegar ábyrgðaraðilinn hefur ekki áður framkvæmt mat á áhrifum á persónuvernd eða þegar þær verða nauðsynlegar í ljósi þess tíma sem liðinn er frá upphaflegu vinnslunni.

- 90) Í þeim tilvikum ætti ábyrgðaraðilinn að láta fara fram mat á áhrifum á persónuvernd áður en vinnslan hefst til þess að meta líkur á og alvarleika mikillar áhættu með tilliti til eðlis, umfangs, samhengis og tilgangs vinnslunnar og uppruna áhættunnar. Þetta mat á áhrifum ætti einkum að fela í sér ráðstafanir, verndarráðstafanir og fyrirkomulag sem ætlað er að draga úr þeirri áhættu, tryggja vernd persónuupplýsinga og sýna fram á að farið sé að þessari reglugerð.
- 91) Þetta ætti einkum að eiga við um umfangsmiklar vinnsluadgerðir sem miða að því að vinna verulegt magn persónuupplýsinga á svæðisbundnum, landsbundnum eða yfirþjóðlegum vettvangi og sem gætu haft áhrif á mikinn fjölda skráðra einstaklinga og sem líklegt má telja að leiði af sér mikla áhættu, t.d. vegna þess hversu viðkvæmar upplýsingarnar eru, þegar í samræmi við þá tækniþekkingu sem náðst hefur er notuð ný tækni í miklum mæli, svo og aðrar vinnsluadgerðir sem leiða af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum þegar þessar aðgerðir gera hinum skráðu erfiðara fyrir með að neyta réttar síns. Einnig ætti að framkvæma mat á áhrifum á persónuvernd þegar unnið er úr persónuupplýsingum vegna tóku ákvarðana er varða tiltekna einstaklinga í kjölfar kerfisbundins og umfangsmikils mats á persónubundnum þáttum sem tengjast einstaklingum og er byggt á gerð persónusniðs úr þessum upplýsingum eða í kjölfar vinnslu á sérstökum flokkum persónuupplýsinga, lífkennaupplýsinga eða upplýsinga um sakfellingar í refsímálum og refsiverð brot eða tengdar öryggisráðstafanir. Á sama hátt er krafist mats á áhrifum á persónuvernd þegar haft er umfangsmikið eftirlit með svæðum sem eru aðgengileg almenningi, einkum þegar notaður er ljósrafeindabúnaður eða vegna annarra aðgerða þar sem lögbært eftirlitsyfirvald telur að vinnslan leiði líklega af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum vegna þess að þær koma í veg fyrir að hinir skráðu neyti réttar síns eða noti þjónustu eða samning, eða vegna þess að þær eru umfangsmiklar og framkvæmdar kerfisbundið. Vinnsla persónuupplýsinga ætti ekki að teljast umfangsmikil ef vinnslan varðar persónuupplýsingar frá einstökum lækni, öðrum faglærðum heilbrigðisstarfsmanni eða lögfræðingi um sjúklinga eða viðskiptavini. Í þeim tilvikum ætti mat á áhrifum á persónuvernd ekki að vera skyldubundið.
- 92) Við tilteknaðar aðstæður kann að vera skynsamlegt og hagkvæmt að hafa viðfangsefni mats á áhrifum á persónuvernd viðtækara en eitt verkefni, t.d. ef opinber yfirvöld eða stofnanir hafa í hyggju að koma á sameiginlegum vettvangi vegna notkunar eða vinnslu eða þegar margir ábyrgðaraðilar ráðgera að koma á sameiginlegu notkunar- eða vinnsluumhverfi innan atvinnugreinar eða -geira eða algengrar, þverlægrar starfsemi.
- 93) Í tengslum við samþykkt laga aðildarríkis, sem eru grundvöllur fyrir framkvæmd verkefna opinberra yfirvaldsins eða stofnunarinnar og gilda um sérstaka vinnsluadgerð eða röð aðgerða sem um er að ræða, geta aðildarríki talið nauðsynlegt að framkvæma slíkt mat áður en vinnsluadgerðirnar hefjast.
- 94) Þegar mat á áhrifum á persónuvernd bendir til þess að vinnslan myndi, vegna skorts á verndarráðstöfunum, öryggisráðstöfunum og aðgerðum til að draga úr áhættu, leiða til mikillar áhættu fyrir réttindi og frelsi einstaklinga og ábyrgðaraðilinn lítur svo á að ekki verði dregið úr henni með hóflegum aðferðum með tilliti til tiltækra tækni og kostnaðar við framkvæmd, ætti að hafa samráð við eftirlitsyfirvaldið áður en hafist er handa við vinnsluadgerðir. Líklegt er að tilteknaðar tegundir vinnslu og umfang og tíðni vinnslu hafi svo mikla áhættu í för með sér sem kann einnig að leiða til skaða eða röskunar á réttindum og frelsi einstaklingsins. Eftirlitsyfirvaldið ætti að bregðast við beiðni um samráð innan tilgreinds tíma. Ef engin viðbrögð koma frá eftirlitsyfirvaldinu innan þess tíma ætti það þó ekki að hafa áhrif á íhlutun eftirlitsyfirvaldsins í samræmi við verkefni þess og valdheimildir sem mælt er fyrir um í þessari reglugerð, m.a. heimild til að banna vinnsluadgerðir. Liður í því samráðsferli er að heimilt er að leggja fyrir eftirlitsyfirvaldið niðurstöðu úr mati á áhrifum á persónuvernd sem framkvæmt er með tilliti til viðkomandi vinnslu, einkum fyrirhugaðar ráðstafanir til að draga úr áhættu fyrir réttindi og frelsi einstaklinga.

- 95) Vinnsluaðilinn ætti að aðstoða ábyrgðaraðilann, eftir því sem nauðsyn krefur og komi fram beiðni um það, við að tryggja að farið sé að þeim skuldbindingum sem leiðir af framkvæmd mats á áhrifum á persónuvernd og fyrirframsamráði við eftirlitsfyrvaldið.
- 96) Samráð við eftirlitsfyrvaldið ætti einnig að fara fram við undirbúning löggjafar- eða stjórnvaldsráðstöfunar sem varðar vinnslu persónuupplýsinga til þess að tryggja að fyrirhuguð vinnsla sé í samræmi við þessa reglugerð og einkum til að takmarka áhættu sem snertir skráðan einstakling.
- 97) Ef vinnslan er í höndum opinbers yfirvalds, að undanskildum dómstólum eða sjálfstæðum dómsyfyrvöldum þegar þau fara með dómvald sitt, ef vinnsla í einkageiranum er í höndum ábyrgðaraðila og meginstarfsemi hans felst í vinnsluaðgerðum sem krefjast umfangsmikillar, reglubundinnar og kerfisbundinnar vöktunar á skráðum einstaklingum eða ef meginverkefni ábyrgðaraðilans eða vinnsluaðilans felast í umfangsmikilli vinnslu sérstakra flokka persónuupplýsinga og upplýsinga er varða sakfellingu í refsímálum og refsiverð brot ætti aðili með sérþekkingu á löggjöf um persónuvernd að aðstoða ábyrgðaraðilann eða vinnsluaðilann við eftirlit með því að þessari reglugerð sé fylgt á innri vettvangi. Í einkageiranum varða meginverkefni ábyrgðaraðila aðalstarfsemi hans en ekki vinnslu persónuupplýsinga sem viðbótarstarfsemi. Ákvarða ætti nauðsynlega sérþekkingu einkum út frá þeim gagnavinnsluaðgerðum sem framkvæmdar eru og þeirri vernd sem nauðsynleg er vegna þeirra persónuupplýsinga sem ábyrgðaraðili eða vinnsluaðili vinnur. Persónuverndarfulltrúar, hvort sem þeir eru starfsmenn ábyrgðaraðilans eða ekki, ættu að vera í aðstöðu til að sinna skyldustörfum sínum og verkefnum óháð öðrum.
- 98) Hvetja ætti samtök eða aðra aðila, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, til að setja sér háttænisreglur, innan marka þessarar reglugerðar, í því skyni að auðvelda skilvirka beitingu hennar, með hliðsjón af sérstökum eiginleikum þeirrar vinnslu sem fer fram á tilteknum sviðum og í samræmi við sérstakar þarfir örfyrirtækja og lítilla og meðalstórra fyrirtækja. Slíkar háttænisreglur gætu einkum afmarkað skyldur ábyrgðaraðila og vinnsluaðila, með tilliti til þeirrar áhættu fyrir réttindi og frelsi einstaklinga sem líklegt er að vinnslan hafi í för með sér.
- 99) Þegar samtök og aðrir aðilar, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, setja sér háttænisreglur, breyta þeim eða rýmka gildissvið þeirra ættu þau að hafa samráð við viðeigandi hagsmunaaðila, m.a. skráða einstaklinga ef unnt er, og taka tillit til athugasemda og skoðana sem fram hafa komið í kjölfar slíks samráðs.
- 100) Til að bæta gagnsæi og fylgni við þessa reglugerð ætti að hvetja til þess að komið verði á vottunarfyrirkomulagi og persónuverndarinnsglum og -merkjum sem gerir skráðum einstaklingum kleift að meta fljótt persónuverndarstig viðkomandi vöru og þjónustu.
- 101) Flæði persónuupplýsinga til og frá löndum utan Sambandsins og til og frá alþjóðastofnunum er nauðsynlegt vegna vaxandi alþjóðaviðskipta og alþjóðlegrar samvinnu. Aukið flæði af þessu tagi hefur haft í för með sér ný viðfangsefni og vanda í tengslum við vernd persónuupplýsinga. Þegar persónuupplýsingum er miðlað frá Sambandinu til ábyrgðaraðila, vinnsluaðila eða annarra viðtakenda í þriðju löndum eða til alþjóðastofnana ætti það ekki að grafa undan þeirri vernd sem þessi reglugerð tryggir einstaklingum í Sambandinu, þ.m.t. við framsendingu persónuupplýsinga frá þriðja landinu eða alþjóðastofnuninni til ábyrgðaraðila eða vinnsluaðila í sama eða öðru þriðja landi eða hjá annarri alþjóðastofnun. Miðlun til þriðju landa eða alþjóðastofnana má þó aðeins fara fram þannig að þessari reglugerð sé fylgt í einu og öllu. Upplýsingunum má því aðeins miðla, með fyrirvara um önnur ákvæði þessarar reglugerðar, að ábyrgðaraðili eða vinnsluaðili hafi farið að skilyrðunum sem mælt er fyrir um í ákvæðum þessarar reglugerðar um miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar.
- 102) Þessi reglugerð hefur ekki áhrif á alþjóðasamninga sem Sambandið hefur gert við þriðju lönd um miðlun

persónuupplýsinga, þ.m.t. um viðeigandi verndarráðstafanir í þágu skráðra einstaklinga. Aðildarríki geta gert alþjóðasamninga sem taka til miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana, að svo miklu leyti sem slíkir samningar hafa ekki áhrif á þessa reglugerð eða önnur ákvæði í lögum Sambandsins og fela í sér ákvæði um viðeigandi vernd grundvallarréttinda skráðra einstaklinga.

- 103) Framkvæmdastjórnin getur ákveðið, þannig að gildi hafi alls staðar í Sambandinu, að þriðja land, yfirráðasvæði eða tilgreindur geiri innan þriðja lands eða alþjóðastofnun veiti fullnægjandi persónuvernd, og þannig skapað réttarvissu og einsleitni í öllu Sambandinu að því er varðar þriðja land eða alþjóðastofnun sem talin er veita slíka vernd. Í þeim tilvikum er leyfilegt að miðla persónuupplýsingum til umrædds þriðja lands eða alþjóðastofnunar án þess að afla frekari heimildar. Framkvæmdastjórnin getur einnig ákveðið að afturkalla slíka ákvörðun eftir að hún hefur tilkynnt þriðja landinu eða alþjóðastofnuninni um það og upplýst að fullu um ástæður.
- 104) Við mat framkvæmdastjórnarinnar á þriðja landi eða á yfirráðasvæði eða tilgreindum geira innan þriðja lands ætti hún, í samræmi við þau grundvallargildi sem Sambandið er byggt á, einkum vernd mannréttinda, að taka tillit til þess hvernig viðkomandi þriðja land virðir grunnreglur réttarríkisins, tryggir aðgang að réttarkerfinu og alþjóðlegum reglum og viðmiðunum um mannréttindi, og til almennra laga og sérlaga, sem og til löggjafar um almannaoðryggi, landvarnir og öryggi ríkisins, auk allsherjarreglu og refsiréttar. Við samþykkt ákvörðunar um það hvort vernd sé fullnægjandi að því er varðar yfirráðasvæði eða tilgreindan geira innan þriðja lands ætti að taka tillit til skýrra og hlutlægra viðmiðana, s.s. tiltekinna vinnsluáðgerða og gildissviðs viðkomandi lagareglna og löggjafar sem eru í gildi í þriðja landinu. Þriðja landið ætti að ábyrgjast að tryggð sé fullnægjandi vernd sem er í meginatriðum sambærileg þeirri sem er tryggð í Sambandinu, einkum þegar vinnsla persónuupplýsinga fer fram í einum eða fleiri tilgreindum geirum. Þriðja landið ætti einkum að tryggja skilvirkt og sjálfstætt eftirlit með persónuvernd og móta verklag vegna samstarfs við persónuverndaryfirvöld í aðildarríkjunum og skráðir einstaklingar ættu að njóta skilvirkra og framfylgjanlegra réttinda og geta leitað réttar síns fyrir stjórnisýslufirvaldi og dómstólum með skilvirkum hætti.
- 105) Auk alþjóðlegra skuldbindinga, sem þriðja landið eða alþjóðastofnunin hefur gengist undir, ætti framkvæmdastjórnin að taka tillit til skuldbindinga sem leiðir af þátttöku þriðja landsins eða alþjóðastofnunarinnar í marghliða eða svæðisbundnum kerfum, einkum í tengslum við vernd persónuupplýsinga, svo og framkvæmdar slíkra skuldbindinga. Einkum ætti að taka tillit til aðildar þriðja lands að samningi Evrópuráðsins frá 28. janúar 1981 um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga og viðbótarbókunar við hann. Framkvæmdastjórnin ætti að hafa samráð við persónuverndarráðið þegar hún leggur mat á umfang verndar í þriðju löndum eða hjá alþjóðastofnunum.
- 106) Framkvæmdastjórnin ætti að fylgjast með framkvæmd ákvarðana um umfang verndar í þriðja landi, á yfirráðasvæði eða í tilgreindum geira innan þriðja lands eða hjá alþjóðastofnun og ætti að fylgjast með framkvæmd ákvarðana sem samþykktar eru á grundvelli 6. mgr. 25. gr. eða 4. mgr. 26. gr. tilskipunar 95/46/EB. Þegar framkvæmdastjórnin tekur ákvarðanir um hvort vernd sé fullnægjandi ætti hún að sjá til þess að fyrir hendi sé fyrirkomulag vegna reglubundinnar endurskoðunar á framkvæmd þeirra. Þessi reglubundna endurskoðun ætti að fara fram í samráði við hlutaðeigandi þriðja land eða alþjóðastofnun og að teknu tilliti til viðeigandi þróunar í þriðja landinu eða hjá alþjóðastofnuninni. Að því er eftirlit og reglubundna endurskoðun varðar ætti framkvæmdastjórnin að taka tillit til sjónarmiða og niðurstaðna Evrópuþingsins og ráðsins, svo og annarra viðeigandi aðila og heimilda. Framkvæmdastjórnin ætti að meta, innan hæfilegs frests, framkvæmd síðarnefndu ákvarðananna og leggja skýrslu um viðeigandi niðurstöður fyrir nefndina í skilningi reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 182/2011 ⁽¹²⁾, sem komið er á fót samkvæmt þessari reglugerð, og fyrir Evrópuþingið og ráðið.
- 107) Framkvæmdastjórnin getur staðfest að þriðja land, yfirráðasvæði eða tilgreindur geiri í þriðja landi eða alþjóðastofnun tryggi ekki lengur fullnægjandi persónuvernd. Af þessum sökum ætti að banna miðlun

⁽¹²⁾ Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 182/2011 frá 16. febrúar 2011 um reglur og almennar meginreglur varðandi tilhögun eftirlits aðildarríkjanna með framkvæmdastjórninni þegar hún beitir framkvæmdavaldi sínu (Stjtið. ESB L 55, 28.2.2011, bls. 13).

persónuupplýsinga til þessa þriðja lands eða alþjóðastofnunar nema fullnægt sé kröfum þessarar reglugerðar um miðlun með fyrirvara um viðeigandi verndarráðstafanir, þ.m.t. bindandi fyrirtækjareglur, og undanþágur vegna sérstakra aðstæðna. Í því tilviki ætti að gera ráð fyrir samráði milli framkvæmdastjórnarinnar og umræddra þriðju landa eða alþjóðastofnana. Framkvæmdastjórnin ætti að tilkynna þriðja landinu eða alþjóðastofnuninni tímanlega um ástæðurnar og hefja viðræður við það eða hana til þess að ráða bót á ástandinu.

108) Þegar ekki hefur verið tekin ákvörðun um það hvort fullnægjandi vernd er fyrir hendi ætti ábyrgðaraðili eða vinnsluaðili að gera ráðstafanir til að bæta upp skort á persónuvernd í þriðja landi með viðeigandi verndarráðstöfunum í þágu skráðs einstaklings. Viðeigandi verndarráðstafanir geta m.a. falist í því að nota bindandi fyrirtækjareglur, stöðluð ákvæði um persónuvernd sem framkvæmdastjórnin hefur samþykkt, stöðluð ákvæði um persónuvernd sem eftirlitsyfirvald hefur samþykkt eða samningsákvæði sem eftirlitsyfirvald hefur heimilað. Þessar verndarráðstafanir ættu að tryggja að farið sé að kröfum um persónuvernd og að virt séu réttindi skráðra einstaklinga sem varða vinnslu innan Sambandsins, þ.m.t. að fyrir liggi framfylgjanleg réttindi skráðra einstaklinga og skilvirk lagaleg úrræði, m.a. að hægt sé að leita réttar síns fyrir stjórnsýsluyfirvöldum eða dómstólum með skilvirkum hætti og að krefjast bóta, í Sambandinu eða í þriðja landi. Þær ættu einkum að varða fylgni við almennar meginreglur um vinnslu persónuupplýsinga og meginreglur um innbyggða og sjálfgefna persónuvernd. Opinber yfirvöld eða stofnanir geta einnig miðlað upplýsingum til opinberra yfirvalda eða stofnana í þriðju löndum eða til alþjóðastofnana sem hafa samsvarandi skyldur eða hlutverk, m.a. á grundvelli ákvæða sem eru felld inn í stjórnvaldsráðstafanir, s.s. samkomulag, sem veita skráðum einstaklingum framfylgjanleg og skilvirk réttindi. Afla ætti heimildar lögbærs eftirlitsyfirvalds ef gert er ráð fyrir verndarráðstöfunum í stjórnvaldsráðstöfunum sem eru ekki lagalega bindandi.

109) Möguleiki ábyrgðaraðila eða vinnsluaðila á að nota stöðluð ákvæði um persónuvernd, sem framkvæmdastjórnin eða eftirlitsyfirvald hefur samþykkt, ætti hvorki að hindra ábyrgðaraðila né vinnsluaðila í að fella stöðluð ákvæði um persónuvernd inn í viðtækari samning, s.s. samning milli ábyrgðaraðilans og annars ábyrgðaraðila, né heldur í að bæta við öðrum ákvæðum eða viðbótarverndarráðstöfunum, að því tilskildu að þau stangist ekki með beinum eða óbeinum hætti á við stöðluðu samningsákvæðin sem framkvæmdastjórnin eða eftirlitsyfirvald hefur samþykkt eða hafi áhrif á grundvallarréttindi eða frelsi skráðra einstaklinga. Hvetja ætti ábyrgðaraðila og vinnsluaðila til að gera frekari verndarráðstafanir með hjálp samningsbundinna skuldbindinga sem koma til viðbótar stöðluðum verndarákvæðum.

110) Fyrirtækjasamtæða eða hópur fyrirtækja í sameiginlegri atvinnustarfsemi ætti að geta notað viðurkenndar bindandi fyrirtækjareglur varðandi alþjóðlega miðlun sína frá Sambandinu til skipulagsheilda innan sömu fyrirtækjasamtæðu eða hóps fyrirtækja í sameiginlegri atvinnustarfsemi, að því tilskildu að þessar fyrirtækjareglur nái yfir allar mikilvægar meginreglur og framfylgjanleg réttindi til að tryggja viðeigandi verndarráðstafanir vegna miðlana eða flokka miðlana persónuupplýsinga.

111) Setja ætti ákvæði um möguleika á miðlun við sérstakar aðstæður þegar skráður einstaklingur hefur veitt ótvírætt samþykki sitt og miðlunin er tilfallandi og nauðsynleg í tengslum við samning eða réttarkröfu, hvort heldur er við dómsmeðferð eða stjórnsýslumeðferð eða aðra málsmeðferð utan dómstóla, þ.m.t. málsmeðferð hjá eftirlitsaðilum. Einnig ætti að gera ráð fyrir möguleika á miðlun þegar brýnir almannahagsmunir, sem mælt er fyrir um í lögum Sambandsins eða lögum aðildarríkis, krefjast þess eða þegar miðlunin er úr skrá sem komið var á fót samkvæmt lögum og ætluð er til þess að almenningur eða þeir sem hafa lögmætra hagsmuna að gæta geti skoðað hana. Í síðarnefnda tilvikinu ætti miðlunin ekki að ná til persónuupplýsinganna í heild sinni eða heilla flokka upplýsinga í skránni og miðlunin ætti, þegar gert er ráð fyrir að þeir sem hafa lögmætra hagsmuna að gæta geti skoðað skrána, aðeins að fara fram að beiðni þeirra eða, ef þeir eiga að vera viðtakendur upplýsinganna, að teknu fullu tilliti til hagsmuna og grundvallarréttinda skráða einstaklingsins.

112) Undanþágurnar ættu einkum að gilda um miðlun upplýsinga sem eru nauðsynlegar vegna mikilvægra

almannahagsmuna, t.d. þegar um er að ræða alþjóðleg upplýsingaskipti milli samkeppnisyfirvalda, skatta- eða tollýfirvalda, milli fjármálaeftirlitsstofnana, milli stofnana sem starfa á sviði almannatrygginga eða lýðheilsu, t.d. við að rekja smitleiðir vegna smitsjúkdóma eða í þeim tilgangi að draga úr og/eða útrýma lyfjamisnotkun í íþróttum. Einnig ætti miðlun persónuupplýsinga að teljast lögmæt þegar hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir brýna hagsmuni skráðs einstaklings eða annars einstaklings, þ.m.t. líkamlega friðhelgi eða líf, ef hinn skráði er ekki fær um að veita samþykki sitt. Þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geta lög Sambandsins eða lög aðildarríkis takmarkað, í ljósi mikilvægra almannahagsmuna, sérstaklega miðlun tiltekinna flokka upplýsinga til þriðja lands eða alþjóðastofnunar. Aðildarríkin ættu að tilkynna framkvæmdastjórninni um slík ákvæði. Telja mætti miðlun persónuupplýsinga um skráðan einstakling, sem er líkamlega eða í lagalegum skilningi ófær um að veita samþykki sitt, til alþjóðlegrar stofnunar á sviði mannúðarmála vegna framkvæmdar verkefnis samkvæmt Genfarsamningunum eða til að framfylgja alþjóðlegum mannúðarlögum sem gilda um vopnuð átök, nauðsynlega í ljósi mikilvægra almannahagsmuna eða þess að það varðar brýna hagsmuni hins skráða.

- 113) Miðlun, sem telja má að verði ekki endurtekin og sem aðeins varðar takmarkaðan fjölda skráðra einstaklinga, gæti einnig verið möguleg með tilliti til mikilvægra lögmætra hagsmuna sem ábyrgðaraðili gætir þegar hagsmunir eða réttindi og frelsi skráðs einstaklings ganga þeim ekki framar og ef ábyrgðaraðilinn hefur kannað allar aðstæður í tengslum við miðlun upplýsinganna. Ábyrgðaraðilinn ætti einkum að skoða eðli persónuupplýsinganna, tilgang og tímalengd fyrirhugaðrar vinnsluadgerðar eða - aðgerða, svo og aðstæður í upprunalandinu, þriðja landinu og endanlegu viðtökulandi og ætti að gera viðeigandi verndarráðstafanir til að vernda grundvallarréttindi og frelsi einstaklinga með tilliti til vinnslu persónuupplýsinga þeirra. Slík miðlun ætti aðeins að vera möguleg í einstaka tilvikum þegar engin annarra nefndra ástæða til miðlunar á við. Taka ætti tillit til lögmætra væntinga samfélagsins um aukna þekkingu þegar um er að ræða vísindalegar eða sagnfræðilegar rannsóknir eða tölfræðilegan tilgang. Ábyrgðaraðilinn ætti að tilkynna eftirlitsyfirvaldinu og hinum skráða um miðlunina.
- 114) Hvað sem öðru líður ætti ábyrgðaraðili eða vinnsluadili, ef framkvæmdastjórnin hefur ekki tekið ákvörðun um hvort persónuvernd sé fullnægjandi í þriðja landi, að nýta sér lausnir sem veita skráðum einstaklingum framfylgjanleg og skilvirk réttindi að því er varðar vinnslu persónuupplýsinga um þá í Sambandinu eftir að miðlun þessara upplýsinga hefur farið fram svo að þeir njóti áfram grundvallarréttinda og verndarráðstafana.
- 115) Sum þriðju lönd samþykkja lög, reglur og aðrar réttargerðir sem lúta að beinu eftirliti með vinnsluadgerðum einstaklinga og lögaðila undir lögsögu aðildarríkjanna. Þetta kann að taka til dóma, sem dómstólar kveða upp eða ákvarðana stjórnvalda í þriðju löndum, sem krefjast þess að ábyrgðaraðili eða vinnsluadili miðli persónuupplýsingum eða birti þær og sem byggjast ekki á alþjóðasamningi á borð við samning um gagnkvæma dómsmálaaðstoð, sem er í gildi milli þriðja landsins, sem leggur fram beiðni, og Sambandsins eða aðildarríkis. Ef beiting þessara laga, reglna og annarra réttargerða er ekki svæðisbundin getur það gengið gegn þjóðarétti og kann að standa í vegi fyrir þeirri vernd sem einstaklingum er tryggð í Sambandinu með þessari reglugerð. Aðeins ætti að heimila miðlun ef skilyrðum þessarar reglugerðar um miðlun til þriðju landa er fullnægt. Þetta getur m.a. átt við þegar birting er nauðsynleg vegna mikilvægra almannahagsmuna sem viðurkenndir eru í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir.
- 116) Þegar persónuupplýsingar fara yfir landamæri utan Sambandsins getur það leitt til aukinnar áhættu fyrir getu einstaklinga til að neyta réttar síns til persónuverndar, einkum verja sig gegn ólögmætri notkun eða birtingu umræddra upplýsinga. Jafnframt geta eftirlitsyfirvöld komist að þeirri niðurstöðu að þau geti ekki fylgt eftir kvörtunum eða sinnt rannsóknum í tengslum við starfsemi utan landamæra sinna. Ófullnægjandi valdheimildir til forvarna eða úrbóta, misræmi milli lagareglna og hindranir sem lúta að framkvæmd á borð við takmarkað fjármagn geta staðið í vegi fyrir viðleitni þeirra til að vinna saman yfir landamæri. Þess vegna þarf að hvetja til nánara samstarfs meðal eftirlitsyfirvalda á sviði persónuverndar til að hjálpa þeim við að skiptast á upplýsingum og vinna að rannsóknum með samsvarandi alþjóðlegum aðilum. Í þeim tilgangi að móta fyrirkomulag alþjóðlegrar samvinnu til að greiða fyrir og veita gagnkvæma aðstoð á alþjóðavettvangi við framkvæmd löggjafar um vernd persónuupplýsinga ættu framkvæmdastjórnin og eftirlitsyfirvöldin að skiptast á upplýsingum og starfa með lögbærum yfirvöldum þriðju landa að

verkefnum sem tengjast beitingu valdheimilda þeirra, á gagnkvæmum grundvelli og í samræmi við þessa reglugerð.

- 117) Þýðingarmikill þáttur í vernd einstaklinga að því er varðar vinnslu persónuupplýsinga þeirra felst í því að koma eftirlitsyfirvöldum á fót í aðildarríkjunum með umboð til að gegna störfum sínum og beita valdheimildum sínum algerlega óháð öðrum. Aðildarríkin ættu að geta komið á fót fleiri en einu eftirlitsyfirvaldi til að endurspegla stjórnskipan sína, stjórnunarhætti og skipulag stjórnsýslu.
- 118) Sjálfstæði eftirlitsyfirvalda ætti ekki að þýða að þau þurfi ekki að hlíta eftirlits- eða vöktunarkerfum í tengslum við útgjöld sín eða eftirliti dómstóla.
- 119) Ef aðildarríki kemur á fót fleiri en einu eftirlitsyfirvaldi ætti það að koma á kerfi samkvæmt lögum til að tryggja skilvirka þátttöku eftirlitsyfirvaldanna í samræmingarkerfinu. Umrætt aðildarríki ætti einkum að tilnefna það eftirlitsyfirvald sem gegnir hlutverki sameiginlegs tengiliðar vegna virkrar þátttöku þessara yfirvalda í kerfinu til þess að tryggja skjóta og snurðulausa samvinnu við önnur eftirlitsyfirvöld, persónuverndarráðið og framkvæmdastjórnina.
- 120) Sérhvert eftirlitsyfirvald ætti að hafa yfir að ráða því fjármagni, þeim mannauði, húsakosti og innviðum sem nauðsynleg eru til að þau geti sinnt verkefnum sínum með skilvirkum hætti, þ.m.t. þeim sem lúta að gagnkvæmri aðstoð og samvinnu við önnur eftirlitsyfirvöld alls staðar í Sambandinu. Sérhvert eftirlitsyfirvald ætti að hafa sérstaka, opinbera árlega fjárhagsáætlun sem getur verið hluti af heildarfjárlögum fylkisins eða ríkisins.
- 121) Mæla ætti fyrir um almenn skilyrði fyrir fulltrúa eftirlitsyfirvaldsins í lögum hvers aðildarríkis og í þeim ætti einkum að kveða á um að þing, ríkisstjórn eða þjóðhöfðingjar aðildarríkisins skipi þessa fulltrúa á grundvelli gagnsærrar málsmeðferðar, að fenginni tillögu ríkisstjórnarinnar, ráðherra hennar, þingsins eða þingdeildar, eða að sjálfstæðum aðila sé falið það verkefni samkvæmt lögum aðildarríkis. Til þess að tryggja sjálfstæði eftirlitsyfirvaldsins ættu fulltrúarnir að koma fram af heilindum, ekki aðhafast neitt það sem er ósamrýmanlegt skyldum þeirra og ekki að stunda önnur launuð eða ólaunuð ósamrýmanleg störf á skipunartíma sínum. Eftirlitsyfirvaldið ætti að hafa eigið starfslið, valið af því sjálfu eða sjálfstæðum aðila, sem er komið á fót samkvæmt lögum aðildarríkis, og ætti það eingöngu að lúta stjórn fulltrúa eftirlitsyfirvaldsins.
- 122) Sérhvert eftirlitsyfirvald ætti að vera til þess bært á yfirráðasvæði eigin aðildarríkis að beita þeim valdheimildum og vinna þau verkefni sem því eru falin samkvæmt þessari reglugerð. Þau ættu einkum að taka til vinnslu í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila á yfirráðasvæði eigin aðildarríkis, vinnslu opinberra yfirvalda eða einkaaðila á persónuupplýsingum í þágu almannahagsmuna, vinnslu sem hefur áhrif á skráða einstaklinga á yfirráðasvæði þess eða vinnslu af hálfu ábyrgðaraðila eða vinnsluaðila, sem hefur ekki staðfestu í Sambandinu, þegar hún beinist að skráðum einstaklingum sem búa á yfirráðasvæði þess. Þar á meðal ætti að vera meðferð kvartana frá skráðum einstaklingi, framkvæmd rannsókna á beitingu þessarar reglugerðar og vitundarefning meðal almennings um áhættur, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga.
- 123) Eftirlitsyfirvöldin ættu að hafa eftirlit með beitingu ákvæðanna samkvæmt þessari reglugerð og stuðla að samræmdri framkvæmd hennar í öllu Sambandinu, til að vernda einstaklinga í tengslum við vinnslu persónuupplýsinga um þá og greiða fyrir frjálsu flæði persónuupplýsinga á innri markaðnum. Í því skyni ættu eftirlitsyfirvöld að hafa samstarf sín á milli og við framkvæmdastjórnina, án þess að nauðsynlegt sé að gera samning milli aðildarríkjanna um gagnkvæma aðstoð eða slíka samvinnu.
- 124) Þegar vinnsla persónuupplýsinga fer fram innan ramma starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu og ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu í fleiru en einu

aðildarríki, eða þegar vinnsla, sem fram fer innan ramma starfsemi stakrar starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu, hefur veruleg áhrif eða búast má við að hún hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki ætti eftirlitsyfirvald yfir höfuðstöðvum ábyrgðaraðila eða vinnsluaðila eða þessari einu starfsstöð ábyrgðaraðila eða vinnsluaðila að gegna hlutverki forystuyfirvalds. Það ætti að hafa samstarf við önnur hlutaðeigandi yfirvöld þegar ábyrgðaraðili eða vinnsluaðili er með starfsstöð á yfirráðsvæði þeirra, skráðir einstaklingar á yfirráðasvæði þeirra verða fyrir verulegum áhrifum eða kvörtun er lögð fram hjá þeim. Ef skráður einstaklingur, sem býr ekki í því aðildarríki, leggur fram kvörtun ætti eftirlitsyfirvaldið, sem kvörtunin er lögð fram hjá, einnig að vera hlutaðeigandi eftirlitsyfirvald. Innan ramma þeirra verkefna sinna að gefa út viðmiðunarreglur varðandi álitaefni, sem upp kunna að koma varðandi beitingu þessarar reglugerðar, ætti persónuverndarráðið að geta gefið út viðmiðunarreglur, einkum um þær viðmiðanir sem taka ber tillit til þegar gengið er úr skugga um hvort viðkomandi vinnsla hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki og hvað teljast vera viðeigandi og rökstudd andmæli.

125) Forystuyfirvaldið ætti að vera til þess bært að samþykka bindandi ákvarðanir um ráðstafanir og beita til þess þeim valdheimildum sem því eru fengnar í samræmi við þessa reglugerð. Í krafti hlutverks síns sem forystuyfirvald ætti eftirlitsyfirvaldið að virkja hlutaðeigandi eftirlitsyfirvöld til þátttöku í ákvarðanatökuferlinu og samhæfa þau. Ef ákveðið er að hafna kvörtun viðkomandi skráðs einstaklings, að öllu leyti eða að hluta til, ætti eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, að taka þá ákvörðun.

126) Forystueftirlitsyfirvaldið og önnur hlutaðeigandi eftirlitsyfirvöld ættu að komast að samkomulagi um ákvörðunina og henni ætti að beina til höfuðstöðva eða hinnar einu starfsstöðvar ábyrgðaraðilans eða vinnsluaðilans og vera bindandi gagnvart honum. Ábyrgðaraðilinn eða vinnsluaðilinn ætti að grípa til nauðsynlegra ráðstafana til að tryggja að farið sé að þessari reglugerð og framkvæmd ákvörðunarinnar sem forystueftirlitsyfirvaldið tilkynnir um til höfuðstöðva ábyrgðaraðilans eða vinnsluaðilans að því er varðar vinnslustarfsemi í Sambandinu.

127) Eftirlitsyfirvald, sem gegnir ekki hlutverki forystueftirlitsyfirvalds, ætti að vera til þess bært að taka á staðbundnum málum þegar ábyrgðaraðili eða vinnsluaðili hefur staðfestu í fleiri en einu aðildarríki en viðfangsefni hinnar tilteknu vinnslu varðar einungis vinnslu sem fram fer í einu aðildarríki og tekur einungis til skráðra einstaklinga í því eina aðildarríki, t.d. þegar það varðar vinnslu persónuupplýsinga um starfsmenn í tilteknu atvinnutengdu samhengi í aðildarríki. Í þeim tilvikum ætti eftirlitsyfirvaldið að tilkynna forystueftirlitsyfirvaldinu um málið án tafar. Eftir að forystueftirlitsyfirvaldinu hefur verið tilkynnt um málið ætti það að ákveða hvort það muni afgreiða það samkvæmt ákvæðinu um samstarf milli forystueftirlitsyfirvaldsins og annarra hlutaðeigandi eftirlitsyfirvalda („afgreiðsla á einum stað“) eða hvort eftirlitsyfirvaldið, sem sendi því tilkynninguna, eigi að afgreiða málið á staðarvísu. Þegar forystueftirlitsyfirvaldið tekur ákvörðun um hvort það muni afgreiða málið ætti það að taka tillit til þess hvort ábyrgðaraðili eða vinnsluaðili er með starfsstöð í aðildarríki eftirlitsyfirvaldsins, sem tilkynnti um málið, til að tryggja skilvirka framfylgd ákvörðunar gagnvart ábyrgðaraðilanum eða vinnsluaðilanum. Ákveði forystueftirlitsyfirvaldið að taka sjálft að sér afgreiðslu málsins ætti eftirlitsyfirvaldið, sem tilkynnti um málið, að eiga kost á því að leggja fram drög að ákvörðun sem forystueftirlitsyfirvaldinu ber að taka itrasta tillit til þegar það útbýr drög sín að ákvörðun innan fyrirkomulagsins um afgreiðslu á einum stað.

128) Reglurnar um forystueftirlitsyfirvald og afgreiðslu á einum stað ættu ekki að gilda þegar opinber yfirvöld eða einkaaðilar annast vinnsluna í þágu almannahagsmuna. Í þeim tilvikum ætti eftirlitsyfirvald aðildarríkisins, þar sem opinbera yfirvaldið eða einkaaðilinn hefur staðfestu, að vera eina eftirlitsyfirvaldið sem er til þess bært að beita þeim valdheimildum sem því eru fengnar samkvæmt þessari reglugerð.

129) Til þess að tryggja samræmt eftirlit og framfylgd þessarar reglugerðar alls staðar í Sambandinu ættu eftirlitsyfirvöld að hafa í hverju aðildarríki á hendi sömu verkefni og skilvirkar valdheimildir, þ.m.t.

heimildir til rannsókna, til að gera ráðstafanir til úrbóta og setja viðurlög og leyfisveitinga- og ráðgjafarheimildir, einkum þegar um er að ræða kvartanir frá einstaklingum og, án þess að það hafi áhrif á valdheimildir yfirvalda sem fara með ákærvald samkvæmt lögum aðildarríkis, til að vekja athygli dómsyfirvalda á brotum gegn þessari reglugerð og fara með mál fyrir dóm. Á meðal slíkra valdheimilda ætti einnig að vera heimild til að taka upp tímabundna eða varanlega takmörkun á vinnslu, þ.m.t. bann. Aðildarríkin geta tilgreint önnur verkefni í tengslum við vernd persónuupplýsinga samkvæmt þessari reglugerð. Valdheimildum eftirlitsyfirvalda ætti að beita í samræmi við viðeigandi réttarfarsreglur sem settar eru fram í lögum Sambandsins og lögum aðildarríkis, af óhlutdrægni og sanngirni og innan hæfilegs tíma. Einkum ætti sérhver ráðstöfun að vera viðeigandi, nauðsynleg og hófleg til að tryggja að farið sé að þessari reglugerð, með hliðsjón af aðstæðum í hverju tilviki fyrir sig, virða rétt hvers aðila til að koma sjónarmiðum sínum á framfæri áður en gripið er til einhverrar þeirrar ráðstöfunar sem væri honum í óhag og þannig útfærð að komist sé hjá óhóflegum kostnaði og óþægindum fyrir viðkomandi einstaklinga. Rannsóknarheimildum að því er varðar aðgang að athafnasvæði ætti að beita í samræmi við sérstakar kröfur í réttarfarslögum aðildarríkisins, s.s. kröfuna um að afla fyrirframheimildar dómsmálafyrivalda. Sérhver lagalega bindandi ráðstöfun eftirlitsyfirvaldsins ætti að vera skrifleg, skýr og ótvíræð, í henni ætti að koma fram hvaða eftirlitsyfirvald gaf hana út, útgáfudagur, á henni ætti að vera undirskrift yfirmanns eða fulltrúa eftirlitsyfirvaldsins sem hann hefur veitt heimild, þar skulu koma fram ástæður fyrir ráðstöfuninni og vísað til réttarins til skilvirks úrræðis til að leita réttar síns. Þetta útilokar ekki viðbótarkröfur samkvæmt réttarfarslögum aðildarríkis. Þegar tekin er lagalega bindandi ákvörðun getur það haft í för með sér endurskoðun dómstóla í aðildarríki eftirlitsyfirvaldsins sem samþykkti ákvörðunina.

- 130) Ef eftirlitsyfirvald, sem kvörtun er lögð fram hjá, er ekki forystueftirlitsyfirvald ætti forystueftirlitsyfirvaldið að starfa náið með eftirlitsyfirvaldinu, sem kvörtunin er lögð fram hjá, í samræmi við ákvæði þessarar reglugerðar um samstarf og samræmi. Í þeim tilvikum ætti forystueftirlitsyfirvaldið, þegar það gerir ráðstafanir sem ætlað er að hafa réttaráhrif, þ.m.t. að leggja á stjórnsýslusektir, að taka ýtrasta tillit til sjónarmiða eftirlitsyfirvaldsins sem kvörtunin var lögð fram hjá og það yfirvald ætti áfram að vera til þess bært að annast hvers kyns rannsóknir á yfirráðasvæði eigin aðildarríkis í samráði við lögbæra eftirlitsyfirvaldið.
- 131) Þegar annað eftirlitsyfirvald ætti að fara með hlutverk forystueftirlitsyfirvalds vegna vinnslustarfsemi ábyrgðaraðila eða vinnsluaðila en efni kvörtunar eða hugsanlegt brot varðar einungis vinnslustarfsemi ábyrgðaraðila eða vinnsluaðila í aðildarríkinu þar sem kvörtunin var lögð fram eða hugsanlegt brot greindist og málið hefur ekki veruleg áhrif, né heldur er buist við að það muni hafa veruleg áhrif, á skráða einstaklinga í öðrum aðildarríkjum ætti eftirlitsyfirvaldið, sem tekur við kvörtuninni eða sem kemst á snoðir um eða er látið vita á annan hátt af aðstæðum sem gætu haft í för með sér hugsanlegt brot á þessari reglugerð, að leitast við að ná góðri sátt við ábyrgðaraðilann og, ef það tekst ekki, beita valdheimildum sínum að fullu. Þetta ætti að ná til tiltekinnar vinnslu sem fram fer á yfirráðasvæði aðildarríkis eftirlitsyfirvaldsins eða, að því er varðar skráða einstaklinga á yfirráðasvæði þess aðildarríkis, vinnslu sem fram fer í tengslum við boð á vörum eða þjónustu sem beint er sérstaklega til skráðra einstaklinga á yfirráðasvæði aðildarríkis eftirlitsyfirvaldsins eða vinnslu sem þarf að meta með hliðsjón af viðeigandi lagaskyldum samkvæmt lögum aðildarríkis.
- 132) Starfsemi eftirlitsyfirvalda, sem miðar að vitundarvakningu og beint er að almenningi, ætti m.a. að fela í sér sérstakar ráðstafanir sem beint er að ábyrgðaraðilum og vinnsluaðilum, þ.m.t. örfyrirtækjum, litlum og meðalstórum fyrirtækjum, og einnig einstaklingum, einkum í fræðsluskyni.
- 133) Eftirlitsyfirvöld ættu að aðstoða hvert annað við framkvæmd verkefna sinna og láta í té gagnkvæma aðstoð til að tryggja samræmda beitingu og framkvæmd þessarar reglugerðar á innri markaðnum. Eftirlitsyfirvald, sem biður um gagnkvæma aðstoð, getur gripið til bráðabirgðaráðstöfunar ef því berst ekkert svar við beiðninni um gagnkvæma aðstoð innan mánaðar frá því að hinu eftirlitsyfirvaldinu barst beiðnin.
- 134) Sérhvert eftirlitsyfirvald ætti, eftir því sem við á, að taka þátt í sameiginlegum aðgerðum ásamt öðrum eftirlitsyfirvöldum. Eftirlitsyfirvaldi, sem berst beiðni, ætti að vera skylt að svara beiðninni innan tiltekins

tíma.

- 135) Til þess að tryggja samræmda beitingu þessarar reglugerðar í öllu Sambandinu ætti að koma á fót samræmingarkerfi um samstarf milli eftirlitsyfirvalda. Einkum ætti að beita kerfinu þegar eftirlitsyfirvald hyggst gera ráðstöfun sem ætlað er að hafa réttaráhrif vegna vinnsluaðgerða sem hafa veigamikil áhrif á verulegan fjölda skráðra einstaklinga í nokkrum aðildarríkjum. Því ætti einnig að beita þegar eitthvert hlutaðeigandi eftirlitsyfirvalda eða framkvæmdastjórnin fer fram á að samræmingarkerfið annist meðferð slíks máls. Kerfið ætti ekki að hafa áhrif á neinar þær ráðstafanir sem framkvæmdastjórnin kann að grípa til þegar hún beitir valdheimildum sínum samkvæmt sáttmálunum.
- 136) Þegar samræmingarkerfið er notað ætti persónuverndarráðið, innan tiltekins tíma, að gefa út álit ef meirihluti fulltrúa þess ákveður það eða ef eitthvert hlutaðeigandi eftirlitsyfirvalda eða framkvæmdastjórnin fer fram á það. Persónuverndarráðið ætti einnig að hafa vald til að taka lagalega bindandi ákvarðanir þegar ágreiningur ríkir milli eftirlitsyfirvalda. Í því skyni ætti það að gefa út, að jafnaði með meirihluta sem nemur tveimur þriðju hlutum fulltrúa þess, lagalega bindandi ákvarðanir í skýrt skilgreindum málum þar sem eftirlitsyfirvöld greinir á um sjónarmið, nánar tiltekið innan samstarfskerfisins milli forystueftirlitsyfirvalds og hlutaðeigandi eftirlitsyfirvalda, um málavexti, einkum hvort um er að ræða brot á þessari reglugerð.
- 137) Skapast getur brýn þörf á að grípa inn í til að vernda réttindi og frelsi skráðra einstaklinga, einkum þegar hætta gæti verið á verulegri hindrun á framfylgd réttinda skráðs einstaklings. Því ætti eftirlitsyfirvaldi að vera heimilt að grípa til, á yfirráðasvæði sínu, tilhlýðilega rökstuddra bráðabirgðaráðstafana með tilgreindan gildistíma sem ekki ætti að vera lengri en þrír mánuðir.
- 138) Beiting slíks kerfis ætti að vera skilyrði fyrir því að ráðstöfun eftirlitsyfirvalds, sem ætlað er að hafa réttaráhrif, teljist lögmæt í þeim tilvikum þar sem beiting þess er skyldubundin. Í öðrum tilvikum sem ná yfir landamæri ætti að beita samstarfskerfinu milli forystueftirlitsyfirvaldsins og hlutaðeigandi eftirlitsyfirvalda og beita mætti gagnkvæmri aðstoð og sameiginlegum aðgerðum milli hlutaðeigandi eftirlitsyfirvalda, tvíhliða eða marghliða, án þess að virkja samræmingarkerfið.
- 139) Til að ýta undir samræmda beitingu þessarar reglugerðar ætti að koma persónuverndarráðinu á fót sem sjálfstæðum aðila Sambandsins. Til að uppfylla markmið sín ætti persónuverndarráðið að hafa réttarstöðu lögaðila. Formaður persónuverndarráðsins kemur fram fyrir hönd þess. Það ætti að leysa af hólmi starfshópin um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga sem komið var á fót með tilskipun 95/46/EB. Í því ættu að eiga sæti yfirmenn eftirlitsyfirvalds hvers aðildarríkis og Evrópsku persónuverndarstofnunarinnar eða fulltrúar þeirra hvers um sig. Framkvæmdastjórnin ætti að taka þátt í starfsemi persónuverndarráðsins án atkvæðisréttar og Evrópska persónuverndarstofnunarinnar ætti að hafa sérstakan atkvæðisrétt. Persónuverndarráðið ætti að stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu, m.a. með ráðgjöf til framkvæmdastjórnarinnar, einkum um umfang verndar í þriðju löndum eða hjá alþjóðastofnunum og með því að ýta undir samstarf eftirlitsyfirvalda í Sambandinu. Persónuverndarráðið ætti að vera sjálfstætt í störfum sínum.
- 140) Persónuverndarráðið ætti að njóta aðstoðar skrifstofu sem Evrópska persónuverndarstofnunin sér því fyrir. Starfsfólk Evrópsku persónuverndarstofnunarinnar, sem kemur að framkvæmd þeirra verkefna sem persónuverndarráðinu eru falin með þessari reglugerð, ætti að vinna verkefni sín alfarið undir stjórn formanns persónuverndarráðsins og heyra undir hann.
- 141) Sérhver skráður einstaklingur ætti að eiga rétt á að leggja fram kvörtun hjá einu eftirlitsyfirvaldi, einkum í aðildarríkinu þar sem hann hefur fasta búsetu, og hafa rétt til skilvirks réttarræðis í samræmi við 47. gr. sáttmálans um grundvallarréttindi ef hann telur að brotið sé á réttindum hans samkvæmt þessari reglugerð eða ef eftirlitsyfirvald sinnir ekki kvörtun, hafnar kvörtun að hluta til eða að öllu leyti eða vísar henni frá eða grípur ekki til aðgerða þar sem aðgerða er þörf til að vernda réttindi hans. Rannsókn á kvörtun ætti að fara fram, með fyrirvara um endurskoðun dómstóla, að því marki sem við á í hverju tilviki.

Eftirlitsyfirvaldið ætti að tilkynna hinum skráða um framvindu og niðurstöðu kvörtunarinnar innan hæfilegs tíma. Ef þörf er á frekari rannsókn málsins eða samræmingu við annað eftirlitsyfirvald ætti að veita hinum skráða í millitiðinni upplýsingar um stöðu málsins. Til að auðvelda framlagningu kvartana ætti hvert eftirlitsyfirvald að gera ráðstafanir á borð við að bjóða upp á kvörtunareyðublað, sem einnig má fylla út rafrænt, án þess þó að útiloka aðra samskiptamöguleika.

142) Telji skráður einstaklingur að brotið hafi verið á réttindum hans samkvæmt þessari reglugerð ætti hann að hafa rétt til að veita stofnun, samtökum eða félagi, sem ekki eru rekin í hagnaðarskyni og sem stofnuð eru í samræmi við lög aðildarríkis, hafa lögboðin markmið og eru virk á sviði verndar persónuupplýsinga, umboð til að leggja fram kvörtun fyrir sína hönd hjá eftirlitsyfirvaldi, nýta réttinn til réttarúrræðis fyrir hönd skráðra einstaklinga eða, ef kveðið er á um það í lögum aðildarríkis, nýta réttinn til að taka við skaðabótum fyrir hönd skráðra einstaklinga. Aðildarríki er heimilt að mæla fyrir um að slík stofnun, samtök eða félag eigi rétt á að leggja fram kvörtun í því aðildarríki, óháð því hvort hinn skráði hefur veitt umboð til þess, og rétt til skilvirks réttarúrræðis hafi það ástæður til að ætla að réttindi skráðs einstaklings hafi verið brotin við vinnslu persónuupplýsinga sem brýtur gegn þessari reglugerð. Ekki má heimila stofnuninni, samtökunum eða félaginu að krefjast bóta fyrir hönd skráðs einstaklings án umboðs hans.

143) Einstaklingur eða lögaðili hefur rétt til þess að höfða mál til ógildingar ákvörðunum persónuverndarráðsins frammi fyrir Dómstólnum samkvæmt þeim skilyrðum sem kveðið er á um í 263. gr. sáttmálans um starfshætti Evrópusambandsins. Sem viðtakendur slíkra ákvarðana þurfa hlutaðeigandi eftirlitsyfirvöld, sem vilja vefengja þær, að höfða mál innan tveggja mánaða frá því að þeim er tilkynnt um þær, í samræmi við 263. gr. sáttmálans um starfshætti Evrópusambandsins. Þegar ákvarðanir persónuverndarráðsins varða beint sérstaka hagsmuni ábyrgðaraðila, vinnsluaðila eða kvartanda getur hann höfðað mál til ógildingar þessum ákvörðunum innan tveggja mánaða frá birtingu þeirra á vefsetri persónuverndarráðsins, í samræmi við 263. gr. sáttmálans um starfshætti Evrópusambandsins. Með fyrirvara um þennan rétt skv. 263. gr. sáttmálans um starfshætti Evrópusambandsins ætti sérhver einstaklingur eða lögaðili að hafa aðgang að skilvirku réttarúrræði fyrir lögbærum innlendum dómstóli að því er varðar ákvörðun eftirlitsyfirvalds sem hefur réttaráhrif gagnvart honum. Slík ákvörðun varðar einkum beitingu eftirlitsyfirvalds á rannsóknarheimildum, valdheimildum til að gera ráðstafanir til úrbóta og leyfisveitingarheimildum sínum eða frávisun eða höfnun kvartana. Þó nær réttur til skilvirks réttarúrræðis ekki til þeirra ráðstafana eftirlitsyfirvalda sem eru ekki lagalega bindandi, s.s. álitsgerða eða ráðgjafar eftirlitsyfirvaldsins. Höfða ætti mál gegn eftirlitsyfirvaldi fyrir dómstólum aðildarríkisins þar sem eftirlitsyfirvaldið hefur staðfestu og reka það í samræmi við réttarfarslög þess aðildarríkis. Þessir dómstólar ættu að fara með fulla lögsögu, m.a. til að rannsaka öll álitamál varðandi staðreyndir eða lög viðkomandi deiluefninu sem þeir hafa fengið til meðferðar.

Hafi eftirlitsyfirvald hafnað kröfu eða vísað henni frá getur sá sem lagði kvörtunina fram höfðað mál fyrir dómstólum í sama aðildarríki. Innan ramma réttarúrræða vegna beitingar þessarar reglugerðar geta innlendir dómstólar, sem telja að ákvörðun um álitaeftirbót sé nauðsynleg til að þeir geti kveðið upp úrskurð, farið fram á, eða verða að fara fram á í því tilviki sem um getur í 267. gr. sáttmálans um starfshætti Evrópusambandsins, að Dómstóllinn kveði upp forúrskurð um túlkun laga Sambandsins, m.a. þessarar reglugerðar, þegar ákvörðun eftirlitsyfirvalds til framkvæmdar ákvörðun persónuverndarráðsins er vefengd fyrir innlendum dómstól og deilt er um gildi ákvörðunar persónuverndarráðsins hefur innlendi dómstóllinn ekki vald til að lýsa ákvörðun þess ógilda heldur verður hann að vísa álitaeftirbótum um gildi til Dómstólsins í samræmi við 267. gr. sáttmálans um starfshætti Evrópusambandsins, eins og Dómstóllinn túlkar hana, ef hann telur ákvörðunina ógilda. Hins vegar má innlendir dómstóll ekki vísa áfram álitamáli um gildi ákvörðunar persónuverndarráðsins að beiðni einstaklings eða lögaðila sem hafði haft tækifæri til að höfða mál til ógildingar þeirri ákvörðun, einkum ef ákvörðunin varðaði beint sérstaka hagsmuni hans, en gerði það ekki innan frestsins sem mælt er fyrir um í 263. gr. sáttmálans um starfshætti Evrópusambandsins.

144) Hafi dómstóll, sem mál er höfðað fyrir gegn ákvörðun eftirlitsyfirvalds, ástæðu til að ætla að höfðað hafi verið mál vegna sömu vinnslu fyrir lögbærum dómstóli í öðru aðildarríki, þar sem t.d. um er að ræða sama viðfangsefni að því er varðar vinnslu af hálfu sama ábyrgðaraðila eða vinnsluaðila eða sömu málsástæður, ætti hann að setja sig í samband við þann dómstól til að fá staðfest hvort um skyld mál sé að ræða. Ef skyld mál er til meðferðar hjá dómstóli í öðru aðildarríki getur hvaða dómstóll sem er, annar en sá sem

málið var fyrst höfðað fyrir, frestað málsmeðferð sinni eða, að beiðni eins málsaðilanna, vísað málinu frá dómi í þágu dómstólsins sem málið var fyrst höfðað fyrir ef sá dómstóll er bær til að fara með málið og lög, sem gilda við þann dómstól, heimila að skyld mál séu sótt sameiginlega. Með skyldum málum er átt við mál sem eru svo tengd innbyrðis að æskilegt er að fara með þau og úrskurða í þeim sameiginlega til að koma í veg fyrir að ósamrýmanlegir dómar verði kveðnir upp ef dæmt er í hverju þeirra sérstaklega.

145) Þegar um er að ræða mál á hendur ábyrgðaraðila eða vinnsluaðila ætti stefnandi að geta valið um það hvort hann höfðar málið fyrir dómstólum aðildarríkja þar sem ábyrgðaraðili eða vinnsluaðili hefur starfsstöð eða þar sem hinn skráði er búsettur nema ábyrgðaraðili sé opinbert yfirvald aðildarríkis sem fer með opinbert vald.

146) Ábyrgðaraðili eða vinnsluaðili ætti að bæta hvert það tjón sem aðili verður fyrir vegna vinnslu sem brýtur í bága við reglugerð þessa. Ábyrgðaraðili eða vinnsluaðili ætti að vera undanþeginn bótaábyrgð ef hann sannar að hann ber enga ábyrgð á tjóni. Hugtakið tjón ætti að túlka vítt í ljósi dómaframkvæmdar Dómstólsins á þann hátt að endurspegli að fullu markmið þessarar reglugerðar. Þetta hefur ekki áhrif á neinar skaðabótakröfur vegna brota á öðrum reglum Sambandslaga eða laga aðildarríkis. Vinnsla, sem brýtur í bága við þessa reglugerð, nær einnig yfir vinnslu sem brýtur í bága við framseldar gerðir og framkvæmdargerðir sem samþykktar eru í samræmi við þessa reglugerð og lög aðildarríkis sem tilgreina nánar reglur þessarar reglugerðar. Skráðir einstaklingar ættu að fá fullar skaðabætur fyrir það tjón sem þeir verða fyrir. Þegar ábyrgðaraðilar eða vinnsluaðilar koma að sömu vinnslu ætti hver ábyrgðaraðili eða vinnsluaðili að vera ábyrgur fyrir öllu tjóninu. Þegar þeir eiga hlut að sama dómsmáli, í samræmi við lög aðildarríkis, geta skaðabætur þó skipst niður á þá eftir þeirri ábyrgð sem hver ábyrgðaraðili eða vinnsluaðili bar á tjóninu sem vinnslan olli, að því tilskildu að skráði einstaklingurinn, sem varð fyrir tjóninu, fái fullar skaðabætur. Ábyrgðaraðili eða vinnsluaðili, sem hefur greitt fullar skaðabætur, getur í kjölfarið gert endurkröfu á aðra ábyrgðaraðila eða vinnsluaðila sem tóku þátt í sömu vinnslu.

147) Þar sem þessi reglugerð hefur að geyma sértækar reglur um lögsögu, einkum að því er varðar mál þar sem leitað er réttarræðis gegn ábyrgðaraðila eða vinnsluaðila, m.a. skaðabóta, ættu almennar lögsögureglur, eins og þær sem um getur í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1215/2012 ⁽¹³⁾, ekki að hafa áhrif á beitingu þessara sértæku reglna.

148) Til að efla framfylgd reglna þessarar reglugerðar ætti að leggja á viðurlög, þ.m.t. stjórnslusektir, við hvers konar brotum á þessari reglugerð, til viðbótar við eða í staðinn fyrir viðeigandi ráðstafanir sem eftirlitsyfirvald gerir samkvæmt þessari reglugerð. Veita má áminningu í stað sektar þegar um er að ræða minni háttar brot eða ef sektin, sem líklegt er að lögð verði á, yrði óhófleg byrði fyrir einstakling. Engu að síður ætti að taka tilhlýðilegt tillit til þess hvers eðlis brotið er, hversu alvarlegt það er og hversu lengi það hefur staðið yfir, hvort það var framið af ásetningi, til hvaða aðgerða var gripið til að draga úr tjóni, hversu mikil ábyrgðin var eða hvort um fyrri brot sem skipta máli er að ræða, hvernig eftirlitsyfirvaldið komst á snoðir um brotið, hvort ráðstöfunum sem settar voru gagnvart ábyrgðaraðila eða vinnsluaðila var fylgt, hvort háttænisreglum var fylgt ásamt öðrum mildandi eða íþyngjandi þáttum. Álagning viðurlaga, þ.m.t. stjórnslusekta, ætti að vera háð viðeigandi réttarfarsreglum í samræmi við almennar meginreglur laga Sambandsins og sáttmálans um grundvallarréttindi, m.a. um skilvirka réttarvernd og sanngjarna málsmeðferð.

149) Aðildarríkin ættu að geta sett reglur um refsiviðurlög vegna brota á þessari reglugerð, þ.m.t. vegna brota á innlendum reglum sem samþykktar eru samkvæmt henni og innan marka hennar. Slík refsiviðurlög geta einnig gert ráð fyrir að viðkomandi sé sviptur þeim ávinningi sem hann hafði af brotum á þessari reglugerð. Hins vegar ætti álagning refsiviðurlaga vegna brota á slíkum innlendum reglum og stjórnsluviðurlögum ekki að leiða til brots á meginreglunni um að verða ekki saksóttur eða refsað tvívegis fyrir sama brot (ne bis in idem), eins og Dómstóllinn hefur túlkað hana.

(13) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1215/2012 frá 12. desember 2012 um dómvald og viðurkenningu á og fullnustu dóma í einkamálum og viðskiptamálum (Stjtið. ESB L 351, 20.12.2012, bls. 1).

150) Til að efla og samræma stjórnsýsluviðurlög vegna brota á þessari reglugerð ætti sérhvert eftirlitsyfirvald að hafa heimild til að leggja á stjórnsýslusektir. Í reglugerðinni ætti að tilgreina brotin ásamt hámarki og viðmiðunum við álagningu tengdra stjórnsýslusekta, sem eftirlitsyfirvaldið ætti að ákveða í hverju tilviki fyrir sig með hliðsjón af öllum viðeigandi kringumstæðum í viðkomandi máli, einkum að teknu tilhlýðilegu tilliti til eðlis, alvarleika og lengdar brotsins og afleiðinga þess og ráðstafana sem gerðar hafa verið til að tryggja að skuldbindingar samkvæmt þessari reglugerð séu uppfylltar og til að koma í veg fyrir eða draga úr afleiðingum brotsins. Þegar stjórnsýslusektir eru lagðar á fyrirtæki er átt við fyrirtæki í samræmi við 101. og 102. gr. sáttmálans um starfshætti Evrópusambandsins. Þegar stjórnsýslusektir eru lagðar á aðila sem ekki eru fyrirtæki ætti eftirlitsyfirvaldið að taka tillit til almenns tekjustigs í aðildarríkinu og fjárhagsstöðu aðilans þegar viðeigandi sektarfjárhæð er ákveðin. Einnig má nota samræmingarkerfið til að stuðla að samræmdri beitingu stjórnsýslusekta. Það ætti að vera aðildarríkjanna að ákvarða hvort og að hvaða marki opinber yfirvöld ættu að sæta stjórnsýslusektum. Það að lögð sé á stjórnsýslusekt eða að gefin sé viðvörðun hefur ekki áhrif á beitingu annarra valdheimilda eftirlitsyfirvalda eða á önnur viðurlög samkvæmt þessari reglugerð.

151) Réttarkerfi Danmerkur og Eistlands heimila ekki stjórnsýslusektir eins og þær sem settar eru fram í þessari reglugerð. Beita má reglunum um stjórnsýslusektir í Danmörku með þeim hætti að þar til bærir innlendir dómstólar leggi sektina á sem refsiviðurlög og í Eistlandi þannig að eftirlitsyfirvald leggi sektina á innan ramma málsmeðferðar vegna minni háttar brots, að því tilskildu að slík beiting reglnanna í þessum aðildarríkjum hafi jafngild áhrif og stjórnsýslusektir sem eftirlitsyfirvöld leggja á. Því ættu þar til bærir innlendir dómstólar að taka tillit til tilmæla eftirlitsyfirvaldsins sem hefur frumkvæðið að álagningu sektarinnar. Álagðar sektir ættu þó ætíð að vera skilvirkar, í réttu hlutfalli við brot og hafa varnaðaráhrif.

152) Þegar þessi reglugerð samræmir ekki stjórnsýsluviðurlög eða ef þörf er á í öðrum tilvikum, t.d. þegar um er að ræða alvarleg brot á þessari reglugerð, ættu aðildarríkin að innleiða kerfi sem kveður á um viðurlög sem eru skilvirk, í réttu hlutfalli við brot og hafa varnaðaráhrif. Það hvort slík viðurlög eigi að vera refsiviðurlög eða stjórnsýslulegs eðlis ætti að ákvarða í lögum aðildarríkjanna.

153) Í lögum aðildarríkjanna ætti að samræma reglur um tjáningar- og upplýsingafrelsi, þ.m.t. í fréttamennsku, fræðimennsku, listum eða bókmenntum, og réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð. Vinnsla persónuupplýsinga, sem fer einungis fram í þágu fréttamennsku eða fræðimennsku eða listrænnar eða bókmenntalegrar tjáningar, ætti að vera háð undanþágum eða frávikum frá tilteknum ákvæðum þessarar reglugerðar ef það er nauðsynlegt til að samræma réttinn til verndar persónuupplýsingum og réttinn til tjáningar- og upplýsingafrelsis sem er tryggður með 11. gr. sáttmálans um grundvallarréttindi. Þetta ætti einkum að gilda um vinnslu persónuupplýsinga á sviði hljóð- og myndmiðlunar og í gagna- og bókasöfnum fréttamiðla. Því ættu aðildarríkin að samþykkja löggjafarráðstafanir þar sem mælt er fyrir um nauðsynlegar undanþágur og frávik til að halda jafnvægi milli þessara grundvallarréttinda. Aðildarríkin ættu að samþykkja slíkar undanþágur og frávik varðandi almennar meginreglur, réttindi skráðra einstaklinga, ábyrgðaraðila og vinnsluaðila, miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, sjálfstæð eftirlitsyfirvöld, samstarf og samræmi og gagnavinnslu við tilteknar aðstæður. Ef slíkar undanþágur og frávik eru mismunandi milli aðildarríkja gilda lög aðildarríkisins sem ábyrgðaraðili heyrir undir. Með tilliti til mikilvægis réttarins til tjáningarfrelsis í hverju lýðræðisþjóðfélagi er nauðsynlegt að túlka hugtök vítt í tengslum við það frelsi, s.s. fréttamennsku.

154) Reglugerð þessi heimilar að tekið sé mið af meginreglunni um aðgang almennings að opinberum skjölum við beitingu hennar. Telja má að aðgangur almennings að opinberum skjölum sé í þágu almannahagsmuna. Persónuupplýsingar í skjölum í vörslu opinbers yfirvalds eða opinberrar stofnunar ætti viðkomandi yfirvaldi eða aðila að vera heimilt að birta almenningi ef kveðið er á um birtinguna í lögum Sambandsins eða lögum aðildarríkis sem opinbera yfirvaldið eða opinbera stofnunin heyrir undir. Slík lög ættu að samræma aðgang almennings að opinberum skjölum og endurnotkun upplýsinga frá hinu opinbera

annars vegar og réttinn til verndar persónuupplýsingum hins vegar og geta því kveðið á um nauðsynlega samræmingu við réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð. Tilvísunin til opinberra yfirvalda og stofnana ætti í því samhengi að taka til allra yfirvalda eða annarra stofnana sem heyra undir lög aðildarríkis um aðgang almennings að skjölum. Tilskipun Evrópuþingsins og ráðsins 2003/98/EB ⁽¹⁴⁾ skerðir ekki og hefur á engan hátt áhrif á umfang verndar einstaklinga með tilliti til vinnslu persónuupplýsinga samkvæmt ákvæðum laga Sambandsins og laga aðildarríkis og einkum breytir hún ekki þeim skyldum og réttindum sem sett eru fram í þessari reglugerð. Einkum ætti sú tilskipun ekki að gilda um gögn, sem enginn eða takmarkaður aðgangur er að samkvæmt reglum um aðgangsrétt til verndar persónuupplýsingum, og um hluta úr skjölum, sem eru aðgengilegir samkvæmt slíkum reglum, þegar skjalshlutarnir innihalda persónuupplýsingar og kveðið hefur verið á um í lögum að endurnotkun þeirra sé ósamrýmanleg lögum um vernd einstaklinga að því er varðar vinnslu persónuupplýsinga.

155) Í lögum aðildarríkis eða í kjarasamningum, þ.m.t. „vinnustaðasamningum“, kann að vera kveðið á um sértækar reglur um vinnslu persónuupplýsinga starfsmanna í atvinnutengdu samhengi, einkum skilyrði fyrir því að vinna megi persónuupplýsingar í atvinnutengdu samhengi á grundvelli samþykkis starfsmannsins og í sambandi við ráðningar, framkvæmd ráðningarsamnings, m.a. uppfyllingu skuldbindinga sem mælt er fyrir um í lögum eða kjarasamningum, stjórnun, undirbúning og skipulagningu vinnunnar, jafnrétti og fjölbreytileika á vinnustað, heilbrigði og öryggi á vinnustað, nýtingu og notkun réttinda og friðinda sem tengjast starfinu, gagnvart einstaklingi eða heildinni, og í þeim tilgangi að ljúka ráðningarsambandi.

156) Vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókn á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi ætti að vera með fyrirvara um viðeigandi verndarráðstafanir varðandi réttindi og frelsi skráðra einstaklinga samkvæmt þessari reglugerð. Þessar verndarráðstafanir ættu að tryggja að tæknilegar og skipulagslegar ráðstafanir séu gerðar, einkum til að sjá til þess að farið sé að meginreglunni um lágmörkun gagna. Frekari vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi skal fara fram þegar ábyrgðaraðili hefur metið hvort framkvæmanlegt sé að ná þessum tilgangi með vinnslu gagna sem gera ekki kleift, eða gera ekki lengur kleift, að bera kennsl á skráða einstaklinga, að því tilskildu að viðeigandi verndarráðstafanir séu fyrir hendi (s.s. notkun gerviauðkenna fyrir upplýsingarnar). Aðildarríkin ættu að kveða á um viðeigandi verndarráðstafanir varðandi vinnslu persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Aðildarríkjum ætti að vera heimilt, með tilteknum skilyrðum og með fyrirvara um viðeigandi verndarráðstafanir fyrir skráða einstaklinga, að setja fram nánari skilgreiningar og undanþágur að því er varðar kröfur um upplýsingar og réttinn til leiðréttingar, eyðingar, til að gleymast, til takmörkunar á vinnslu, til að flytja eigin gögn og til að andmæla vinnslu persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Viðkomandi skilyrði og verndarráðstafanir geta haft í för með sér að skráðir einstaklingar þurfi að fylgja tiltekinni málsmeðferð til að geta nýtt sér þessi réttindi, ef við á í ljósi þess tilgangs sem stefnt er að með þessari tilteknu vinnslu, auk tæknilegra og skipulagslegra ráðstafana sem miða að því að lágmarka vinnslu persónuupplýsinga í samræmi við meðalhófsregluna og nauðsynjarregluna. Vinnsla persónuupplýsinga í vísindaskyni ætti einnig að vera í samræmi við aðra viðeigandi löggjöf, s.s. um klínískar prófanir.

157) Með því að tengja saman upplýsingar úr mismunandi skráum geta vísindamenn öðlast nýja og afar verðmæta þekkingu á útbreiddu heilsufarsástandi á borð við hjarta- og æðasjúkdóma, krabbamein og þunglyndi. Með notkun skráa er hægt að efla rannsóknaniðurstöður, þar sem þær byggjast á stærra þýði. Í félagsvísindum gera rannsóknir á grundvelli skráa vísindamönnum kleift að öðlast mikilvæga þekkingu á langtímafylgni milli félagslegra aðstæðna af ýmsum toga, s.s. atvinnuleysis og menntunar, og annarra aðstæðna í lífi fólks. Rannsóknaniðurstöður, sem fást með notkun skráa, gefa trausta og vandaða þekkingu sem nota má til grundvallar við mótun og framkvæmd þekkingarstefnu, til að bæta lífsgæði margra og bæta skilvirkni félagsþjónustunnar. Til að greiða fyrir vísindarannsóknum er heimilt að vinna

(14) Tilskipun Evrópuþingsins og ráðsins 2003/98/EB frá 17. nóvember 2003 um endurnotkun upplýsinga frá hinu opinbera (Stjóð. ESB L 345, 31.12.2003, bls. 90).

persónuupplýsingar í þágu rannsókna á sviði vísinda að uppfylltum viðeigandi skilyrðum og verndarráðstöfunum í lögum Sambandsins eða lögum aðildarríkis.

- 158) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga vegna skjalavistunar en þó ætti að hafa í huga að reglugerðin á ekki við um látna einstaklinga. Opinber yfirvöld, opinberir aðilar eða einkaaðilar, sem halda skrár sem tengjast almannahagsmunum, ættu að vera þjónustuaðilar sem hafa samkvæmt lögum Sambandsins eða lögum aðildarríkis lagaskyldu til að afla, varðveita, meta, skipuleggja, lýsa, veita upplýsingar um, kynna, dreifa og veita aðgang að skrár sem hafa varanlegt gildi fyrir almannahagsmunum. Aðildarríkin ættu einnig að hafa heimild til að kveða á um frekari vinnslu persónuupplýsinga vegna skjalavistunar, t.d. í því skyni að veita sérstakar upplýsingar um stjórnmálahegðun í ríkjum þar sem áður ríkti einræði, um þjóðarmorð, glæpi gegn mannúð, einkum helförina, eða stríðsglæpi.
- 159) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga í þágu vísindarannsókna. Að því er þessa reglugerð varðar ber að túlka vinnslu persónuupplýsinga í þágu vísindarannsókna vítt þannig að undir hana falli t.d. tækniþróun og tilraunaverkefni, grunnrannsóknir, hagnýtar rannsóknir og rannsóknir sem einkaaðilar fjármagna. Auk þess ætti hún að taka tillit til þess markmiðs Sambandsins, skv. 1. mgr. 179. gr. sáttmálans um starfshætti Evrópusambandsins, að koma á evrópsku rannsóknasvæði. Rannsóknir í þágu almannahagsmuna á sviði lýðheilsu ættu einnig að teljast þjóna vísindalegum tilgangi Til að uppfylla þær sérstöku kröfur sem gerðar eru til vinnslu persónuupplýsinga í þágu vísindarannsókna ættu sérstök skilyrði að gilda, einkum að því er varðar útgáfu eða aðra birtingu persónuupplýsinga í þágu vísindarannsókna. Gefi niðurstöður vísindarannsókna, einkum á heilbrigðissviði, ástæðu til að gera frekari ráðstafanir í þágu hins skráða ættu almennar reglur þessarar reglugerðar að gilda í ljósi þessara ráðstafana.
- 160) Þessi reglugerð ætti einnig að gilda um vinnslu persónuupplýsinga í þágu sagnfræðirannsókna. Þetta ætti auk þess að ná til sagnfræðirannsókna og rannsókna í erfðafræðilegum tilgangi en þó ætti að hafa í huga að reglugerðin ætti ekki að gilda um látna einstaklinga.
- 161) Að því er varðar veitingu samþykkis fyrir þátttöku í vísindalegri rannsóknastarfsemi í klínískum prófunum ættu viðeigandi ákvæði reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 536/2014 ⁽¹⁵⁾ að gilda.
- 162) Þessi reglugerð ætti að gilda um vinnslu persónuupplýsinga í tölfræðilegum tilgangi. Í lögum Sambandsins eða lögum aðildarríkis ætti að ákvarða, innan marka þessarar reglugerðar, tölfræðilegt innihald, eftirlit með aðgangi, nákvæmar skilgreiningar á vinnslu persónuupplýsinga í tölfræðilegum tilgangi og viðeigandi ráðstafanir til að standa vörð um réttindi og frelsi skráðra einstaklinga og tryggja trúnað í tengslum við tölfræðilegar upplýsingar. Tölfræðilegur tilgangur telst vera hver sú aðgerð sem felst í söfnun og vinnslu persónuupplýsinga sem nauðsynlegar eru vegna tölfræðilegra kannana eða til að ná fram tölfræðilegum niðurstöðum. Þessar tölfræðilegu niðurstöður má nota frekar í ýmiss konar tilgangi, þ.m.t. til vísindarannsókna. Tölfræðilegur tilgangur þýðir að niðurstöður vinnslu í tölfræðilegum tilgangi eru ekki persónuupplýsingar heldur samantekin gögn og að þessar niðurstöður eða persónuupplýsingarnar eru ekki notaðar til stuðnings ráðstöfunum eða ákvörðunum viðvíkjandi tilteknum einstaklingi.
- 163) Vernda ætti trúnaðarupplýsingar sem hagskýrsluyfirvöld Sambandsins og hagskýrsluyfirvöld aðildarríkjanna safna til að gera opinberar hagskýrslur fyrir Evrópu og aðildarríkin. Þróa ætti og semja evrópskar hagskýrslur og miðla þeim í samræmi við meginreglur um hagskýrslur, eins og þær eru settar fram í 2. mgr. 338. gr. sáttmálans um starfshætti Evrópusambandsins, en jafnframt ættu innlendar hagskýrslur einnig að uppfylla lög aðildarríkis. Í reglugerð Evrópuþingsins og ráðsins (EB) nr. 223/2009 ⁽¹⁶⁾ er kveðið á um nánari skilgreiningar á trúnaðarskyldum við hagskýrslugerð að því er varðar evrópskar

⁽¹⁵⁾ Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 536/2014 frá 16. apríl 2014 um klínískar prófanir á mannalyfjum og niðurfellingu á tilskipun 2001/20/EB (Stjóð. ESB L 158, 27.5.2014, bls. 1).

⁽¹⁶⁾ Reglugerð Evrópuþingsins og ráðsins (EB) nr. 223/2009 frá 11. mars 2009 um evrópskar hagskýrslur og niðurfellingu reglugerðar Evrópuþingsins og ráðsins (EB, KBE) nr. 1101/2008 um afhendingu gagna sem eru háð trúnaðarkvæðum í hagskýrslum til Hagstofu Evrópubandalaganna, reglugerðar ráðsins (EB) nr. 322/97 um hagskýrslur Bandalagsins og ákvörðunar ráðsins 89/382/EEB, KBE um að koma á fót hagskýrsluáætlunarnefnd Evrópubandalaganna (Stjóð. ESB. L 87, 31.3.2009, bls. 164).

hagskýrslur.

- 164) Að því er varðar valdheimildir eftirlitsyfirvalda til að fá hjá ábyrgðaraðila eða vinnsluaðila aðgang að persónuupplýsingum og aðgang að athafnasvæðum þeirra mega aðildarríki samþykkja með lögum, innan marka þessarar reglugerðar, sértækar reglur til að standa vörð um þagnarskyldu eða aðrar samsvarandi trúnaðarskyldur, að því marki sem nauðsynlegt er til að samræma réttinn til verndar persónuupplýsingum og þagnarskyldu. Þetta hefur ekki áhrif á fyrirbyggjandi skuldbindingar aðildarríkis um að samþykkja reglur um þagnarskyldu ef lög Sambandsins kveða á um það.
- 165) Þessi reglugerð virðir þá stöðu sem kirkjudeildir og trúarsamtök eða trúfélög hafa í aðildarríkjunum samkvæmt fyrirbyggjandi stjórnskipunarlögum og dregur hana ekki í efa, eins og viðurkennt er í 17. gr. sáttmálans um starfshætti Evrópusambandsins.
- 166) Til að ná markmiðum þessarar reglugerðar, þ.e. að vernda grundvallarréttindi og frelsi einstaklinga og einkum rétt þeirra til verndar persónuupplýsingum og tryggja frjálsa miðlun persónuupplýsinga innan Sambandsins, ætti að framselja framkvæmdastjórninni vald til að samþykkja gerðir í samræmi við 290. gr. sáttmálans um starfshætti Evrópusambandsins. Einkum ætti að samþykkja framseldar gerðir um viðmiðanir og kröfur varðandi vottunarfyrirkomulag, upplýsingar sem veita ber með stöðluðum táknumyndum og aðferðir við að setja fram slíkar táknumyndir. Einkar mikilvægt er að framkvæmdastjórnin hafi viðeigandi samráð meðan á undirbúningsvinnu hennar stendur, þ.m.t. við sérfræðinga. Við undirbúning og samningu framseldra gerða ætti framkvæmdastjórnin að tryggja samhlíða, tímanlega og viðeigandi afhendingu viðkomandi skjala til Evrópuþingsins og ráðsins.
- 167) Til að tryggja samræmd skilyrði vegna framkvæmdar þessarar reglugerðar ætti að fella framkvæmdastjórninni framkvæmdarvald þegar kveðið er á um það í þessari reglugerð. Þessu valdi ætti að beita í samræmi við reglugerð (ESB) nr. 182/2011. Í þessu sambandi ætti framkvæmdastjórnin að íhuga sértækar ráðstafanir fyrir örfyrirtæki, lítil og meðalstór fyrirtæki.
- 168) Beita ætti rannsóknarmálsmeðferðinni við samþykkt framkvæmdargerða um föst samningsákvæði milli ábyrgðaraðila og vinnsluaðila og milli vinnsluaðila, hátternisreglur, tæknistaðla og fyrirkomulag við vottun, fullnægjandi vernd sem þriðja land, yfirráðasvæði eða tilgreindur geiri innan þess þriðja lands eða alþjóðastofnun veitir, stöðluð verndarákvæði, snið og aðferðir við rafræn upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsyfirvalda að því er varðar bindandi fyrirtækjareglur, gagnkvæma aðstoð og fyrirkomulag við rafræn upplýsingaskipti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins.
- 169) Framkvæmdastjórnin ætti að samþykkja framkvæmdargerðir sem taka gildi þegar í stað ef fyrir liggja sannanir um að þriðja land, yfirráðasvæði eða tilgreindur geiri innan þess þriðja lands eða alþjóðastofnun tryggji ekki fullnægjandi öryggi og ef brýna nauðsyn ber til.
- 170) Þar eð aðildarríkin geta ekki fyllilega náð markmiði þessarar reglugerðar, þ.e. að tryggja einstaklingum í Sambandinu sambærilega vernd og frjálst flæði persónuupplýsinga í öllu Sambandinu, og því verður betur náð á vettvangi Sambandsins, vegna umfangs og áhrifa aðgerðarinnar, er Sambandinu heimilt að samþykkja ráðstafanir í samræmi við nálægðarregluna eins og kveðið er á um í 5. gr. sáttmálans um Evrópusambandið. Í samræmi við meðalhöfsregluna, eins og hún er sett fram í þeirri grein, er ekki gengið lengra en nauðsyn krefur í þessari reglugerð til að ná því markmiði.
- 171) Þessi reglugerð ætti að fella úr gildi tilskipun 95/46/EB. Vinnslu, sem er þegar hafin á þeim degi er reglugerð þessi kemur til framkvæmda, ætti að færa til samræmis við reglugerð þessa innan tveggja ára

frá gildistöku hennar. Þegar vinnsla er byggð á samþykki samkvæmt tilskipun 95/46/EB er ekki nauðsynlegt að skráður einstaklingur gefi samþykki sitt aftur ef það var gefið með hætti sem samrýmist skilyrðum þessarar reglugerðar, til að gera ábyrgðaraðila kleift að halda slíkri vinnslu áfram eftir þann dag sem reglugerð þessi kemur til framkvæmda. Ákvarðanir sem framkvæmdastjórnin hefur samþykkt og heimildir sem eftirlitsyfirvöld hafa veitt á grundvelli tilskipunar 95/46/EB eru áfram í gildi uns þeim er breytt, þau eru leyst af hólmi eða þau eru felld niður.

172)Haft var samráð við Evrópsku persónuverndarstofnunina í samræmi við 2. mgr. 28. gr. reglugerðar (EB) nr. 45/2001 og skilaði hún álit 7. mars 2012 ⁽¹⁷⁾.

173)Reglugerð þessi ætti að gilda um öll mál er varða vernd grundvallarréttinda og mannfrelsis í tengslum við vinnslu persónuupplýsinga sem ekki heyra undir sérstakar skuldbindingar með sama markmiði sem settar eru fram í tilskipun Evrópuþingsins og ráðsins 2002/58/EB ⁽¹⁸⁾, þ. á m. skyldur ábyrgðaraðila og réttindi einstaklinga. Til þess að skýra tengslin milli þessarar reglugerðar og tilskipunar 2002/58/EB ætti að breyta þeirri tilskipun til samræmis við hana. Þegar reglugerð þessi hefur verið samþykkt ætti að endurskoða tilskipun 2002/58/EB í því skyni að tryggja samræmi hennar við þessa reglugerð.

SAMÞYKKT REGLUGERÐ ÞESSA:

I. KAFLI

Almenn ákvæði

1. gr.

Viðfangsefni og markmið

1. Í þessari reglugerð er mælt fyrir um reglur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um reglur er varða frjálsa miðlun persónuupplýsinga.
2. Þessi reglugerð verndar grundvallarréttindi og frelsi einstaklinga, einkum rétt þeirra til verndar persónuupplýsingum.
3. Hvorki skal takmarka né banna frjálsa miðlun persónuupplýsinga innan Sambandsins af ástæðum er varða vernd einstaklinga í tengslum við vinnslu persónuupplýsinga.

2. gr.

Efnislegt gildissvið

1. Þessi reglugerð gildir 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 skráningarkerfi.
2. Þessi reglugerð gildir ekki um vinnslu persónuupplýsinga:
 - a) í starfsemi sem fellur utan gildissviðs laga Sambandsins,
 - b) af hálfu aðildarríkjanna vegna starfsemi sem fellur undir gildissvið 2. kafla V. bóls sáttmálans um Evrópusambandið,

⁽¹⁷⁾ Stjóð. ESB C 192, 30.6.2012, bls. 7.

⁽¹⁸⁾ Tilskipun Evrópuþingsins og ráðsins 2002/58/EB frá 12. júlí 2002 um vinnslu persónuupplýsinga og um verndum einkalífs á sviði rafræna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti) (Stjóð. EB L 201, 31.7.2002, bls. 37).

- c) af hálfu einstaklings ef vinnslan er hluti af starfsemi sem er einungis í þágu hans sjálfs eða fjölskyldu hans,
- d) af hálfu lögbærra yfirvalda í tengslum við það að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoðryggi.
3. Reglugerð (EB) nr. 45/2001 gildir um vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins á persónuupplýsingum. Laga skal reglugerð (EB) nr. 45/2001 og aðrar réttargerðir Sambandsins, sem gilda um slíka vinnslu persónuupplýsinga, að meginreglum og reglum þessarar reglugerðar í samræmi við 98. gr.
4. Þessi reglugerð hefur ekki áhrif á beitingu tilskipunar 2000/31/EB, einkum reglur í 12.–15. gr. hennar um bótaábyrgð þjónustuveitenda sem eru milliliðir.

3. gr.

Gildissvæði

1. Þessi reglugerð gildir um vinnslu persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila í Sambandinu, óháð því hvort vinnslan sjálf fer fram í Sambandinu.
2. Þessi reglugerð gildir um vinnslu ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga innan Sambandsins þegar vinnslustarfsemin tengist því að:
- a) bjóða þessum skráðu einstaklingum í Sambandinu vöru eða þjónustu, án tillits til þess hvort það er gert gegn greiðslu, eða
- b) hafa eftirlit með hegðun þeirra að svo miklu leyti sem hegðun þeirra á sér stað innan Sambandsins.
3. Þessi reglugerð gildir um vinnslu persónuupplýsinga af hálfu ábyrgðaraðila sem ekki hefur staðfestu innan Sambandsins en þó á stað þar sem lög aðildarríkis gilda samkvæmt þjóðarétti.

4. gr.

Skilgreiningar

Í reglugerð þessari er merking eftirfarandi hugtaka sem hér segir:

- 1) „persónuupplýsingar“: hvers kyns 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,
- 2) „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,
- 3) „takmörkun á vinnslu“: að auðkenna varðveittar persónuupplýsingar með það að markmiði að takmarka vinnslu þeirra í framtíðinni,
- 4) „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,

- 5), „notkun gerviauðkenna“: þegar unnið er með persónuupplýsingar á þann hátt að ekki sé lengur hægt að rekja þær til tiltekins skráðs einstaklings án viðbótarupplýsinga, að því tilskildu að slíkum viðbótarupplýsingum sé haldið aðgreindum og að beitt sé tæknilegum og skipulagslegum ráðstöfunum til að tryggja að persónuupplýsingarnar sé ekki hægt að rekja til persónugreinds eða persónugreinanlegs einstaklings,
- 6), „skráningarkerfi“: sérhvert skipulegt safn persónuupplýsinga sem er aðgengilegt samkvæmt tilteknum viðmiðunum, hvort heldur það er miðlægt, dreift eða skipt upp eftir notkun eða staðsetningu,
- 7), „ábyrgðaraðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem ákvarðar, einn eða í samvinnu við aðra, tilgang og aðferðir við vinnslu persónuupplýsinga; ef tilgangur og aðferðir við slíka vinnslu eru ákveðin í lögum Sambandsins eða lögum aðildarríkis er heimilt að tilgreina ábyrgðaraðila eða sérstakar viðmiðanir fyrir tilnefningu hans í lögum Sambandsins eða lögum aðildarríkis,
- 8), „vinnsluaðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila,
- 9), „viðtakandi“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem fær í hendur persónuupplýsingar, hvort sem hann er þriðji aðili eða ekki. Opinber yfirvöld, sem kunna að fá persónuupplýsingar sem svar við einstökum fyrirspurnum í samræmi við lög Sambandsins eða lög aðildarríkis, skulu þó ekki teljast viðtakendur; vinnsla þessara opinberu yfirvalda á gögnunum skal samrýmast gildandi reglum um persónuvernd samkvæmt tilgangi vinnslunnar,
- 10), „þriðji aðili“: einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða aðili annar en skráði einstaklingurinn, ábyrgðaraðili, vinnsluaðili og einstaklingar eða lögaðilar sem hafa, undir beinni stjórn ábyrgðaraðila eða vinnsluaðila, heimild til að vinna persónuupplýsingar,
- 11), „samþykki“ skráðs einstaklings: óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan,
- 12), „öryggisbrot við meðferð persónuupplýsinga“: brot á öryggi sem leiðir til óviljandi eða ólögmatrær eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glattist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi,
- 13), „erfðafræðilegar upplýsingar“: 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,
- 14), „lífkennaupplýsingar“: 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,
- 15), „heilsufarusupplýsingar“: persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings, þ.m.t. heilbrigðisþjónustu sem hann hefur fengið, og sem gefa upplýsingar um heilsufar hans,
- 16), „höfuðstöðvar“:
 - a) að því er varðar ábyrgðaraðila með starfsstöðvar í fleiri en einu aðildarríki, sá staður þar sem hann hefur yfirstjórn sína í Sambandinu nema ákvarðanir um tilgang og aðferðir við vinnslu persónuupplýsinga séu teknar í annarri starfsstöð ábyrgðaraðila í Sambandinu og síðarnefnda starfsstöðin sé sú sem hefur vald til að koma slíkum ákvörðunum til framkvæmda en í því tilviki skal starfsstöðin, sem tekið hefur slíkar ákvarðanir, teljast vera höfuðstöðvar,
 - b) að því er varðar vinnsluaðila með starfsstöðvar í fleiri en einu aðildarríki, sá staður þar sem hann hefur yfirstjórn sína í Sambandinu eða, hafi hann enga yfirstjórn í Sambandinu, starfsstöð vinnsluaðila í Sambandinu þar sem helsta vinnslustarfsemi innan ramma starfsemi starfsstöðvar vinnsluaðila fer fram, að því marki sem vinnsluaðili falli undir tilteknar skuldbindingar samkvæmt þessari reglugerð,
- 17), „fulltrúi“: einstaklingur eða lögaðili með staðfestu í Sambandinu, tilnefndur skriflega af ábyrgðaraðila eða vinnsluaðila skv. 27. gr., sem kemur fram sem fulltrúi ábyrgðaraðila eða vinnsluaðila að því er varðar skuldbindingar þeirra, hvors um sig, samkvæmt þessari reglugerð,

- 18), „fyrirtæki“: einstaklingur eða lögaðili sem stundar atvinnustarfsemi, óháð því hvert rekstrarform þess er að lögum, þ.m.t. sameignarfélög eða samtök sem stunda atvinnustarfsemi að staðaldri,
- 19), „fyrirtækjasamstæða“: ráðandi fyrirtæki og undirfyrirtæki þess,
- 20), „bindandi fyrirtækjareglur“: reglur um persónuvernd sem ábyrgðaraðili eða vinnsluaðili með staðfestu á yfirráðasvæði aðildarríkis fylgir varðandi miðlun eða endurtekna miðlun persónuupplýsinga til ábyrgðaraðila eða vinnsluaðila í einu eða fleiri þriðju löndum innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stundar sameiginlega atvinnustarfsemi,
- 21), „eftirlitsyfirvald“: sjálfstætt opinbert yfirvald sem aðildarríki kemur á fót skv. 51. gr.,
- 22), „hlutaðeigandi eftirlitsyfirvald“: eftirlitsyfirvald sem vinnsla persónuupplýsinga varðar vegna þess að:
- a) ábyrgðaraðili eða vinnsluaðili hefur staðfestu á yfirráðasvæði aðildarríkis þess eftirlitsyfirlvalds,
 - b) skráðir einstaklingar, sem búa í aðildarríki þess eftirlitsyfirlvalds, verða fyrir verulegum áhrifum eða líklegt er að þeir verði fyrir verulegum áhrifum af vinnslunni eða
 - c) kvörtun hefur verið lögð fram hjá því eftirlitsyfirlvaldi,
- 23), „vinnsla yfir landamæri“: annaðhvort:
- a) vinnsla persónuupplýsinga sem fram fer í tengslum við starfsemi starfsstöðva ábyrgðaraðila eða vinnsluaðila innan Sambandsins í fleiri en einu aðildarríki, þegar ábyrgðaraðili eða vinnsluaðili hefur staðfestu í fleiri en einu aðildarríki, eða
 - b) vinnsla persónuupplýsinga sem fram fer í tengslum við starfsemi einnar starfsstöðvar ábyrgðaraðila eða vinnsluaðila innan Sambandsins en hefur veruleg áhrif eða líklegt er að hafi veruleg áhrif á skráða einstaklinga í fleiri en einu aðildarríki,
- 24), „viðeigandi og rökstudd andmæli“: andmæli gegn drögum að ákvörðun varðandi það hvort brotið sé gegn þessari reglugerð eða hvort fyrirhuguð aðgerð í tengslum við ábyrgðaraðilann eða vinnsluaðilann samrýmist henni sem sýna greinilega fram á þá áhættu sem drögin að ákvörðuninni hafa í för með sér fyrir grundvallarréttindi og frelsi skráðra einstaklinga og, eftir því sem við á, frjálst flæði persónuupplýsinga innan Sambandsins,
- 25), „þjónusta í upplýsingasamfélaginu“: þjónusta eins og hún er skilgreind í b-lið 1. mgr. 1. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2015/1535 ⁽¹⁹⁾,
- 26), „alþjóðastofnun“: stofnun og undirskipaðir aðilar hennar sem heyra undir þjóðarétt eða annar aðili sem komið er á fót með samningi milli tveggja eða fleiri landa eða á grundvelli hans.

II. KAFLI

Meginreglur

5. gr.

Meginreglur um vinnslu persónuupplýsinga

1. Persónuupplýsingar skulu vera:

- a) unnar með lögmatum, sanngjörnum og gagnsæjum hætti gagnvart skráðum einstaklingi („lögmati, sanngirni og gagnsæi“),
- b) fengnar í tilgreindum, skýrum og lögmatum tilgangi og ekki unnar frekar á þann hátt að ósamrýmanlegt sé þeim tilgangi; frekari vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsóknna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi skal, í samræmi við 1. mgr. 89. gr., ekki teljast

⁽¹⁹⁾ Tilskipun Evrópuþingsins og ráðsins (ESB) 2015/1535 frá 9. september 2015 um tilhögun miðlunar upplýsinga um tæknilegar reglugerðir og reglur um þjónustu í upplýsingasamfélaginu (Stjóð. ESB L 241, 17.9.2015, bls. 1).

ósamrýmanleg upphaflegum tilgangi („takmörkun vegna tilgangs“),

- c) nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilganginn með vinnslunni („lágmarkun gagna“),
 - d) áreiðanlegar og, ef nauðsyn krefur, uppfærðar; gera skal allar eðlilegar ráðstafanir til að tryggja að persónuupplýsingum, sem eru óáreiðanlegar, með hliðsjón af tilganginum með vinnslu þeirra, verði eytt eða þær leiðréttar án tafar („áreiðanleiki“),
 - e) varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf er á miðað við tilganginn með vinnslu upplýsinganna; heimilt er að geyma persónuupplýsingar lengur að því tilskildu að vinnsla þeirra þjóni einungis skjalavistun í þágu almannahagsmuna, rannsóknnum á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi, í samræmi við 1. mgr. 89. gr., og sé með fyrirvara um að gerðar verði þær viðeigandi tæknilegu og skipulagslegu ráðstafanir til að vernda réttindi og frelsi skráða einstaklingsins sem reglugerð þessi krefst („geymslutakmörkun“),
 - f) unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt, þ.m.t. vernd gegn óleyfilegri eða ólögumætri vinnslu og gegn glötun, eyðileggingu eða tjóni fyrir slysni, með viðeigandi tæknilegum og skipulagslegum ráðstöfunum („heilleiki og trúnaður“).
2. Ábyrgðaraðili skal vera ábyrgur fyrir því að farið sé að ákvæðum 1. mgr. og geta sýnt fram á það („ábyrgðarskylda“).

6. gr.

Lögmæti vinnslu

1. Vinnsla skal einungis teljast lögmæt ef og að því marki sem a.m.k. eitt af eftirfarandi atriðum á við:
- a) skráður einstaklingur hefur gefið samþykki sitt fyrir vinnslu á persónuupplýsingum sínum í þágu eins eða fleiri tiltekinna markmiða,
 - b) vinnsla er nauðsynleg vegna framkvæmdar samnings sem skráður einstaklingur á aðild að eða til þess að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður,
 - c) vinnslan er nauðsynleg til uppfylla lagaskyldu sem hvílir á ábyrgðaraðila,
 - d) vinnslan er nauðsynleg til að vernda brýna hagsmuni hins skráða eða annars einstaklings,
 - e) vinnslan er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með,
 - f) vinnsla er nauðsynleg vegna lögmætra hagsmuna sem ábyrgðaraðili eða þriðji aðili gætir nema hagsmunir eða grundvallarréttindi og frelsi hins skráða, sem krefjast verndar persónuupplýsinga, vegi þyngra, einkum þegar hinn skráði er barn.

Ákvæði f-liðar fyrstu undirgreinar skulu ekki eiga við um vinnslu opinberra yfirvalda við störf sín.

2. Aðildarríkjunum er heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglna þessarar reglugerðar að því er varðar vinnslu þannig að samrýmist c- og e-lið 1. mgr., með því að setja fram með ítarlegri hætti sértækar kröfur til vinnslunnar og aðrar ráðstafanir til að tryggja lögmæta og sanngjarna vinnslu, þ.m.t. varðandi aðrar sérstakar vinnsluáðstæður eins og kveðið er á um í IX. kafla.

3. Mæla skal fyrir um grundvöll vinnslunnar, sem um getur í c- og e-lið 1. mgr., í:

- a) lögum Sambandsins eða
- b) lögum aðildarríkis sem ábyrgðaraðili heyrir undir.

Tilgangur vinnslunnar skal ákvarðaður á þeim lagagrundvelli eða, að því er varðar vinnsluna sem um getur í e-lið 1. mgr., vera nauðsynlegur vegna framkvæmdar verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með. Lagagrundvöllurinn getur m.a. verið sértæk ákvæði til að aðlaga beitingu reglna þessarar reglugerðar, m.a. um: almenn skilyrði varðandi lögmæta vinnslu ábyrgðaraðilans, tegund gagna sem vinnslan varðar, hlutaðeigandi skráða einstaklinga, hvaða stofnanir mega fá persónuupplýsingarnar í hendur og í hvaða tilgangi, takmörkun vegna tilgangs, varðveislutímabil og vinnsluáðgerðir og verklag við vinnslu, þ.m.t. ráðstafanir til að tryggja að vinnsla fari fram á lögmætan og sanngjarnan hátt, s.s. ráðstafanir varðandi aðrar sérstakar vinnsluáðstæður eins og kveðið er á um í IX. kafla. Lög Sambandsins eða lög aðildarríkis skulu þjóna hagsmunum almennings og hæfa því lögmæta markmiði sem stefnt er að.

4. Þegar vinnsla í öðrum tilgangi en þeim sem er að baki söfnun persónuupplýsinganna byggist ekki á samþykki skráða einstaklingsins eða á lögum Sambandsins eða lögum aðildarríkis, sem teljast nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi til að standa vörð um þau markmið sem getið er um í 1. mgr. 23. gr., skal ábyrgðaraðilinn, til þess að ganga úr skugga um hvort vinnsla í öðrum tilgangi samrýmist þeim tilgangi sem var forsenda söfnunar persónuupplýsinganna í upphafi, m.a. taka tillit til:

- a) hvers kyns tengsla milli þess tilgangs sem er að baki söfnun persónuupplýsinganna og tilgangs með fyrirhugaðri frekari vinnslu,
- b) þess í hvaða samhengi persónuupplýsingunum var safnað, einkum að því er varðar tengsl milli skráðra einstaklinga og ábyrgðaraðilans,
- c) eðlis persónuupplýsinganna, einkum þess hvort sérstakir flokkar persónuupplýsinga eru unnir, skv. 9. gr., eða hvort persónuupplýsingar er varða sakfellingar í refsímálum og refsiverð brot eru unnar, í samræmi við 10. gr.,
- d) hugsanlegra afleiðinga fyrirhugaðrar frekari vinnslu upplýsinganna fyrir skráða einstaklinga,
- e) þess hvort viðeigandi verndarráðstafanir hafi verið gerðar sem geta m.a. falist í dulkóðun eða notkun gerviauðkenna.

7. gr.

Skilyrði fyrir samþykki

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

8. gr.

Skilyrði sem gilda um samþykki barns í tengslum við þjónustu í upplýsingasamfélaginu

1. Þegar a-liður 1. mgr. 6. gr. á við, í tengslum við það þegar barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti, skal vinnsla persónuupplýsinga barnsins teljast lögmæt ef það hefur náð a.m.k. 16 ára aldri. Hafi barn ekki náð 16 ára aldri skal vinnslan einungis teljast lögmæt ef, og að því marki sem, forsjáraðili barnsins gefur eða heimilar samþykkið.

Aðildarríkin geta í lögum kveðið á um lægri aldur að því er þetta varðar en þó ekki lægri en 13 ár.

2. 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.

3. Ákvæði 1. mgr. hafa ekki áhrif á almenn samningalög aðildarríkjanna, s.s. reglur um gildi, gerð eða áhrif samnings þegar um er að ræða barn.

9. gr.

Vinnsla sérstakra flokka persónuupplýsinga

1. Bannað er að vinna persónuupplýsingar er varða kynþátt eða þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð eða heimspekilega sannfæringu eða þátttöku í stéttarfélagi og að vinna erfðafræðilegar upplýsingar, lífkennaupplýsingar í því skyni að persónugreina einstakling með einkvæmum hætti, heilsufarsupplýsingar eða upplýsingar er varða kynlíf einstaklings eða kynhneigð.

2. Ákvæði 1. mgr. gilda ekki ef eitt af eftirfarandi á við:

a) skráður einstaklingur hefur veitt ótvírætt samþykki sitt fyrir vinnslu þessara persónuupplýsinga í þágu eins eða fleiri tiltekinna markmiða nema kveðið sé á um það í lögum Sambandsins eða lögum aðildarríkis að hinum skráða sé óheimilt að aflétta banninu sem um getur í 1. mgr.,

b) vinnslan er nauðsynleg til þess að ábyrgðaraðilinn eða skráði einstaklingurinn geti staðið við skuldbindingar sínar og nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf og löggjöf um almannatryggingar og félagslega vernd, að því marki sem vinnslan er heimil samkvæmt lögum Sambandsins eða lögum aðildarríkis eða kjarasamningi samkvæmt lögum aðildarríkis, þar sem kveðið er á um viðeigandi verndarráðstafanir í tengslum við grundvallarréttindi og hagsmuni hins skráða,

c) vinnslan er nauðsynleg til að vernda brýna hagsmuni skráða einstaklingsins eða annars einstaklings ef hinn skráði er líkamlega eða í lagalegum skilningi ófær um að veita samþykki sitt,

d) vinnslan fer fram, með viðeigandi verndarráðstöfunum, sem liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila sem starfar ekki í hagnaðarskyni og hefur markmið af stjórnmálalegum, heimspekilegum, trúarlegum eða stéttarfélagslegum toga og með því skilyrði að vinnslan nái einungis til meðlima, eða fyrrum meðlima, aðilans eða þeirra sem eru í reglulegu sambandi við hann í tengslum við tilgang hans og að persónuupplýsingar séu ekki fengnar þriðja aðila í hendur án samþykkis skráðu einstaklinganna,

e) vinnslan tengist persónuupplýsingum sem skráði einstaklingurinn hefur augljóslega gert opinberar,

f) vinnslan er nauðsynleg til að unnt sé að stofna, hafa uppi eða verja réttarkröfur eða þegar dómstólar fara með dómssvald,

g) vinnsla er nauðsynleg, af ástæðum sem varða verulega almannahagsmuni, á grundvelli laga Sambandsins eða laga aðildarríkis sem skulu hafa því markmiði sem stefnt er að, virða kjarna réttarins til persónuverndar

og kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða,

- h) vinnslan er nauðsynleg til að unnt sé að fyrirbyggja sjúkdóma eða vegna atvinnusjúkdómalækninga, til að meta vinnufærni starfsmanns, greina sjúkdóma, láta í té umönnun eða meðferð á sviði heilbrigðis- eða félagsþjónustu eða stjórna heilbrigðis- eða félagsþjónustu og -kerfum á grundvelli laga Sambandsins eða aðildarríkis eða samkvæmt samningi við heilbrigðisstarfsmann og með fyrirvara um skilyrðin og verndarráðstafanirnar sem um getur í 3. mgr.,
- i) vinnslan er nauðsynleg af ástæðum er varða almannahagsmuni á sviði lýðheilsu, s.s. til að verjast alvarlegum heilsufarsógnum sem ná yfir landamæri eða tryggja að strangar kröfur séu gerðar um gæði og öryggi heilbrigðisþjónustu og lyfja eða lækningatækja, á grundvelli laga Sambandsins eða laga aðildarríkis sem kveða á um viðeigandi og sértækar ráðstafanir til að vernda réttindi og frelsi hins skráða, einkum þagnarskyldu,
- j) vinnsla er nauðsynleg vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi í samræmi við 1. mgr. 89. gr., á grundvelli laga Sambandsins eða laga aðildarríkis sem skulu hafa því markmiði sem stefnt er að, virða kjarna réttarins til persónuverndar og kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða.

3. Vinnsla persónuupplýsinganna, sem um getur í 1. mgr., er heimil í þeim tilgangi sem um getur í h-lið 2. mgr. ef upplýsingarnar eru unnar af eða á ábyrgð fagmanns sem fellur undir þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum sem innlendir þar til bærir aðilar hafa sett eða öðrum aðila sem einnig er bundinn þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum sem settar eru af innlendum þar til bærum aðilum.

4. Aðildarríkjunum er heimilt að viðhalda eða setja frekari skilyrði, þ.m.t. takmarkanir, með hliðsjón af vinnslu erðaðfræðilegra upplýsinga, lífkennauplýsinga eða heilsufarsupplýsinga.

10. gr.

Vinnsla persónuupplýsinga er varða sakfellingar í refsímálum og refsiverð brot

Vinnsla persónuupplýsinga, er varða sakfellingar í refsímálum og refsiverð brot eða tengdar öryggisráðstafanir á grundvelli 1. mgr. 6. gr., skal einungis fara fram undir eftirliti opinbers yfirvalds eða þegar vinnsla er heimiluð samkvæmt lögum Sambandsins eða lögum aðildarríkis þar sem kveðið er á um viðeigandi verndarráðstafanir í tengslum við réttindi og frelsi skráðra einstaklinga. Ítarlega skrá yfir refsídóma skal varðveita undir eftirliti opinbers yfirvalds.

11. gr.

Vinnsla sem ekki krefst persónugreiningar

1. Ef tilgangurinn með vinnslu ábyrgðaraðila á persónuupplýsingum krefst þess ekki, eða krefst þess ekki lengur, að ábyrgðaraðilinn geti persónugreint skráðan einstakling er ábyrgðaraðilanum ekki skylt að viðhalda, afla sér eða vinna viðbótarupplýsingar til að unnt sé að persónugreina hinn skráða í þeim tilgangi einum að uppfylla ákvæði þessarar reglugerðar.

2. Þegar ábyrgðaraðili, í tilvikum sem um getur í 1. mgr. þessarar greinar, getur sýnt fram á að hann sé ekki í aðstöðu til að persónugreina skráðan einstakling skal hann tilkynna hinum skráða um það ef mögulegt er. Í þeim tilvikum gilda 15.–20. gr. ekki nema hinn skráði veiti, í þeim tilgangi að neyta réttar síns samkvæmt þessum greinum, viðbótarupplýsingar sem gera kleift að persónugreina hann.

III. KAFLI

Réttindi skráðs einstaklings

1. þáttur

Gagnsæi og nánari reglur

12. gr.

Gagnsæi upplýsinga, tilkynninga og nánari reglur til að skráður einstaklingur geti neytt réttar síns

1. Ábyrgðaraðili skal gera viðeigandi ráðstafanir til að láta skráðum einstaklingi í té þær upplýsingar sem um getur í 13. og 14. gr. og tilkynningar skv. 15.–22. gr. og 34. gr. í tengslum við vinnslu á gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi og skýru og einföldu máli, einkum þegar um er að ræða upplýsingar sem beint er sérstaklega til barns. Upplýsingarnar skulu veittar skriflega eða á annan hátt, þ.m.t., eftir því sem við á, á rafrænu formi. Fari skráður einstaklingur fram á það má veita upplýsingarnar munnlega, að því tilskildu að hinn skráði sanni á sér deili með öðrum hætti.
2. Ábyrgðaraðili skal auðvelda skráðum einstaklingi að neyta réttar síns skv. 15.–22. gr. Í þeim tilvikum, sem um getur í 2. mgr. 11. gr., skal ábyrgðaraðilinn ekki neita að verða við beiðni hins skráða um að neyta réttar síns skv. 15.–22. gr. nema ábyrgðaraðilinn sýni fram á að hann sé ekki í aðstöðu til að staðfesta deili á hinum skráða.
3. Ábyrgðaraðilinn skal veita skráðum einstaklingi upplýsingar um aðgerðir, sem gripið er til vegna beiðni skv. 15.–22. gr., án ótilhlýðilegrar tafar og hvað sem öðru líður innan mánaðar frá viðtöku beiðninnar. Lengja má frestinn um tvo mánuði til viðbótar ef þörf er á, með hliðsjón af fjölda beiðna og því hversu flóknar þær eru. Ábyrgðaraðili skal tilkynna hinum skráða um slíkar framlengingar innan mánaðar frá viðtöku beiðninnar, ásamt ástæðunum fyrir töfinni. Leggi hinn skráði fram beiðnina rafrænt skulu upplýsingarnar látnar í té með rafrænum hætti þar sem kostur er nema hinn skráði fari fram á annað.
4. Verði ábyrgðaraðili ekki við beiðni skráðs einstaklings skal hann tilkynna honum, án tafar og í síðasta lagi innan mánaðar frá viðtöku beiðninnar, um ástæðurnar fyrir því að það var ekki gert og um möguleikann á að leggja fram kvörtun hjá eftirlitsyfirvaldi og leita réttarræðis.
5. Upplýsingar, sem veittar eru skv. 13. og 14. gr., og hvers konar tilkynningar og aðgerðir, sem gripið er til skv. 15.–22. gr. og 34. gr., skulu vera án endurgjalds. Séu beiðnir frá skráðum einstaklingi augljóslega tilefnislausar eða óhóflegar, einkum vegna endurtekningar, er ábyrgðaraðila heimilt að gera annaðhvort:
 - a) setja upp sanngjarnt gjald með tilliti til stjórnsýslukostnaðar við upplýsingagjöfina eða tilkynningarnar eða aðgerðirnar sem farið er fram á eða
 - b) neita að verða við beiðninni.Það skal vera ábyrgðaraðilans að sýna fram á að beiðni sé tilefnislaus eða óhófleg.
6. Með fyrirvara um 11. gr. getur ábyrgðaraðili farið fram á að veittar séu nauðsynlegar viðbótarupplýsingar til að staðfesta deili á hinum skráða þyki honum leika verulegur vafi á því hver sá einstaklingur sé sem leggur fram beiðnina sem um getur í 15.–21. gr.
7. Hægt er að láta staðlaðar táknmyndir fylgja upplýsingunum, sem veita ber skráðum einstaklingum skv. 13. og 14. gr., til að veita marktækt yfirlit yfir fyrirhugaða vinnslu á auðsýnilegan, skiljanlegan og auðlæsilegan hátt. Táknmyndirnar skulu vera með tölvulesanlegu sniði þegar þær eru settar fram rafrænt.
8. Framkvæmdastjórninni skal falið vald til þess að samþykkja framseldar gerðir í samræmi við 92. gr. til að ákvarða hvaða upplýsingar setja má fram með táknmyndum og aðferðirnar við að setja fram staðlaðar táknmyndir.

2. þáttur

Upplýsingar og aðgangur að persónuupplýsingum

13. gr.

Upplýsingar sem ber að veita við öflun persónuupplýsinga hjá skráðum einstaklingi

1. Þegar persónuupplýsinga er aflað hjá skráðum einstaklingi um hann sjálfan skal ábyrgðaraðilinn, við söfnun persónuupplýsinganna, skýra hinum skráða frá öllum eftirfarandi atriðum:
 - a) heiti og samskiptaupplýsingum ábyrgðaraðilans og, eftir atvikum, fulltrúa hans,
 - b) samskiptaupplýsingum persónuverndarfulltrúa, ef við á,
 - c) tilganginum með fyrirhugaðri vinnslu persónuupplýsinganna og hver lagagrundvöllur hennar er,
 - d) þegar vinnslan byggist á f-lið 1. mgr. 6. gr., hvaða lögmætu hagsmunir það eru sem ábyrgðaraðili eða þriðji aðili gætir,
 - e) viðtakendum eða flokkum viðtakenda persónuupplýsinganna, ef einhverjir eru,
 - f) ef við á, því að ábyrgðaraðili hyggist miðla persónuupplýsingum til þriðja lands eða alþjóðastofnunar og hvort ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi liggi fyrir eða, í tilviki miðlana sem um getur í 46. eða 47. gr. eða í annarri undirgrein 1. mgr. 49. gr., tilvísun til viðeigandi eða hæfilegra verndarráðstafana og leiða til að fá afrit af þeim eða upplýsingar um hvar þær hafa verið gerðar aðgengilegar.
2. Til viðbótar við þær upplýsingar, sem um getur í 1. mgr., skal ábyrgðaraðilinn, á þeim tíma þegar persónuupplýsingunum er safnað, veita hinum skráða eftirtalдар frekari upplýsingar sem nauðsynlegar eru til að tryggja sanngjarna og gagnsæja vinnslu:
 - a) hversu lengi persónuupplýsingarnar verða geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,
 - b) að fyrir hendi sé réttur til að fara fram á það við ábyrgðaraðila að fá aðgang að persónuupplýsingum, láta leiðrétta þær, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar eða til að andmæla vinnslu, auk réttarins til að flytja eigin gögn,
 - c) þegar vinnslan byggist á a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr., að fyrir hendi sé réttur til að draga samþykki sitt til baka hvenær sem er, án þess þó að það hafi áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni,
 - d) réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi,
 - e) hvort það að veita persónuupplýsingar sé krafa samkvæmt lögum eða samkvæmt samningi eða krafa sem er forsenda þess að hægt sé að gera samning og einnig hvort skráðum einstaklingi sé skylt að láta persónuupplýsingarnar í té og mögulegar afleiðingar þess ef hann veitir ekki upplýsingarnar,
 - f) hvort fram fari sjálfvirk ákvarðanatöku, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr., og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.
3. Ef ábyrgðaraðilinn hyggst vinna persónuupplýsingarnar frekar í öðrum tilgangi en þeim sem lá að baki söfnun þeirra skal hann láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum viðeigandi viðbótarupplýsingum eins og kveðið er á um í 2. mgr.

4. Ákvæði 1., 2. og 3. mgr. gilda ekki ef og að því marki sem hinn skráði hefur þegar fengið vitneskju um þessi atriði.

14. gr.

Upplýsingar sem ber að veita þegar persónuupplýsingar hafa ekki fengist hjá skráðum einstaklingi

1. Hafi persónuupplýsingar ekki fengist hjá skráðum einstaklingi skal ábyrgðaraðili skýra honum frá eftirfarandi atriðum:

- a) heiti og samskiptaupplýsingum ábyrgðaraðilans og, eftir atvikum, fulltrúa hans,
- b) samskiptaupplýsingum persónuverndarfulltrúa, ef við á,
- c) tilganginum með fyrirhugaðri vinnslu persónuupplýsinganna og hver lagagrundvöllur hennar er,
- d) flokkum viðkomandi persónuupplýsinga,
- e) viðtakendum eða flokkum viðtakenda persónuupplýsinganna, ef einhverjir eru,
- f) ef við á, að ábyrgðaraðili hyggist miðla persónuupplýsingum til viðtakanda í þriðja landi eða alþjóðastofnun og hvort ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi liggja fyrir eða ekki eða, í tilviki miðlana sem um getur í 46. eða 47. gr. eða í annarri undirgrein 1. mgr. 49. gr., tilvísun til viðeigandi eða hæfilegra verndarráðstafana og leiða til að fá afrit af þeim eða upplýsingar um hvar þær hafa verið gerðar aðgengilegar.

2. Til viðbótar við upplýsingarnar, sem um getur í 1. mgr., skal ábyrgðaraðilinn veita skráðum einstaklingi eftirfarandi upplýsingar sem nauðsynlegar eru til að tryggja sanngjarna og gagnsæja vinnslu gagnvart hinum skráða:

- a) hversu lengi persónuupplýsingarnar verða geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,
- b) þegar vinnslan byggist á f-lið 1. mgr. 6. gr., hvaða lögmætu hagsmunir það eru sem ábyrgðaraðili eða þriðji aðili gætir,
- c) að fyrir hendi sé réttur til að fara fram á það við ábyrgðaraðila að fá aðgang að persónuupplýsingum, láta leiðrétta þær, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar og til að andmæla vinnslu, auk réttarins til að flytja eigin gögn,
- d) þegar vinnslan byggist á a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr., að fyrir hendi sé réttur til að draga samþykki sitt til baka hvenær sem er, án þess þó að það hafi áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni,
- e) réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi,
- f) hvaðan persónuupplýsingarnar eru fengnar og, ef við á, hvort um hafi verið ræða upplýsingar sem eru aðgengilegar almenningi,
- g) hvort fram fari sjálfvirk ákvarðanataka, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr. og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir hinn skráða.

3. Ábyrgðaraðili skal veita upplýsingarnar, sem um getur í 1. og 2. mgr.:

- a) innan hæfilegs tíma eftir að hafa fengið persónuupplýsingarnar, þó í síðasta lagi mánuði síðar, og hafa hliðsjón af þeim sérstöku kringumstæðum sem eiga við um vinnslu persónuupplýsinganna,

b) ef nota á persónuupplýsingarnar til samskipta við skráðan einstakling, í síðasta lagi þegar fyrst er haft samband við hann eða

c) ef fyrirhugað er að fá öðrum viðtakanda persónuupplýsingarnar í hendur, í síðasta lagi þegar það er gert í fyrsta sinn.

4. Ef ábyrgðaraðilinn hyggst vinna persónuupplýsingarnar frekar í öðrum tilgangi en lá að baki öflunar þeirra skal hann láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum viðeigandi viðbótarupplýsingum eins og kveðið er á um í 2. mgr.

5. Ákvæði 1.–4. mgr. gilda ekki ef og að því marki sem:

a) skráði einstaklingurinn hefur þegar fengið upplýsingarnar,

b) ekki er unnt að veita slíkar upplýsingar eða það kostar óhóflega fyrirhöfn, einkum þegar um er að ræða vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfærðilegum tilgangi, með fyrirvara um þau skilyrði og verndarráðstafanir sem um getur í 1. mgr. 89. gr., eða að því marki sem líklegt er að skyldan, sem um getur í 1. mgr. þessarar greinar, geri það ómögulegt eða hamli því verulega að markmið þeirrar vinnslu náist. Í þeim tilvikum skal ábyrgðaraðilinn gera viðeigandi ráðstafanir til að vernda réttindi, frelsi og lögmæta hagsmuni hins skráða, þ.m.t. með því að gera upplýsingarnar aðgengilegar almenningi,

c) skýrt er mælt fyrir um öflun eða miðlun upplýsinganna í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir og sem kveða á um viðeigandi ráðstafanir til að vernda lögmæta hagsmuni hins skráða eða

d) þegar persónuupplýsingar eru bundnar trúnaði á grundvelli þagnarskyldu í samræmi við lög Sambandsins eða lög aðildarríkis, þ.m.t. lögbundinnar þagnarskyldu.

15. gr.

Réttur skráðs einstaklings til aðgangs

1. Skráður einstaklingur skal hafa rétt til að fá staðfestingu á því frá ábyrgðaraðila hvort verið sé að vinna persónuupplýsingar er varða hann sjálfan og, ef svo er, rétt til aðgangs að persónuupplýsingunum og að upplýsingum um eftirfarandi atriði:

a) tilgang vinnslunnar,

b) viðkomandi flokka persónuupplýsinga,

c) viðtakendur eða flokka viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, einkum viðtakendur í þriðju löndum eða alþjóðastofnanir,

d) ef mögulegt er, hversu lengi fyrirhugað er að varðveita persónuupplýsingarnar eða, ef það reynist ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það,

e) að fyrir liggja réttur til að fara fram á það við ábyrgðaraðila að láta leiðrétta persónuupplýsingar, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar eða til að andmæla slíkri vinnslu,

f) réttinn til að leggja fram kvörtun hjá eftirlitsyfirlaldi,

g) ef persónuupplýsinganna er ekki aflað hjá hinum skráða, allar fyrirliggjandi upplýsingar um uppruna þeirra,

h) hvort fram fari sjálfvirk ákvarðanatöku, þ.m.t. gerð persónusniðs, sem um getur í 1. og 4. mgr. 22. gr. og, a.m.k. í þeim tilvikum, marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar slíkrar vinnslu fyrir skráða einstaklinginn.

2. Þegar persónuupplýsingum er miðlað til þriðja lands eða alþjóðastofnunar skal skráður einstaklingur eiga rétt á að fá upplýsingar um viðeigandi verndarráðstafanir skv. 46. gr. í tengslum við miðlunina.

3. Ábyrgðaraðili skal láta í té afrit af þeim persónuupplýsingum sem eru í vinnslu. Honum er heimilt að innheimta sanngjarnt gjald, byggt á umsýslukostnaði, fari skráði einstaklingurinn fram á fleiri eintök. Leggi hinn skráði beiðnina fram rafrænt skulu upplýsingarnar látnar í té með rafrænu sniði sem almennt er notað nema hann fari fram á annað.

4. Rétturinn til að fá afrit, sem um getur í 3. mgr., skal ekki skerða réttindi og frelsi annarra.

3. þáttur

Leiðrétting og eyðing

16. gr.

Réttur til leiðréttingar

Skráður einstaklingur á rétt á að óáreiðanlegar persónuupplýsingar er varða hann sjálfan leiðrétta af ábyrgðaraðila án ótilhlýðilegrar tafar. Að teknu tilliti til tilgangsins með vinnslunni skal hinn skráði eiga rétt á að láta fullgera ófullkomnar persónuupplýsingar, þ.m.t. með því að leggja fram yfirlýsingu til viðbótar.

17. gr.

Réttur til eyðingar („réttur til að gleymast“)

1. Skráður einstaklingur skal eiga rétt á að ábyrgðaraðilinn eyði persónuupplýsingum er hann varða án ótilhlýðilegrar tafar og skal ábyrgðaraðilanum skyldt að eyða persónuupplýsingunum án ótilhlýðilegrar tafar ef ein eftirtalinna ástæðna á við:

- a) persónuupplýsingarnar eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun þeirra eða annarri vinnslu þeirra,
- b) hinn skráði dregur til baka samþykkið sem vinnslan byggist á skv. a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr. og ekki er annar lagagrundvöllur fyrir vinnslunni,
- c) hinn skráði andmælir vinnslunni skv. 1. mgr. 21. gr. og ekki eru fyrir hendi lögmætar ástæður fyrir vinnslunni sem ganga framár eða hann andmælir vinnslunni skv. 2. mgr. 21. gr.,
- d) vinnsla persónuupplýsinganna var ólögmæt,
- e) eyða þarf persónuupplýsingunum til að uppfylla lagaskyldu sem hvílir á ábyrgðaraðila samkvæmt lögum Sambandsins eða lögum aðildarríkis,
- f) persónuupplýsingunum var safnað í tengslum við boð um þjónustu í upplýsingasamfélaginu sem um getur í 1. mgr. 8. gr.

2. Hafi ábyrgðaraðili gert persónuupplýsingar opinberar og honum er gert skyldt skv. 1. mgr. að afmá þær skal hann, með hliðsjón af fyrirliggjandi tækni og kostnaði við framkvæmdina, gera eðlilegar ráðstafanir, þ.m.t. tæknilegar ráðstafanir, til að upplýsa ábyrgðaraðila, sem vinna persónuupplýsingarnar, um að skráði einstaklingurinn hafi farið fram á að slíkir ábyrgðaraðilar afmái hvers kyns tengla í eða afrit eða eftirmyndir af þessum persónuupplýsingum.

3. Ákvæði 1. og 2. mgr. gilda ekki að því marki sem vinnsla er nauðsynleg:

- a) til að neyta réttarins til tjáningar- og upplýsingafrelsis,
- b) til að framfylgja lagaskyldu um vinnslu sem hvílir á ábyrgðaraðilanum samkvæmt lögum Sambandsins eða lögum aðildarríkis eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með,
- c) með skírskotun til almannahagsmuna á sviði lýðheilsu í samræmi við h- og i-lið 2. mgr. 9. gr. og 3. mgr. 9. gr.,
- d) vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi í samræmi við 1. mgr. 89. gr., að því marki sem líklegt er að rétturinn, sem um getur í 1. mgr., geri það ómögulegt eða hamli því verulega að markmið þeirrar vinnslu náist eða
- e) til að stofna, hafa uppi eða verja réttarkröfur.

18. gr.

Réttur til takmörkunar á vinnslu

1. Skráður einstaklingur skal hafa rétt til þess að ábyrgðaraðili takmarki vinnslu þegar eitt af eftirfarandi á við:
 - a) hinn skráði vefengir að persónuupplýsingar séu réttar, þangað til ábyrgðaraðilinn hefur fengið tækifæri til að staðfesta að þær séu réttar,
 - b) vinnslan er ólögmæt og hinn skráði andmælir því að persónuupplýsingunum sé eytt og fer fram á takmarkaða notkun þeirra í staðinn,
 - c) ábyrgðaraðilinn þarf ekki lengur á persónuupplýsingunum að halda fyrir vinnsluna en skráði einstaklingurinn þarfnast þeirra til þess að stofna, hafa uppi eða verja réttarkröfur,
 - d) skráði einstaklingurinn hefur andmælt vinnslunni skv. 1. mgr. 21. gr. á meðan beðið er sannprófunar á því hvort hagsmunir ábyrgðaraðila gangi framar lögmætum hagsmunum hins skráða.
2. Þegar vinnsla hefur verið takmörkuð skv. 1. gr. skal einungis vinna slíkar persónuupplýsingar, að varðveislu undanskilinni, með samþykki skráða einstaklingsins eða til að stofna, hafa uppi eða verja réttarkröfur eða til að vernda réttindi annars einstaklings eða lögaðila eða með skírskotun til brýnna almannahagsmuna Sambandsins eða aðildarríkis.
3. Ábyrgðaraðili skal tilkynna skráðum einstaklingi, sem fengið hefur fram takmörkun á vinnslu skv. 1. mgr., um það áður en takmörkuninni á vinnslunni er aflétt.

19. gr.

Tilkynningarskylda varðandi leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu

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

20. gr.

Réttur til flytja eigin gögn

1. Skráður einstaklingur skal eiga rétt á að fá persónuupplýsingar er varða hann sjálfan, sem hann hefur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu sniði og eiga rétt á að senda þessar upplýsingar til annars ábyrgðaraðila án þess að ábyrgðaraðilinn, sem veittar voru persónuupplýsingarnar, hindri það ef:
 - a) vinnslan byggist á samþykki skv. a-lið 1. mgr. 6. gr. eða a-lið 2. mgr. 9. gr. eða samningi skv. b-lið 1. mgr. 6. gr. og
 - b) vinnslan er sjálfvirk.
2. Þegar skráði einstaklingurinn neytir réttar síns til þess að flytja eigin gögn skv. 1. mgr. skal hann eiga rétt á að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars ef það er tæknilega framkvæmanlegt.
3. Það að neyta réttarins, sem um getur í 1. mgr. þessarar greinar, skal ekki hafa áhrif á 17. gr. Sá réttur skal ekki gilda um vinnslu sem er nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með.
4. Rétturinn, sem um getur í 1. mgr., skal ekki skerða réttindi og frelsi annarra.

4. þáttur

Andmælaréttur og sjálfvirk einstaklingsmiðuð ákvarðanataka

21. gr.

Andmælaréttur

1. Skráður einstaklingur skal eiga rétt á að andmæla hvenær sem er, vegna sérstakra aðstæðna sinna, vinnslu persónuupplýsinga er varða hann sjálfan og sem byggist á e- eða f-lið 1. mgr. 6. gr., þ.m.t. gerð persónusniðs á grundvelli þessara ákvæða. Ábyrgðaraðili skal ekki vinna persónuupplýsingarnar frekar nema hann geti sýnt fram á mikilvægar lögmætar ástæður fyrir vinnslunni sem ganga framars hagsmunum, réttindum og frelsi hins skráða eða því að stofna, hafa uppi eða verja réttarkröfur.
2. Þegar persónuupplýsingar eru unnar í þágu beinnar markaðssetningar skal skráði einstaklingurinn hvenær sem er eiga rétt á að andmæla vinnslu persónuupplýsinga sem varða hann sjálfan vegna slíkrar markaðssetningar, þ.m.t. gerð persónusniðs að því marki sem það tengist slíkri beinni markaðssetningu.
3. Ef hinn skráði andmælir vinnslu í þágu beinnar markaðssetningar skal ekki vinna persónuupplýsingarnar frekar í slíkum tilgangi.
4. Í síðasta lagi þegar fyrst er haft samband við skráða einstaklinginn skal honum sérstaklega gerð grein fyrir réttinum, sem um getur í 1. og 2. mgr., og skal hann settur skýrt fram og aðgreindur frá öðrum upplýsingum.
5. Með skirskotun til notkunar á þjónustu í upplýsingasamfélaginu og þrátt fyrir tilskipun 2002/58/EB er hinum skráða heimilt að neyta andmælaréttar síns rafrænt með notkun tækniforskrifta.
6. Þegar persónuupplýsingar eru unnar í þágu rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi í samræmi við 1. mgr. 89. gr. skal skráði einstaklingurinn eiga rétt á, vegna sérstakra aðstæðna sinna, að andmæla vinnslu persónuupplýsinga er varða hann sjálfan nema vinnslan sé nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna.

22. gr.

Sjálfvirk einstaklingsmiðuð ákvarðanataka, þ.m.t. gerð persónusniðs

1. Skráður einstaklingur skal eiga rétt á því að ekki sé tekin ákvörðun eingöngu á grundvelli sjálfvirkar gagnavinnslu, þ.m.t. gerðar persónusniðs, sem hefur réttaráhrif að því er hann sjálfan varðar eða snertir hann á sambærilegan hátt að verulegu leyti.
2. Ákvæði 1. mgr. gilda ekki ef ákvörðunin:
 - a) er forsenda þess að unnt sé að gera eða framkvæma samning milli skráða einstaklingsins og ábyrgðaraðila,
 - b) er heimiluð í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðili heyrir undir og þar sem einnig er kveðið á um viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða eða
 - c) byggist á afdráttarlausu samþykki hins skráða.
3. Í þeim tilvikum, sem um getur í a- og c-lið 2. mgr., skal ábyrgðaraðili gagna gera viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni skráða einstaklingsins, a.m.k. réttinn til mannlegrar íhlutunar af hálfu ábyrgðaraðilans, til að láta skoðun sína í ljós og til að vefengja ákvörðunina.
4. Ákvarðanir, sem um getur í 2. mgr., skulu ekki vera byggðar á sérstökum flokkum persónuupplýsinga, sem um getur í 1. mgr. 9. gr., nema a- eða g-liður 2. mgr. 9. gr. eigi við og fyrir hendi séu viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða.

5. þáttur

Takmarkanir

23. gr.

Takmarkanir

1. Í Sambandslögum eða lögum aðildarríkis, sem ábyrgðaraðili eða vinnsluaðili gagna heyrir undir, er heimilt að takmarka með löggjafarráðstöfun gildissvið þeirra skyldna og réttinda, sem um getur í 12.–22. gr. og í 34. gr., og einnig í 5. gr. að því marki sem ákvæði hennar samsvara réttindum og skyldum sem kveðið er á um í 12.–22. gr., ef slík takmörkun virðir eðli grundvallarréttinda og mannfrelsis og telst nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi með hliðsjón af:
- a) þjóðaröryggi,
 - b) landvörnum,
 - c) almannaoöryggi,
 - d) því að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, þ.m.t. að vernda gegn og koma í veg fyrir ógnir við almannaoöryggi,
 - e) öðrum mikilvægum markmiðum sem þjóna almannahagsmunum Sambandsins eða aðildarríkis, einkum mikilvægum efnahagslegum eða fjárhagslegum hagsmunum Sambandsins eða aðildarríkis, þ.m.t. gjaldeyrismálum, fjárlögum og skattamálum, lýðheilsu og almannatryggingum,
 - f) því að verja sjálfstæði dómskerfisins og dómsmeðferð,
 - g) forvörnum, rannsóknum, uppljóstrunum og lögsóknum vegna brota á siðareglum lögverndaðra starfsgreina,
 - h) eftirlits-, skoðunar- eða reglusetningarstörfum sem tengjast, þótt aðeins sé það endrum og eins, beitingu opinbers valds í þeim tilvikum sem um getur í a- til e-lið og í g-lið,
 - i) vernd skráðs einstaklings eða réttindum og frelsi annarra,
 - j) því að einkaréttarlegum kröfum sé fullnægt.
2. Í löggjafarráðstöfun, sem um getur í 1. mgr., skulu einkum vera a.m.k. sértæk ákvæði, ef við á, er varða:
- a) tilgang vinnslunnar eða tegundir vinnslu,
 - b) tegundir persónuupplýsinga,
 - c) gildissvið þeirra takmarkana sem settar eru,
 - d) verndarráðstafanir til að koma í veg fyrir misnotkun eða ólögsmætan aðgang eða miðlun,
 - e) tilgreiningu ábyrgðaraðila eða flokka ábyrgðaraðila,
 - f) varðveislutímabil og viðeigandi verndarráðstafanir með tilliti til eðlis, umfangs og tilgangs með vinnslu eða tegunda vinnslu,
 - g) áhættu fyrir réttindi og frelsi skráðra einstaklinga og
 - h) rétt skráðra einstaklinga til að fá upplýsingar um takmörkunina nema það kunni að skaða tilgang hennar.

IV. KAFLI

Ábyrgðaraðili og vinnsluaðili

1. þáttur

Almennar skyldur

24. gr.

Ábyrgð ábyrgðaraðila

1. Með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðilinn gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að vinnslan fari fram í samræmi við þessa reglugerð. Ráðstafanirnar skal endurskoða og uppfæra ef nauðsyn ber til.
2. Þar sem það samrýmist meðalhófi í tengslum við vinnslustarfsemina skulu ráðstafanirnar, sem um getur í 1. mgr., m.a. fela í sér að ábyrgðaraðili innleiði viðeigandi persónuverndarstefnur.
3. Sé samþykktum háttanisreglum fylgt, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar.

25. gr.

Innbyggð og sjálfgefin persónuvernd

1. Með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skal ábyrgðaraðilinn, bæði þegar ákveðnar eru aðferðir við vinnsluna og þegar vinnslan sjálf fer fram, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, s.s. notkun gerviauðkenna, sem hannaðar eru til að framfylgja meginreglum um persónuvernd, s.s. lágmörkun gagna, með skilvirkum hætti og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur þessarar reglugerðar og vernda réttindi skráðra einstaklinga.
2. Ábyrgðaraðilinn 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. Þessi skylda gildir um það hversu miklum persónuupplýsingum er safnað, að hvaða marki unnið er með þær, hversu lengi þær eru varðveittar og aðgang að þeim. Einkum skal tryggja með slíkum ráðstöfunum að það sé sjálfgefið að persónuupplýsingar verði ekki gerðar aðgengilegar ótakmörkuðum fjölda fólks án ihlutunar viðkomandi einstaklings.
3. Nota má samþykkt vottunarfyrirkomulag, skv. 42. gr., til að sýna fram á að kröfur 1. og 2. mgr. þessarar greinar séu uppfylltar.

26. gr.

Sameiginlegir ábyrgðaraðilar

1. Ef tveir eða fleiri ábyrgðaraðilar ákveða sameiginlega tilgang vinnslunnar og aðferðir við hana skulu þeir teljast vera sameiginlegir ábyrgðaraðilar. Þeir skulu, á gagnsæjan hátt, ákveða ábyrgð hvers um sig á því að skuldbindingar samkvæmt þessari reglugerð séu uppfylltar, einkum hvað snertir beitingu réttinda hinna skráðu, og skyldur hvers um sig til að láta í té upplýsingarnar sem um getur í 13. og 14. gr., með samkomulagi sín á milli nema ábyrgð hvers ábyrgðaraðila um sig sé, og að því marki sem hún er, ákveðin í lögum Sambandsins eða lögum aðildarríkis sem ábyrgðaraðilarnir heyra undir. Í samkomulaginu má tilnefna tengilið fyrir skráða einstaklinga.

2. Samkomulagið, sem um getur í 1. mgr., skal endurspegla með tilhlýðilegum hætti hlutverk og tengsl hvers hinna sameiginlegu ábyrgðaraðila gagnvart skráðum einstaklingum. Megininntak samkomulagsins skal gert aðgengilegt skráðum einstaklingi.
3. Óháð skilmálum samkomulagsins, sem um getur í 1. mgr., er skráðum einstaklingi heimilt að neyta réttar síns samkvæmt þessari reglugerð að því er varðar og gagnvart hverjum ábyrgðaraðila um sig.

27. gr.

Fulltrúar ábyrgðaraðila eða vinnsluaðila sem ekki hafa staðfestu í Sambandinu

1. Þegar 2. mgr. 3. gr. á við skal ábyrgðaraðilinn eða vinnsluaðilinn tilnefna skriflega fulltrúa sinn innan Sambandsins.
2. Skyldan, sem mælt er fyrir um í 1. mgr., skal ekki eiga við um:
 - a) vinnslu sem fer fram endrum og eins, felur ekki í sér umfangsmikla meðferð sérstakra flokka upplýsinga, eins og um getur í 1. mgr. 9. gr., eða meðferð persónuupplýsinga í tengslum við sakfellingu í refsímálum og refsiverð brot sem um getur í 10. gr., og sem ekki er líkleg til að leiða af sér áhættu að því er varðar réttindi og frelsi einstaklinga, að teknu tilliti til eðlis, samhengis, umfangs og tilgangs vinnslunnar eða
 - b) opinbert yfirvald eða stofnun.
3. Fulltrúinn skal hafa staðfestu í einu af aðildarríkjum þeirra skráðu einstaklinga sem persónuupplýsingar eru unnar um í tengslum við boð til þeirra á vörum eða þjónustu eða sem fylgst er með hegðun hjá.
4. Fulltrúinn skal hafa umboð ábyrgðaraðila eða vinnsluaðila til þess að vera sá aðili sem einkum og sér í lagi eftirlitsyfirvöld og skráðir einstaklingar geta snúið sér til, til viðbótar við eða í stað ábyrgðaraðilans eða vinnsluaðilans, með öll þau mál sem tengjast vinnslunni, í því skyni að tryggja að farið sé að þessari reglugerð.
5. Þó að ábyrgðaraðili eða vinnsluaðili tilnefni fulltrúa hefur það ekki áhrif á lögsóknir sem hefja mætti gegn ábyrgðaraðilanum eða vinnsluaðilanum sjálfum.

28. gr.

Vinnsluaðili

1. Þegar öðrum er falin vinnsla fyrir hönd ábyrgðaraðila skal ábyrgðaraðilinn einungis leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnslan uppfylli kröfur þessarar reglugerðar og að vernd réttinda skráða einstaklingsins sé tryggð.
2. 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 tækifæri til að andmæla slíkum breytingum.
3. Vinnsla af hálfu vinnsluaðila skal falla undir samning eða aðra réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis sem skuldbindur vinnsluaðila gagnvart ábyrgðaraðilanum og þar sem tilgreint er viðfangsefni og tímalengd vinnslunnar, eðli og tilgangur hennar, tegund persónuupplýsinga og flokkar skráðra einstaklinga og skyldur og réttindi ábyrgðaraðilans. Í samningi eða annarri réttargerð skal einkum mæla fyrir um að vinnsluaðili:
 - a) vinni einungis persónuupplýsingarnar samkvæmt skjalfestum fyrirmælum ábyrgðaraðila, þ.m.t. að því er

varðar miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis sem vinnsluaðilinn heyrir undir; í því tilviki skal vinnsluaðilinn upplýsa ábyrgðaraðila um það lagaskilyrði áður en vinnslan hefst nema lögin banni slíka upplýsingagjöf vegna mikilvægra almannahagsmuna,

- b) tryggi að aðilar, sem hafa heimild til vinnslu persónuupplýsinga, hafi gengist undir trúnaðarskyldu eða heyrir undir viðeigandi lögboðna trúnaðarskyldu,
 - c) geri allar ráðstafanir sem krafist er skv. 32. gr.,
 - d) virði skilyrði 2. og 4. mgr. varðandi ráðningu annars vinnsluaðila,
 - e) aðstoði, að teknu tilliti til eðlis vinnslunnar, ábyrgðaraðilann með viðeigandi tæknilegum og skipulagslegum ráðstöfunum, að því marki sem hægt er, við að uppfylla þá skyldu sína að svara beiðnum um að skráðir einstaklingar fái neytt réttar síns sem mælt er fyrir um í III. kafla,
 - f) aðstoði ábyrgðaraðila við að tryggja að skyldur skv. 32.–36. gr. séu uppfylltar, að teknu tilliti til eðlis vinnslunnar og upplýsinga sem vinnsluaðili hefur aðgang að,
 - g) eyði eða skili, að vali ábyrgðaraðila, öllum persónuupplýsingum til ábyrgðaraðilans eftir að veitingu þjónustunnar, sem tengist vinnslunni, lýkur og eyði öllum afritum nema þess sé krafist í lögum Sambandsins eða lögum aðildarríkis að persónuupplýsingar séu varðveittar,
 - h) geri ábyrgðaraðila aðgengilegar allar upplýsingar, sem nauðsynlegar eru til að sýna fram á að skuldbindingarnar, sem mælt er fyrir um í þessari grein, séu uppfylltar, gefi kost á úttektum, þ.m.t. eftirlitsskoðunum, sem ábyrgðaraðilinn eða annar úttektaraðili í umboði hans hafi með höndum, og leggi sitt af mörkum til þeirra.
- Að því er varðar h-lið fyrstu undirgreinar skal vinnsluaðili þegar í stað láta ábyrgðaraðila vita ef fyrirmæli brjóta, að hans mati, í bága við þessa reglugerð eða önnur ákvæði Sambandsins eða aðildarríkis um persónuvernd.

4. Ráði vinnsluaðili annan vinnsluaðila til að inna af hendi tiltekna vinnslustarfsemi fyrir hönd ábyrgðaraðila leggja sömu skyldur varðandi persónuvernd og settar eru fram í samningnum eða annarri réttargerð milli ábyrgðaraðila og vinnsluaðila, eins og um getur í 3. mgr., á þann vinnsluaðila með samningi eða annarri réttargerð samkvæmt lögum Sambandsins eða lögum aðildarríkis, þar sem veittar eru einkum nægar tryggingar fyrir því að gerðar séu viðeigandi tæknilegar og skipulagslegar ráðstafanir þannig að vinnslan uppfylli kröfur þessarar reglugerðar. Uppfylli þessi viðbótarvinnsluaðili ekki persónuverndarskyldur sínar skal upphaflegi vinnsluaðilinn áfram bera fulla ábyrgð gagnvart ábyrgðaraðila á því að hinn vinnsluaðilinn efni skuldbindingar sínar.

5. Fylgi vinnsluaðili samþykktum háttænisreglum, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á nægilegar tryggingar eins og um getur í 1. og 4. mgr. þessarar greinar.

6. Án þess að það hafi áhrif á einstakan samning milli ábyrgðaraðila og vinnsluaðila getur samningurinn eða önnur réttargerð, sem um getur í 3. og 4. mgr. þessarar greinar, verið byggð, að öllu leyti eða að hluta til, á föstum samningsákvæðum sem um getur í 7. og 8. mgr. þessarar greinar, m.a. þegar þau eru hluti vottunar sem veitt er ábyrgðaraðila eða vinnsluaðila skv. 42. og 43. gr.

7. Framkvæmdastjórnin getur mælt fyrir um föst samningsákvæði um þau mál sem um getur í 3. og 4. mgr. þessarar greinar og í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

8. Eftirlitsyfirvald getur tekið upp föst samningsákvæði um þau mál sem um getur í 3. og 4. mgr. þessarar greinar og í samræmi við samræmingarkerfið sem um getur í 63. gr.

9. Samningurinn eða hin réttargerðin, sem um getur í 3. og 4. mgr., skal vera skrifleg, þ.m.t. á rafrænu formi.

10. Með fyrirvara um 82., 83. og 84. gr. skal vinnsluaðili, sem brýtur í bága við þessa reglugerð þegar hann ákveður tilgang og aðferðir við vinnsluna, teljast vera ábyrgðaraðili að því er varðar þá vinnslu.

29. gr.

Vinnsla í umboði ábyrgðaraðila eða vinnsluaðila

Vinnsluaðili og sérhver aðili, sem starfar í umboði ábyrgðaraðila eða vinnsluaðila og hefur aðgang að persónuupplýsingum, skal því aðeins vinna þessar upplýsingar að fyrir liggi fyrirmæli ábyrgðaraðila nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis.

30. gr.

Skrár yfir vinnslustarfsemi

1. Sérhver ábyrgðaraðili og, eftir atvikum, fulltrúi ábyrgðaraðila skal halda skrá yfir vinnslustarfsemi sem fram fer á ábyrgð hans. Í skránni skulu allar eftirfarandi upplýsingar koma fram:

- a) heiti og samskiptaupplýsingar ábyrgðaraðila og, eftir atvikum, sameiginlegs ábyrgðaraðila, fulltrúa ábyrgðaraðila og persónuverndarfulltrúa,
- b) tilgangur vinnslunnar,
- c) lýsing á flokkum skráðra einstaklinga og flokkum persónuupplýsinga,
- d) flokkar viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, m.a. viðtakenda í þriðju löndum eða alþjóðastofnanir,
- e) ef við á, miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar, þ.m.t. um hvaða þriðja land eða alþjóðastofnun er að ræða, og, ef um er að ræða miðlun sem um getur í annarri undirgrein 1. mgr. 49. gr., gögn um viðeigandi verndarráðstafanir,
- f) ef mögulegt er, fyrirhuguð tímamörk varðandi eyðingu mismunandi gagnaflokka,
- g) ef mögulegt er, almenn lýsing á þeim tæknilegu og skipulagslegu öryggisráðstöfunum sem um getur í 1. mgr. 32. gr.

2. Sérhver vinnsluaðili og, eftir atvikum, fulltrúi vinnsluaðila skal halda skrá yfir alla flokka vinnslustarfsemi sem framkvæmd er fyrir hönd ábyrgðaraðila og í henni skulu koma fram:

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

3. Skrárnar, sem um getur í 1. og 2. mgr., skulu vera skriflegar, þ.m.t. á rafrænu formi.

4. Ábyrgðaraðili eða vinnsluaðili og, eftir atvikum, fulltrúi ábyrgðaraðilans eða vinnsluaðilans skulu gera skrána aðgengilega eftirlitsfirvaldinu að beiðni þess.

5. Skyldurnar, sem um getur í 1. og 2. mgr., skulu ekki eiga við um fyrirtæki eða stofnun sem hefur færri en 250 starfsmenn nema vinnslan, sem innt er þar af hendi, sé líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, vinnslan sé ekki tilfallandi eða taki til sérstakra flokka upplýsinga, eins og um getur í 1. mgr. 9. gr., eða persónuupplýsinga er varða sakfellingar í refsímálum og refsiverð brot sem um getur í 10. gr.

31. gr.

Samvinna við eftirlitsfirvald

Ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúar þeirra skulu, að fenginni beiðni, hafa samvinnu við eftirlitsfirvaldið við framkvæmd verkefna þess.

2. þáttur

Öryggi persónuupplýsinga

32. gr.

Öryggi við vinnslu

1. Með hliðsjón af nýjustu tækni, kostnaði við framkvæmd og eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu, mislíklegri og misalvarlegri, fyrir réttindi og frelsi einstaklinga skulu ábyrgðaraðili og vinnsluaðili gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja viðunandi öryggi miðað við áhættuna, m.a. eftir því sem við á:

- a) nota gerviauðkenni og dulkóðun persónuupplýsinga,
 - b) geta tryggt viðvarandi trúnað, samfellu, tiltækileika og álagsspol vinnslukerfa og -þjónustu,
 - c) geta endurheimt tímanlega tiltækileika og aðgang að persónuupplýsingum ef til efnislegs eða tæknilegs atviks kemur,
 - d) taka upp ferli til að prófa og meta reglulega skilvirkni tæknilegra og skipulagslegra ráðstafana til að tryggja öryggi vinnslunnar.
2. Þegar viðunandi öryggi er metið skal einkum hafa hliðsjón af þeirri áhættu sem vinnslan hefur í för með sér, einkum að því er varðar óviljandi eða ólögmdæta eyðingu persónuupplýsinga, sem eru sendar, geymdar eða unnar á annan hátt, eða að þær glattist, breytist, verði birtar eða veittur aðgangur að þeim í leyfisleysi.
3. Sé samþykktum háttisreglum fylgt, eins og um getur í 40. gr., eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr., má nota það til að sýna fram á að kröfur 1. mgr. þessarar greinar séu uppfylltar.
4. Ábyrgðaraðili og vinnsluaðili skulu gera ráðstafanir til að tryggja að sérhver einstaklingur, sem starfar í umboði ábyrgðaraðila eða vinnsluaðila og hefur aðgang að persónuupplýsingum, vinni þessar upplýsingar því aðeins að fyrir liggi fyrirmæli ábyrgðaraðila nema honum sé það skylt samkvæmt lögum Sambandsins eða lögum aðildarríkis.

33. gr.

Tilkynning til eftirlitsfirvalds um öryggisbrot við meðferð persónuupplýsinga

1. 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 eftirlitsfirvaldinu sem er lögbært skv. 55. gr. nema ólíklegt þyki að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga. Sé eftirlitsfirvaldinu ekki tilkynnt um brotið innan 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni.

2. Vinnsluaðili skal tilkynna ábyrgðaraðila um það án ótilhlýðilegrar tafar ef hann verður var við öryggisbrot við meðferð persónuupplýsinga.
3. Í tilkynningunni, sem um getur í 1. mgr., skal a.m.k.:
 - a) lýsa eðli öryggisbrots við meðferð persónuupplýsinga, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem það varðar og flokkum og áætluðum fjölda skráninga persónuupplýsinga sem um er að ræða,
 - b) gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar,
 - c) lýsa líklegum afleiðingum öryggisbrots við meðferð persónuupplýsinga,
 - d) lýsa þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna öryggisbrots við meðferð persónuupplýsinga, þ.m.t., eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif þess.
4. Ef, og að því marki sem, ekki er mögulegt að láta upplýsingarnar í té á sama tíma er heimilt að veita þær í áföngum án ástæðulausrar frekari tafar.
5. Ábyrgðaraðili skal skrá niður hvers kyns öryggisbrot við meðferð persónuupplýsinga og tilgreina málsatvik í tengslum við viðkomandi brot, áhrif þess og aðgerðir til úrbóta sem gripið var til. Þessi skráning skal gera eftirlitsyfirlögin kleift að sannreyna að farið sé að ákvæðum þessarar greinar.

34. gr.

Skráðum einstaklingi gert viðvart um öryggisbrot við meðferð persónuupplýsinga

1. 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.
2. Í tilkynningunni til hins skráða, sem um getur í 1. mgr. þessarar greinar, skal lýsa á skýru og einföldu máli eðli öryggisbrots við meðferð persónuupplýsinga og hún skal innihalda a.m.k. þær upplýsingar og ráðstafanir sem um getur í b-, c- og d-lið 3. mgr. 33. gr.
3. Þess skal ekki krafist að skráðum einstaklingi sé gert viðvart ef eitthvert eftirtalinna skilyrða er uppfyllt:
 - a) ábyrgðaraðilinn hefur gert viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og þessar ráðstafanir voru gerðar varðandi þær persónuupplýsingar sem öryggisbrot við meðferð persónuupplýsinga hafði áhrif á, einkum ráðstafanir til að gera persónuupplýsingar ólæsilegar hverjum þeim sem ekki hefur aðgangsheimild að þeim, s.s. með dulkóðun,
 - b) ábyrgðaraðilinn hefur gert ráðstafanir í kjölfarið sem tryggja að ólíklegt sé að aftur komi til jafnmikillar áhættu fyrir réttindi og frelsi skráðra einstaklinga og um getur í 1. mgr.,
 - c) það myndi hafa í för með sér óhóflega fyrirhöfn. Í því tilviki skal í staðinn birta almenna tilkynningu eða grípa til svipaðrar ráðstöfunar þar sem hinum skráðu er gert viðvart með jafnáhrifaríkum hætti.
4. Hafi ábyrgðaraðili ekki þegar látið skráða einstaklinginn vita af öryggisbroti við meðferð persónuupplýsinga getur eftirlitsyfirlögin, eftir að hafa metið líkur á því að brotið leiði af sér mikla áhættu, annaðhvort krafist þess að hann geri það eða ákveðið að einhver þeirra skilyrða, sem um getur í 3. mgr., séu uppfyllt.

3. þáttur

Mat á áhrifum á persónuvernd og fyrirframsamráð

35. gr.

Mat á áhrifum á persónuvernd

1. 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 ábyrgðaraðilinn láta fara fram mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan hefst. Eitt og sama mat getur tekið til nokkurra svipaðra vinnsluaðgerða sem geta haft í för með sér svipaða áhættuþætti.

2. Ábyrgðaraðilinn skal leita ráða hjá persónuverndarfulltrúa, hafi slíkur fulltrúi verið tilnefndur, þegar hann framkvæmir mat á áhrifum á persónuvernd.

3. Þess skal einkum krafist að fram fari mat á áhrifum á persónuvernd, sem um getur í 1. mgr., þegar um er að ræða:

a) kerfisbundið og umfangsmikið mat á persónulegum þáttum, sem tengjast einstaklingum, sem byggist á sjálfvirkri vinnslu, þ.m.t. gerð persónusniðs, og sem leiðir til töku ákvarðana sem hafa réttaráhrif fyrir einstaklinginn eða snerta hann verulega með svipuðum hætti,

b) umfangsmikla vinnslu sérstakra flokka upplýsinga sem um getur í 1. mgr. 9. gr. eða persónuupplýsinga er varða sakfellingar í refsímálum og refsiverð brot sem um getur í 10. gr. eða

c) kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi.

4. Eftirlitsyfirvaldið skal koma á fót og birta skrá yfir þær tegundir vinnsluaðgerða þar sem krafist er mats á áhrifum á persónuvernd skv. 1. mgr. Eftirlitsyfirvaldið skal senda persónuverndarráðinu, sem um getur í 68. gr., þessar skrár.

5. Eftirlitsyfirvaldinu er einnig heimilt að koma á fót og birta skrá yfir þær tegundir vinnsluaðgerða þar sem ekki er krafist mats á áhrifum á persónuvernd. Eftirlitsyfirvaldið skal senda persónuverndarráðinu þessar skrár.

6. Ef í skránum, sem um getur í 4. og 5. mgr., er að finna vinnslustarfsemi, sem tengist því að bjóða skráðum einstaklingum vörur eða þjónustu eða hafa eftirlit með hegðun þeirra í fleiri en einu aðildarríki eða sem gæti haft veruleg áhrif á frjálsa miðlun persónuupplýsinga innan Sambandsins, skal lögbært eftirlitsyfirvald beita samræmingarkerfinu, sem um getur í 63. gr., áður en þessar skrár eru samþykktar.

7. Þegar þessar upplýsingar eru birtar skal a.m.k. eftirfarandi koma fram:

a) kerfisbundin lýsing á fyrirhuguðum vinnsluaðgerðum og tilganginum með vinnslunni, þ.m.t., eftir atvikum, lögmætum hagsmunum ábyrgðaraðilans,

b) mat á því hvort vinnsluaðgerðirnar eru nauðsynlegar og hóflegar miðað við tilganginn með þeim,

c) mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga sem um getur í 1. mgr. og

d) ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu, þ.m.t. verndarráðstafanir, öryggisráðstafanir og fyrirkomulag við að tryggja vernd persónuupplýsinga og sýna fram á að farið sé að þessari reglugerð, að teknu tilliti til réttinda og lögmætra hagsmuna skráðra einstaklinga og annarra einstaklinga sem í hlut eiga.

8. Taka skal tilhlýðilegt tillit til þess hvort hlutaðeigandi ábyrgðaraðilar eða vinnsluaðilar fylgja samþykktum háttænisreglum, sem um getur í 40. gr., þegar áhrif vinnsluaðgerða téðra ábyrgðaraðila eða vinnsluaðila eru metin, einkum að því er varðar mat á áhrifum á persónuvernd.

9. Þegar við á, skal ábyrgðaraðili leita álits skráðra einstaklinga eða fulltrúa þeirra á fyrirhugaðri vinnslu, án þess að það hafi áhrif á vernd viðskiptahagsmuna eða almannahagsmuna eða öryggi vinnsluaðgerða.

10. Ef vinnsla skv. c- eða e-lið 1. mgr. 6. gr. á sér lagagrundvöll í lögum Sambandsins eða lögum aðildarríkis, sem ábyrgðaraðili heyrir undir, og þau lög gilda um þá tilteknu vinnsluaðgerð eða -aðgerðir sem um er að ræða og mat á áhrifum á persónuvernd hefur þegar farið fram, sem hluti af almennu áhrifamati í tengslum við samþykkt þess lagagrundvallar, gilda 1.–7. mgr. ekki nema aðildarríkin telji nauðsynlegt að láta slíkt mat fara fram áður en vinnslustarfsemin hefst.

11. Ef nauðsyn krefur skal ábyrgðaraðilinn láta fara fram endurskoðun til að meta hvort vinnslan fari fram í samræmi við matið á áhrifum á persónuvernd, a.m.k. þegar breyting verður á þeirri áhættu sem fylgir vinnsluaðgerðunum.

36. gr.

Fyrirframsamráð

1. Ef mat á áhrifum á persónuvernd skv. 35. gr. gefur til kynna að vinnslan myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við eftirlitsyfirvaldið áður en vinnsla hefst.
2. Telji eftirlitsyfirvaldið 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 eftirlitsyfirvaldið, innan átta vikna frá að því 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 58. gr. Lengja má frestinn um sex vikur með hliðsjón af því hversu flókin fyrirhuguð vinnsla er. Eftirlitsyfirvaldið skal tilkynna ábyrgðaraðila og, eftir atvikum, vinnsluaðila um slíkar framlengingar innan mánaðar frá viðtöku beiðni um samráð, ásamt ástæðunum fyrir töfnni. Þessa fresti má framlengja þar til eftirlitsyfirvaldið hefur fengið þær upplýsingar sem það óskar eftir vegna samráðsins.
3. Þegar ábyrgðaraðili hefur samráð við eftirlitsyfirvaldið skv. 1. mgr. skal hann gefa því upp:
 - a) eftir atvikum, ábyrgðarsvið ábyrgðaraðila, sameiginlegra ábyrgðaraðila og vinnsluaðila, sem koma að vinnslunni, hvers um sig, einkum þegar um er að ræða vinnslu innan fyrirtækjasamstæðu,
 - b) tilgang fyrirhugaðrar vinnslu og aðferðir við hana,
 - c) ráðstafanir og verndarráðstafanir sem gerðar eru til að vernda réttindi og frelsi skráðra einstaklinga samkvæmt þessari reglugerð,
 - d) ef við á, samskiptaupplýsingar persónuverndarfulltrúa,
 - e) mat á áhrifum á persónuvernd sem kveðið er á um í 35. gr. og
 - f) hverjar þær upplýsingar aðrar sem eftirlitsyfirvaldið fer fram á.
4. Aðildarríkin skulu hafa samráð við eftirlitsyfirvaldið við undirbúning tillögu að löggjafarráðstöfun, sem tengist vinnslu og þjóðþing skal samþykka, eða stjórnvaldsráðstöfun sem byggir á slíkri löggjafarráðstöfun.
5. Þrátt fyrir 1. mgr. má krefjast þess í lögum aðildarríkis að ábyrgðaraðilar hafi samráð við og fái fyrirframleyfi eftirlitsyfirvalds í tengslum við vinnslu ábyrgðaraðila sem annast framkvæmd verkefnis í þágu almannahagsmuna, þ.m.t. vinnslu sem tengist félagslegri vernd og lýðheilsu.

4. þáttur

Persónuverndarfulltrúi

37. gr.

Tilnefning persónuverndarfulltrúa

1. Ábyrgðaraðili og vinnsluaðili skulu tilnefna persónuverndarfulltrúa í sérhverju tilviki þar sem:
 - a) vinnsla er í höndum opinbers yfirvalds eða stofnunar, að undanskildum dómstólum þegar þeir fara með dómsveld sitt,
 - b) meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í vinnsluaðgerðum sem krefjast, sakir eðlis síns, umfangs og/eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum eða
 - c) meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í umfangsmikilli vinnslu sérstakra flokka upplýsinga skv. 9. gr. og persónuupplýsinga er varða sakfellingar í refsímálum og refsiverð brot sem um getur í 10. gr.

2. Fyrirtækjasamstæðu er heimilt að skipa einn persónuverndarfulltrúa að því tilskildu að sérhver starfsstöð hafi greiðan aðgang að honum.
3. Ef ábyrgðaraðili eða vinnsluaðili er opinbert yfirvald eða stofnun er heimilt að tilnefna einn persónuverndarfulltrúa fyrir fleiri en eitt slíkt yfirvald eða stofnun, að teknu tilliti til stjórnskipulags þeirra og stærðar.
4. Í öðrum tilvikum en þeim sem um getur í 1. mgr. er ábyrgðaraðili eða vinnsluaðili eða samtökum og öðrum aðilum, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, heimilt eða jafnvel skylt, sé þess krafist í lögum Sambandsins eða lögum aðildarríkis, að tilnefna persónuverndarfulltrúa. Persónuverndarfulltrúinn getur komið fram fyrir hönd slíkra samtaka og annarra aðila sem eru fulltrúar ábyrgðaraðila eða vinnsluaðila.
5. Persónuverndarfulltrúinn skal tilnefndur á grundvelli faglegrar hæfni sinnar og einkum sérþekkingar á lögum og lagaframkvæmd á sviði persónuverndar og getu sinnar til að vinna þau verkefni sem um getur í 39. gr.
6. Persónuverndarfulltrúinn getur verið starfsmaður ábyrgðaraðila eða vinnsluaðila eða sinnt verkefnum á grundvelli þjónustusamnings.
7. Ábyrgðaraðili eða vinnsluaðili skal birta samskiptaupplýsingar persónuverndarfulltrúans og senda eftirlitsyfirvaldinu þær.

38. gr.

Staða persónuverndarfulltrúa

1. Ábyrgðaraðili og vinnsluaðili skulu tryggja að persónuverndarfulltrúi komi, með viðeigandi hætti og tímanlega, að öllum málum sem tengjast vernd persónuupplýsinga.
2. Ábyrgðaraðili og vinnsluaðili skulu styðja persónuverndarfulltrúann við framkvæmd þeirra verkefna sem um getur í 39. gr. með því að láta honum í té nauðsynleg úrræði til að innkaupa af hendi, auk aðgangs að persónuupplýsingum og vinnsluáðgerðum, og gera honum kleift að viðhalda sérþekkingu sinni.
3. Ábyrgðaraðili og vinnsluaðili skulu tryggja að persónuverndarfulltrúi fái engin fyrirmæli varðandi framkvæmd þessara verkefna. Ábyrgðaraðili eða vinnsluaðili skal hvorki víkja honum úr starfi né refsa honum fyrir framkvæmd verkefna sinna. Persónuverndarfulltrúi skal heyra beint undir æðsta stjórnunarstig hjá ábyrgðaraðila eða vinnsluaðila.
4. Skráðir einstaklingar geta haft samband við persónuverndarfulltrúann með öll mál sem tengjast vinnslu á persónuupplýsingum þeirra og því hvernig þeir geta neytt réttar síns samkvæmt þessari reglugerð.
5. Persónuverndarfulltrúi skal bundinn þagnarskyldu eða trúnaði um framkvæmd verkefna sinna í samræmi við lög Sambandsins eða lög aðildarríkis.
6. Persónuverndarfulltrúi má sinna öðrum verkefnum og skyldustörfum. Ábyrgðaraðili eða vinnsluaðili skal tryggja að slík verkefni og skyldustörf leiði ekki til hagsmunaárekstra.

39. gr.

Verkefni persónuverndarfulltrúa

1. Persónuverndarfulltrúi skal sinna a.m.k. eftirfarandi verkefnum:
 - a) upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar samkvæmt þessari reglugerð og öðrum ákvæðum Sambandsins eða aðildarríkis um persónuvernd og veita þeim ráðgjöf þar að lútandi,
 - b) fylgjast með því að farið sé að ákvæðum þessarar reglugerðar, öðrum ákvæðum Sambandsins eða aðildarríkis um persónuvernd og stefnum ábyrgðaraðila eða vinnsluaðila varðandi vernd persónuupplýsinga, þ.m.t.

úthlutun ábyrgðar, vitundarvakningu og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi og tilheyrandi úttektir,

- c) veita ráðgjöf, sé farið fram á það, varðandi mat á áhrifum á persónuvernd og fylgjast með framkvæmd þess skv. 35. gr.,
 - d) vinna með eftirlitsyfirvaldinu,
 - e) vera tengiliður fyrir eftirlitsyfirvaldið varðandi mál sem tengjast vinnslu, þ.m.t. fyrirframsamráðið sem um getur í 36. gr., og leita ráða, eftir því sem við á, varðandi önnur málefni.
2. Persónuverndarfulltrúi skal við framkvæmd verkefna sinna taka tilhlýðilegt tillit til þeirrar áhættu sem fylgir vinnslustarfseminni, með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar.

5. þáttur

Hátternisreglur og vottun

40. gr.

Hátternisreglur

1. Aðildarríkin, eftirlitsyfirvöld, persónuverndarráðið og framkvæmdastjórnin skulu hvetja til þess að samdar verði hátternisreglur, sem eiga að stuðla að rétttri beitingu þessarar reglugerðar, með tilliti til sérkenna hinna ýmsu vinnslusviða og sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja.
2. Samtökum og öðrum aðilum, sem eru fulltrúar flokka ábyrgðaraðila eða vinnsluaðila, er heimilt að semja hátternisreglur, eða breyta slíkum reglum eða rýmka þær, í því skyni að kveða nánar á um beitingu þessarar reglugerðar, t.d. að því er varðar:
 - a) sanngjarna og gagnsæja vinnslu,
 - b) lögmæta hagsmuni ábyrgðaraðila í tilteknu samhengi,
 - c) söfnun persónuupplýsinga,
 - d) notkun gerviauðkenna við vinnslu persónuupplýsinga,
 - e) upplýsingar sem veittar eru almenningi og skráðum einstaklingum,
 - f) það að skráðir einstaklingar geti neytt réttar síns,
 - g) upplýsingar sem veittar eru börnum og þeim til verndar og það hvernig afla beri samþykkis forsjáraðila,
 - h) þær ráðstafanir og aðferðir sem um getur í 24. og 25. gr. og ráðstafanir til að tryggja öryggi vinnslu sem um getur í 32. gr.,
 - i) tilkynningar til eftirlitsyfirvalda um öryggisbrot við meðferð persónuupplýsinga og það að skráðum einstaklingum sé gert viðvart um slík brot,
 - j) miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana eða
 - k) málsmeðferð utan dómstóla og aðra málsmeðferð við lausn deilumála til að leysa deilur er varða vinnslu milli ábyrgðaraðila og skráðra einstaklinga, sbr. þó réttindi hinna skráðu skv. 77. og 79. gr.
3. Auk þess að ábyrgðaraðilar eða vinnsluaðilar, sem heyra undir þessa reglugerð, beiti hátternisreglum, sem samþykktar eru skv. 5. mgr. þessarar greinar og hafa almennt gildi skv. 9. mgr. þessarar greinar, geta ábyrgðaraðilar eða vinnsluaðilar, sem ekki heyra undir þessa reglugerð skv. 3. gr., einnig gert það til að tryggja að viðeigandi verndarráðstafanir séu fyrir hendi innan ramma miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana samkvæmt þeim skilmálum sem um getur í e-lið 2. mgr. 46. gr. Slíkir ábyrgðaraðilar eða vinnsluaðilar skulu skuldbinda sig, með bindandi og framfylgjanlegum hætti, til að beita

Þessum viðeigandi verndarráðstöfunum, m.a. að því er varðar réttindi skráðra einstaklinga, með samningi eða öðrum lagalega bindandi gerningum.

4. Háttænisreglur, sem um getur í 2. mgr. þessarar greinar, skulu fela í sér fyrirkomulag sem gerir aðilanum, sem um getur í 1. mgr. 41. gr., kleift að annast skyldubundið eftirlit með því að ábyrgðaraðilar eða vinnsluaðilar, sem skuldbinda sig til að beita þeim, fylgi ákvæðum þeirra, án þess þó að það hafi áhrif á verkefni og valdheimildir eftirlitsyfirvalda sem lögbær eru skv. 55. eða 56. gr.

5. Samtök og aðrir aðilar, sem um getur í 2. mgr. þessarar greinar, sem hafa í hyggju að semja háttænisreglur eða breyta reglum eða rýmka reglur sem fyrir eru, skulu leggja drög að reglum, breytingu eða rýmkun fyrir það eftirlitsyfirvald sem lögbært er skv. 55. gr. Eftirlitsyfirvaldið skal gefa álit sitt á því hvort drögin að háttænisreglum, breytingin eða rýmkunin samrýmist þessari reglugerð og samþykkja drögin, breytinguna eða rýmkunina ef það telur að með þeim séu tryggðar nægilegar og viðeigandi verndarráðstafanir.

6. Ef drögin að háttænisreglum, breytingin eða rýmkunin er samþykkt í samræmi við 5. mgr. og ef viðkomandi háttænisreglur varða ekki vinnslustarfsemi í fleiri en einu aðildarríki skal eftirlitsyfirvaldið skrá reglurnar og birta þær.

7. Varði drögin að háttænisreglum vinnslustarfsemi í fleiri en einu aðildarríki skal eftirlitsyfirvaldið, sem lögbært er skv. 55. gr., áður en það samþykkir drögin, breytinguna eða rýmkunina, leggja þau fyrir persónuverndarráðið samkvæmt þeirri málsmæðferð sem um getur í 63. gr. og skal ráðið gefa álit sitt á því hvort drögin að reglunum, breytingin eða rýmkunin samrýmist þessari reglugerð eða, í þeim aðstæðum sem um getur í 3. mgr. þessarar greinar, tryggi viðeigandi verndarráðstafanir.

8. Staðfesti álitíð, sem um getur í 7. mgr., að drögin að háttænisreglum, breytingin eða rýmkunin samrýmist þessari reglugerð eða, í þeim aðstæðum sem um getur í 3. mgr., tryggi viðeigandi verndarráðstafanir skal persónuverndarráðið leggja álit sitt fyrir framkvæmdastjórnina.

9. Framkvæmdastjórninni er heimilt að ákveða, með framkvæmdargerðum, að háttænisreglurnar, breytingin eða rýmkunin, sem hlotið hafa samþykki og hún fær til umfjöllunar skv. 8. mgr. þessarar greinar, hafi almennt gildi innan Sambandsins. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmæðferðina sem um getur í 2. mgr. 93. gr.

10. Framkvæmdastjórnin skal sjá til þess að samþykktar reglur, sem ákveðið hefur verið að hafi almennt gildi í samræmi við 9. mgr., fái viðeigandi kynningu.

11. Persónuverndarráðið skal safna saman öllum samþykktum háttænisreglum, breytingum og rýmkunum í skrá og gera þær aðgengilegar almenningi með viðeigandi hætti.

41. gr.

Eftirlit með samþykktum háttænisreglum

1. Með fyrirvara um verkefni og valdheimildir lögbærs eftirlitsyfirvalds skv. 57. og 58. gr. má eftirlit með því að háttænisreglum skv. 40. gr. sé fylgt vera í höndum aðila sem ræður yfir viðeigandi sérþekkingu á viðfangsefni reglnanna og hefur fengið faggildingu í þeim tilgangi frá lögbæru eftirlitsyfirvaldi.

2. Aðili skv. 1. mgr., getur fengið faggildingu til að hafa eftirlit með því að háttænisreglum sé fylgt ef hann hefur:

a) sýnt fram á sjálfstæði sitt og sérþekkingu á viðfangsefni reglnanna með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi,

b) komið á verklagi sem gerir honum kleift að meta hæfi hlutaðeigandi ábyrgðaraðila og vinnsluaðila til að beita háttænisreglunum, hafa eftirlit með því að þeir fari að ákvæðum þeirra og endurskoða starfsemi þeirra með reglubundnum hætti,

- c) komið á verklagi og kerfum til að annast meðferð kvartana um brot á reglunum eða á því hvernig ábyrgðaraðili eða vinnsluaðili framkvæmir, eða hefur framkvæmt, reglurnar og til að gera þetta verklag og þessi kerfi gagnsæ fyrir skráða einstaklinga og almenning og
- d) sýnt fram á, með fullnægjandi hætti að mati lögbærs eftirlitsyfirvalds, að verkefni hans og skyldustörf leiði ekki til hagsmunaáreksturs.
3. Lögbæra eftirlitsyfirvaldið skal leggja fyrir persónuverndarráðið drög að viðmiðunum um faggildingu aðila, eins og um getur í 1. mgr. þessarar greinar, samkvæmt samræmingarkerfinu sem um getur í 63. gr.
4. Með fyrirvara um verkefni og valdheimildir lögbæra eftirlitsyfirvaldsins og ákvæði VIII. kafla skal aðili, eins og um getur í 1. mgr. þessarar greinar, með fyrirvara um viðeigandi verndarráðstafanir, gripa til viðeigandi aðgerða ef ábyrgðaraðili eða vinnsluaðili brýtur gegn reglunum, þ.m.t. tímabundinnar eða varanlegrar útilokunar ábyrgðaraðilans eða vinnsluaðilans frá reglunum. Hann skal tilkynna lögbæru eftirlitsyfirvaldi um slíkar aðgerðir og ástæðurnar fyrir þeim.
5. Lögbæra eftirlitsyfirvaldið skal afturkalla faggildingu aðila, eins og um getur í 1. mgr., ef skilyrðin fyrir faggildingu eru ekki, eða eru ekki lengur, uppfyllt eða ef aðgerðir aðilans brjóta í bága við þessa reglugerð.
6. Þessi grein gildir ekki um vinnslu af hálfu opinberra yfirvalda og stofnana.

42. gr.

Vottun

1. Aðildarrikin, eftirlitsyfirvöldin, persónuverndarráðið og framkvæmdastjórnin skulu hvetja til þess, einkum á vettvangi Sambandsins, að komið verði á fót vottunarfyrirkomulagi vegna persónuverndar ásamt persónuverndarinnisglum og -merkjum til að sýna fram á að vinnsla ábyrgðaraðila og vinnsluaðila uppfylli ákvæði þessarar reglugerðar. Taka skal tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja.
2. Auk þess að ábyrgðaraðilar eða vinnsluaðilar, sem heyra undir þessa reglugerð, komi á fót vottunarfyrirkomulagi vegna persónuverndar ásamt persónuverndarinnisglum eða -merkjum skv. 5. mgr. þessarar greinar geta ábyrgðaraðilar og vinnsluaðilar, sem heyra ekki undir þessa reglugerð skv. 3. gr., komið slíku á til að sýna fram á að fyrir hendi séu viðeigandi verndarráðstafanir innan ramma miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana samkvæmt þeim skilmálum sem um getur í e-lið 2. mgr. 46. gr. Slíkir ábyrgðaraðilar eða vinnsluaðilar skulu skuldbinda sig, með bindandi og framfylgjanlegum hætti, til að beita þessum viðeigandi verndarráðstöfunum, m.a. að því er varðar réttindi skráðra einstaklinga, með samningi eða öðrum lagalega bindandi gerningum.
3. Vottunin skal vera valfrjáls og aðgengileg í gagnsæju ferli.
4. Vottun samkvæmt þessari grein dregur ekki úr þeirri skyldu ábyrgðaraðila eða vinnsluaðila að fara að ákvæðum þessarar reglugerðar og hún hefur ekki áhrif á verkefni og valdheimildir eftirlitsyfirvalda sem eru lögbær skv. 55. eða 56. gr.
5. Vottunaraðilarnir, sem um getur í 43. gr., eða lögbært eftirlitsyfirvald skulu gefa út vottun samkvæmt þessari grein, á grundvelli viðmiðana sem lögbæra eftirlitsyfirvaldið samþykkir skv. 3. mgr. 58. gr. eða persónuverndarráðið skv. 63. gr. Samþykki persónuverndarráðið viðmiðanirnar getur það leitt til almennrar vottunar, Evrópska persónuverndarmerkisins.
6. Ábyrgðaraðili eða vinnsluaðili, sem óskar eftir vottun á vinnslu sinni samkvæmt vottunarkerfinu, skal láta vottunaraðilanum, sem um getur í 43. gr., eða, þar sem við á, lögbæra eftirlitsyfirvaldinu í té allar upplýsingar sem nauðsynlegar eru og þann aðgang að vinnslustarfsemi sinni sem nauðsynlegur er til að leiða vottunarferlið til lykta.

7. Vottunin skal gefin út til handa ábyrgðaraðila eða vinnsluaðila til þriggja ára að hámarki og hana má endurnýja, með sömu skilyrðum, að því tilskildu að viðeigandi kröfur séu áfram uppfylltar. Séu kröfur varðandi vottunina ekki, eða ekki lengur, uppfylltar skulu vottunaraðilarnir, sem um getur í 43. gr., eða lögbæra eftirlitsyfirvaldið, eftir því sem við á, afturkalla vottunina.

8. Persónuverndarráðið skal safna öllu vottunarfyrirkomulagi og persónuverndarinnsglum og -merkjum saman í skrá og gera aðgengilegt almenningi með viðeigandi hætti.

43. gr.

Vottunaraðilar

1. Með fyrirvara um verkefni og valdheimildir lögbæra eftirlitsyfirvaldsins skv. 57. og 58. gr. skulu vottunaraðilar með viðeigandi sérþekkingu á persónuvernd annast, ef nauðsyn krefur, útgáfu og endurnýjun vottunar, eftir að hafa tilkynnt það eftirlitsyfirvaldinu til að gera því kleift að beita valdheimildum sínum skv. h-lið 2. mgr. 58. gr. Aðildarríkin skulu tryggja að þessir vottunaraðilar séu faggiltir af öðrum eða báðum eftirtalinna aðila:

a) eftirlitsyfirvaldinu sem lögbært er skv. 55. eða 56. gr.,

b) faggildingarstofu í aðildarríki sem tilgreind er í samræmi við reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 ⁽²⁰⁾ í samræmi við Evrópustaðal EN-ISO/IEC 17065/2012 og viðbótarkröfur sem settar eru af eftirlitsyfirvaldinu sem lögbært er skv. 55. eða 56. gr.

2. Vottunaraðilar, sem um getur í 1. mgr., skulu aðeins hljóta faggildingu í samræmi við þá málsgrein ef þeir hafa:

a) sýnt fram á sjálfstæði sitt og sérþekkingu á viðfangsefni vottunarinnar með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi,

b) skuldbundið sig til að virða viðmiðanirnar sem um getur í 5. mgr. 42. gr. og samþykktar eru af eftirlitsyfirvaldinu sem er lögbært skv. 55. eða 56. gr. eða af persónuverndarráðinu skv. 63. gr.,

c) komið á verklagi hvað varðar útgáfu, reglubundna endurskoðun og afturköllun persónuverndarvottunar, persónuverndarinnsgla eða -merkja,

d) komið á fót verklagi og kerfum til að annast meðferð kvartana um brot gegn ákvæðum vottunarinnar eða á því hvernig ábyrgðaraðili eða vinnsluaðili framkvæmir eða hefur framkvæmt vottunina og til að gera þetta verklag og þessi kerfi gagnsæ fyrir skráða einstaklinga og almenning og

e) sýnt fram á, með hætti sem lögbæru eftirlitsyfirvaldi þykir fullnægjandi, að verkefni þeirra og skyldustörf leiði ekki til hagsmunaáreksturs.

3. Faggilding vottunaraðila, eins og um getur í 1. og 2. mgr. þessarar greinar, skal fara fram á grundvelli viðmiðana sem samþykktar eru af eftirlitsyfirvaldinu sem er lögbært skv. 55. eða 56. gr. eða persónuverndarráðinu skv. 63. gr. Ef um er að ræða faggildingu skv. b-lið 1. mgr. þessarar greinar skulu þessar kröfur koma til viðbótar þeim sem gert er ráð fyrir í reglugerð (EB) nr. 765/2008 og tæknireglunum sem lýsa aðferðum og verklagsreglum vottunaraðilanna.

4. Vottunaraðilarnir, sem um getur í 1. mgr., skulu bera ábyrgð á réttu mati, sem leiðir til vottunar eða afturköllunar á vottun, með fyrirvara um ábyrgð ábyrgðaraðila eða vinnsluaðila á því að farið sé að þessari reglugerð. Gefa skal faggildinguna út til fimm ára að hámarki og hana má endurnýja með sömu skilyrðum, að því tilskildu að vottunaraðili uppfylli kröfur þessarar greinar.

⁽²⁰⁾ Reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggildingu og markaðseftirlit í tengslum við markaðssetningu á vörum og um niðurfellingu reglugerðar (EBE) nr. 339/93 (Stjóð. ESB L 218, 13.8.2008, bls. 30).

5. Vottunaraðilarnir, sem um getur í 1. mgr., skulu láta lögbærum eftirlitsyfirvöldum í té rökstuðning fyrir því að veita eða afturkalla umbeðna vottun.
6. Eftirlitsyfirvaldið skal birta kröfurnar sem um getur í 3. mgr. þessarar greinar og viðmiðanirnar sem um getur í 5. mgr. 42. gr. á aðgengilegu formi. Eftirlitsyfirvöldin skulu einnig senda persónuverndarráðinu þessar kröfur og viðmiðanir. Persónuverndarráðið skal safna öllu vottunarfyrirkomulagi og persónuverndarinnsglum saman í skrá og gera aðgengilegt almenningi með viðeigandi hætti.
7. Með fyrirvara um VIII. kafla skal lögbæra eftirlitsyfirvaldið eða faggildingarstofan í aðildarríki afturkalla faggildingu vottunaraðila skv. 1. mgr. þessarar greinar ef skilyrðin fyrir faggildingunni eru ekki, eða eru ekki lengur, uppfyllt eða ef aðgerðir vottunaraðilans brjóta í bága við þessa reglugerð.
8. Framkvæmdastjórninni skal falið vald til þess að samþykkja framseldar gerðir í samræmi við 92. gr. í þeim tilgangi að tilgreina þær kröfur sem taka þarf tillit til í vottunarfyrirkomulagi vegna persónuverndar sem um getur í 1. mgr. 42. gr.
9. Framkvæmdastjórnin getur samþykkt framkvæmdargerðir þar sem mælt er fyrir um tækniáðla fyrir vottunarfyrirkomulag og persónuverndarinnsgli og -merki og fyrirkomulag til að kynna og viðurkenna slíkt vottunarfyrirkomulag, innsigli og merki. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

V. KAFLI

Miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana

44. gr.

Almennar meginreglur um miðlun upplýsinga

Með fyrirvara um önnur ákvæði þessarar reglugerðar skal aðeins miðla persónuupplýsingum, sem eru í vinnslu eða eru ætlaðar til vinnslu að lokinni miðlun þeirra til þriðja lands eða til alþjóðastofnunar, ef ábyrgðaraðilinn og vinnsluadilinn uppfylla skilyrðin sem mælt er fyrir um í þessum kafla, þ.m.t. til framsendingar persónuupplýsinga frá þriðja landi eða alþjóðastofnun til annars þriðja lands eða annarrar alþjóðastofnunar. Beita skal öllum ákvæðum í þessum kafla þannig að tryggja megi að ekki sé grafið undan vernd einstaklinga sem tryggð er með þessari reglugerð.

45. gr.

Miðlun á grundvelli ákvörðunar um hvort vernd sé fullnægjandi

1. Miðlun persónuupplýsinga til þriðja lands eða til alþjóðastofnunar er heimil ef framkvæmdastjórnin hefur ákveðið að þriðja landið, yfirráðasvæði eða einn eða fleiri tilgreindir geirar innan viðkomandi þriðja lands eða umrædd alþjóðastofnun tryggi fullnægjandi vernd. Slík miðlun þarfnast ekki sérstakrar heimildar.
2. Þegar framkvæmdastjórnin metur hvort vernd sé fullnægjandi skal hún einkum taka mið af eftirfarandi þáttum:
 - a) grunnreglum réttarríkisins, virðingu fyrir mannréttindum og mannfrelsi, viðeigandi löggjöf, jafnt almennt löggjöf sem sérlöggjöf, þ. á m. varðandi almannaoðryggi, landvarnir, þjóðaröryggi og refsirétt og aðgang opinberra yfirvalda að persónuupplýsingum, ásamt framkvæmd umræddrar löggjafar, reglum um persónuvernd, starfsreglum og öryggisráðstöfunum, þ.m.t. reglum um miðlun persónuupplýsinga til annars þriðja lands eða alþjóðastofnunar sem fylgt er í umræddu landi eða hjá alþjóðastofnun, dómaframkvæmd, sem og skilvirkum og fullnustuhæfum réttindum skráðra einstaklinga og stjórnsýslu- og dómsúrlausn fyrir skráða einstaklinga hvað varðar miðlun persónuupplýsinga um þá,
 - b) hvort fyrir hendi er sjálfstætt og skilvirkt eftirlitsyfirvald, eitt eða fleiri, í þriðja landinu eða sem alþjóðastofnun fellur undir, sem ber ábyrgð á að tryggja og framfylgja því að farið sé að reglum um persónuvernd, þ. á m. með fullnægjandi valdheimildir til að framfylgja þeim, á að veita skráðum einstaklingum aðstoð og ráðleggingar þegar þeir nýta sér réttindi sín og á samvinnu við eftirlitsyfirvöld í

aðildarríkjunum og

c) alþjóðlegum skuldbindingum sem þriðja landið eða alþjóðastofnunin hefur tekist á hendur eða öðrum skyldum samkvæmt lagalega bindandi samningum eða gerningum, sem og þátttöku í marghliða eða svæðisbundnum kerfum, einkum í tengslum við vernd persónuupplýsinga.

3. Framkvæmdastjórnin getur, eftir að hún hefur metið hvort umfang verndar er fullnægjandi, ákveðið á grundvelli framkvæmdargerðar, að þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindur geiri innan þriðja lands, eða alþjóðastofnun, tryggi fullnægjandi vernd í skilningi 2. mgr. þessarar greinar. Í framkvæmdargerðinni skal kveða á um fyrirkomulag reglubundinnar endurskoðunar, a.m.k. á fjögurra ára fresti, þar sem tekið skal tillit til viðeigandi þróunar í þriðja landinu eða hjá alþjóðastofnuninni. Í framkvæmdargerðinni skal tilgreina svæðis- og geirabundið gildissvið og, eftir atvikum, tilgreina eftirlitsyfirvald eða -yfirvöld sem um getur í b-lið 2. mgr. þessarar greinar. Framkvæmdargerðin skal samþykkt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

4. Framkvæmdastjórnin skal fylgjast jafnt og þétt með þróun mála í þriðju löndum og hjá alþjóðastofnunum sem gætu haft áhrif á framkvæmd ákvarðana sem samþykktar eru skv. 3. mgr. þessarar greinar og 6. mgr. 25. gr. tilskipunar 95/46/EB.

5. Framkvæmdastjórnin skal, að því marki sem nauðsynlegt telst, afturkalla, breyta eða fella tímabundið úr gildi ákvörðunina, sem um getur í 3. mgr. þessarar greinar, á grundvelli framkvæmdargerða, án afturvirkni, ef fyrirbyggjandi upplýsingar leiða í ljós, einkum í kjölfar endurskoðunarinnar sem um getur í 3. mgr. þessarar greinar, að þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindur geiri innan þriðja lands eða alþjóðastofnun tryggi ekki lengur fullnægjandi vernd í skilningi 2. mgr. þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

Þegar brýna nauðsyn ber til í tilhlýðilega rökstuddum tilvikum skal framkvæmdastjórnin samþykkja framkvæmdargerðir sem öðlast gildi án tafar í samræmi við málsmeðferðina sem um getur í 3. mgr. 93. gr.

6. Framkvæmdastjórnin skal hefja viðræður við þriðja landið eða alþjóðastofnunina með það fyrir augum að ráða bót á ástandinu sem varð til þess að ákvörðunin var tekin skv. 5. mgr.

7. Ákvörðun skv. 5. mgr. þessarar greinar hefur ekki áhrif á miðlun persónuupplýsinga til þriðja lands, yfirráðasvæðis eða eins eða fleiri tilgreindra geira innan þessa þriðja lands eða viðkomandi alþjóðastofnunar skv. 46.–49. gr.

8. Framkvæmdastjórnin skal birta í *Stjórnartíðindum Evrópusambandsins* og á vefsetri sínu skrá yfir þau þriðju lönd, yfirráðasvæði og tilgreindu geira innan þriðja lands og alþjóðastofnanir sem hún hefur ákveðið að veiti ekki, eða ekki lengur, fullnægjandi vernd.

9. Ákvarðanir sem framkvæmdastjórnin hefur samþykkt á grundvelli 6. mgr. 25. gr. tilskipunar 95/46/EB gilda áfram uns þeim er breytt, þær eru leystar af hólmi eða þær eru felldar niður með ákvörðun framkvæmdastjórnarinnar sem er samþykkt í samræmi við 3. eða 5. mgr. þessarar greinar.

46. gr.

Miðlun sem fellur undir viðeigandi verndarráðstafanir

1. Ef ekki er tekin ákvörðun skv. 3. mgr. 45. gr. getur ábyrgðaraðili eða vinnsluaðili því aðeins miðlað persónuupplýsingum til þriðja lands eða alþjóðastofnunar að hann hafi gert viðeigandi verndarráðstafanir og með því skilyrði að fyrir hendi séu framfylgjanleg réttindi og skilvirk lagaleg úrræði fyrir skráða einstaklinga.

2. Viðeigandi verndarráðstafanir, sem um getur í 1. mgr., geta, án þess að krafist sé sérstakrar heimildar frá eftirlitsyfirvaldi, falist í eftirfarandi:

a) lagalega bindandi og framfylgjanlegum gerningi milli opinberra yfirvalda eða stofnana,

b) bindandi fyrirtækjareglum í samræmi við 47. gr.,

c) stöðluðum ákvæðum um persónuvernd sem framkvæmdastjórnin hefur samþykkt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.,

- d) stöðluðum ákvæðum um persónuvernd sem eftirlitsyfirvald hefur samþykkt og framkvæmdastjórnin viðurkennt í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.,
 - e) viðurkenndum háttarisreglum skv. 40. gr., ásamt bindandi og framfylgjanlegum skuldbindingum ábyrgðaraðilans eða vinnsluaðilans í þriðja landinu um að beita viðeigandi verndarráðstöfunum, einnig að því er varðar réttindi skráðra einstaklinga, eða
 - f) viðurkenndu vottunarkerfi skv. 42. gr., ásamt bindandi og framfylgjanlegum skuldbindingum ábyrgðaraðilans eða vinnsluaðilans í þriðja landinu um að beita viðeigandi verndarráðstöfunum, einnig að því er varðar réttindi hinna skráðu.
3. Með fyrirvara um heimild frá lögbæru eftirlitsyfirvaldi geta viðeigandi verndarráðstafanir, sem um getur í 1. mgr., einnig falist einkum í eftirfarandi:
- a) samningsákvæðum milli ábyrgðaraðilans eða vinnsluaðilans og ábyrgðaraðila, vinnsluaðila eða viðtakanda persónuupplýsinganna í þriðja landinu eða hjá alþjóðastofnuninni eða
 - b) ákvæðum sem felld eru inn í stjórnvaldsráðstafanir milli opinberra yfirvalda eða stofnana sem ná yfir framfylgjanleg og skilvirk réttindi skráðra einstaklinga.
4. Eftirlitsyfirvaldið skal beita samræmingarkerfinu sem um getur í 63. gr. í þeim tilvikum sem um getur í 3. mgr. þessarar greinar.
5. Heimildir, sem aðildarríki eða eftirlitsyfirvald veitir á grundvelli 2. mgr. 26. gr. tilskipunar 95/46/EB, gilda áfram þar til eftirlitsyfirvaldið breytir þeim, leysir þær af hólmi eða fellir þær niður, ef nauðsyn krefur. Ákvarðanir, sem framkvæmdastjórnin hefur samþykkt á grundvelli tilskipunar 95/46/EB, gilda áfram þar til þeim er breytt, þær eru leystar af hólmi eða þær eru felldar niður, ef nauðsyn krefur, með ákvörðun framkvæmdastjórnarinnar sem er samþykkt í samræmi við 2. mgr. þessarar greinar.

47. gr.

Bindandi fyrirtækjareglur

1. Lögbær eftirlitsyfirvöld skulu samþykkja bindandi fyrirtækjareglur í samræmi við samræmingarkerfið sem tilgreint er í 63. gr., að því tilskildu að þær:
- a) séu lagalega bindandi og að þær gildi um og þeim sé framfylgt af sérhverjum hlutaðeigandi aðila að fyrirtækjasamstæðu eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, þ.m.t. starfsmönnum þeirra,
 - b) veiti skráðum einstaklingum framfylgjanleg réttindi með ótvíræðum hætti með hliðsjón af vinnslu persónuupplýsinga um þá og
 - c) uppfylli kröfurnar sem mælt er fyrir um í 2. gr.
2. Í bindandi fyrirtækjareglum, sem um getur í 1. mgr., skal tilgreina a.m.k.:
- a) skipulag og samskiptaupplýsingar viðkomandi fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi og sérhvers aðila samstæðunnar eða hópsins,
 - b) miðlun eða endurtekna miðlun upplýsinga, þ.m.t. hvaða flokka persónuupplýsinga er um að ræða, tegund og tilgang vinnslu, hvaða hópur skráðra einstaklinga verður fyrir áhrifum af henni og hvaða þriðja land eða þriðju lönd er um að ræða,
 - c) lagalega bindandi eðli þeirra, jafnt inn á við sem út á við,
 - d) beitingu almennra meginreglna um persónuvernd, einkum um takmörkun vegna tilgangs, lágmörkun gagna, takmörkun á varðveislutímabili, gæði gagna, innbyggða og sjálfgefna persónuvernd, lagagrundvöll vinnslu, vinnslu sérstakra flokka persónuupplýsinga, ráðstafanir til að tryggja persónuvernd og kröfur sem lúta að framsendingu til aðila sem eru ekki háðir bindandi fyrirtækjareglum,
 - e) réttindi skráðra einstaklinga að því er varðar vinnslu og leiðir til að neyta þeirra réttinda, þ.m.t. réttinn til

að falla ekki undir ákvarðanir sem byggjast eingöngu á sjálfvirkri vinnslu, m.a. gerð persónusniðs í samræmi við 22. gr., til að leggja fram kvörtun hjá lögbæru eftirlitsfirvaldi og hjá lögbærum dómstólum aðildarríkjanna í samræmi við 79. gr. og til að rétta hlut sinn og, eftir því sem við á, til bóta vegna brots á bindandi fyrirtækjareglum,

- f) viðurkenningu ábyrgðaraðila eða vinnsluaðila, sem hafa staðfestu á yfirráðasvæði aðildarríkis, á ábyrgð vegna hvers kyns brota gegn bindandi fyrirtækjareglum af hálfu hlutaðeigandi aðila sem hafa ekki staðfestu í Sambandinu; ábyrgðaraðilinn eða vinnsluaðilinn skal því aðeins vera undanþeginn bótaábyrgð, að fullu eða að hluta, að hann færi sönnur á að viðkomandi aðili sé ekki ábyrgur fyrir tilvikinu sem leiddi til tjónsins,
 - g) hvernig skráðum einstaklingum eru veittar upplýsingar um bindandi fyrirtækjareglur, einkum ákvæðin sem um getur í d-, e- og f-lið þessarar málsgreinar, auk 13. og 14. gr.,
 - h) verkefni persónuverndarfulltrúa sem eru tilnefndir í samræmi við 37. gr. eða annars aðila eða stofnunar sem hefur með höndum eftirlit með því að bindandi fyrirtækjareglum sé fylgt innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi, ásamt eftirliti með starfsþjálfun og meðferð kvörtunarmála,
 - i) málsmæðferð vegna kvörtunarmála,
 - j) fyrirkomulag innan fyrirtækjasamstæðunnar eða hóps fyrirtækja, sem stunda sameiginlega atvinnustarfsemi, til að tryggja sannprófun á því að farið sé að bindandi fyrirtækjareglum. Þetta fyrirkomulag skal fela í sér úttektir á persónuvernd og aðferðir við að tryggja að gripið sé til aðgerða til úrbóta til að vernda réttindi hins skráða. Tilkynna ætti þeim aðila eða stofnun, sem um getur í h-lið, og stjórn fyrirtækisins, sem er ráðandi í fyrirtækjasamstæðu eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, um niðurstöður sannprófunarinnar og þær ættu að vera aðgengilegar lögbærum eftirlitsfirvöldum fari þau fram á það,
 - k) fyrirkomulag skýrslugjafar og skráningar á breytingum á reglunum og skýrslugjafar um breytingarnar til eftirlitsfirvaldsins,
 - l) fyrirkomulag samvinnu við eftirlitsfirvaldið til að tryggja reglufylgni aðila að fyrirtækjasamstæðunni eða hópi fyrirtækja sem stunda sameiginlega atvinnustarfsemi, einkum með því að sjá til þess að eftirlitsfirvaldið fái aðgang að niðurstöðum sannprófunar á þeim ráðstöfunum sem um getur í j-lið,
 - m) fyrirkomulag vegna skýrslugjafar til lögbærs eftirlitsfirvalds um þau lagaskilyrði sem aðili að fyrirtækjasamstæðu eða hópi fyrirtækja, sem stunda sameiginlega atvinnustarfsemi, þarf að hlíta í þriðja landi sem líklegt er að hafi umtalsverð neikvæð áhrif á þær tryggingar sem felast í bindandi fyrirtækjareglum og
 - n) viðeigandi þjálfun starfsmanna, sem hafa stöðugan eða reglulegan aðgang að persónuupplýsingum, á sviði persónuverndar.
3. Framkvæmdastjórnin getur tilgreint nánar snið og aðferðir við upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsfirvalda að því er varðar bindandi fyrirtækjareglur í skilningi þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmæðferðina sem um getur í 2. mgr. 93. gr.

48. gr.

Miðlun eða birting sem ekki er heimiluð samkvæmt lögum Sambandsins

Dóma, sem dómstólar kveða upp, og ákvarðanir stjórnsýslufirvalds í þriðja landi, sem krefjast þess að ábyrgðaraðili eða vinnsluaðili miðli persónuupplýsingum eða birti þær, má því aðeins viðurkenna eða framfylgja með einhverjum hætti að slíkt byggist á alþjóðasamningi, s.s. samningi um gagnkvæma dómsmálaoðstöð, sem er í gildi milli þriðja landsins sem leggur fram beiðni og Sambandsins eða aðildarríkis, án þess að það hafi áhrif á aðrar ástæður til miðlunar samkvæmt þessum kafla.

49. gr.

Undanþágur vegna sérstakra aðstæðna

1. Ef ekki liggur fyrir ákvörðun um að vernd sé fullnægjandi skv. 3. mgr. 45. gr. eða viðeigandi verndarráðstafanir skv. 46. gr., þ.m.t. bindandi fyrirtækjareglur, skal miðlun eða endurtekin miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar aðeins fara fram að uppfylltu einu af eftirfarandi skilyrðum:
 - a) skráði einstaklingurinn hefur veitt ótvírætt samþykki sitt fyrir fyrirhugaðri miðlun eftir að honum hefur verið tilkynnt um mögulega áhættu sem miðlunin kann að hafa í för með sér fyrir hann vegna þess að ekki liggur fyrir ákvörðun um að vernd sé fullnægjandi og viðeigandi verndarráðstafanir hafa ekki verið gerðar,
 - b) miðlunin er nauðsynleg vegna framkvæmdar samnings milli skráða einstaklingsins og ábyrgðaraðilans eða ráðstafana sem gerðar eru að beiðni hins skráða áður en til gerðar samnings kemur,
 - c) miðlunin er nauðsynleg fyrir gerð eða framkvæmd samnings í þágu hins skráða, sem ábyrgðaraðilinn og annar einstaklingur eða lögaðili gera sín í milli,
 - d) miðlunin er nauðsynleg vegna mikilvægra almannahagsmuna,
 - e) miðlunin er nauðsynleg til að stofna, hafa uppi eða verja réttarkröfur,
 - f) miðlunin er nauðsynleg til að vernda brýna hagsmuni hins skráða eða annarra aðila ef hinn skráði er líkamlega eða í lagalegum skilningi ófær um að gefa samþykki sitt,
 - g) upplýsingum er miðlað af skrá sem er samkvæmt lögum Sambandsins eða lögum aðildarríkis ætlað að veita almenningi upplýsingar og er aðgengileg annaðhvort öllum almenningi eða hverjum þeim sem getur sýnt fram á að hann hafi lögmætra hagsmuna að gæta, en aðeins að svo miklu leyti sem skilyrði fyrir aðgangi, sem mælt er fyrir um í lögum Sambandsins eða lögum aðildarríkis, séu uppfyllt í því tilviki.

Ef ekki er hægt að byggja miðlun á ákvæði í 45. eða 46. gr., þ.m.t. ákvæðum um bindandi fyrirtækjareglur, og engin af undanþágunum vegna sérstakra aðstæðna, sem um getur í fyrstu undirgrein þessarar málsgreinar, á við er aðeins heimilt að miðla persónuupplýsingum til þriðja lands eða til alþjóðastofnunar ef miðlunin er ekki endurtekin, varðar aðeins takmarkaðan fjölda skráðra einstaklinga, er nauðsynleg vegna mikilvægra lögmætra hagsmuna sem ábyrgðaraðili gætir þegar hagsmunir eða réttindi og frelsi hins skráða vega ekki þyngra og ef ábyrgðaraðilinn hefur kannað allar aðstæður er varða miðlun upplýsinganna og hefur, á grundvelli þess mats, gert viðeigandi verndarráðstafanir að því er varðar vernd persónuupplýsinga. Ábyrgðaraðilinn skal upplýsa eftirlitsyfirlaldið um miðlunina. Auk þess að láta í té þær upplýsingar, sem um getur í 13. og 14. gr., skal ábyrgðaraðilinn upplýsa hinn skráða um miðlunina og þá mikilvægu, lögmætu hagsmuni sem gætt er.

2. Miðlun skv. g-lið fyrstu undirgreinar 1. mgr. skal ekki taka til persónuupplýsinganna í heild sinni eða heilla flokka upplýsinga í skránni. Ef skráin er ætluð til skoðunar fyrir þá sem hafa lögmætra hagsmuna að gæta skal miðlun aðeins fara fram að beiðni þessara aðila eða ef þeir eiga að vera viðtakendur upplýsinganna.
3. Ákvæði a-, b- og c-liðar fyrstu undirgreinar 1. mgr. og annarrar undirgreinar hennar gilda ekki um starfsemi opinberra yfirvalda við beitingu þeirra á opinberu valdi.
4. Viðurkenna skal almannahagsmuni, sem um getur í d-lið fyrstu undirgreinar 1. mgr., í lögum Sambandsins eða í lögum þess aðildarríkis sem ábyrgðaraðilinn heyrir undir.
5. Þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geta lög Sambandsins eða lög aðildarríkis takmarkað með ótvíræðum hætti miðlun sérstakra flokka persónuupplýsinga til þriðja lands eða alþjóðastofnunar á grundvelli mikilvægra almannahagsmuna. Aðildarríkin skulu tilkynna framkvæmdastjórninni um slík ákvæði.
6. Ábyrgðaraðilinn eða vinnsluaðilinn skal staðfesta matið og viðeigandi verndarráðstafanir, sem um getur í annarri undirgrein 1. mgr. þessarar greinar, í skránni sem um getur í 30. gr.

50. gr.

Alþjóðleg samvinna um vernd persónuupplýsinga

Þegar um er að ræða þriðju lönd eða alþjóðastofnanir skulu framkvæmdastjórnin og eftirlitsyfirvöld gera viðeigandi ráðstafanir til að:

- a) þróa fyrirkomulag alþjóðlegrar samvinnu til að greiða fyrir skilvirkri framkvæmd löggjafar um vernd persónuupplýsinga,
- b) veita gagnkvæma alþjóðlega aðstoð við framfylgd löggjafar um vernd persónuupplýsinga, m.a. með tilkynningum, framsendingu kvörtunamála, aðstoð við rannsóknir og upplýsingaskiptum, með fyrirvara um viðeigandi verndarráðstafanir til verndar persónuupplýsingum og öðrum grundvallarréttindum og mannfrelsi,
- c) fá viðkomandi hagsmunaaðila til að taka þátt í umfjöllun og starfi sem miðar að því að efla alþjóðlega samvinnu við framfylgd löggjafar um vernd persónuupplýsinga,
- d) stuðla að skiptum á og skjalahaldi um löggjöf og starfsvenjur á sviði verndar persónuupplýsinga, einkum um ágreining við þriðju lönd um lögsögu.

VI. KAFLI

Sjálfstæð eftirlitsyfirvöld

1. þáttur

Sjálfstæði

51. gr.

Eftirlitsyfirvald

1. Sérhvert aðildarríki skal sjá til þess að eitt eða fleiri sjálfstæð opinber yfirvöld beri ábyrgð á að fylgjast með beitingu þessarar reglugerðar til þess að vernda grundvallarréttindi og frelsi einstaklinga í tengslum við vinnslu persónuupplýsinga og til að greiða fyrir frjálsu flæði persónuupplýsinga innan Sambandsins („eftirlitsyfirvald“).
2. Sérhvert eftirlitsyfirvald skal stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu. Í þessum tilgangi skulu eftirlitsyfirvöldin eiga samstarf sín í milli og við framkvæmdastjórnina í samræmi við VII. kafla.
3. Ef fleiri en einu eftirlitsyfirvaldi er komið á fót í aðildarríki skal aðildarríkið tilnefna það eftirlitsyfirvald sem á að koma fram fyrir hönd þessara yfirvalda í persónuverndarráðinu og skal koma á kerfi til að tryggja að hin yfirvöldin fari að þeim reglum sem varða samræmingarkerfið sem um getur í 63. gr.
4. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt samkvæmt þessum kafla og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

52. gr.

Sjálfstæði

1. Sérhvert eftirlitsyfirvald skal vera algerlega sjálfstætt í störfum sínum og þegar það beitir valdheimildum sínum í samræmi við þessa reglugerð.
2. Fulltrúi eða fulltrúar hvers eftirlitsyfirvalds skulu, í störfum sínum og þegar þeir beita valdheimildum sínum í samræmi við þessa reglugerð, vera lausir við utanaðkomandi áhrif, jafnt bein sem óbein, og skulu hvorki leita eftir né taka við fyrirmælum frá öðrum aðilum.

3. Fulltrúi eða fulltrúar hvers eftirlitsyfirvalds skulu ekki aðhafast neitt það sem er ósamrýmanlegt skyldum þeirra og skulu ekki stunda önnur ósamrýmanleg störf á skipunartíma sínum, hvorki launuð né ólaunuð.
4. Sérhvert aðildarríki skal tryggja að hvert eftirlitsyfirvald hafi yfir að ráða þeim mannauði, tækniúrræðum og fjármagni, húsakosti og innviðum sem nauðsynleg eru til að það geti unnið störf sín og beitt valdheimildum sínum með skilvirkum hætti, þ. á m. í tengslum við gagnkvæma aðstoð, samvinnu og þátttöku í starfi persónuverndarráðsins.
5. Sérhvert aðildarríki skal sjá til þess að hvert eftirlitsyfirvald velji og hafi eigið starfslið og ætti það eingöngu að lúta stjórn fulltrúa hlutaðeigandi eftirlitsyfirvalds.
6. Sérhvert aðildarríki skal sjá til þess að hvert eftirlitsyfirvald sæti eftirliti með fjárreiðum, sem hefur ekki áhrif á sjálfstæði þess, og að það hafi sérstaka opinbera, árlega fjárhagsáætlun sem getur verið hluti af heildarfjárlögum fylkisins eða ríkisins.

53. gr.

Almenn skilyrði varðandi fulltrúa eftirlitsyfirvaldsins

1. Aðildarríkin skulu kveða á um að sérhver fulltrúi eftirlitsyfirvalda þeirra sé skipaður samkvæmt gagnsærri málsmeðferð af:
 - þingi þeirra,
 - ríkisstjórn þeirra,
 - þjóðhöfðingja þeirra eða
 - óháðri stofnun sem falin er skipunin samkvæmt lögum aðildarríkisins.
2. Sérhver fulltrúi skal búa yfir menntun og hæfi, reynslu og færni, einkum á sviði verndar persónuupplýsinga, sem honum er nauðsynleg til að hann geti sinnt skyldustörfum sínum og beitt valdheimildum sínum.
3. Skyldustörfum fulltrúa skal ljúka þegar skipunartími hans rennur út, hann segir starfinu lausu eða lætur af störfum fyrir aldurs sakir, í samræmi við lög hlutaðeigandi aðildarríkis.
4. Aðeins skal víkja fulltrúa brott ef um alvarlegt misferli er að ræða eða ef hann fullnægir ekki lengur þeim skilyrðum sem krafist er vegna skyldustarfa hans.

54. gr.

Reglur um stofnun eftirlitsyfirvalds

1. Sérhvert aðildarríki skal kveða á um öll eftirfarandi atriði í lögum:
 - a) stofnun sérhvers eftirlitsyfirvalds,
 - b) menntun og hæfisskilyrði sem krafist er vegna skipunar fulltrúa sérhvers eftirlitsyfirvalds,
 - c) reglur og verklagsreglur að því er varðar skipun fulltrúa sérhvers eftirlitsyfirvalds,
 - d) skipunartíma fulltrúa sérhvers eftirlitsyfirvalds sem ekki skal vera skemmri en fjögur ár, að undanskilinni fyrstu skipun eftir 24. maí 2016, sem getur verið til skemmri tíma ef það er nauðsynlegt til að standa vörð um sjálfstæði eftirlitsyfirvaldsins með því að nota áfangabundið skipunarferli,

- e) hvort og þá hversu oft heimilt er að endurnýja skipun fulltrúa sérhvers eftirlitsyfirvalds,
- f) skilyrði varðandi skyldur fulltrúa sérhvers eftirlitsyfirvalds og starfsmanna þess, bann við aðgerðum, störfum og friðindum sem eru ósamrýmanleg þeim á skipunartímanum og að honum loknum og reglur um starfslok.
2. Fulltrúi eða fulltrúar sérhvers eftirlitsyfirvalds og starfsmenn þess skulu, í samræmi við lög Sambandsins eða lög aðildarríkis, vera bundnir þagnarskyldu, bæði á skipunartíma og eftir að honum lýkur, með tilliti til trúnaðarupplýsinga sem þeir hafa fengið við skyldustörf sín eða við beitingu valdheimilda sinna. Meðan á skipunartíma þeirra stendur skal þagnarskylda þeirra einkum gilda um tilkynningar einstaklinga um brot gegn þessari reglugerð.

2. þáttur

Valdsvið, verkefni og valdheimildir

55. gr.

Valdsvið

1. Sérhvert eftirlitsyfirvald skal vera til þess bært að sinna þeim verkefnum sem því eru falin og beita þeim valdheimildum sem því hafa verið veittar í samræmi við þessa reglugerð á yfirráðasvæði eigin aðildarríkis.
2. Þegar vinnsla er í höndum opinberra yfirvalda eða einkaaðila, sem starfa á grundvelli c- eða e-liðar 1. mgr. 6. gr., skal eftirlitsyfirvald hlutaðeigandi aðildarríkis teljast lögbært. Í þeim tilvikum á 56. gr. ekki við.
3. Eftirlitsyfirvöld skulu ekki vera til þess bær að hafa eftirlit með vinnsluaðgerðum dómstóla þegar þeir fara með dómsvald sitt.

56. gr.

Valdsvið forystueftirlitsyfirvalds

1. Með fyrirvara um 55. gr. skal eftirlitsyfirvald yfir höfuðstöðvum eða hinni einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans teljast til þess bært að koma fram sem forystueftirlitsyfirvald vegna vinnslu yfir landamæri sem sá ábyrgðaraðili eða vinnsluaðili annast í samræmi við málsmeðferðina sem kveðið er á um í 60. gr.
2. Þrátt fyrir 1. mgr. skal sérhvert eftirlitsyfirvald teljast til þess bært að fjalla um kvörtun sem lögð er fyrir það eða mögulegt brot gegn þessari reglugerð ef viðfangsefnið tengist eingöngu starfsstöð í aðildarríki þess eða hefur eingöngu veruleg áhrif á skráða einstaklinga í aðildarríki þess.
3. Í þeim tilvikum sem um getur í 2. mgr. þessarar greinar skal eftirlitsyfirvaldið tilkynna forystueftirlitsyfirvaldinu um málavöxtu án tafar. Forystueftirlitsyfirvaldið skal, innan þriggja vikna frá því að tilkynningin berst, ákveða hvort það muni fjalla um málið í samræmi við málsmeðferðina sem kveðið er á um í 60. gr., að teknu tilliti til þess hvort ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu í aðildarríki eftirlitsyfirvaldsins sem tilkynnti um það.
4. Ef forystueftirlitsyfirvaldið ákveður að fjalla um málið gildir málsmeðferðin sem kveðið er á um í 60. gr. Eftirlitsyfirvaldið, sem sendi tilkynninguna til forystueftirlitsyfirvaldsins, getur sent því drög að ákvörðun. Forystueftirlitsyfirvaldið skal taka ýtrasta tillit til umræddra draga þegar það semur drög að ákvörðuninni sem um getur í 3. mgr. 60. gr.
5. Ef forystueftirlitsyfirvaldið ákveður að fjalla ekki um málið skal eftirlitsyfirvaldið, sem tilkynnti forystueftirlitsyfirvaldinu um það, fjalla um málið skv. 61. og 62. gr.

6. Forystueftirlitsyfirvaldið skal vera eini tengiliður ábyrgðaraðilans eða vinnsluaðilans vegna vinnslu hans yfir landamæri.

57. gr.

Verkefni

1. Með fyrirvara um önnur verkefni, sem sett eru fram í þessari reglugerð, skal sérhvert eftirlitsyfirvald, á eigin yfirlýðingum:

- a) fylgjast með og framfylgja beitingu þessarar reglugerðar,
- b) efla vitund og skilning almennings á áhættu, reglum, verndarráðstöfunum og réttindum í tengslum við vinnslu. Gefa skal starfsemi sem beinist einkum að börnum sérstakan gaum,
- c) veita þjóðþingi, ríkisstjórn og öðrum stofnunum og aðilum ráðgjöf, í samræmi við landslög aðildarríkis, um ráðstafanir á sviði lagasetningar og stjórnsýslu sem tengist vernd réttinda og frelsis einstaklinga að því er varðar vinnslu,
- d) efla vitund ábyrgðaraðila og vinnsluaðila um skyldur sínar samkvæmt þessari reglugerð,
- e) veita, að fenginni beiðni, skráðum einstaklingi upplýsingar um það hvernig hann getur neytt réttinda sinna samkvæmt þessari reglugerð og, ef við á, starfa með eftirlitsyfirvöldum í öðrum aðildarríkjum í því skyni,
- f) fjalla um kvartanir sem skráður einstaklingur eða stofnun, samtök eða félag leggja fram í samræmi við 80. gr. og rannsaka, að því marki sem við á, efni kvörtunarinnar og upplýsa kvartandann um framvindu og niðurstöður rannsóknarinnar innan hæfilegs tíma, einkum ef nauðsyn er á frekari rannsóknum eða samræmingu við annað eftirlitsyfirvald,
- g) eiga samstarf við önnur eftirlitsyfirvöld, þ.m.t. með því að skiptast á upplýsingum, og veita gagnkvæma aðstoð, með það fyrir augum að tryggja samkvæmni í beitingu og framfylgd þessarar reglugerðar,
- h) gera rannsókn á beitingu þessarar reglugerðar, m.a. á grundvelli upplýsinga frá öðru eftirlitsyfirvaldi eða öðru opinberu yfirvaldi,
- i) fylgjast með þróun sem skiptir máli, að svo miklu leyti sem hún hefur áhrif á vernd persónuupplýsinga, einkum þróun upplýsinga- og fjarskiptatækni og viðskiptahátta,
- j) samþykkja föst samningsákvæði sem um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr.,
- k) útbúa og viðhalda skrá í tengslum við kröfu um mat á áhrifum á persónuvernd skv. 4. mgr. 35. gr.,
- l) veita ráðgjöf um vinnsluaðgerðir sem um getur í 2. mgr. 36. gr.,
- m) hvetja til þess að samdar verði háttarnisreglur skv. 1. mgr. 40. gr. og gefa álit á og samþykkja háttarnisreglur sem tryggja fullnægjandi verndarráðstafanir skv. 5. mgr. 40. gr.,
- n) hvetja til þess að vottunarfyrirkomulagi vegna persónuverndar og persónuverndarinnisglum og -merkjum verði komið á skv. 1. mgr. 42. gr. og samþykkja viðmiðanir vegna vottunar skv. 5. mgr. 42. gr.,
- o) eftir atvikum, láta fara fram reglubundna endurskoðun á vottunum sem eru gefnar út í samræmi við 7. mgr. 42. gr.,
- p) semja og birta drög að viðmiðunum um faggildingu aðila sem hefur eftirlit með háttarnisreglum skv. 41. gr. og vottunaraðila skv. 43. gr.,
- q) annast faggildingu aðila vegna eftirlits með háttarnisreglum skv. 41. gr. og vottunaraðila skv. 43. gr.,
- r) heimila samningsákvæði og ákvæði sem um getur í 3. mgr. 46. gr.,
- s) samþykkja bindandi fyrirtækjareglur skv. 47. gr.,
- t) taka þátt í starfsemi persónuverndarráðsins,
- u) halda innri skrár yfir brot á þessari reglugerð og ráðstafanir sem gerðar eru í samræmi við 2. mgr. 58. gr.

og

v) sinna öðrum störfum sem tengjast vernd persónuupplýsinga.

2. Sérhvert eftirlitsyfirvald skal auðvelda framlagningu kvartana, sem um getur í f-lið 1. mgr., með því að gera ráðstafanir á borð við kvörtunareyðublað, sem einnig má fylla út rafrænt, án þess þó að aðrir samskiptamöguleikar séu útilokaðir.

3. Sérhvert eftirlitsyfirvald skal sinna störfum sínum, skráðum einstaklingum og, eftir atvikum, persónuverndarfulltrúanum að kostnaðarlausu.

4. Þegar beiðnir eru augljóslega tilefnislausar eða óhóflegar, einkum vegna þess að þær eru endurteknar, er eftirlitsyfirvaldinu heimilt að setja upp sanngjarnt gjald, á grundvelli stjórnsýslukostnaðar, eða neita að fjalla um beiðnina. Það skal vera eftirlitsyfirvaldsins að sýna fram á að beiðni sé tilefnislaus eða óhófleg.

58. gr.

Valdheimildir

1. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi rannsóknarheimildir:

a) heimild til að fyrirskipa að ábyrgðaraðilinn og vinnsluaðilinn og, eftir atvikum, fulltrúi ábyrgðaraðilans eða vinnsluaðilans veiti hvers kyns upplýsingar sem það þarfnast vegna skyldustarfa sinna,

b) heimild til að láta fara fram rannsóknir í formi úttekta á persónuvernd,

c) heimild til að láta fara fram endurskoðun á vottunum sem eru gefnar út skv. 7. mgr. 42. gr.,

d) heimild til að tilkynna ábyrgðaraðila eða vinnsluaðila um meint brot á þessari reglugerð,

e) heimild til að fá hjá ábyrgðaraðila og vinnsluaðila aðgang að öllum persónuupplýsingum og öllum upplýsingum sem nauðsynlegar eru vegna verkefna þess,

f) heimild til að fá aðgang að húsnæði ábyrgðaraðila og vinnsluaðila, þ.m.t. hvers kyns gagnavinnslubúnaði og -aðferðum, í samræmi við réttarfarslög Sambandsins eða aðildarríkis.

2. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi valdheimildir til að gera ráðstafanir til úrbóta:

a) heimild til að veita ábyrgðaraðila eða vinnsluaðila viðvörðun um að líklegt sé að fyrirhugaðar vinnsluaðgerðir brjóti í bága við ákvæði þessarar reglugerðar,

b) heimild til að veita ábyrgðaraðila eða vinnsluaðila áminningu ef vinnsluaðgerðir hafa brotið í bága við þessa reglugerð,

c) heimild til að fyrirskipa að ábyrgðaraðili eða vinnsluaðili fari að beiðnum hins skráða um að fá að neyta réttinda sinna samkvæmt þessari reglugerð,

d) heimild til að fyrirskipa að ábyrgðaraðili eða vinnsluaðili færi vinnsluaðgerðir til samræmis við ákvæði þessarar reglugerðar, eftir því sem við á, með tilteknum hætti og innan tiltekins tíma,

e) heimild til að fyrirskipa að ábyrgðaraðili tilkynni hinum skráða um öryggisbrot við meðferð persónuupplýsinga,

f) heimild til að setja tímabundna eða varanlega takmörkun á vinnslu, þ.m.t. bann,

g) heimild til að fyrirskipa leiðréttingu eða eyðingu persónuupplýsinga eða takmörkun á vinnslu þeirra skv. 16., 17. og 18. gr. og að slíkar aðgerðir verði tilkynntar viðtakendum sem fengið hafa persónuupplýsingarnar í hendur skv. 2. mgr. 17. gr. og 19. gr.,

h) heimild til að afturkalla vottun eða fyrirskipa að vottunaraðilinn afturkalli vottun sem gefin var út skv. 42. og 43. gr. eða fyrirskipa að vottunaraðilinn gefi ekki út vottun ef kröfum vegna vottunarinnar er ekki, eða er ekki lengur, fullnægt,

i) heimild til að leggja á stjórnsýslusekt skv. 83. gr., til viðbótar við eða í stað ráðstafana sem um getur í þessari

málgrein, allt eftir aðstæðum í hverju einstöku máli,

j) heimild til að fyrirskipa tímabundna stöðvun gagnaflæðis til viðtakanda í þriðja landi eða til alþjóðastofnunar.

3. Sérhvert eftirlitsyfirvald skal hafa allar eftirfarandi leyfisveitinga- og ráðgjafarheimildir:

a) heimild til að veita ábyrgðaraðila ráðgjöf í samræmi við fyrirframsamráðsferlið sem um getur í 36. gr.,

b) heimild til að leggja, að eigin frumkvæði eða samkvæmt beiðni, álitsgerðir fyrir þjóðþing eða ríkisstjórn aðildarríkisins eða, í samræmi við lög aðildarríkisins, aðrar stofnanir og aðila, sem og almenning, um hvert það málefni sem tengist vernd persónuupplýsinga,

c) heimild til að leyfa vinnslu sem um getur í 5. mgr. 36. gr., sé slíkrar fyrirframheimildar krafist samkvæmt lögum aðildarríkisins,

d) heimild til að gefa út álit og samþykkja drög að hátternisreglum skv. 5. mgr. 40. gr.,

e) heimild til að faggilda vottunaraðila skv. 43. gr.,

f) heimild til að gefa út vottanir og samþykkja viðmiðanir fyrir vottun í samræmi við 5. mgr. 42. gr.,

g) heimild til að samþykkja stöðluð ákvæði um persónuvernd sem um getur í 8. mgr. 28. gr. og d-lið 2. mgr. 46. gr.,

h) heimild til að leyfa samningsákvæði sem um getur í a-lið 3. mgr. 46. gr.,

i) heimild til að leyfa stjórnvaldsráðstafanir sem um getur í b-lið 3. mgr. 46. gr.,

j) heimild til að samþykkja bindandi fyrirtækjareglur skv. 47. gr.

4. Beiting þeirra valdheimilda, sem eftirlitsyfirvaldinu eru veittar samkvæmt þessari grein, skal vera með fyrirvara um viðeigandi verndarráðstafanir, þ. á m. skilvirk réttarúræði og sanngjarna málsmeðferð sem sett er fram í lögum Sambandsins og lögum aðildarríkis í samræmi við sáttmálann um grundvallarréttindi.

5. Sérhvert aðildarríki skal kveða á um í lögum að eftirlitsyfirvald þess hafi heimild til að vekja athygli dómsyfirvalda á brotum gegn þessari reglugerð og, eftir því sem við á, hefja eða taka þátt í málarekstri til þess að framfylgja ákvæðum hennar.

6. Sérhvert aðildarríki getur kveðið á um í lögum að eftirlitsyfirvald þess hafi valdheimildir til viðbótar þeim sem um getur í 1., 2. og 3. mgr. Beiting þessara valdheimilda skal ekki draga úr skilvirkri framkvæmd VII. kafla.

59. gr.

Skýrslur um starfsemi

Sérhvert eftirlitsyfirvald skal semja ársskýrslu um starfsemi sína sem má m.a. innihalda skrá yfir tegundir brota sem hafa verið tilkynnt og tegundir ráðstafana sem gerðar hafa verið í samræmi við 2. mgr. 58. gr. Þessar skýrslur skal senda þjóðþingi, ríkisstjórn og öðrum yfirlöndum eins og tilgreint er í lögum aðildarríkisins. Þær skulu gerðar aðgengilegar almenningi, framkvæmdastjórninni og persónuverndarráðinu.

VII. KAFLI

Samstarf og samræming

1. þáttur

Samstarf

60. gr.

Samstarf milli forystueftirlitsyfirvaldsins og annarra hlutaðeigandi eftirlitsyfirvalda

1. Forystueftirlitsyfirvaldið skal starfa með öðrum hlutaðeigandi eftirlitsyfirvöldum í samræmi við þessa grein með það fyrir augum að ná samstöðu. Forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld skulu skiptast á öllum viðeigandi upplýsingum.
2. Forystueftirlitsyfirvaldið getur hvenær sem er óskað eftir því að önnur hlutaðeigandi eftirlitsyfirvöld veiti gagnkvæma aðstoð skv. 61. gr. og getur framkvæmt sameiginlegar aðgerðir skv. 62. gr., einkum við rannsóknir eða þegar fylgst er með framkvæmd ráðstöfunar sem varðar ábyrgðaraðila eða vinnsluaðila með staðfestu í öðru aðildarríki.
3. Forystueftirlitsyfirvaldið skal án tafar senda viðeigandi upplýsingar um málið til hinna eftirlitsyfirvaldanna sem í hlut eiga. Það skal án tafar senda drög að ákvörðun til hinna eftirlitsyfirvaldanna sem í hlut eiga til að fá álit þeirra og taka tilhlýðilegt tillit til sjónarmiða þeirra.
4. Ef eitthvert hinna eftirlitsyfirvaldanna sem í hlut eiga leggur fram viðeigandi og rökstudd andmæli gegn drögum að ákvörðuninni innan fjögurra vikna frá því að samráð fer fram í samræmi við 3. mgr. þessarar greinar skal forystueftirlitsyfirvaldið vísa málinu til samræmingarkerfisins sem um getur í 63. gr. sé það ekki fylgjandi þessum viðeigandi og rökstuddu andmælum eða telji það að andmælin séu ekki viðeigandi eða rökstudd.
5. Ef forystueftirlitsyfirvaldið hyggst fylgja þeim viðeigandi og rökstuddu andmælum sem lögð voru fram skal það senda hinum eftirlitsyfirvöldunum sem í hlut eiga endurskoðuð drög að ákvörðun til að fá álit þeirra. Taka skal endurskoðuð drög að ákvörðuninni til umfjöllunar samkvæmt málsmeðferðinni, sem um getur í 4. mgr., innan tveggja vikna.
6. Ef ekkert hinna eftirlitsyfirvaldanna sem í hlut eiga hefur andmælt drögum að ákvörðuninni, sem forystueftirlitsyfirvaldið lagði fyrir þau, innan frestsins sem um getur í 4. og 5. mgr., skal líta svo á að forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld séu sammála um umrædd drög að ákvörðun og skulu þau bundin af þeim.
7. Forystueftirlitsyfirvaldið skal samþykkja ákvörðunina og tilkynna hana höfuðstöðvum eða einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans, eftir atvikum, og veita hinum eftirlitsyfirvöldunum sem í hlut eiga og persónuverndarráðinu upplýsingar um viðkomandi ákvörðun, þ.m.t. samantekt um þær staðreyndir og ástæður sem máli skipta. Eftirlitsyfirvaldið, sem kvörtun hefur verið lögð fram hjá, skal tilkynna kvartandanum um ákvörðunina.
8. Ef kvörtun er vísað frá eða henni hafnað skal eftirlitsyfirvaldið, sem kvörtun hefur verið lögð fram hjá, samþykkja ákvörðunina, þrátt fyrir 7. mgr., og tilkynna það kvartandanum og upplýsa ábyrgðaraðilann um það.
9. Ef forystueftirlitsyfirvaldið og hlutaðeigandi eftirlitsyfirvöld eru sammála um að vísa frá eða hafna hluta af kvörtun og fjalla um aðra hluta hennar skal samþykkja sérstaka ákvörðun fyrir hvern þessara hluta kvörtunarefnisins. Forystueftirlitsyfirvaldið skal samþykkja ákvörðunina um þann hluta sem varðar aðgerðir í tengslum við ábyrgðaraðilann, tilkynna það höfuðstöðvum eða hinni einu starfsstöð ábyrgðaraðilans eða vinnsluaðilans á yfirráðasvæði aðildarríkis síns og upplýsa kvartandann um það, en eftirlitsyfirvald kvartandans skal samþykkja ákvörðunina um þann hluta sem varðar frávísun eða höfnun umræddrar kvörtunar og tilkynna þá ákvörðun kvartandanum og upplýsa ábyrgðaraðilann eða vinnsluaðilann þar um.
10. Ábyrgðaraðili eða vinnsluaðili skal, eftir að þeim hefur borist tilkynning um ákvörðunina skv. 7. og 9. mgr., gera nauðsynlegar ráðstafanir til að tryggja að ákvörðuninni verði fylgt að því er varðar vinnsluaðgerðir sem tengjast öllum starfsstöðvum hans í Sambandinu. Ábyrgðaraðilinn eða vinnsluaðilinn skal tilkynna forystueftirlitsyfirvaldinu um þær ráðstafanir sem hafa verið gerðar til að framfylgja ákvörðuninni og skal það upplýsa önnur hlutaðeigandi eftirlitsyfirvöld um það.
11. Ef hlutaðeigandi eftirlitsyfirvald hefur ástæðu til að ætla, í undantekningartilvikum, að brýn nauðsyn sé á að grípa til aðgerða til að vernda hagsmuni skráðra einstaklinga gildir flýtimeðferðin sem um getur í 66. gr.
12. Forystueftirlitsyfirvaldið og önnur hlutaðeigandi eftirlitsyfirvöld skulu senda hvert öðru upplýsingarnar, sem krafist er samkvæmt þessari grein, með rafrænum hætti og nota til þess staðlað snið.

61. gr.

Gagnkvæm aðstoð

1. Eftirlitsyfirvöld skulu veita hvert öðru viðeigandi upplýsingar og gagnkvæma aðstoð til þess að framkvæma og beita þessari reglugerð með samræmdum hætti og skulu gera ráðstafanir til að starfa saman á árangursríkan hátt. Gagnkvæm aðstoð skal einkum ná yfir óskir um upplýsingar og eftirlitsráðstafanir, s.s. beiðnir um fyrirframleyfisveitingar og samráð, skoðanir og rannsóknir.
2. Sérhvert eftirlitsyfirvald skal gera allar viðeigandi ráðstafanir sem nauðsynlegar eru til að bregðast við beiðni annars eftirlitsyfirvalds án ástæðulausrar tafar og eigi síðar en einum mánuði eftir að beiðnin berst. Slíkar ráðstafanir geta einkum falið í sér að senda viðeigandi upplýsingar um framkvæmd rannsókna.
3. Beiðni um aðstoð skal innihalda allar nauðsynlegar upplýsingar, þ.m.t. um tilgang og ástæður beiðninnar. Upplýsingar sem miðlað er má aðeins nota í þeim tilgangi sem lá að baki beiðninni.
4. Eftirlitsyfirvaldið, sem beiðninni er beint til, skal ekki neita að verða við beiðninni nema:
 - a) viðfangsefni beiðninnar eða þær ráðstafanir, sem óskað er eftir að yfirvaldið grípi til, falli ekki undir heimildir þess eða
 - b) það að verða við beiðninni myndi brjóta í bága við þessa reglugerð eða lög Sambandsins eða lög aðildarríkis sem eftirlitsyfirvaldið, sem beiðninni er beint til, heyrir undir.
5. Eftirlitsyfirvaldið, sem beiðninni er beint til, skal tilkynna eftirlitsyfirvaldinu, sem lagði fram beiðnina, um niðurstöðurnar eða, eftir því sem við á, framvindu þeirra ráðstafana sem gerðar voru til að bregðast við beiðninni. Eftirlitsyfirvaldið, sem beiðninni er beint til, skal gefa upp ástæður ef það neitar að verða við beiðni skv. 4. mgr.
6. Eftirlitsyfirvöld, sem beiðninni er beint til, skulu að jafnaði veita upplýsingar sem önnur eftirlitsyfirvöld biðja um með rafrænum hætti og nota til þess staðlað snið.
7. Eftirlitsyfirvöld, sem beiðninni er beint til, skulu ekki krefjast gjalds fyrir aðgerðir sem þau grípa til samkvæmt beiðni um gagnkvæma aðstoð. Eftirlitsyfirvöld geta komið sér saman um reglur til að bæta hvert öðru skaða vegna sérstakra útgjalda sem hljóta af því þegar gagnkvæm aðstoð er veitt í undantekningartilvikum.
8. Ef eftirlitsyfirvald veitir ekki upplýsingarnar, sem um getur í 5. mgr. þessarar greinar, innan eins mánaðar frá því að beiðni berst frá öðru eftirlitsyfirvaldi getur eftirlitsyfirvaldið, sem leggur fram beiðnina, samþykkt bráðabirgðaráðstöfun á yfirráðasvæði eigin aðildarríkis í samræmi við 1. mgr. 55. gr. Í því tilviki skal líta svo á að brýnni þörf á að grípa til aðgerða skv. 1. mgr. 66. gr. hafi verið fullnægt og að hún krefjist skjótrar bindandi ákvörðunar persónuverndarráðsins skv. 2. mgr. 66. gr.
9. Framkvæmdastjórnin getur, með framkvæmdargerðum, ákvarðað snið og tilhögun gagnkvæmrar aðstoðar, sem um getur í þessari grein, og fyrirkomulag við upplýsingaskipti með rafrænum hætti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins, einkum staðlaða sniðið sem um getur í 6. mgr. þessarar greinar. Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

62. gr.

Sameiginlegar aðgerðir eftirlitsyfirvalda

1. Eftirlitsyfirvöldin skulu, eftir því sem við á, grípa til sameiginlegra aðgerða, þ.m.t. sameiginlegra rannsókna og sameiginlegra framfylgdarráðstafana, sem fulltrúar eða starfsmenn eftirlitsyfirvalda annarra aðildarríkja taka þátt í.
2. Ef ábyrgðaraðilinn eða vinnsluaðilinn hefur starfsstöðvar í fleiri en einu aðildarríki eða ef búast má við að vinnsluaðgerðir hafi umtalsverð áhrif á verulegan fjölda skráðra einstaklinga í fleiri en einu aðildarríki

hefur eftirlitsyfirvald hvers þessara aðildarríkja rétt til að taka þátt í sameiginlegum aðgerðum.

Eftirlitsyfirvaldið, sem er lögbært skv. 1. eða 4. mgr. 56. gr., skal bjóða eftirlitsyfirvaldi frá sérhverju þessara aðildarríkja að taka þátt í sameiginlegum aðgerðum og skal án tafar bregðast við beiðni eftirlitsyfirvalds um þátttöku.

3. Eftirlitsyfirvald getur, í samræmi við lög aðildarríkis og að fenginni heimild sendieftirlitsyfirvaldsins, veitt fulltrúum eða starfsfólki sendieftirlitsyfirvaldsins, sem tekur þátt í sameiginlegum aðgerðum, valdheimildir, þ.m.t. rannsóknarheimildir, eða, að svo miklu leyti sem heimilt er samkvæmt lögum aðildarríkis gistieftirlitsyfirvaldsins, leyft fulltrúum eða starfsfólki sendieftirlitsyfirvaldsins að beita rannsóknarheimildum sínum í samræmi við lög aðildarríkis sendieftirlitsyfirvaldsins. Aðeins er heimilt að beita slíkum rannsóknarheimildum undir leiðsögn fulltrúa eða starfsfólks gistieftirlitsyfirvaldsins og í þeirra viðurvist. Fulltrúar eða starfsfólk sendieftirlitsyfirvaldsins skal falla undir lög aðildarríkis gistieftirlitsyfirvaldsins.

4. Þegar starfsmenn sendieftirlitsyfirvalds eru að störfum í öðru aðildarríki, í samræmi við 1. mgr., skal aðildarríki gistieftirlitsyfirvaldsins bera ábyrgð á störfum þeirra, þ.m.t. bótaábyrgð, vegna hvers þess tjóns sem þeir valda með aðgerðum sínum í samræmi við löggjöf þess aðildarríkis þar sem þeir eru að störfum.

5. Aðildarríkið þar sem tjónið varð skal bæta tjónið með sömu skilyrðum og eiga við um tjón sem þess eigin starfsmenn valda. Ef starfsmenn sendieftirlitsyfirvaldsins hafa valdið aðila tjóni á yfirráðasvæði annars aðildarríkis skal aðildarríki sendieftirlitsyfirvaldsins endurgreiða hinu aðildarríkinu að fullu þær fjárhæðir sem það hefur greitt þeim sem eiga rétt á bótum fyrir þeirra hönd.

6. Með fyrirvara um réttindi gagnvart þriðju aðilum og að undanskilinni 5. mgr. skal hvert aðildarríki, í því tilviki sem kveðið er á um í 1. mgr., forðast að krefja annað aðildarríki um endurgreiðslu skaðabóta vegna tjóns sem um getur í 4. mgr.

7. Ef sameiginleg aðgerð er fyrirhuguð og eftirlitsyfirvald fullnægir ekki skuldbindingunni, sem mælt er fyrir um í öðrum málslíð 2. mgr. þessarar greinar, innan eins mánaðar er hinum eftirlitsyfirvöldunum heimilt að samþykkja bráðabirgðaráðstöfun sem gildir á yfirráðasvæði þess í samræmi við 55. gr. Í því tilviki skal líta svo á að brýnni þörf á að grípa til aðgerða skv. 1. mgr. 66. gr. hafi verið fullnægt og krefjast álits eða skjótrar bindandi ákvörðunar persónuverndarráðsins skv. 2. mgr. 66. gr.

2. þáttur

Samræmi

63. gr.

Samræmingarkerfi

Til að stuðla að samræmdri beitingu þessarar reglugerðar í öllu Sambandinu skulu eftirlitsyfirvöldin eiga samstarf sín í milli og, ef við á, við framkvæmdastjórnina með hjálp samræmingarkerfisins, eins og fram kemur í þessum þætti.

64. gr.

Álit persónuverndarráðsins

1. Persónuverndarráðið skal gefa út álit ef lögbært eftirlitsyfirvald hyggst samþykkja einhverja af neðangreindum ráðstöfunum. Lögbæra eftirlitsyfirvaldið skal í því skyni senda persónuverndarráðinu drög að ákvörðuninni ef hún:

- a) miðar að samþykkt skrár yfir vinnsluáðgerðir sem falla undir kröfu um mat á áhrifum á persónuvernd skv. 4. mgr. 35. gr.,
- b) varðar málefni skv. 7. mgr. 40. gr. um það hvort drög að háttænisreglum, eða breytingar eða útvíkkun háttænisreglna, samrýmast þessari reglugerð,
- c) miðar að samþykkt viðmiðana um faggildingu aðila skv. 3. mgr. 41. gr. eða vottunaraðila skv. 3. mgr. 43.

gr.,

d) miðar að ákvörðun staðlaðra ákvæða um persónuvernd sem um getur í d-lið 2. mgr. 46. gr. og 8. mgr. 28. gr.,

e) miðar að því að heimila samningsákvæði sem um getur í a-lið 3. mgr. 46. gr. eða

f) miðar að samþykkt bindandi fyrirtækjareglna í skilningi 47. gr.

2. Eftirlitsfirvald, formaður persónuverndarráðsins eða framkvæmdastjórnin getur óskað eftir því að persónuverndarráðið rannsaki málefni, sem hafa almenna skírskotun eða afleiðingar í fleiri en einu aðildarríki, með það fyrir augum að fá álit þess, einkum ef lögbært eftirlitsfirvald fer ekki að skyldum um gagnkvæma aðstoð í samræmi við 61. gr. eða sameiginlegar aðgerðir í samræmi við 62. gr.

3. Í þeim tilvikum, sem um getur í 1. og 2. mgr., skal persónuverndarráðið gefa út álit sitt varðandi það mál sem var vísað til þess að því tilskildu að það hafi ekki þegar gefið út álit um sama efni. Fulltrúar í persónuverndarráðinu skulu samþykkja álitid með einföldum meirihluta innan átta vikna. Lengja má frestinn um sex vikur til viðbótar með hliðsjón af því hversu flókið málið er. Að því er varðar drög að ákvörðuninni, sem um getur í 1. mgr., sem er dreift til fulltrúa í persónuverndarráðinu í samræmi við 5. mgr. skal líta svo á að fulltrúi sé samþykkur drögnum ef hann hefur ekki hreyft andmælum innan hæfilegs frests sem formaður tilgreinir.

4. Eftirlitsfirvöld og framkvæmdastjórnin skulu, án ástæðulausrar tafar, senda persónuverndarráðinu hvers kyns viðeigandi upplýsingar með rafrænum hætti og á stöðluðu sniði, m.a., eftir atvikum, samantekt um staðreyndir málsins, drög að ákvörðuninni, ástæður þess að nauðsynlegt er talið að kveða á um slíka ráðstöfun og sjónarmið annarra hlutaðeigandi eftirlitsfirvalda.

5. Formaður persónuverndarráðsins skal tilkynna með rafrænum hætti, án ástæðulausrar tafar:

a) fulltrúum í persónuverndarráðinu og framkvæmdastjórninni um allar viðeigandi upplýsingar sem því hafa verið sendar á stöðluðu sniði. Skrifstofa persónuverndarráðsins skal, ef nauðsyn krefur, láta þýða viðeigandi upplýsingar og

b) eftirlitsfirvaldinu, sem um getur í 1. og 2. mgr., eftir því sem við á, og framkvæmdastjórninni um álitid og birta það.

6. Lögbæra eftirlitsfirvaldið skal ekki samþykkja drög sín að ákvörðuninni sem um getur í 1. mgr. innan þeirra tímamarka sem um getur í 3. mgr.

7. Eftirlitsfirvaldið, sem um getur í 1. mgr., skal taka ýtrasta tillit til álits persónuverndarráðsins og skal, innan tveggja vikna frá því að álitid berst, senda formanni persónuverndarráðsins tilkynningu með rafrænum hætti um hvort það muni standa við drögin að ákvörðuninni eða gera breytingar á þeim og, ef svo er, hin breyttu drög að ákvörðuninni á stöðluðu sniði.

8. Ef hlutaðeigandi eftirlitsfirvald upplýsir formann persónuverndarráðsins innan frestsins, sem um getur í 7. mgr. þessarar greinar, um að það hyggist ekki fara að álitu persónuverndarráðsins, í heild eða að hluta, og færir rök fyrir því, gildir 1. mgr. 65. gr.

65. gr.

Lausn deilumála með hjálp persónuverndarráðsins

1. Til þess að tryggja rétta og samræmda beitingu þessarar reglugerðar í hverju einstöku tilviki skal persónuverndarráðið samþykkja bindandi ákvörðun í eftirfarandi tilvikum:

a) ef hlutaðeigandi eftirlitsfirvald hefur, í því tilviki sem um getur í 4. mgr. 60. gr., haft uppi viðeigandi og rökstudd andmæli gegn drögum að ákvörðun forstuyfirvaldsins eða forstuyfirvaldið hefur hafnað slíkum andmælum þar sem þau séu ekki viðeigandi eða rökstudd. Þessi bindandi ákvörðun skal ná yfir öll málefni sem fjallað er um í þessum viðeigandi og rökstuddu andmælum, einkum hvort um er að ræða brot gegn

þessari reglugerð,

b) ef ágreiningur er uppi um hvert af hlutaðeigandi eftirlitsyfirvöldum telst vera lögbært að því er varðar höfuðstöðvarnar,

c) ef lögbært eftirlitsyfirvald óskar ekki eftir áliti persónuverndarráðsins í tilvikum sem um getur í 1. mgr. 64. gr. eða fylgir ekki áliti sem persónuverndarráðið hefur gefið út skv. 64. gr. Í því tilviki getur hlutaðeigandi eftirlitsyfirvald eða framkvæmdastjórnin vísað málinu til persónuverndarráðsins.

2. Persónuverndarráðið skal samþykkja ákvörðunina, sem um getur í 1. mgr., með tveimur þriðju hlutum atkvæða fulltrúa í ráðinu innan eins mánaðar frá því að málið var lagt fyrir það. Lengja má frestinn um einn mánuð til viðbótar með hliðsjón af því hversu flókið málið er. Ákvörðunin, sem um getur í 1. mgr., skal vera rökstudd og henni skal beint til forystueftirlitsyfirvaldsins og allra hlutaðeigandi eftirlitsyfirvalda og vera bindandi fyrir þau.

3. Ef persónuverndarráðið hefur ekki getað tekið ákvörðun innan þeirra tímamarka, sem um getur í 2. mgr., skal það samþykkja ákvörðunina, innan tveggja vikna frá lokum annars mánaðarins sem um getur í 2. mgr., með einföldum meirihluta atkvæða fulltrúa í ráðinu. Ef atkvæði fulltrúa í persónuverndarráðinu falla að jöfnu skal ákvörðunin samþykkt með atkvæði formannsins.

4. Hlutaðeigandi eftirlitsyfirvöld skulu ekki samþykkja ákvörðun um það mál sem vísað er til persónuverndarráðsins skv. 1. mgr. á þeim tímabilum sem um getur í 2. og 3. mgr.

5. Formaður persónuverndarráðsins skal tilkynna, án ótilhlýðilegrar tafar, hlutaðeigandi eftirlitsyfirvöldum um ákvörðunina sem um getur í 1. mgr. Hann skal tilkynna framkvæmdastjórninni um það. Birta skal ákvörðunina á vefsetri persónuverndarráðsins án tafar eftir að eftirlitsyfirvaldið hefur tilkynnt um endanlega ákvörðun sem um getur í 6. mgr.

6. Forystueftirlitsyfirvaldið eða, eftir atvikum, eftirlitsyfirvaldið sem kvörtunin var lögð fram hjá skal samþykkja endanlega ákvörðun sína á grundvelli ákvörðunarinnar, sem um getur í 1. mgr. þessarar greinar, án ótilhlýðilegrar tafar og eigi síðar en einum mánuði eftir að persónuverndarráðið tilkynnir um ákvörðun sína. Forystueftirlitsyfirvaldið eða, eftir atvikum, eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, skal upplýsa persónuverndarráðið um hvaða dag endanleg ákvörðun þess er tilkynnt annars vegar ábyrgðaraðilanum eða vinnsluaðilanum og hins vegar skráða einstaklingnum. Endanleg ákvörðun hlutaðeigandi eftirlitsyfirvalda skal samþykkt samkvæmt skilmálunum í 7., 8. og 9. mgr. 60. gr. Í endanlegri ákvörðun skal vísa í ákvörðunina, sem um getur í 1. mgr. þessarar greinar, og tilgreina að ákvörðunin, sem um getur í þeirri málsgrein, verði birt á vefsetri persónuverndarráðsins í samræmi við 5. mgr. þessarar greinar. Ákvörðunin, sem um getur í 1. mgr. þessarar greinar, skal fylgja endanlegu ákvörðuninni.

66. gr.

Flýtimeðferð

1. Í undantekningartilvikum er hlutaðeigandi eftirlitsyfirvaldi heimilt, þegar það telur brýna nauðsyn á að grípa til aðgerða til verndar réttindum og frelsi skráðra einstaklinga, með undanþágu frá samræmingarkerfinu sem um getur í 63., 64. og 65. gr. eða málsmæðferðinni sem um getur í 60. gr., að samþykkja tafarlaust bráðabirgðaráðstafanir sem er ætlað að hafa réttaráhrif á yfirráðasvæði þess og hafa tiltekinn gildistíma sem skal ekki vera lengri en þrír mánuðir. Eftirlitsyfirvaldið skal án tafar tilkynna öðrum hlutaðeigandi eftirlitsyfirvöldum, persónuverndarráðinu og framkvæmdastjórninni um þessar ráðstafanir og ástæðurnar fyrir samþykkt þeirra.

2. Ef eftirlitsyfirvald hefur gert ráðstöfun skv. 1. mgr. og telur brýnt að samþykkja endanlegar ráðstafanir getur það óskað eftir flýtiáliti eða bindandi flýtiákvörðun persónuverndarráðsins og tilgreint ástæður fyrir beiðni um slíkt álit eða ákvörðun.

3. Sérhvert eftirlitsyfirvald getur óskað eftir flýtiáliti eða bindandi flýtiákvörðun persónuverndarráðsins, eftir því sem við á, ef lögbært eftirlitsyfirvald hefur ekki gert viðeigandi ráðstafanir við aðstæður sem kalla á

að brugðist verði við með skjótum hætti til að vernda réttindi og frelsi skráðra einstaklinga, og gefið upp ástæður fyrir beiðni um slíkt álit eða ákvörðun, m.a. hvers vegna brýnt er að grípa til aðgerða.

4. Þrátt fyrir 3. mgr. 64. gr. og 2. mgr. 65. gr. skal samþykkja flýtiálit eða bindandi flýtiákvörðun, sem um getur í 2. og 3. mgr. þessarar greinar, innan tveggja vikna með einföldum meirihluta atkvæða fulltrúa í persónuverndarráðinu.

67. gr.

Upplýsingaskipti

Framkvæmdastjórnin getur samþykkt almennar framkvæmdargerðir til þess að tilgreina nánar fyrirkomulag við upplýsingaskipti með rafrænum hætti milli eftirlitsyfirvalda og milli eftirlitsyfirvalda og persónuverndarráðsins, einkum staðlaða sniðið sem um getur í 64. gr.

Þessar framkvæmdargerðir skulu samþykktar í samræmi við rannsóknarmálsmeðferðina sem um getur í 2. mgr. 93. gr.

3. þáttur

Evrópska persónuverndarráðið

68. gr.

Evrópska persónuverndarráðið

1. Evrópska persónuverndarráðinu („persónuverndarráðið“) er hér með komið á fót sem stofnun á vegum Sambandsins og skal það hafa réttarstöðu lögaðila.
2. Formaður persónuverndarráðsins kemur fram fyrir hönd þess.
3. Í því skulu eiga sæti yfirmaður eins eftirlitsyfirvalds hvers aðildarríkis og Evrópsku persónuverndarstofnunarinnar eða fulltrúar þeirra hvers um sig.
4. Ef fleiri en eitt eftirlitsyfirvald í aðildarríki bera ábyrgð á að fylgjast með beitingu ákvæða samkvæmt þessari reglugerð skal skipa sameiginlegan fulltrúa í samræmi við löggjöf þess aðildarríkis.
5. Framkvæmdastjórnin hefur rétt til að taka þátt í starfsemi og fundum persónuverndarráðsins án atkvæðisréttar. Framkvæmdastjórnin skal tilnefna fulltrúa sinn. Formaður persónuverndarráðsins skal upplýsa framkvæmdastjórnina um störf sín.
6. Í þeim tilvikum, sem um getur í 65. gr., skal Evrópska persónuverndarstofnunin aðeins hafa atkvæðisrétt um ákvarðanir er varða meginreglur og reglur sem eiga við um stofnanir, aðila, skrifstofur og sérstofnanir Sambandsins sem svara efnislega til meginreglna og reglna þessarar reglugerðar.

69. gr.

Sjálfstæði

1. Persónuverndarráðið skal vera sjálfstætt í störfum sínum og þegar það beitir valdheimildum sínum skv. 70. og 71. gr.
2. Persónuverndarráðið skal í störfum sínum og þegar það beitir valdheimildum sínum hvorki leita eftir né taka við fyrirælum frá öðrum aðilum, með fyrirvara um beiðnir framkvæmdastjórnarinnar sem um getur í b-lið 1. mgr. 70. gr. og í 2. mgr. 70. gr.

70. gr.

Verkefni persónuverndarráðsins

1. Persónuverndarráðið skal tryggja samræmi í beitingu þessarar reglugerðar. Í því skyni skal persónuverndarráðið, annaðhvort að eigin frumkvæði eða, ef við á, að beiðni framkvæmdastjórnarinnar, einkum:
 - a) fylgjast með og tryggja rétta beitingu þessarar reglugerðar í tilvikum sem kveðið er á um í 64. og 65. gr., án þess að það hafi áhrif á verkefni landsbundinna eftirlitsyfirvalda,
 - b) veita framkvæmdastjórninni ráðgjöf um hvers kyns mál er tengjast vernd persónuupplýsinga í Sambandinu, m.a. varðandi tillögur að breytingum á þessari reglugerð,
 - c) veita framkvæmdastjórninni ráðgjöf um snið og aðferðir við upplýsingaskipti milli ábyrgðaraðila, vinnsluaðila og eftirlitsyfirvalda að því er varðar bindandi fyrirtækjareglur,
 - d) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í tengslum við verklag við að afmá tengla, afrit eða eftirmyndir af persónuupplýsingum hjá fjarskiptaþjónustu sem er aðgengileg almenningi, eins og um getur í 2. mgr. 17. gr.,
 - e) kanna, að eigin frumkvæði, að beiðni fulltrúa sins eða framkvæmdastjórnarinnar, hvers kyns álitaefni sem varða beitingu þessarar reglugerðar og gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur til þess að hvetja til samræmdrar beitingar hennar,
 - f) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar til að tilgreina nánar viðmiðanir og skilyrði fyrir ákvörðunum sem byggðar eru á gerð persónusniðs skv. 2. mgr. 22. gr.,
 - g) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar staðfestingu á öryggisbroti við meðferð persónuupplýsinga og ákvörðun ótilhlýðilegrar tafar sem um getur í 1. og 2. mgr. 33. gr. og þær tilteknu aðstæður þegar ábyrgðaraðili eða vinnsluaðili verður að tilkynna um slíkt öryggisbrot við meðferð persónuupplýsinga,
 - h) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar aðstæður þegar líklegt er að öryggisbrot við meðferð persónuupplýsinga leiði af sér mikla áhættu fyrir réttindi og frelsi þeirra einstaklinga sem um getur í 1. mgr. 34. gr.,
 - i) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar að því er varðar nánari tilgreiningu á viðmiðunum og kröfum varðandi miðlun persónuupplýsinga á grundvelli bindandi fyrirtækjareglna sem ábyrgðaraðilar hlíta og bindandi fyrirtækjareglna sem vinnsluaðilar hlíta og frekari kröfum sem nauðsynlegar eru til að tryggja vernd persónuupplýsinga hlutaðeigandi skráðra einstaklinga sem um getur í 47. gr.,
 - j) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar í þeim tilgangi að tilgreina nánar viðmiðanir og skilyrði varðandi miðlun persónuupplýsinga skv. 1. mgr. 49. gr.,
 - k) semja viðmiðunarreglur fyrir eftirlitsyfirvöld um beitingu þeirra ráðstafana sem um getur í 1., 2. og 3. mgr. 58. gr. og álagningu stjórnisýslusekta skv. 83. gr.,
 - l) endurskoða beitingu viðmiðunarreglna, tilmæla og bestu starfsvenja, sem um getur í e- og f-lið, í reynd,
 - m) gefa út viðmiðunarreglur, tilmæli og bestu starfsvenjur í samræmi við e-lið þessarar málsgreinar til að koma á sameiginlegri málsméðferð að því er varðar tilkynningar einstaklinga um brot gegn ákvæðum þessarar reglugerðar skv. 2. mgr. 54. gr.,
 - n) hvetja til þess að samdar verði háttarnisreglur og að komið verði á vottunarfyrirkomulagi vegna persónuverndar og persónuverndarinnisgla og -merkja skv. 40. og 42. gr.,
 - o) annast faggildingu vottunaraðila og endurskoða hana reglubundið skv. 43. gr. og halda opinbera skrá yfir faggilta aðila skv. 6. mgr. 43. gr. og faggilta ábyrgðaraðila eða vinnsluaðila með staðfestu í þriðju löndum skv. 7. mgr. 42. gr.,
 - p) tilgreina kröfur, sem um getur í 3. mgr. 43. gr., að því er varðar faggildingu vottunaraðila skv. 42. gr.,

- q) láta framkvæmdastjórninni í té álitserð um vottunarkröfurnar sem um getur í 8. mgr. 43. gr.,
- r) láta framkvæmdastjórninni í té álitserð um tákmyndirnar sem um getur í 7. mgr. 12. gr.,
- s) láta framkvæmdastjórninni í té álitserð vegna mats á því hvort vernd sé fullnægjandi í þriðja landi eða hjá alþjóðastofnun, einnig vegna mats á því hvort þriðja land, yfirráðasvæði eða einn eða fleiri tilgreindir geirar innan umrædds þriðja lands eða alþjóðastofnun tryggi ekki lengur fullnægjandi vernd. Í því skyni skal framkvæmdastjórnin láta persónuverndarráðinu í té öll nauðsynleg gögn, þ.m.t. bréfaskipti við ríkisstjórn þriðja landsins að því er varðar umrætt þriðja land, yfirráðasvæði eða tilgreindan geira, eða við alþjóðastofnunina,
- t) leggja fram álit varðandi drög að ákvörðunum eftirlitsyfirvalda samkvæmt samræmingarkerfinu sem um getur í 1. mgr. 64. gr., málefni, sem lögð eru fram skv. 2. mgr. 64. gr. og gefa út bindandi ákvarðanir skv. 65. gr., m.a. í þeim tilvikum sem um getur í 66. gr.,
- u) stuðla að samvinnu og skilvirkum tvíhliða og marghliða skiptum á upplýsingum og bestu starfsvenjum milli eftirlitsyfirvaldanna,
- v) stuðla að sameiginlegum þjálfunaráætlunum og greiða fyrir starfsmannaskiptum milli eftirlitsyfirvalda og, ef við á, gagnvart eftirlitsyfirvöldum þriðju landa eða alþjóðastofnunum,
- w)stuðla að skiptum á þekkingu og gögnum um persónuverndarlöggjöf og starfsvenjur við eftirlitsyfirvöld á sviði persónuverndar um heim allan,
- x)gefa út álit um háttænisreglur sem eru samdar á vettvangi Sambandsins skv. 9. mgr. 40. gr. og
- y)halda rafræna skrá, sem er aðgengileg almenningi, yfir ákvarðanir sem eftirlitsyfirvöld og dómstólar taka um mál sem tekin eru til meðferðar í samræmingarkerfinu.

2. Þegar framkvæmdastjórnin óskar eftir ráðgjöf persónuverndarráðsins getur hún tilgreint frest með hliðsjón af því hversu brýnt málið er.

3. Persónuverndarráðið skal framsenda álit sitt, viðmiðunarreglur, tilmæli og bestu starfsvenjur til framkvæmdastjórnarinnar og til nefndarinnar sem um getur í 93. gr. og birta opinberlega.

4. Persónuverndarráðið skal, eftir því sem við á, hafa samráð við hagsmunaaðila og gefa þeim tækifæri til að leggja fram athugasemdir innan hæfilegs tíma. Persónuverndarráðið skal, með fyrirvara um 76. gr., gera niðurstöður samráðsferlisins aðgengilegar almenningi.

71. gr.

Skýrslur

1. Persónuverndarráðið skal semja ársskýrslu um vernd einstaklinga með tilliti til vinnslu í Sambandinu og, ef við á, þriðju löndum og hjá alþjóðastofnunum. Skýrslan skal birt opinberlega og send til Evrópuþingsins, ráðsins og framkvæmdastjórnarinnar.

2. Í skýrslunni skal m.a. koma fram endurskoðun á því hvernig viðmiðunarreglum, tilmælum og bestu starfsvenjum, sem um getur í 1-lið 1. mgr. 70. gr., er beitt í reynd sem og bindandi ákvörðunum sem um getur í 65. gr.

72. gr.

Málsmeðferð

1. Persónuverndarráðið skal taka ákvarðanir með einföldum meirihluta fulltrúa sinna nema kveðið sé á um annað í þessari reglugerð.

2. Persónuverndarráðið skal setja sér starfsreglur með tveimur þriðju hlutum atkvæða fulltrúa sinna og skipuleggja starfsfyrirkomulag sitt.

73. gr.

Formaður

1. Persónuverndarráðið skal kjósa formann og tvo varaformenn úr röðum fulltrúa sinna með einföldum meirihluta.
2. Skipunartími formanns og varaformanna er fimm ár og má endurnýja hann einu sinni.

74. gr.

Verkefni formanns

1. Formaðurinn skal sinna eftirfarandi verkefnum:
 - a)boða til funda í persónuverndarráðinu og undirbúa fundardagskrá,
 - b)tilkynna forystueftirlitsyfirvaldinu og hlutaðeigandi eftirlitsyfirvöldum um ákvarðanir sem persónuverndarráðið samþykkir skv. 65. gr.,
 - c) tryggja tímanlega framkvæmd verkefna persónuverndarráðsins, einkum að því er varðar samræmingarkerfið sem um getur í 63. gr.
2. Persónuverndarráðið skal mæla fyrir um skiptingu verkefna milli formanns og varaformanna í starfsreglum sínum.

75. gr.

Skrifstofa

1. Persónuverndarráðið skal hafa skrifstofu sem Evrópska persónuverndarstofnunin sér því fyrir.
2. Skrifstofan vinnur verkefni sín alfarið samkvæmt fyrirmælum formanns persónuverndarráðsins.
3. Starfsfólk Evrópsku persónuverndarstofnunarinnar, sem tekur þátt í framkvæmd verkefna sem persónuverndarráðinu eru falin með þessari reglugerð, skal fylgja öðrum boðleiðum en það starfsfólk sem tekur þátt í framkvæmd verkefna sem Evrópsku persónuverndarstofnuninni eru falin.
4. Persónuverndarráðið og Evrópska persónuverndarstofnunin skulu, eftir því sem við á, setja fram og birta viljayfirlýsingu til framkvæmdar þessari grein, þar sem skilmálar samstarfs þeirra eru ákvarðaðir og sem á við um starfsfólk Evrópsku persónuverndarstofnunarinnar sem tekur þátt í framkvæmd verkefna sem persónuverndarráðinu eru falin með þessari reglugerð.
5. Skrifstofan skal veita persónuverndarráðinu stuðning á sviði greiningar, stjórnunar og skipulags.
6. Skrifstofan ber einkum ábyrgð á:
 - a)daglegum rekstri persónuverndarráðsins,
 - b)samskiptum milli fulltrúa í persónuverndarráðinu, formanns þess og framkvæmdastjórnarinnar,
 - c) samskiptum við aðrar stofnanir og við almenning,
 - d) notkun rafrænna miðla fyrir innri og ytri samskipti,
 - e) þýðingum á viðeigandi upplýsingum,
 - f) undirbúningi fyrir fundi persónuverndarráðsins og eftirfylgni í kjölfar þeirra,

g) undirbúningi, gerð og birtingu álitsgerða, ákvarðana um lausn deilumála milli eftirlitsyfirvalda og annars texta sem persónuverndarráðið samþykkir.

76. gr.

Trúnaðarskyldur

1. Trúnaður skal ríkja um umfjallanir persónuverndarráðsins ef það telur slíkt nauðsynlegt, eins og kveðið er á um í starfsreglum þess.
2. Um aðgang að skjölum, sem send eru fulltrúum í persónuverndarráðinu, sérfræðingum og fulltrúum þriðju aðila, fer samkvæmt reglugerð Evrópuþingsins og ráðsins (EB) nr. 1049/2001⁽²¹⁾.

VIII. KAFLI

Úrræði, bótaábyrgð og viðurlög

77. gr.

Réttur til að leggja fram kvörtun hjá eftirlitsyfirvaldi

1. Sérhver skráður einstaklingur skal, án þess að það hafi áhrif á önnur stjórnsýslu- eða réttarræði, hafa rétt til að leggja fram kvörtun hjá eftirlitsyfirvaldi, einkum í því aðildarríki þar sem hann hefur fasta búsetu, vinnur eða þar sem meint brot átti sér stað ef hann telur að vinnsla persónuupplýsinga um hann brjóti í bága við þessa reglugerð.
2. Eftirlitsyfirvaldið, sem kvörtunin var lögð fram hjá, skal upplýsa kvartandann um framvindu og niðurstöður kvörtunarinnar, m.a. möguleikann á réttarræði skv. 78. gr.

78. gr.

Réttur til skilvirks úrræðis til að leita réttar síns gagnvart eftirlitsyfirvaldi

1. Hver einstaklingur eða lögaðili skal, án þess að það hafi áhrif á önnur stjórnsýsluúrræði eða úrræði utan dómstóla, hafa rétt til raunhæfs úrræðis vegna lagalega bindandi ákvörðunar eftirlitsyfirvalds sem hann varðar.
2. Hver skráður einstaklingur skal, án þess að það hafi áhrif á önnur stjórnsýsluúrræði eða úrræði utan dómstóla, hafa rétt til raunhæfs úrræðis til að leita réttar síns ef eftirlitsyfirvaldið, sem er lögbært skv. 55. og 56. gr., tekur kvörtun ekki til meðferðar eða upplýsir hinn skráða ekki innan þriggja mánaða um framvindu eða niðurstöður kvörtunarinnar sem lögð var fram skv. 77. gr.
3. Mál gegn eftirlitsyfirvaldi skal höfðað fyrir dómstólum í aðildarríkinu þar sem eftirlitsyfirvaldið hefur staðfestu.
4. Ef mál er höfðað gegn ákvörðun eftirlitsyfirvalds eftir að persónuverndarráðið hefur lagt fram álit sitt eða ákvörðun í samræmingarkerfinu skal eftirlitsyfirvaldið framsenda viðkomandi álit eða ákvörðun til dómstólsins.

⁽²¹⁾ Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1049/2001 frá 30. maí 2001 um almennan aðgang að skjölum Evrópuþingsins, ráðsins og framkvæmdastjórnarinnar (Stjóð. EB L 145, 31.5.2001, bls. 43).

79. gr.

Réttur til skilvirks úrræðis til að leita réttar síns gagnvart ábyrgðaraðila eða vinnsluaðila

1. Sérhver skráður einstaklingur skal, án þess að það hafi áhrif á önnur fyrirliggjandi stjórnsýsluúrræði eða úrræði utan dómstóla, m.a. réttinn til að leggja fram kvörtun hjá eftirlitsyfirvaldi skv. 77. gr., hafa rétt til skilvirks úrræðis til að leita réttar síns ef hann telur að brotið hafi verið gegn réttindum hans samkvæmt þessari reglugerð á grundvelli þess að vinnsla persónuupplýsinga um hann samrýmist ekki þessari reglugerð.
2. Höfða skal mál gegn ábyrgðaraðila eða vinnsluaðila fyrir dómstólum í aðildarríkinu þar sem ábyrgðaraðilinn eða vinnsluaðilinn hefur staðfestu. Að öðrum kosti er heimilt að höfða slíkt mál fyrir dómstólum aðildarríkisins þar sem skráði einstaklingurinn hefur fasta búsetu nema ábyrgðaraðilinn eða vinnsluaðilinn sé opinbert yfirvald aðildarríkis sem fer með opinbert vald.

80. gr.

Fyrirsvar skráðra einstaklinga

1. Skráður einstaklingur skal hafa rétt til að veita stofnun, samtökum eða félagi, sem ekki eru rekin í hagnaðarskyni og sem stofnuð eru í samræmi við lög aðildarríkis, hafa lögboðin markmið í þágu almannahagsmuna og eru virk á sviði verndar réttinda og frelsis skráðra einstaklinga að því er varðar vernd persónuupplýsinga um þá, umboð til að leggja fram kvörtun fyrir hans hönd, að neyta þeirra réttinda sem um getur í 77., 78. og 79. gr., fyrir hans hönd og að neyta réttarins til skaðabóta, sem um getur í 82. gr., fyrir hans hönd ef kveðið er á um það í lögum aðildarríkisins.
2. Aðildarríki er heimilt að mæla fyrir um að stofnun, samtök eða félag, sem um getur í 1. mgr. þessarar greinar, hafi rétt, óháð því hvort hinn skráði hefur veitt umboð til þess, til að leggja fram, í viðkomandi aðildarríki, kvörtun hjá því eftirlitsyfirvaldi sem er lögbært skv. 77. gr. og að neyta þeirra réttinda, sem um getur í 78. og 79. gr., hafi þau ástæðu til að ætla að réttindi skráðs einstaklings samkvæmt þessari reglugerð hafi verið brotin vegna vinnslunnar.

81. gr.

Frestun málsmeðferðar

1. Hafi lögbær dómstóll aðildarríkis fengið upplýsingar um dómsmál, sem varðar sama málefni vegna vinnslu af hálfu sama ábyrgðaraðila eða vinnsluaðila og er til meðferðar hjá dómstól í öðru aðildarríki, skal hann hafa samband við dómstólinn í því aðildarríki til að fá staðfest hvort um slíkt dómsmál er að ræða.
2. Ef mál um sama álitaefni vegna vinnslu sama ábyrgðaraðila eða vinnsluaðila er til meðferðar fyrir dómstóli í öðru aðildarríki getur hvaða þar til bær dómstóll sem er, annar en sá sem málið var fyrst höfðað fyrir, frestað málsmeðferð sinni.
3. Ef málið er til meðferðar á fyrsta dómstigi getur hvaða dómstóll sem er, annar en sá sem málið var fyrst höfðað fyrir, einnig vísað málinu frá samkvæmt kröfu eins málsaðilans ef sá dómstóll, sem mál er fyrst höfðað fyrir, hefur dómssvald um kröfurnar og lög, sem gilda við þann dómstól, heimila að skyldar kröfur séu sóttar sameiginlega.

82. gr.

Bótaréttur og bótaábyrgð

1. Hver sem hefur orðið fyrir eignatjóni eða óefnislegu tjóni vegna brots á ákvæðum þessarar reglugerðar skal eiga rétt á skaðabótum frá ábyrgðaraðila eða vinnsluaðila fyrir það tjón sem hann hefur orðið fyrir.

2. Ábyrgðaraðili, sem tekur þátt í vinnslu, skal bera ábyrgð á því tjóni sem hlýst af vinnslu sem brýtur í bága við þessa reglugerð. Vinnsluaðili skal því aðeins bera ábyrgð á tjóni, sem hlýst af vinnslu, hafi hann ekki uppfyllt skyldur samkvæmt þessari reglugerð, sem beinast sérstaklega að vinnsluaðilum, eða ef hann hefur ekki fylgt lögmaðum fyrirmælum ábyrgðaraðilans eða farið gegn þeim.
3. Ábyrgðaraðili eða vinnsluaðili skal vera undanþeginn bótaábyrgð skv. 2. mgr. ef hann getur fært sönnur á að hann beri enga ábyrgð á atburðinum sem olli tjóninu.
4. Ef fleiri en einn ábyrgðaraðili eða vinnsluaðili, eða bæði ábyrgðaraðili og vinnsluaðili, koma að sömu vinnslu og ef þeir bera, skv. 2. og 3. mgr., ábyrgð á tjóni sem hlýst af vinnslu skal hver ábyrgðaraðili eða vinnsluaðili vera ábyrgur fyrir öllu tjóninu til að tryggja hinum skráða fullar skaðabætur.
5. Ef ábyrgðaraðili eða vinnsluaðili hefur greitt fullar skaðabætur vegna tjónsins, í samræmi við 4. mgr., skal hann eiga rétt á að krefjast þess að aðrir ábyrgðaraðilar eða vinnsluaðilar, sem komu að sömu vinnslu, endurgreiði þann hluta bótanna sem samsvarar hlutdeild þeirra í ábyrgð á tjóninu, í samræmi við skilyrðin sem sett eru fram í 2. mgr.
6. Dómsmál til að neyta réttarins til bóta skulu rekin fyrir dómstólum sem eru til þess bærir samkvæmt lögum aðildarríkisins sem um getur í 2. mgr. 72. gr.

83. gr.

Almenn skilyrði fyrir álagningu stjórnsýslusekta

1. Sérhvert eftirlitsyfirvald skal sjá til þess að álagning stjórnsýslusekta samkvæmt þessari grein vegna brota á reglugerð þessari, sem um getur í 4., 5. og 6. mgr., sé í hverju tilviki skilvirk, í réttu hlutfalli við brot og hafi varnaðaráhrif.
2. Leggja skal á stjórnsýslusektir, allt eftir aðstæðum í hverju tilviki, til viðbótar við eða í stað ráðstafana sem um getur í a- til h-lið og j-lið 2. mgr. 58. gr. Þegar ákveðið er hvort beita skuli stjórnsýslusekt og upphæð sektarinnar er ákveðin í hverju tilviki fyrir sig skal taka tilhlýðilegt tillit til eftirfarandi:
 - a) þess 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,
 - b) þess hvort brotið var framið af ásetningi eða af gáleysi,
 - c) aðgerða sem ábyrgðaraðilinn eða vinnsluaðilinn hefur gripið til í því skyni að draga úr tjóni skráðra einstaklinga,
 - d) þess 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.,
 - e) fyrri brota ábyrgðaraðila eða vinnsluaðila sem máli skipta, ef einhver eru,
 - f) umfangs samvinnu við eftirlitsyfirvaldið til þess að bæta úr brotinu og draga úr mögulegum, skaðlegum áhrifum þess,
 - g) þess hvaða flokka persónuupplýsinga brotið hafði áhrif á,
 - h) þess með hvaða hætti eftirlitsyfirvaldinu var gert kunnugt um brotið, einkum hvort, og þá að hvaða leyti, ábyrgðaraðili eða vinnsluaðili tilkynnti um brotið,
 - i) fylgni við ráðstafanir, sem um getur í 2. mgr. 58. gr., ef áður hefur verið mælt fyrir um slíkar ráðstafanir gegn hlutaðeigandi ábyrgðaraðila eða vinnsluaðila að því er varðar sama efni,
 - j) fylgni við viðurkenndar háttarnisreglur skv. 40. gr. eða viðurkennt vottunarfyrirkomulag skv. 42. gr. og
 - k) 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.

3. Ef ábyrgðaraðili eða vinnsluaðili brýtur, af ásetningi eða af gáleysi, gegn fleiri en einu ákvæði þessarar reglugerðar við sömu eða tengdar vinnsluadgerðir skal heildarfjárhæð stjórnsýslusektarinnar ekki vera hærri en fjárhæðin sem er tilgreind fyrir alvarlegasta brotið.

4. Brot gegn eftirfarandi ákvæðum skulu, í samræmi við 2. mgr., varða stjórnsýslusektum sem nema allt að 10 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 2% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra:

a)skyldum ábyrgðaraðila og vinnsluaðila skv. 8. gr., 11. gr., 25.–39. gr. og 42.–43. gr.,

b)skyldum vottunaraðila skv. 42. og 43. gr.,

c) skyldum eftirlitsaðila skv. 4. mgr. 41. gr.

5. Brot gegn eftirfarandi ákvæðum skulu, í samræmi við 2. mgr., varða stjórnsýslusektum sem nema allt að 20 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra:

a)grundvallarreglum um vinnslu, þ.m.t. skilyrðum fyrir samþykki, skv. 5., 6., 7. og 9. gr.,

b)réttindum skráðra einstaklinga skv. 12.–22. gr.,

c) miðlun persónuupplýsinga til viðtakanda í þriðja landi eða alþjóðastofnunar skv. 44.–49. gr.,

d) skyldum samkvæmt lögum aðildarríkis sem samþykkt eru skv. IX. kafla,

e) ekki er farið að fyrirmælum eða tímabundinni eða varanlegri takmörkun á vinnslu eða tímabundinni stöðvun gagnaflæðis af hálfu eftirlitsyfirvaldsins skv. 2. mgr. 58. gr. eða ekki er farið að skyldu til að veita aðgang skv. 1. mgr. 58. gr.

6. Ef ekki er farið að fyrirmælum eftirlitsyfirvaldsins, eins og um getur í 2. mgr. 58. gr., skal það varða, í samræmi við 2. mgr. þessarar greinar, stjórnsýslusektum sem nema allt að 20 000 000 evrum eða, ef um er að ræða fyrirtæki, allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra.

7. Með fyrirvara um valdheimildir eftirlitsyfirvalda til að gera ráðstafanir til úrbóta skv. 2. mgr. 58. gr. er hverju aðildarríki heimilt að mæla fyrir um reglur um það hvort og að hve miklu leyti heimilt er að leggja stjórnsýslusektir á opinber yfirvöld og stofnanir með staðfestu í aðildarríkinu.

8. Beiting eftirlitsyfirvaldsins á valdheimildum sínum samkvæmt þessari grein skal lúta viðeigandi réttarforsreglum í samræmi við lög Sambandsins og lög aðildarríkis, m.a. um skilvirka réttarvernd og sanngjarna málsmeðferð.

9. Ef ákvæði um stjórnsýslusektir er ekki að finna í réttarkerfi aðildarríkisins er heimilt að beita þessari grein þannig að lögbært eftirlitsyfirvald eigi frumkvæði að sektinni og þar til bærir landsdómstólar leggi hana á en jafnframt sé tryggt að þessi lagalegu úrræði séu skilvirk og hafi jafngild áhrif og stjórnsýslusektir sem eftirlitsyfirvöld leggja á. Álagðar sektir skulu þó ætíð vera skilvirkar, í réttu hlutfalli við brot og hafa varnaðaráhrif. Viðkomandi aðildarríki skulu tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði laga sem þau samþykkja samkvæmt þessari málsgrein og skulu án tafar tilkynna um síðari breytingalög eða breytingar sem hafa áhrif á þau.

84. gr.

Viðurlög

1. Aðildarríkin skulu ákvarða reglur um önnur viðurlög við brotum gegn þessari reglugerð, einkum brotum sem varða ekki stjórnsýslusektum skv. 83. gr., og skulu gera allar nauðsynlegar ráðstafanir til að sjá til þess að þeim sé komið til framkvæmda. Slík viðurlög skulu vera skilvirk, í réttu hlutfalli við brot og hafa varnaðaráhrif.

2. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt skv. 1. mgr. og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

IX. KAFLI

Ákvæði sem varða sérstakar vinnsluáðstæður

85. gr.

Vinnsla og tjáningar- og upplýsingafrelsi

1. Aðildarríki skulu samkvæmt lögum samræma réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð og réttinn til tjáningar- og upplýsingafrelsis, þ.m.t. vinnslu vegna fréttamennsku og starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar.
2. Að því er varðar vinnslu í þágu fréttamennsku eða starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar skulu aðildarríkin kveða á um undanþágur eða frávik frá II. kafla (meginreglur), III. kafla (réttindi skráðs einstaklings), IV. kafla (ábyrgðaraðili og vinnsluáðili), V. kafla (miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana), VI. kafla (sjálfstæð eftirlitsyfirvöld), VII. kafla (samstarf og samræming) og IX. kafla (gagnavinnsla við tiltekna aðstæður) ef það er nauðsynlegt til þess að samræma réttinn til verndar persónuupplýsingum og réttinn til tjáningar- og upplýsingafrelsis.
3. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni um ákvæði landslaga sem þau hafa samþykkt skv. 2. mgr. og skulu þau án tafar tilkynna um síðari breytingalög eða breytingar sem hafa áhrif á þau.

86. gr.

Vinnsla og aðgangur almennings að opinberum skjölum

Opinberu yfirvaldi, opinberri stofnun eða einkaaðila er heimilt að afhenda persónuupplýsingar úr opinberum skjölum, sem yfirvaldið, stofnunin eða aðilinn hefur í sinni vörslu vegna framkvæmdar verkefnis í þágu almannahagsmuna, í samræmi við lög Sambandsins eða lög aðildarríkis sem opinbera yfirvaldið eða stofnunin heyrir undir, til þess að samræma aðgang almennings að opinberum skjölum og réttinn til verndar persónuupplýsingum samkvæmt þessari reglugerð.

87. gr.

Vinnsla landsbundins auðkennisnúmers

Aðildarríkjum er heimilt að ákvarða frekar hvaða sértæku skilyrði gilda um vinnslu landsbundinna auðkennisnúmera eða annarra almennra auðkenna. Í því tilviki skal því aðeins nota landsbundið auðkennisnúmer eða annað almennt auðkenni að gerðar séu viðeigandi verndarráðstafanir varðandi réttindi og frelsi skráða einstaklingsins samkvæmt þessari reglugerð.

88. gr.

Vinnsla í atvinnutengdu samhengi

1. Aðildarríkjum er heimilt, með lögum eða kjarasamningum, að kveða á um sértækar reglur til að tryggja vernd réttinda og frelsis við vinnslu persónuupplýsinga starfsmanns í atvinnutengdu samhengi, einkum að því er varðar ráðningu, framkvæmd ráðningarsamnings, m.a. uppfyllingu skuldbindinga sem mælt er fyrir um í lögum eða kjarasamningum, stjórnun, undirbúning og skipulagningu vinnunnar, jafnrétti og fjölbreytileika á vinnustaðnum, heilbrigði og öryggi á vinnustað, vernd eigna vinnuveitanda eða viðskiptavinar og það að starfstengd réttindi og fríðindi séu nýtt og þeirra notið sameiginlega eða einstaklingsbundið, sem og í þeim tilgangi að ljúka ráðningarsambandi.

2. Þessar reglur skulu ná yfir viðeigandi og sértækar ráðstafanir til að vernda mannlega reisn skráða einstaklingsins, lögmæta hagsmuni hans og grundvallarréttindi, með sérstöku tilliti til gagnsæis vinnslunnar, miðlunar persónuupplýsinga innan fyrirtækjasamstæðu eða hóps fyrirtækja sem stunda sameiginlega atvinnustarfsemi og vöktunar kerfa á vinnustað.
3. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um ákvæði landslaga sem þau hafa samþykkt skv. 1. mgr. og skulu án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

89. gr.

Verndarráðstafanir og undanþágur sem varða vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfærðilegum tilgangi

1. Vinnsla vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfærðilegum tilgangi skal vera háð viðeigandi ráðstöfunum til verndar réttindum og frelsi skráða einstaklingsins í samræmi við þessa reglugerð. Þessar verndarráðstafanir skulu tryggja að tæknilegar og skipulagslegar ráðstafanir séu gerðar, einkum til þess að tryggja að farið sé að meginreglunni um lágmörkun gagna. Notkun gerviauðkenna getur verið á meðal þessara ráðstafana, að því tilskildu að ná megi þessum markmiðum með þeim hætti. Ef hægt er að ná umræddum markmiðum með frekari vinnslu sem leyfir ekki, eða leyfir ekki lengur, persónugreiningu skráðra einstaklinga skal þessum markmiðum náð með þeim hætti.
2. Þegar vinnsla persónuupplýsinga fer fram í þágu rannsókna á sviði vísinda eða sagnfræði eða í tölfærðilegum tilgangi geta lög Sambandsins eða lög aðildarríkis kveðið á um undanþágur frá þeim réttindum sem um getur í 15., 16., 18. og 21. gr., með fyrirvara um skilyrði og verndarráðstafanir sem um getur í 1. mgr. þessarar greinar, að svo miklu leyti sem telja má að slík réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum og slíkar undanþágur eru nauðsynlegar til að þeim verði náð.
3. Þegar vinnsla persónuupplýsinga fer fram vegna skjalavistunar í þágu almannahagsmuna geta lög Sambandsins eða lög aðildarríkis kveðið á um undanþágur frá þeim réttindum, sem um getur í 15., 16., 18., 19., 20. og 21. gr., með fyrirvara um skilyrði og verndarráðstafanir sem um getur í 1. mgr. þessarar greinar, að svo miklu leyti sem telja má að þessi réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum og slíkar undanþágur eru nauðsynlegar til að þeim verði náð.
4. Þegar vinnsla, sem um getur í 2. og 3. mgr., þjónar á sama tíma öðrum tilgangi skulu undanþágurnar aðeins gilda um vinnslu í þeim tilgangi sem um getur í þeim málsgreinum.

90. gr.

Þagnarskylda

1. Aðildarríkin geta samþykkt sértækar reglur til að fastsetja valdheimildir eftirlitsyfirvaldanna, sem mælt er fyrir um í e- og f-lið 1. mgr. 58. gr., með tilliti til ábyrgðaraðila eða vinnsluaðila, sem falla undir þagnarskyldu samkvæmt lögum Sambandsins eða lögum aðildarríkis eða reglum sem þar til bærir innlendir aðilar setja, eða aðrar jafngildar skuldbindingar um leynd þegar slíkt reynist nauðsynlegt og hóflegt til að samræma réttinn til verndar persónuupplýsingum og þagnarskyldu. Þessar reglur skulu aðeins gilda með hliðsjón af persónuupplýsingum sem ábyrgðaraðili eða vinnsluaðili hefur fengið í hendur í kjölfar eða við starfsemi sem fellur undir þessa þagnarskyldu.
2. Sérhvert aðildarríki skal tilkynna framkvæmdastjórninni eigi síðar en 25. maí 2018 um reglur sem þau hafa samþykkt skv. 1. mgr. og skulu þau án tafar tilkynna um síðari breytingar sem hafa áhrif á þau.

91. gr.

Reglur kirkjudeilda og trúarsamtaka um vernd persónuupplýsinga

1. Ef kirkjudeildir og trúarsamtök eða trúfélög í aðildarríki beita alhliða reglum, þegar þessi reglugerð öðlast gildi, er varða vernd einstaklinga í tengslum við vinnslu, geta slíkar reglur gilt áfram, að því tilskildu að þær séu færðar til samræmis við þessa reglugerð.
2. Kirkjudeildir og trúarsamtök, sem beita alhliða reglum í samræmi við 1. mgr. þessarar greinar, skulu sæta eftirliti sjálfstæðs eftirlitsyfirvalds, sem getur verið sértækt, að því tilskildu að það fullnægi skilyrðunum sem mælt er fyrir um í VI. kafla þessarar reglugerðar.

X. KAFLI

Framseldar gerðir og framkvæmdargerðir

92. gr.

Beiting framsals

1. Framkvæmdastjórninni er falið vald til að samþykkja framseldar gerðir, sbr. þó skilyrðin sem mælt er fyrir um í þessari grein.
2. Það framsal valds, sem um getur í 8. mgr. 12. gr. og 8. mgr. 43. gr., skal falið framkvæmdastjórninni um óákveðinn tíma frá 24. maí 2016.
3. Evrópuþinginu eða ráðinu er hvenær sem er heimilt að afturkalla framsal valds sem um getur í 8. mgr. 12. gr. og 8. mgr. 43. gr. Með ákvörðun um afturköllun skal bundinn endi á framsal þess valds sem tilgreint er í þeirri ákvörðun. Hún öðlast gildi daginn eftir birtingu hennar í *Stjórnartíðindum Evrópusambandsins*, eða síðar, eftir því sem tilgreint er í ákvörðuninni. Hún skal ekki hafa áhrif á gildi framseldra gerða sem þegar eru í gildi.
4. Um leið og framkvæmdastjórnin samþykkir framselda gerð skal hún jafnframt tilkynna það Evrópuþinginu og ráðinu.
5. Framseld gerð, sem er samþykkt skv. 8. mgr. 12. gr. og 8. mgr. 43. gr., skal því aðeins öðlast gildi að Evrópuþingið eða ráðið hafi ekki haft uppi nein andmæli innan þriggja mánaða frá tilkynningu um gerðina til Evrópuþingsins og ráðsins eða ef bæði Evrópuþingið og ráðið hafa upplýst framkvæmdastjórnina, áður en fresturinn er liðinn, um þá fyrirætlan sína að hreyfa ekki andmælum. Þessi frestur skal framlengdur um þrjá mánuði að frumkvæði Evrópuþingsins eða ráðsins.

93. gr.

Nefndarmeðferð

1. Framkvæmdastjórnin skal njóta aðstoðar nefndar. Þessi nefnd skal vera nefnd í skilningi reglugerðar (ESB) nr. 182/2011.
2. Þegar vísað er til þessarar málsgreinar gilda ákvæði 5. gr. reglugerðar (ESB) nr. 182/2011.
3. Þegar vísað er til þessarar málsgreinar gildir 8. gr. reglugerðar (ESB) nr. 182/2011 í tengslum við 5. gr. hennar.

XI. KAFLI

Lokaákvæði

94. gr.

Niðurfelling á tilskipun 95/46/EB

1. Tilskipun 95/46/EB er felld úr gildi frá og með 25. maí 2018.
2. Líta ber á tilvísanir í niðurfelldu tilskipunina sem tilvísanir í þessa reglugerð. Líta ber á tilvísanir í starfshópin um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga, sem komið var á fót með 29. gr. tilskipunar 95/46/EB, sem tilvísanir í Evrópska persónuverndarráðið sem komið er á fót með þessari reglugerð.

95. gr.

Tengsl við tilskipun 2002/58/EB

Í þessari reglugerð skal ekki leggja viðbótarskyldur á herðar einstaklingum eða lögaðilum í tengslum við veitingu rafrænnar fjarskiptaþjónustu, sem er öllum aðgengileg, á almennum fjarskiptanetum í Sambandinu að því er varðar málefni þar sem þeir falla undir sértækar skyldur með sama markmið og sett er fram í tilskipun 2002/58/EB.

96. gr.

Tengsl við áður gerða samninga

Alþjóðasamningar, sem taka til miðlunar persónuupplýsinga til þriðju landa eða alþjóðastofnana, sem aðildarríkin gerðu fyrir 24. maí 2016 og samrýmast lögum Sambandsins, sem giltu fyrir þennan dag, skulu gilda áfram uns þeim er breytt, þeir eru leystir af hólmi eða afturkallaðir.

97. gr.

Skýrslur framkvæmdastjórnarinnar

1. Framkvæmdastjórnin skal, eigi síðar en 25. maí 2020 og á fjögurra ára fresti eftir það, leggja skýrslu fyrir Evrópuþingið og ráðið um mat og endurskoðun þessarar reglugerðar. Skýrslurnar skulu gerðar opinberar.
2. Framkvæmdastjórnin skal, í tengslum við matið og endurskoðunina sem um getur í 1. mgr., einkum kanna beitingu og framkvæmd:
 - a)V. kafla um miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, með sérstöku tilliti til ákvarðana sem samþykktar eru skv. 3. mgr. 45. gr. þessarar reglugerðar og ákvarðana sem eru samþykktar á grundvelli 6. mgr. 25. gr. tilskipunar 95/46/EB,
 - b)VII. kafla um samstarf og samræmingu.
3. Að því er 1. mgr. varðar getur framkvæmdastjórnin óskað eftir upplýsingum frá aðildarríkjum og eftirlitsyfirlöðum.

4. Þegar framkvæmdastjórnin framkvæmir mat og endurskoðun, sem um getur í 1. og 2. mgr., skal hún taka tillit til afstöðu og niðurstaðna Evrópuþingsins, ráðsins og annarra viðeigandi aðila eða heimilda.
5. Framkvæmdastjórnin skal, ef nauðsyn krefur, leggja fram viðeigandi tillögur að breytingum á þessari reglugerð, einkum með tilliti til þróunar á sviði upplýsingatækni og í ljósi framfara í upplýsingasamfélaginu.

98. gr.

Endurskoðun annarra réttargerða Sambandsins á sviði persónuverndar

Framkvæmdastjórnin skal, ef við á, leggja fram tillögur að nýrri löggjöf með það fyrir augum að breyta öðrum réttargerðum Sambandsins um vernd persónuupplýsinga til að tryggja samræmda og samhæfða vernd einstaklinga með tilliti til vinnslu. Þetta á einkum við um reglur um vernd einstaklinga með tilliti til vinnslu stofnana, aðila, skrifstofa og sérstofnana Sambandsins og um frjálsa miðlun slíkra upplýsinga.

99. gr.

Gildistaka og beiting

1. Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.
2. Hún kemur til framkvæmda frá og með 25. maí 2018.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 27. apríl 2016.

Fyrir hönd Evrópuþingsins, Fyrir hönd ráðsins,

M. SCHULZ
forseti.

J.A. HENNIS-PLASSCHAERT
forseti.

Fylgiskjal II

Óformleg drög (16.03.2018)

Skjal nr. 17/00282-1

Mál nr. 17/00282

ÁKVÖRÐUN SAMEIGINLEGU EES-NEFNDARINNAR nr.

frá

um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 (sem inniheldur skrána sem kveðið er á um í 101. gr.) við EES-samninginn

SAMEIGINLEGA EES-NEFNDIN HEFUR,

með vísan til samningsins um Evrópska efnahagssvæðið (hér eftir „EES-samningurinn), einkum 98. gr., að teknu tilliti til eftirfarandi:

- 1) Fella ber inn í EES-samninginn 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 (almenna persónuverndarreglugerðin) ⁽²²⁾.
- 2) Gagnavernd fellur undir grundvallarréttindi sem varin eru í ýmsum alþjóðlegum mannréttindasamningum.
- 3) Mikilvægt er að réttindi og skyldur þeirra sem annast eftirlit með gagnavinnslu og gagnavinnslu á EES-svæðinu séu jafnar.
- 4) Ákvörðun þessi kveður á um að eftirlitsyfirvöld EFTA-ríkjanna skuli taka fullan þátt í fyrirkomulaginu sem varðar „afgreiðslu á einum stað“ og samræmingarkerfið og hafa sömu réttindi og skyldur og eftirlitsyfirvöld aðildarríkja ESB í Evrópska persónuverndarráðinu („persónuverndarráðið“) sem komið er á fót með reglugerð (ESB) 2016/679, án þess þó að eiga rétt á því að neyta atkvæðisréttar og bjóða sig fram í formanns- eða varaformannskjöri til persónuverndarráðsins. Því skulu eftirlitsyfirvöld EFTA-ríkjanna taka þátt í starfsemi persónuverndarráðsins, m.a. starfi hvers kyns undirhópa sem persónuverndarráðið kann að setja á laggirnar til þess að annast störf sín, og fá allar upplýsingar sem nauðsynlegar svo þátttaka sé skilvirk, þ.m.t., eftir því sem nauðsyn krefur, með fullum aðgangi að hvers kyns kerfum fyrir upplýsingaskipti sem persónuverndarráðið kann að setja upp.
- 5) Reglugerð (ESB) 2016/679 fellir úr gildi [, frá og með 25. maí 2018,] tilskipun Evrópuþingsins og ráðsins 95/46/EB ⁽²³⁾, sem hefur verið felld inn í EES-samninginn og ber því að fella gerðina brott úr samningnum [frá og með 25. maí 2018].
- 6) XI. viðauki og bókun 37 við EES-samninginn breytist því í samræmi við það.

TEKIÐ EFTIRFARANDI ÁKVÖRÐUN:

1. gr.

Eftirfarandi kemur í stað texta liðar 5e (tilskipun Evrópuþingsins og ráðsins 95/46/EB) í XI. viðauka við EES-samninginn [frá og með 25. maí 2018]:

„**32016 R 0679**: 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

⁽²²⁾ Stjtið. ESB L 119, 4.5. 2016, bls. 1.

⁽²³⁾ Stjtið. ESB L 281, 23.11. 1995, bls. 31.

niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) (Stjtið. ESB L 119, 4.5.2016, bls. 1).

Ákvæði reglugerðarinnar skulu, að því er samning þennan varðar, aðlöguð sem hér segir:

- a) Eftirlitsyfirvöld EFTA-ríkjanna skulu taka þátt í starfsemi Evrópska persónuverndarráðsins, hér á eftir nefnt „persónuverndarráðið“. Því skulu þau hafa sömu réttindi og skyldur og eftirlitsyfirvöld aðildarríkja ESB í persónuverndarráðinu, án þess þó að eiga rétt á því að neyta atkvæðisréttar og bjóða sig fram í formanns- eða varaformannskjöri til ráðsins, nema kveðið sé á um annað í samningi þessum. Persónuverndarráðið skal skrá afstöðu eftirlitsyfirvalda EFTA-ríkjanna sérstaklega.

Haga skal starfsreglum persónuverndarráðsins þannig að eftirlitsyfirvöld EFTA-ríkjanna og Eftirlitsstofnun EFTA geti tekið fullan þátt, að undanskildum rétti til þess að neyta atkvæðisréttar og bjóða sig fram í formanns- og varaformannskjöri persónuverndarráðsins.

- b) Þrátt fyrir ákvæði bókunar 1 við samning þennan, og nema kveðið sé á um annað í samningi þessum, ber að skilja hugtökin „aðildarríki(n)“ og „lögbær yfirvöld“ þannig að þau taki EFTA-ríkjanna og eftirlitsyfirvalda þeirra til viðbótar við merkingu þeirra í reglugerðinni, í þeirri röð.

- c) Skilja ber tilvísanir til laga Sambandsins og ákvæða Sambandsins um gagnavernd sem tilvísanir til EES-samningsins eða ákvæða um gagnavernd sem í honum eru, í þeirri röð.

- d) Að því er EFTA-ríkin varðar er orðunum „sem gildir skv. EES-samningnum“ bætt við á eftir orðunum „ákvörðun framkvæmdastjórnarinnar um það hvort vernd sé fullnægjandi“ bætt við á eftir f-lið 1. mgr. 13. gr. og f-lið 1. mgr. 14. gr.

- e) Að því er EFTA-ríkin varðar er eftirfarandi bætt við á eftir 1. mgr. í 45. gr.:

„1a. Þar til sameiginlega EES-nefndin hefur ákveðið að fella inn í EES-samninginn framkvæmdargerð sem samþykkt er í samræmi við 3. eða 5. gr. þessarar greinar getur EFTA-ríki ákveðið að beita ráðstöfunum sem þar er kveðið á um.

Hvert EFTA-ríki skal ákveða og upplýsa framkvæmdastjórnina og Eftirlitsstofnun EFTA, áður en allar framkvæmdargerðir sem samþykktar eru í samræmi við 3. mgr. og 5. mgr. þessarar greinar taka gildi, þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerðina inn í EES-samninginn, að beita ráðstöfununum sem þar er kveðið á um á sama tíma og aðildarríki ESB eða ekki. Ef ekki hefur verið tekin ákvörðun um hið gagnstæða skal hvert EFTA-ríki beita ráðstöfununum sem eru í framkvæmdargerð sem hefur verið samþykkt skv. 3. eða 5. mgr. þessarar greinar á sama tíma og aðildarríki ESB.

Þrátt fyrir ákvæði 102. gr. samningsins getur EFTA-ríki hætt beitingu slíkra ráðstafana ef samkomulag um að fella framkvæmdargerð sem samþykkt er í samræmi við 3. eða 5. mgr. þessarar greinar næst ekki í sameiginlegu EES-nefndinni innan tólf mánaða frá því framkvæmdargerðin öðlast gildi, og skal tilkynna það til framkvæmdastjórnarinnar og Eftirlitsstofnun EFTA án tafar.

Aðrir aðilar að EES-samningnum skulu þrátt fyrir 3. mgr. 1. gr. takmarka eða banna frjálst flæði persónuupplýsinga til EFTA-ríkis sem ekki beitir ráðstöfununum í framkvæmdargerð sem samþykkt hefur verið skv. 5. gr. þessarar greinar á sama hátt og þessar ráðstafanir koma í veg fyrir miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar.“

- f) Þegar ESB hefur viðræður við þriðju lönd eða alþjóðastofnanir í því skyni að samþykkja ákvörðun um fullnægjandi vernd í samræmi við 45. gr., skulu EFTA-ríkin upplýst um það með tilhlýðilegum hætti. Í þeim tilvikum þar sem þriðja landið eða alþjóðastofnunin tekst á hendur tiltekna skuldbindingar að því er varðar vinnslu gagna frá aðildarríkjunum, mun ESB taka tillit til aðstæðna EFTA-ríkjanna og ræða við þriðju lönd eða alþjóðastofnanir mögulegt fyrirkomulag hugsanlegrar beitingar í kjölfarið af hálfu EFTA-ríkjanna.

- g) Eftirfarandi verður bætt við d-lið 2. mgr. 46. gr.

„Eftirlitsyfirvöld EFTA-ríkjanna skulu hafa sama rétt og eftirlitsyfirvöld ESB til þess að senda stöðluð ákvæði um persónuvernd til framkvæmdastjórnarinnar til samþykkis í samræmi við rannsóknarmálsmeðferðina sem vísað er til í 2. mgr. 93. gr.“

- h) Að því er EFTA-ríkin varðar er eftirfarandi málsgrein bætt við á eftir 2. mgr. í 46. gr.:

„2a. Þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerð inn í EES-samninginn er unnt að mæla fyrir um viðeigandi verndarráðstafanir sem vísað er til í c- og d-liðum 2. mgr. 46. gr. með stöðluðum ákvæðum um persónuvernd þar sem EFTA-ríki beitir ráðstöfununum sem þar er kveðið á um.

Hvert EFTA-ríki skal ákveða og upplýsa framkvæmdastjórnina og Eftirlitsstofnun EFTA um, áður en allar framkvæmdargerðir sem samþykktar eru í samræmi við c- og d-lið 2. mgr. 46. gr. öðlast gildi, hvort það muni, þar til sameiginlega EES-nefndin hefur ákveðið að fella framkvæmdargerðina inn í EES-samninginn, beita ráðstöfununum sem þar er kveðið á um á sama tíma og aðildarríki ESB eða ekki. Ef ekki hefur verið tekin ákvörðun um hið gagnstæða skal hvert EFTA-ríki beita ráðstöfununum sem kveðið er á um í framkvæmdargerð sem hefur verið samþykkt skv. c- og d-lið 2. mgr. 46. gr. á sama tíma og aðildarríki ESB.

Þrátt fyrir ákvæði 102. gr. samningsins getur EFTA-ríki hætt beitingu slíkra ráðstafana ef samningur um að fella framkvæmdargerð sem samþykkt er í samræmi við c- og d-lið 2. mgr. 46. gr. næst ekki í sameiginlegu EES-nefndinni innan tólf mánaða frá því framkvæmdargerðin öðlast gildi, og skal tilkynna það til framkvæmdastjórnarinnar og Eftirlitsstofnunar EFTA án tafar.“

- i) Í 4. mgr. 58. gr. gilda orðin „í samræmi við sáttmálann um grundvallarréttindi“ ekki að því er EFTA-ríkin varðar.
- j) Í 59. gr. er orðunum „Eftirlitsstofnun EFTA“ bætt við á eftir orðinu „framkvæmdastjórninni“.
- k) Eftirlitsstofnun EFTA skal hafa rétt til þátttöku í fundum persónuverndarráðsins, þó án atkvæðisréttar. Eftirlitsstofnun EFTA skal tilnefna fulltrúa sinn.
- l) Þar sem það samrýmist framkvæmd Eftirlitsstofnunar EFTA á starfssviði sínu samkvæmt 109. gr. samnings þessa skal stofnunin hafa rétt á að óska eftir ráðgjöf eða álit persónuverndarráðsins og skiptast á upplýsingum við það í samræmi við 63. gr., 2. mgr. 64. gr., c-lið 1. mgr. 65. gr. og e-lið 1. mgr. 70. gr. Orðunum „Eftirlitsstofnun EFTA“ er bætt við á eftir orðinu „framkvæmdastjórn“ í 63. gr., 2. mgr. 64. gr., c-lið 1. mgr. 65. gr. og e-lið 1. mgr. 70. gr.
- m) Formaður persónuverndarráðsins eða skrifstofa skal tilkynna Eftirlitsstofnun EFTA um starfsemi persónuverndarráðs þar sem það á við í samræmi við a- og b-lið 5. mgr. 64. gr., 5. mgr. 65. gr. og b-lið 6. mgr. 75. gr. Orðunum „Eftirlitsstofnun EFTA“ er bætt við á eftir „framkvæmdastjórninni“ í a- og b-lið 5. mgr. 64. gr. og 5. mgr. 65. gr. og „Eftirlitsstofnunar EFTA“ á eftir orðinu „framkvæmdastjórnarinnar“ í b-lið 6. mgr. 75. gr.

Þar sem það samrýmist framkvæmd Eftirlitsstofnunar EFTA á starfssviði sínu samkvæmt 109. gr. samnings þessa skal stofnunin eiga rétt á að fá upplýsingar frá eftirlitsstofnun þess EFTA-ríkis sem um er að ræða skv. 1. mgr. 66. gr. Í 1. mgr. 66. gr. er orðunum „og, þar sem við á, Eftirlitsstofnun EFTA“ bætt við á eftir orðinu „framkvæmdastjórninni“.
- n) Í 1. mgr. 71. gr. er orðunum „fastanefnd EFTA-ríkjanna, Eftirlitsstofnun EFTA“ bætt við á eftir orðinu „ráðsins“.
- o) Í 1. mgr. 73. gr. er eftirfarandi setningu bætt við:
„Fulltrúar persónuverndarráðsins frá EFTA-ríkjunum eiga ekki rétt á að gegna formennsku eða varaformennsku.““

2. gr.

Texti 13. liðar bókunar 37 við EES-samninginn (Starfshópur um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga) fellur brott.

3. gr.

Íslenskur og norskur texti reglugerðar (ESB) 2016/679, sem verður birtur í EES-viðbæti við *Stjórnartíðindi Evrópusambandsins*, telst fullgiltur.

4. gr.

Ákvörðun þessi öðlast gildi [...], að því tilskildu að allar tilkynningar skv. 1. mgr. 103. gr. EES-samningsins hafi farið fram (*).

() Engin stjórnskipuleg skilyrði gefin til kynna. Stjórnskipuleg skilyrði gefin til kynna.

5. gr.

Ákvörðun þessi skal birt í EES-deild *Stjórnartíðinda Evrópusambandsins* og EES-viðbæti við þau.

Gjört í Brussel.

Sameiginleg yfirlýsing samningsaðila

vegna ákvörðunar nr. XX frá DD.MM.ÁÁ sem fellir 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 (almenna persónuverndarreglugerðin) inn í EES-samninginn.

Samningsaðilarnir, með tveggja stoða kerfi EES-samningsins í huga og með tilliti til beinna og bindandi áhrifa ákvarðana Evrópska persónuverndarráðsins fyrir innlend eftirlitsyfirvöld í EFTA-ríkjunum innan EES:

- taka mið af þeirri staðreynd að ákvörðunum Evrópska persónuverndarráðsins er beint að innlendum eftirlitsyfirvöldum,
- viðurkenna að þessi lausn hefur ekki fordæmisgildi fyrir aðlögun gerða ESB sem verða felldar inn í EES-samninginn í framtíðinni.

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. 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 gerða svo sem með umritun. Engu að síður er ráðgert í reglugerðinni að í allmörgum atritum 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 13. apríl 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 vegna þátttöku sinnar í Schengen-samstarfinu en það er ekki viðfangsefni frumvarps þessa. Þá er í undirbúningi að ný reglugerð ESB taki gildi 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 stjksl. 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 stjórnsmálaleg réttindi. Í greinargerð með stjksl. 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 álitaefti 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 löginn 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 löginn 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 lögnum 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 vísindarannsóknnum á heilbrigðissviði með lögum nr. 44/2014.

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

3.1. Almenn.

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 SP 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 Evrópusambandinu 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 viðtækari 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 þrífist. 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). Persónuverndarstofnanir 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 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 (löggæslutílskipunin).

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 mismikill 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 láréttar 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 fjarlægji, 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 innbyggða og sjálfvirka persónuvernd og að halda sérstakar vinnsluskrár. Þá verður dregið úr heimildum til vinnslu persónuupplýsinga í þágu sjálfvirkar 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 sem fjallað er um í 63.-67. gr. reglugerðarinnar. 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 ákvarðanir í hans málum um framkvæmd ákvæða reglugerðarinnar. Í 134. lið formála reglugerðarinnar er tekið fram að samræmingarkerfinu sé ætlað að koma á samræmdri framkvæmd reglugerðar í öllu Sambandinu. Bent er á að einkum ætti að beita kerfinu þegar persónuverndarstofnun í einu ríki hyggst gera ráðstöfun sem ætlað er að hafa réttaráhrif vegna vinnsluadgerða sem hafa veigamikil áhrif á verulegan fjölda skráðra einstaklinga í nokkrum aðildarríkjum. Því ætti einnig að beita þegar eitthvert hlutaðeigandi eftirlitsstjórnvald eða framkvæmdastjórnin fer fram á að samræmingarkerfið annist meðferð slíks máls. Reglugerðin stefnir þannig að stórauðni samáði og samvinnu á milli eftirlitsstjórnvalda. Komi þá upp ágreiningur þeirra í milli um framkvæmd ákvæða reglugerðarinnar mun ný stofnun, Evrópska persónuverndarráðið, skera úr honum.

Ætlunin er að framangreindar ráðstafanir og samræmingarkerfi 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.

Í reglugerðinni er einnig vísað til þarfa minni fyrirtækja. Í 13. lið formála hennar er m.a. bent á að með hliðsjón af sérstökum aðstæðum örfyrirtækja, lítilla og meðalstórra fyrirtækja sé sett fram undanþága í þessari reglugerð varðandi skráahald fyrirtækja með færri en 250 starfsmenn. Enn fremur eru aðildarríkin og eftirlitsyfirvöld þeirra hvött til að taka tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja við beitingu reglugerðarinnar.

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. Almenn

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.

Í lok aprílmánaðar 2018 var þingsályktunartillaga til að heimila ríkisstjórninni að staðfesta fyrir Íslands hönd fyrirhugaða ákvörðun sameiginlegu EES-nefndarinnar um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) og bókun 37 (sem inniheldur skrána sem kveðið er á um í 101. gr.) við EES-samninginn frá 2. maí 1992 um að fella inn í samninginn 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 (almenna persónuverndarreglugerðin). Þá lágu fyrir drög að ákvörðun sameiginlegu EES-nefndarinnar um upptöku á persónuverndarreglugerðinni í EES-samninginn. Eru drögin í umsagnarferli hjá stofnunum ESB sem ekki er lokið þegar frumvarp þetta er lagt fram.

Þær sérstöku aðstæður eru því uppi að þegar frumvarpið kemur til meðferðar hjá Alþingi hefur þingsályktunartillaga verið lögð fram sem gerir ráð fyrir því að Alþingi veiti ríkisstjórninni fyrirfram heimild til að staðfesta fyrirhugaða ákvörðun sameiginlegu EES-nefndarinnar um upptöku gerðarinnar í samninginn, þar sem formleg ákvörðun nefndarinnar liggur ekki fyrir. Á sama tíma er afar mikilvægt að frumvarpið verði að lögum og taki gildi sem næst því tímamarki sem reglugerðin kemur til framkvæmda í ESB-ríkjunum þann 25. maí 2018. Ella skapast ósamræmi í reglum EFTA-ríkjanna innan Evrópska efnahagssvæðisins við þær reglur sem gilda í ESB-ríkjunum um um persónuvernd. Það getur valdið vandkvæðum m.a. í tengslum við miðlun persónuupplýsinga á Evrópska efnahagssvæðinu.

Eins og fjallað er um í skýringum við gildistökuákvæði frumvarps þessa í 53. gr. fellur það innan valdheimilda löggjafans að meta hvort rétt er að samþykkja frumvarpið við þessar aðstæður í þeirri vissu að stuttur tíma líði þar til formleg ákvörðun sameiginlegu EES-nefndarinnar um upptöku gerðarinnar í EES-samninginn liggi fyrir. Þess má geta að Norðmenn

hafa farið sömu leið þar sem frumvarp til nýrra persónuverndarlaga var lagt fram á norska Stórþinginu í lok marsmánaðar.

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

Samkvæmt 68. gr. reglugerðarinnar er sem fyrr segir nýrri eftirlitsstofnun komið á fót, Evrópska persónuverndarráðinu. Í því skulu eiga sæti yfirmenn eins eftirlitsstjórnvalds 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 starfshóp samkvæmt 29. gr. ESB-tilskipunarinnar og tekur við þeim sem lýst var að framan, þ.e. útgáfu leiðbeininga og álita um túlkun ákvæða reglugerðarinnar. Til viðbótar fær ráðið fjölmörg önnur verkefni og valdheimildir, þar á meðal er því framselt vald til þess að taka bindandi ákvarðanir gagnvart innlendum eftirlitsstofnunum í ákveðnum tilvikum. Í þessu tilliti hafa vaknað ýmis álítaefni um aðlögun fyrir upptöku reglugerðarinnar í EES-samninginn en þessi verkefni ráðsins koma til vegna ákvæða 63.–67. gr. reglugerðarinnar um framkvæmd þess samræmingarkerfis sem lýst var að framan. Kerfinu er komið á fót til að stuðla að samræmdri beitingu reglugerðarinnar í öllu Sambandinu. Með upptöku gerðarinnar í EES-samninginn eykst mjög samvinna á milli eftirlitsstofnana á sviði persónuverndar innan Evrópska efnahagssvæðisins. Af Íslands hálfu reynir þá á aðkomu Persónuverndar, sem er lögbært eftirlitsstjórnvald hér á landi samkvæmt ákvæðum reglugerðarinnar.

Við upptöku gerðarinnar voru ýmsir kostir skoðaðir í tengslum við aðlögun að stofnanakerfi hennar og hvernig mætti samræma það EES-samningnum. Við mat á þeim valkostum var m.a. leitað ráðgjafar hjá Stefáni Má Stefánssyni prófessor við lagadeild Háskóla Íslands, sbr. álitsgerð hans um efnið frá 14. desember 2017, svo og hjá Ólafi Jóhanni Einarssyni lögmanni og fyrrverandi framkvæmdastjóra hjá Eftirlitsstofnun EFTA. Sem fyrr segir liggja nú fyrir drög að ákvörðun sameiginlegu EES-nefndarinnar um upptöku gerðarinnar í EES-samninginn dags. 16. mars 2018 og er beðið afstöðu stofnana ESB til þeirra. Eru drögin meðfylgjandi sem fylgiskjal við frumvarp þetta í íslenskri þýðingu.

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 stöða kerfi EES-samningsins. Úr varð að velja þá leið sem kennd er við „fulla aðkomu Evrópska persónuverndarráðsins“ og er henni lýst í drögum að ákvörðun sameiginlegu EES-nefndarinnar. Í því felst að ráðið mun taka bindandi ákvarðanir gagnvart persónuverndarstofnun EFTA-ríkis innan EES á sama hátt og gagnvart aðildarríki ESB. Fulltrúar persónuverndarstofnana EFTA-ríkjanna innan EES munu sitja í Evrópska persónuverndarráðinu, án atkvæðisréttar, en munu hafa fullan tillögurétt og málfrælsi og afstaða fulltrúa EFTA ríkjanna verður skráð sérstaklega. Um þetta fyrirkomulag hefur verið vísað til fyrri fordæma varðandi þátttöku fulltrúa EFTA-ríkjanna innan EES í stjórnnum sérstofnana ESB af svipuðu tagi. Þar má benda á þátttöku EFTA-ríkjanna í Evrópsku vinnuverndarstofnuninni og Evrópsku 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.

Auk þess munu persónuverndarstofnanir EFTA-ríkjanna taka þátt í annarri starfsemi persónuverndarráðsins, m.a. starfi hvers kyns undirhópa sem ráðið kann að setja á laggirnar til þess að annast störf sín, og fá allar nauðsynlegar upplýsingar svo þátttaka verði skilvirk, þ.m.t., eftir því sem nauðsyn krefur, með fullum aðgangi að hvers kyns kerfum fyrir upplýsingaskipti sem persónuverndarráðið kann að setja upp.

Í drögum að ákvörðun sameiginlegu EES-nefndarinnar kemur einnig fram að þegar ESB hefur viðræður við þriðju lönd eða alþjóðastofnanir í því skyni að samþykkja ákvörðun um fullnægjandi vernd í samræmi við 45. gr. reglugerðarinnar, skulu EFTA-ríkin upplýst um það með tilhlýðilegum hætti. Í þeim tilvikum þar sem þriðja landið eða alþjóðastofnunin tekst á hendur tiltekna skuldbindingar að því er varðar vinnslu gagna frá aðildarríkjunum, mun ESB taka tillit til aðstæðna EFTA-ríkjanna og ræða við þriðju lönd eða alþjóðastofnanir mögulegt fyrirkomulag framkvæmdar reglugerðar í kjölfarið af hálfu EFTA-ríkjanna.

Nánar verður fjallað um stjórnskipuleg álitæfni tengd framsali ríkisvalds til Evrópska persónuverndarráðsins og öðrum atriðum reglugerðarinnar 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 aldersmark 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 valdheimildir 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.)

* Almennit 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-, meðalhöfs-, áreiðanleika- og varðveisluregluna. (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 afli 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.)

* Lögd 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 vinnsluáðgerða 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 ríkjum verði eflar verulega, sjálfstæði tryggt og valdheimildir og eftirlitsúrræði stórukin (57. og 58. gr.)

* Mælt er fyrir um háar stjórnvaldssektir vegna brota á lögnum, 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 endurspeglar hitt meginmarkmiðið með setningu hennar, þ.e. að greiða fyrir frjálsum 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 eftirlitsákvæðanir 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 efnistöð.

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 nógildandi lög um efnistöð 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 efnistöð 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 umörða eða breyta texta þeirra í innlendum lagatexta. Af skoðun á fyrirbyggjandi 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 geyma sérreglur um frávík frá eða viðbætur við reglugerðina, en reglugerðin stendur þá sem meginréttarheimildin.

Það var mat starfshópsins við ákvörðun um efnistöð 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 sem heimilt er að gera, helstu hugtök og efni nokkurra kjarnaákvæða reglugerðarinnar. Í athugasemdum við hvert og eitt frumvarpsákvæði er þannig að finna

skýringar sem eiga við um meginákvæði reglugerðarinnar, t.d. hvort um nýmæli er að ræða, skýringar sem finna má í formálsorðum reglugerðarinnar og tilvísun til álita og leiðbeininga starfshóps samkvæmt 29. gr. ESB sem þegar hafa verið gefnar út um túlkun og beitingu ýmissa lykilákvæða og hugtaka í reglugerðinni. Leitast er við að fylgja orðalagi ákvæða reglugerðarinnar 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 birti meginákvæði og verði henni til fyllingar og viðbótar. Þá er mikilvægt að allar reglur um efnið og skýringar á meginefni þeirra 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 viðtæk áhrif fyrir samfélagið allt en ekki t.d. sérhæfð svið í atvinnulífinu einvörðungu. Þá er stoð fyrir þessari framsetningu einnig sótt í 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 er rétt að benda á að í frumvarpinu er að finna ýmsar sérreglur um tiltekin svið sem þegar eru 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 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“. Þá vakna álitamál um hugtakið „eftirlitsyfirvald“ sem kemur víða fyrir reglugerðinni sem 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 „eftirlitsstjórnvald“. 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.

Þá ræður úrslitum, skapist vafi um hvort samræmi er á milli texta laganna og reglugerðarinnar að í 5. gr. frumvarpsins er mælt fyrir um að texti reglugerðarinnar skuli ráða, eins og nánar er rakið í frumvarppskýringum um það ákvæði.

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, leyfissskylda 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.

8. Samræmi við stjórnarskrá

Í frumvarpi þessu felst framsal valdheimilda til handa Evrópska persónuverndarráðinu í tilteknum málum eins og fram kom í kafla 5.3 í frumvarpi þessu. Þarf því að leggja mat á hvort slíkt framsal samræmist fyrirmælum stjórnarskrárinnar um meðferð ríkisvalds, einkum um það hvort farið er út fyrir þau mörk sem leidd verða af 2. gr. stjórnarskrárinnar. Greinin mælir fyrir um þrískiptingu ríkisvaldsins í löggjafar-, framkvæmdar- og dómvald sem skuli vera í höndum þeirra sem taldir eru upp í ákvæðinu og jafnframt eru æðstu handhafar ríkisvalds hver á sínu sviði. Ljóst er að meginregla 2. gr. um að ríkisvald sé á hendi innlendra valdhafa hefur sætt ýmsum undantekningum á undanföllum áratugum samkvæmt almennum lögum eða byggjast á venju eða dómafordæmum. Hefur aðild Íslands að EES-samningnum árið 1993 og þá ekki síður gerðir sem verið teknar upp í samninginn á undanföllum áratugum þar sem valdheimildir hafa í auknum mæli verið framseldar til alþjóðastofnana í EES-samstarfinu vakið margvísleg álitafni um hvort farið er út fyrir mörk stjórnarskrárinnar, þar sem hvergi er getið um heimild til að framselja ríkisvald til alþjóðlegra stofnana. Um þessi efni var m.a. ítarlega fjallað í álitargerð prófessorana Bjargar Thorarensen og Stefáns Máss Stefánssonar frá 25 apríl 2012 um stjórnskipulegar heimildir landsréttar og möguleika á innleiðingu reglugerða ESB um eftirlit með fjármálamörkuðum í EES-samninginn sem þá voru í undirbúningi.

Í álitargerðinni kom fram að þeir þættir sem líta beri til við mat á svigrúmi löggjafans til framsals valdheimilda séu eftirfarandi; 1) hvaða valdheimildir ríkisins eru framseldar 2) að hverjum þær beinast 3) þátttöku Íslands í ákvarðanatöku og gagnkvæmni 4) umfangs og eðlis valdheimildanna og 5) samfélagslegra markmiða. Vega þurfi og meta þessa þætti saman til að finna heildarmynd, en enginn einn þeirra ráði úrslitum. Burtséð frá því hver er niðurstaða þess mats, er bent á það í álitargerðinni að í EES-samstarfinu vakni stöðugt fleiri álitafni um hvort farið sé út fyrir mörk stjórnarskrárinnar með þróun EES-samningsins og innleiðingu nýrra gerða sem stefna að auknu valdframsali til alþjóðastofnana á nýjum málefnasviðum. Þannig hafi forsendur breyst í ýmsu tilliti frá því að samningurinn tók gildi. Niðurstaða álitargerðarinnar er að sú heildarmynd sem mótast hefur frá því EES-samningurinn tók gildi gefi tilefni til að endurmeta þá stöðu sem er uppi varðandi framsal ríkisvalds vegna nýrra gerða sem teknar hafa verið upp í samninginn eða fyrirsjáanlega þarf að taka upp í hann. Því sé mikilvægt að huga að nauðsynlegum stjórnarskrárbreytingum til þess að tryggja að löggjafinn starfi innan þeirra marka sem leidd verða af stjórnarskránni um alþjóðlegt samstarf. Engar slíkar breytingar hafa þó náð fram að ganga frá því að álitargerðin var rituð.

Þýðingu hefur að greina nánar eðli mögulegs framsals ríkisvalds samkvæmt persónuverndarreglugerð ESB og að hverjum ákvarðanir beinast til að meta samrýmanleika við stjórnarskrá. Sem fyrr segir vöknud álitafni um aðlögun fyrir EES-samninginn vegna ákvæða í 63.– 67. gr. reglugerðarinnar um framkvæmd samræmingarkerfis hennar. Í 64. gr. er mælt fyrir um í hvaða tilvikum Evrópska persónuverndarráðið skuli gefa út álit. Það á við ef lögbært eftirlitsstjórnvald hyggst samþykkja einhverja af þeim ráðstöfunum sem fjallað er um í 1. mgr. greinarinnar. Meðal atriða sem þar eru talin er samþykkt skrár yfir vinnsluáðgerðir sem falla undir kröfu um mat á persónuvernd, samþykkt viðmiðana um faggildingu vottunaraðila eða ákvörðun um stöðluð ákvæði um persónuvernd. Vekja álit ráðsins af þessum toga ekki upp spurningar um framsal enda ekki um bindandi niðurstöður að ræða þegar rætt er um framsal valdheimilda ráðsins koma hins vegar til álita heimildir þess samkvæmt 65. gr. reglugerðarinnar til að samþykkja *bindandi ákvörðun* í eftirfarandi tilvikum:

a) ef hlutaðeigandi eftirlitstjórnvald hefur, í því tilviki sem um getur í 4. mgr. 60. gr., haft uppi viðeigandi og rökstudd andmæli gegn drögum að ákvörðun forystustjórnvalds eða forystustjórnvald hefur hafnað slíkum andmælum þar sem þau séu ekki viðeigandi eða rökstudd.

b) ef ágreiningur er uppi um hvert af hlutaðeigandi eftirlitsstjórnvöldum telst vera lögbært að því er varðar höfuðstöðvarnar,

c) ef lögbært eftirlitsstjórnvald óskar ekki eftir áliti persónuverndarráðsins í tilvikum sem um getur í 1. mgr. 64. gr. eða fylgir ekki áliti sem persónuverndarráðið hefur gefið út skv. 64. gr. Í því tilviki getur hlutaðeigandi eftirlitsyfirvald eða framkvæmdastjórnin vísað málinu til persónuverndarráðsins.

Ljóst er að framangreindar ákvarðanir persónuverndarráðsins beinast ekki að einstaklingum og lögaðilum, heldur að eftirlitsstjórnvöldum aðildarríkja, sem hér á landi er Persónuvernd eins og fyrr segir. Þannig verður Persónuvernd sem stjórnvald bundin af niðurstöðu ráðsins. Sú ákvörðun sem Persónuvernd tekur í framhaldinu og byggist á niðurstöðu ráðsins kann þó vissulega að hafa áhrif fyrir þá einstaklinga eða lögpersónur sem ákvörðunin varðar. Með þessum hætti virðast bindandi ákvarðanir persónuverndarráðs geta snert einstaklinga og fyrirtæki í aðildarríkjunum a.m.k. með óbeinum hætti. Því til viðbótar ættu slíkar ákvarðanir persónuverndarráðsins ekki að sæta endurskoðun landsdómstóla, sbr. nánar 143. lið formála reglugerðarinnar, þar sem fram kemur að innlendir dómstólar hafi ekki vald til að lýsa slíka ákvörðun ógilda heldur verður hinn innlendi dómstóll að vísa álitaefninu um gildi til dómstóls Evrópusambandsins. Er það raunar almenna reglan um meðferð ákvarðana sem stofnanir ESB taka. Engu að síður er ekki hægt að girða fyrir að einstaklingur leiti úrlausnar dómstóla um gildi stjórnarvaldsákvörðunar sem Persónuvernd tekur, enda er sá réttur stjórnarskrárvarinn, sbr. 60. og 70. gr. stjórnarskrárinnar.

Þar sem ljóst þótti að upptaka reglugerðarinnar í EES-samninginn mundi fela í sér stjórnskipuleg álitaefni var leitað til Stefáns Más Stefánssonar lagaprófessors, til að meta inntak þeirra og hvaða leiðir væru færar til að taka þær upp í samninginn með tilliti til íslenskrar stjórnskipunar. Í álitsgerð hans frá 14. desember 2017 var farið yfir hvaða valkostir væru til staðar um aðlögun að stofnanakerfi reglugerðarinnar og álitamál um framsal ríkisvalds. Bent var á að lausn gæti falist í því að Eftirlitstofnun EFTA tæki ákvarðanir sínar á grundvelli uppkasts frá Evrópska persónuverndarráðinu. Sú lausn hefði vissa stoð í fordæmum í reglugerðum um eftirlit með fjármálamörkuðum. Hún myndi að vissu leyti tryggja samræmda beitingu reglna á þessu sviði og ekki raska því hlutverki sem dómstólar ESB og EES hefðu á grundvelli EES samningsins. Í þessu sambandi var einnig leitað ráðgjafar hjár

Niðurstaðan í sameiginlegu EES-nefndinni var hins vegar að velja þá leið sem kennd er við „fulla aðkomu persónuverndarráðsins“ og lýst var í kafla 5.3. í frumvarpi þessu. Í því felst að ráðið mun taka bindandi ákvarðanir gagnvart eftirlitsstjórnvaldi EFTA-ríkis innan EES. Munu fulltrúar EFTA-ríkjanna innan EES sitja í evrópska persónuverndarráðinu, án atkvæðisréttar, en með fullan tillögurétt og málfrelsi. Um þetta fyrirkomulag hefur m.a. verið vísað til fyrri fordæma varðandi þátttöku fulltrúa EFTA-ríkjanna innan EES í stjórnnum sérstofnana ESB. Dæmi um slíka tilhögun eru fjármálaeftirlitsstofnanir ESB, Evrópska vinnuverndarstofnunin og Lyfjastofnun Evrópu.

Af þessu er ljóst að stofnun ESB mun taka bindandi ákvarðanir gagnvart eftirlitsyfirvöldum EFTA-ríkjanna, þ.e. Persónuvernd hér á landi án þess að íslenska ríkið hafi beina aðkomu að þeirri ákvörðun, nema með þátttöku í umræðum um hana á vettvangi ráðsins. Þó munu fulltrúar Persónuverndar hafa fullan þátttökurétt í samræmingarkerfinu og einnar afgreiðslukerfinu. Stofnunin getur þannig tekið fullan þátt í rannsókn mála sem varða vinnslu yfir landamæri, og eftir atvikum tekið ákvarðanir sem binda íslensk fyrirtæki sem viðhafa vinnslu yfir landamæri, sem persónuverndarstofnanir í öðrum Evrópuríkjum eru bundnar af.

Telja verður að framsal valds til Evrópska persónuverndarráðsins í þessum málum sé lítilsháttar, það er aðeins á sviði framkvæmdarvalds í þröngt afmörkuðum tilvikum og bindur aðeins stjórnvöld en ekki einstaklinga eða fyrirtæki. Það fer því ekki út fyrir það svigrúm sem löggjafinn hefur til þessa talið vera til staðar um framsal ríkisvalds til þessa, og gengur t.d. mun skemur en það framsal sem varð með innleiðingu reglugerða ESB um eftirlit með fjármálamörkuðum í EES-samninginn, sbr. lög nr. 24/2017 um evrópskt eftirlitskerfi á fjármálamarkaði. Fram til þessa hefur Evrópulöggjöf á sviði persónuverndar, þ.m.t. ESB-tilskipunin, ekki kallað á slíkt framsal. Ótvírætt er því að með framsali á ríkisvaldi til hins nýja Evrópska persónuverndarráðs bætist við enn eitt nýtt málefna svið á vettvangi EES-samstarfsins sem krefst slíks valdframsals.

Hvað dómsháttur varðar er í fyrrgreindri álitsgerð Stefáns Más Stefánssonar lagt mat á 143. gr. formála reglugerðarinnar um rétt einstaklinga og lögaðila til að höfða mál til ógildingar

ákvörðunum persónuverndarráðsins fyrir ESB-dómstólum samkvæmt ákvæði 263. gr. sáttmálans um starfshætti ESB. Í álitargerðinni er bent á að kjarni málsins sé að persónuverndarstofnun sem ákvörðun hefur verið beint að en vill vefengja ákvörðun stofnunar ESB geti höfðað ógildingarmál þar um að fullnægðum þeim skilyrðum sem fram koma í greininni. Einstaklingar og lögpersónur hafi almennt ekki sömu heimild (enda ákvörðun ekki beint að þeim). Þessir aðilar hafi þó málssóknarrétt ef ákvörðun telst varða þá *beint og sérstaklega*. Slík tilvik eru hins vegar ekki algeng. Tekið er fram í álitargerðinni að réttarstaðan sé í öllum aðalatriðum lík þessu EFTA megin. Í umræddri 1. mgr. 143. gr. formála reglugerðarinnar komi einnig fram að einstaklingur eða lögaðili skuli hafa virkt réttarúrræði fyrir dómstólum viðkomandi ríkis teljist hann hafa lögvarða hagsmuni af slíkri málsókn. Það eigi einkum við varðandi beitingu eftirlitsstofnunar á rannsóknarheimildum, valdheimildum til að gera ráðstafanir til úrbóta og leyfisveitingarheimildum auk frávísunar eða höfnunar á kvörtunum. Þessa réttarvernd hafi einstaklingar og lögaðilar samkvæmt íslenskum lögum þannig að sú réttarvend telst vera fyrir hendi. Samkvæmt þessu ættu engin vandkvæði að vera fyrir hendi sem snerta 1. mgr. 143. lið formála reglugerðarinnar.

Þá er í álitargerðinni lagt mat á 2. mgr. í fyrrgreindum lið formálans þess efnis að hafi eftirlitsvald hafnað kröfu eða vísað frá geti sá sem lagði fram kvörtun höfðað mál fyrir dómstólum í aðildarríki. Viðkomandi dómstóli sé þá heimilt og *stundum skylt* að óska eftir forúrskurði dómstóls ESB um túlkun laga sambandsins. Forúrskurður dómstóls ESB feli í sér bindandi niðurstöðu fyrir viðkomandi dómstól aðildarríkis og aðila málsins. Sé sama regla heimfærð upp á EFTA-ríkin (34. gr. samningsins EFTA ríkjanna um stofnun eftirlitsstofnunar og dómstóls) komi fram sá munur að dómstólum EFTA ríkjanna sé heimilt en *aldrei skylt* að leita álits EFTA- dómstólsins sem auk þess gefur aðeins *ráðgefandi álit* sem telst ekki bindandi fyrir viðkomandi landsdómstóla. Þá komi fram í þessu ákvæði formálans að þegar ákvörðun persónuverndarstofnunar um að framkvæma ákvörðun persónuverndarráðsins sé vefengd fyrir innlendum dómstól og deilt um gildi ákvörðunar persónuverndarráðsins hafi innlendi dómstóllinn ekki vald til að lýsa ákvörðun þess ógilda heldur verði hann að vísa álitafninu um gildi til dómstóls ESB í samræmi við 267. gr. sáttmálans um starfshætti Evrópusambandsins, eins og Dómstóllinn túlkar hana, ef hann telur ákvörðunina ógilda.

Bent er á þarna komi fram munur á ESB- og EES- rétti sem hefur þýðingu að því leyti að dómstóll ESB hafi heimild í forúrskurði til að ógilda ákvörðun stofnunar ESB. EFTA-dómstóllinn hafi ekki sambærilega heimild. Þá bætist við eins og fyrr segir að dómstólum EFTA ríkjanna sé heimilt en aldrei skylt að leita álits EFTA dómstólsins sem auk þess gefi aðeins *ráðgefandi álit*. Niðurstaðan í álitargerðinni hvað varðar dómsvald er að verði reglugerðin tekin upp í íslenskan rétt geti íslenskir aðilar látið á það reyna fyrir íslenskum dómstólum hvort tiltekin ákvörðun Persónuverndar standist íslensk lög, þar á meðal stjórnarskrá, t.d. með kröfu um ógildingu. Skipti í því sambandi engu máli þótt ákvörðun stofnunarinnar kunni að vera byggð á (eða bundin við) ákvörðun Evrópska persónuverndarráðsins. Íslenskir dómstólar hafi hins vegar ekki vald til að dæma um hvort hin erlenda ákvörðun (sem kann að vera undirliggjandi íslenskri ákvörðun) sé lögmæt samkvæmt ESB- eða EES- rétti.

9. Samráð.

Drög að íslenskri þýðingu á persónuverndarreglugerð ESB voru birt opinberlega árið 2016 en ljóst er að ákvæði hennar eru meginheimildin um gildandi reglur á sviðinu og breytir frumvarpið ekki þeim kjarnaatriðum sem þar koma fram.

Vinna við gerð frumvarpsins hófst í lok nóvembermánaðar 2017 eftir að dómsmálaráðherra skipaði starfshóp um verkefnið sem lýst var í 1. kafla greinargerðar þessarar. Á fyrstu stigum í vinnu starfshópsins var m.a. haft samráð við utanríkisráðuneyti og forsætisráðuneyti um vinnuáætlun, tihögun vinnu, þýðingar á reglugerðinni og framsetningu. Þá var dómsmálaráðherra gerð grein fyrir framvindu vinnunnar og afhent frumdrög að frumvarpinu þann 22. janúar 2018, ásamt minnisblaði um meginatriði þess og valkosti um afstöðu til ýmissa atriða, s.s. um framsetningu þess og setningu sérreglna þar sem víkja mætti frá eða bæta við ákvæði reglugerðarinnar.

Þann 1. febrúar 2018 bauð dómsmálaráðuneytið til samráðsfundar fulltrúa starfshópsins og ráðuneytisins með nokkrum aðilum í atvinnulífinu, Sambandi íslenskra sveitarfélaga svo og fulltrúum ýmissa stofnana þar sem frumdrögum frumvarpsins var dreift og efni þess rætt.

Þann 13. mars 2018 voru drög að frumvarpinu ásamt almennum athugasemdum birt á samráðsgátt Stjórnarráðsins og óskað var eftir umsögnum um efni þess. Bæði einstaklingar, fyrirtæki og stofnanir sendu inn umsagnir um frumvarpið eða gerðu athugasemdir við efni þess en það voru eftirtaldir: Advel Lögmenn, Bæjarráð Hafnarfjarðar, Creditinfo, Einkaleyfastofa, Fjeldsted & Blöndal lögmannsstofa, Guðmundur Arnar Kristínarson, Hagsmunasamtök heimilanna, Hagstofa Íslands, Isavia, Íslensk erfðagreining, Landssamtök lífeyrissjóða, Persónuvernd, Reykjavíkurborg, Samband íslenskra sveitarfélaga, Samtök fyrirtækja í velferðarþjónustu, Steinþór Bjarni Grímsson, sveitarstjórn Hrunamannahrepps, Tollstjóri og Þjóðskjalasafn Íslands. Þá var send inn sameiginleg umsögn undirrituð af fulltrúum Samtaka atvinnulífsins, Samorku, Samtaka ferðaþjónustunnar, Samtaka fjármálafyrirtækja, Samtaka fyrirtækja í sjávarútvegi, Samtaka iðnaðarins, Samtaka verslunar og þjónustu og Viðskiptaráðs Íslands. Starfshópurinn fór yfir allar umsagnir og athugasemdir sem bárust og leiddu þær til ýmissa breytinga á texta frumvarpsins eða sérstakra skýringa í athugasemdum við einstök ákvæði.

Á vegum Persónuverndar hefur umfangsmikið kynningarstarf farið fram á efni og áhrifum reglugerðarinnar allt frá árinu 2016. Hefur stofnunin staðið fyrir eða starfsmenn hennar flutt erindi um efnið á fjölmörgum fundum og ráðstefnum faghópa, fyrirtækja og stofnana, m.a. á sviði heilbrigðis- og menntamála þar sem fjallað hefur verið um helstu breytingar og nauðsynlegan undirbúning vegna gildistöku reglugerðarinnar. Þá hefur stofnunin gefið út og birt á heimasíðu sinni margvíslegt fræðsluefni sem og leiðbeiningar um framkvæmd tiltekinna ákvæða í reglugerðinni, s.s. um persónuverndarfulltrúa, öryggisbrot, samþykki fyrir vinnslu persónuupplýsinga svo og um skyldur ábyrgðaraðila og vinnsluaðila samkvæmt hinu nýja regluverki.

Að ósk dómsmálaráðuneytisins tilnefndu ráðuneytin tengiliði í samráðshóp sem hafði það hlutverk að fara yfir ákvæði sérlaga um persónuvernd í því skyni að meta hvaða breytingar kynnu að vera nauðsynlegar vegna innleiðingar persónuverndarreglugerðar ESB. Fengu tengiliðir ráðuneytanna send drög að frumvarpinu í byrjun febrúar. Hvert ráðuneyti bar ábyrgð á að meta hvaða breytingar væru nauðsynlegar nú þegar, samhliða framlagningu frumvarpsins í svonefndum bandormi, en þar er einkum um að ræða tæknilegar breytingar vegna tilvísana til gildandi laga. Ljóst er að endurskoðun á ákvæðum sérlaga er að öðru leyti verkefni sem þarf að huga að í fleiri áföngum á næstu misserum.

10. Mat á áhrifum.

Eins og fram hefur komið hefur frumvarpið það að meginmarkmiði að tryggja vernd á friðhelgi einkalífs svo og að íslenskt regluverk um persónuvernd og vinnslu persónuupplýsinga verði uppfært til samræmis við þróun í Evrópu og í samræmi við alþjóðaskuldbindingar. Ávinningur fyrir samfélagið felst m.a. í því að tryggja einstaklingum aukna vernd og aukin réttindi við meðferð persónuupplýsinga þeirra til samræmis við þær meginreglur sem felast í nýju persónuverndarregluverki ESB. Við það myndist aukið traust til þeirra aðila sem vinna með persónuupplýsingar en slíkt traust er ein af nauðsynlegum forsendum til að hinn stafræni innri markaður haldi áfram að þróast og virki sem skyldi. Strangar kröfur til ábyrgðar- og vinnsluaðila um að tryggja öryggi persónuupplýsinga draga úr hættu á öryggisbrestum með tilheyrandi tjóni fyrir einstaklinga. Áherslan á aukna persónuvernd í þágu einstaklinga birtist einkum í ákvæðum sem veita þeim meiri stjórn á eigin persónuupplýsingum. Með samræmdum reglum og kerfi sem tryggir samstillta túlkun og framkvæmd er stefnt að því að fyrirbyggja að misræmi geti komið upp sem trufla flæði upplýsinga yfir landamæri og torveldi viðskipti. Ávinningur fyrir samfélagið felst því einnig í bættari stöðu fyrirtækja og jafnari samkeppnisgrundvelli á hinum stafræna innri markaði.

Hinar nýju reglur um persónuvernd munu þannig ótvírætt hafa áhrif á samfélagið allt en ekki eingöngu sérhæfð svið í atvinnulífinu svo dæmi sé tekið. Þær stuðla að hugarfarsbreytingu hvað varðar meðferð persónuupplýsinga, umgengni um slíkar upplýsingar og þýðingu þeirra. Þá verða allir, bæði stjórnvöld og fyrirtæki stór og smá, að tileinka sér hinar nýju reglur og vinna eftir þeim til framtíðar. Af þessu er ljóst að áhrif frumvarpsins þegar það verður að lögum verða víðtæk og snerta nær öll svið samfélagsins, þar á meðal meira eða minna alla atvinnustarfsemi, heilbrigðiskerfið og menntakerfið, svo og öll opinber stjórnvöld, svo nefnd séu nokkur dæmi.

Persónuvernd er sú stofnun í stjórnsýslunni sem samþykkt frumvarpsins mun eðli máls samkvæmt hafa mest áhrif á, enda eru henni færð bæði umfangsmikil og ný verkefni og valdheimildir við gildistöku laganna. Síðan stofnunin tók til starfa árið 2001 hefur hún lítt stækkað, árið 2017 voru fastir starfsmenn hennar einungis sjö, en á fyrsta starfsári hennar voru þeir sex. Á sama tíma hefur málafjöldi stofnunarinnar vaxið ár frá ári og rúmlega þrefaldast frá upphafi. Þá hefur fræðslu- og kynningarstarf undanfarin tvö ár vegna undirbúnings fyrir gildistöku reglugerðarinnar verið umtalsverð viðbót við lögmælt verkefni hennar. Ljóst er að hið nýja lagaumhverfi leggur fjölmörg ný og umfangsmikil verkefni á Persónuvernd. Skapast mun verulega aukið álag í stofnuninni þar sem nauðsynlegt er að setja og fylgja eftir verklagsreglum um framkvæmd laganna og sinna ríkri upplýsinga- og leiðbeiningarskyldu sem stofnunin hefur gagnvart fyrirtækjum og stofnunum, bæði í lagalegu og tæknilegu tilliti. Í ljósi nýrra reglna um álagningu stjórnvaldssekta leggja þeir sem vinna með persónuupplýsingar eðlilega kapp á að fylgja til hlítar ákvæðum laganna og uppfylla skyldur sínar samkvæmt þeim. Hefur Persónuvernd mikilvægu hlutverki að gegna til að styðja við þá þróun á öllum sviðum samfélagsins. Þá mun þátttaka Persónuverndar í Evrópska persónuverndarráðinu auka mjög þunga í alþjóðlegu samstarfi á vegum stofnunarinnar en það kallar á meiri mannafla en nú er til staðar. Til að mynda er fyrirhugað að fundir ráðsins verði haldnir mánaðarlega í stað fimm til sex funda á ári, eins og nú er í 29. gr. starfshópnum. Auk þess munu fulltrúar Persónuverndar hafa þátttökurétt í starfi hvers kyns undirhópa sem ráðið kann að setja á laggirnar, sækja fundi þeirra og fá allar upplýsingar sem nauðsynlegar eru svo þátttaka stofnunarinnar sé skilvirk, þ.m.t. fullan aðgang að hvers kyns kerfum sem persónuverndarráðið kanna að setja upp.

Í öllum Evrópuríkjum hafa verið gerðar ráðstafanir til að efla og styrkja persónuverndarstofnanir og víðast hvar hefur starfsmönnum verið fjölgað umtalsvert til að undirbúa breytingar og takast á við aukin verkefni samkvæmt nýrri löggjöf. Skref var tekið í þá átt að auka fjárheimildir Persónuverndar á árinu 2018, þegar þær hækkuðu úr 114,2 millj. kr. í 205,8 millj. kr. og fékkst þá nokkurt svigrúm til að bæta við starfsmönnum, þar á meðal tveimur sérfræðingum á sviði upplýsingaöryggis, enda ljóst að eftirlits- og ráðgjafarhlutverk stofnunarinnar á því sviði mun aukast verulega samkvæmt fyrir mælum reglugerðarinnar og laganna. Ljóst er þó að meira þarf til svo að stofnunin geti sinnt lögmæltum verkefnum sínum samkvæmt reglugerðinni og ýmsum sérlögum sem fjalla um vinnslu persónuupplýsinga, bæði nýjum verkefnum og þeim sem safnast hafa upp. Í lok árs 2017 voru opin og ólokin verkefni 516 en í apríl 2018 voru þau 658 talsins. Nýskráð mál voru tæplega tvö þúsund, en vænta má að þeim muni fjölga umtalsvert samhliða gildistöku á hinni nýju löggjöf. Verður því að ætla að fyrir árið 2019 og næstu ár þar á eftir verði að bæta við talsvert fleiri starfsmönnum og hækka fjárheimildir því til samræmis, til að gera Persónuvernd kleift að inna af hendi lögmælt verkefni sín auk þess sem ljóst er að nýjar og krefjandi áskoranir tengdar vinnslu persónuupplýsinga á borð við gríðargögn, internet allra hluta, gervigreind, sjálflærandi vélar o.fl., munu hafa mikil áhrif á verkefni stofnunarinnar um ókomin ár.

Í reglugerð ESB er að finna ákvæði um valdheimildir Evrópska persónuverndarráðsins sem tekur bindandi ákvarðanir gagnvart Persónuvernd í ákveðnum málum skv. 65. gr. reglugerðarinnar og lýst var í 8. kafla að framan. Þetta á að meginstefnu við í tengslum við framkvæmd á samræmingarkerfi reglugerðarinnar og lúta þessar heimildir einkum að samskiptum persónuverndarstofnana í fleiri en einu aðildarríki. Hafa verður í huga að þessar valdheimildir eru á þröngu sviði og ekki mjög líklegt að oft muni reyna á þær gagnvart Persónuvernd á Íslandi. Fyrst og fremst mun persónuverndarráðið veita Persónuvernd, líkt og öðrum persónuverndarstofnunum í ríkjum Evrópu, ráðgjöf og semja viðmiðunarreglur og tilmæli um framkvæmd reglugerðarinnar, auk þess að vera vettvangur samvinnu stofnananna. Sýnileg áhrif persónuverndarráðsins hér á landi í tengslum við framkvæmd reglugerðarinnar verða því tæpast nokkur, enda verður áfram sú skipan að eftirlit með framkvæmd persónuverndarlaga verður á hendi Persónuverndar.

Um einstakar greinar frumvarpsins.

Um 1. gr.

Greinin lýsir markmiðum frumvarpsins. Í 1. mgr. er lýst tvíþættu markmiði sem lýtur að innleiðingu reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga. Annars vegar

að ákvæði reglugerðarinnar, eins og hún var tekin upp í EES-samninginn séu lögfest og hins vegar að sett séu í lög ákvæði til fyllingar og viðbótar reglugerðinni. Með því vísast til þess að í frumvarpinu eru settar sérreglur um ýmis atriði þar sem reglugerðin gerir ráð fyrir að aðildarríki hafi svigrúm til útfærslu eða skyldur til að festa tiltekin atriði í lög eins og rætt var um í almennum athugasemdum að framan. Eins og þar var einnig lýst er í frumvarpinu gerð tillaga um heildstæða löggjöf um efnið og þar birtast nokkur kjarnaákvæði reglugerðarinnar að því marki sem nauðsynlegt er vegna samræmis og til þess að gera ákvæði landslaga skiljanleg almenningi.

Í 2. mgr. er byggt á efnislegu markmiði reglugerðarinnar sem lýst er í 1.-3. mgr. aðfaraorða og 1. gr. hennar og er ákvæðið samhljóða 1. mgr. 1. gr. núgildandi laga. Er einkum skírskotað til viðtekinna viðhorfa um friðhelgi einkalífs eins og þau hafa mótast í framkvæmd, á grundvelli 71. gr. stjórnarskrárinnar og 8. gr. mannréttindasáttmála Evrópu. Með tilliti til markmiða reglugerðarinnar er í ákvæðinu einnig skírskotað til viðhorfa um mikilvægi áreiðanleika og gæða við vinnslu persónuupplýsinga svo og að tryggja skuli frjálst flæði þeirra á innri markaði Evrópska efnahagssvæðisins.

Í 3. mgr. sem er efnislega samhljóða 2. mgr. 1. gr. núgildandi laga er því lýst yfir að sérstök stofnun Persónuvernd, annist eftirlit með framkvæmd persónuverndarlöggjafarinnar og gildir það jafnt um ákvæði reglugerðarinnar, sérreglur sem lagt er til að verði fest í lög samkvæmt frumvarpinu svo og reglur sem settar verða samkvæmt þeim, sbr. nánar ákvæði VII. kafla. Þá er þess jafnframt getið að evrópsk eftirlitsstofnun samkvæmt reglugerðinni sé Evrópska persónuverndarráðið, sem sett er á fót með henni og starfar samkvæmt ákvæðum VII. kafla hennar. Hér vísast til reglugerðarinnar en ekki er þörf á að setja sérákvæði í frumvarpinu um verkefni og valdheimildir persónuverndarráðsins. Samhengis vegna þykir þó rétt að geta hér stöðu ráðsins sem eftirlitsstofnunar á Evrópska efnahagssvæðinu. Sambærilega tilvísun til þess hvaða evrópsku eftirlitsstofnanir starfa samkvæmt reglugerðum sem innleiddar eru með lögum má t.d. finna í 2. gr. laga um evrópskt eftirlitskerfi á fjármálamarkaði nr. 24/2017.

Um 2. gr.

Í ákvæðinu er lagt til að reglugerð Evrópuþingsins og ráðsins um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB, eins og hún er aðlöguð og tekin upp í samninginn um Evrópska efnahagssvæðið skuli hafa lagagildi hér á landi. Þá er tekið fram að reglugerðin sé birt sem fylgiskjal með lögum. Með því er undirstrikað mikilvægi þess að lögin og texti reglugerðarinnar séu þannig tengd saman enda standa þau í órjúfanlegu sambandi og mikilvægt að hafa yfirsýn yfir allt regluverkið fyrir þá sem vinna eftir því. Þá eru drög að ákvörðun sameiginlegu EES-nefndarinnar einnig birt sem fylgiskjal enda fæst þannig heildarmynd af því hvaða breytingar aðlögunin hefur í för með sér.

Um 3. gr.

Í þessari grein frumvarpsins eru talin upp í 11 töluliðum og skilgreind helstu hugtök og orð sem vísað er til í ákvæðum frumvarpsins. Í 4. gr. reglugerðarinnar eru settar fram skilgreiningar á mun fleiri hugtökum eða í 26 töluliðum. Þessi munur skýrist af því að frumvarpið er talsvert styttra en reglugerðin og geymir sem fyrr segir aðeins sérreglur svo og helstu kjarnaatriði reglugerðarinnar, en að öðru leyti er vísað til ítarlegri ákvæða í texta reglugerðarinnar þar sem fleiri hugtök birtast.

Skilgreiningar sem eru settar fram í þessu frumvarpsákvæði lúta þannig að helstu lykilhugtökum og verða túlkað rúmt í samræmi við markmið laganna að vernda réttindi einstaklinga. Þær eru samhljóða samsvarandi skilgreiningum í reglugerðinni en mikilvægt er að fullt samræmi sé þar á milli. Auk þess er að finna í þessu ákvæði hugtök sem fjallað er um í sérreglum frumvarpsins, s.s. um rafræna vöktun. Flest þeirra hugtaka sem fjallað er um í 3. gr. frumvarpsins eru efnislega óbreytt frá 2. gr. núgildandi laga nr. 77/2000 og 2. gr. tilskipunar ESB frá 1995. Sum hafa þó breyst og ný hafa bæst við. Í skýringum við hvern og einn tölulið hér á eftir verður gerð grein fyrir megininntaki hvers hugtaks en jafnframt er gerð grein fyrir helstu breytingum og nýmælum frá núgildandi lögum og ESB-tilskipuninni.

1. *Reglugerðin.* Hér er átt við ESB reglugerðina sem frumvarpið stefnir að því að lögfesta og allvíða er vísað til í frumvarpinu.

2. *Persónuupplýsingar*. Hugtakið persónuupplýsingar er víðfeðmt og tekur til allra upplýsinga, álita og umsagna sem beint eða óbeint má tengja tilteknum einstaklingi, þ.e. upplýsingar sem eru persónugreindar eða persónugreinanlegar. Skilgreining frumvarpsins er samhljóða 1. tölul. 4. gr. reglugerðarinnar. Í núgildandi lögum byggir skilgreiningin á a-lið 2. gr. tilskipunarinnar, að því viðbættu að skilgreining laganna er einnig látin ná til persónuupplýsinga látinna manna, sem tilskipunin tók ekki til. Frumvarpið ráðgerir breytingar á þessu, sem nánar verður lýst hér á eftir.

Líkt og tilskipunin geri reglugerðin ráð fyrir því að persónuupplýsingahugtakið nái aðeins til upplýsinga um einstaklinga en hvorki til stofnana, fyrirtækja né annarra lögpersóna. Í því sambandi má einnig benda á 14. lið formála reglugerðarinnar sem tilgreinir sérstaklega að hún nái ekki yfir vinnslu upplýsinga er varða lögaðila, einkum fyrirtæki sem stofnuð eru sem lögaðilar, þ.m.t. upplýsinga um heiti lögaðila, rekstrarform hans og samskiptaupplýsingar.

Það útilokar þó ekki að í lögum séu sérreglur sem veita fyrirtækjum betri vernd, en dæmi þess má sjá í 15. gr. frumvarpsins þar sem fjallað er um réttindi lögaðila í tengslum við vinnslu fjárhagsupplýsingastofa á upplýsingum um fjárhagsmálefni og lánstraust í því skyni að miðla þeim til annarra. Með hinum skráða í skilningi frumvarpsgreinarinnar er átt við þann einstakling sem upplýsingarnar fjalla um. Hugtakið á við þótt ekki sé um eiginlega skrá í hefðbundnum skilningi að ræða ef upplýsingum hefur verið safnað saman og þær varðveittar, en nánar verður fjallað um skrárhugtakið undir 5. tölul. ákvæðisins.

Samkvæmt 27. lið formála reglugerðarinnar á hún ekki við um persónuupplýsingar látinna einstaklinga, en jafnframt er tekið fram að aðildarríkjum sé heimilt að setja reglur um vinnslu slíkra persónuupplýsinga. Sú leið er farið í frumvarpi þessu að hafa skilgreiningar að öllu leyti eins, og því fellur niður tilvísun til látinna einstaklinga sem er að finna í núgildandi lögum. Í framkvæmd laganna hefur lítt reynt á álitamál um vinnslu persónuupplýsinga um látna menn.

Eins og fram kom í skýringum með skilgreiningu núgildandi laga voru upplýsingar um látna einstaklinga einkum taldar falla undir verndarsvið laganna ef þær tengdust lifandi einstaklingum, svo sem upplýsingar um arfgenga sjúkdóma. Í raun er þá komið inn á svið persónuupplýsinga þessara lifandi einstaklinga, sem falla þá hvort eð er undir skilgreiningu 2. tölul. 3. gr. frumvarpsins. Þessi ályktun fær m.a. stoð í dómi Hæstaréttar frá 27. nóvember 2003 í máli nr. 151/2003 þar sem fjallað var um flutning persónuupplýsinga úr sjúkraskrárm í gagnagrunn á heilbrigðissviði samkvæmt lögum nr. 139/1998. Stefndandi málsins byggði aðild sína á því að hún ætti persónulegra hagsmuna að gæta af því að upplýsingar úr sjúkraskrárm föður hennar sem var látinn yrðu ekki fluttar í gagnagrunninn, þar sem ráða mætti af slíkum upplýsingum atriði varðandi arfgenga eiginleika föðurins, sem einnig gætu átt við um hana. Féllst dómurinn á að vegna friðhelgi einkalífs síns hefði hún hagsmuni af því að koma í veg fyrir að upplýsingar af þessum toga um föður hennar yrðu fluttar í gagnagrunninn og þar með rétt til að hafa uppi þær dómkröfur sem hún gerði í málinu. Í stað þess að skilgreining frumvarpsins á persónuupplýsingum nái til látinna manna, gerir frumvarpið ráð fyrir því að gildissvið laganna geti náð til vinnslu persónuupplýsinga um látna einstaklinga í 5 ár frá andláti þeirra og lengur í ákveðnum tilvikum. Verður nánar vikið að þeirri reglu í skýringum með 4. gr. frumvarpsins um efnislegt gildissvið laganna.

Kjarni persónuupplýsingahugtaksins lýtur að því að upplýsingar megi rekja til einstaklings, beint eða óbeint. Til þess að upplýsingar séu persónugreinanlegar (rekjanlegar) skal tekið mið af öllum aðferðum sem eðlilegt er að hugsa sér að ábyrgðaraðili eða annar aðili beiti til að bera kennsl á viðkomandi einstakling. Skilgreining reglugerðarinnar bætir nokkrum fleiri dæmum við þau sem talin voru upp í tilskipuninni um það hvenær einstaklingur er persónugreinanlegur og er þar meðal annars tekið mið af tækniþróun undanfarna áratugi. Þar er nú, auk fyrri atriða sem talin voru upp í tilskipuninni vísað til auðkenna eins og staðsetningargagna, netauðkenna og erfðafræðilegra þátta.

Í 26. lið formála reglugerðarinnar er nánar lýst inntaki persónuupplýsingahugtaksins og frekari dæmi tekin. Samkvæmt því skulu meginreglur um vernd ekki gilda um upplýsingar sem hafa verið aftengdar einstaklingum þannig að ekki sé lengur unnt að persónugreina hina skráðu. Persónuupplýsingar sem hafa verið færðar undir svokölluð gerviauðkenni (e. *pseudonymisation*), sem kann þó að vera hægt að rekja til einstaklings með notkun viðbótarupplýsinga, skulu teljast upplýsingar um persónugreinanlegan einstakling. Sambærileg sjónarmið gilda um persónuupplýsingar sem hafa verið dulkóðaðar en ef dulkóðunarlykli hefur ekki verið eytt, teljast þær til persónuupplýsinga.

Til þess að ákvarða hvort einstaklingur sé persónugreinanlegur ætti að taka mið af öllum þeim aðferðum sem ástæða er til að ætla að annaðhvort ábyrgðaraðili eða annar aðili geti beitt til að bera kennsl á viðkomandi einstakling með beinum eða óbeinum hætti. Til að ganga úr skugga um hvort fremur líklegt megi telja að aðferðum verði beitt til að bera kennsl á einstakling ætti að taka tillit til allra hlutlægra þátta, s.s. kostnaðar við það og þess tíma sem það tæki, að teknu tilliti til þeirrar tækni sem fyrir hendi er þegar vinnslan fer fram og til tækniþróunar. Meginreglur um persónuvernd ættu því ekki að eiga við um nafnlausar upplýsingar, þ.e. upplýsingar sem tengjast ekki persónugreindum eða persónugreinanlegum einstaklingi, eða persónuupplýsingar sem hafa verið aftengdar persónuauðkennum þannig að ekki er lengur unnt að persónugreina hinn skráða. Skilgreiningin nær því ekki til vinnslu slíkra nafnlausra upplýsinga, s.s. í tölfraðilegum tilgangi eða vegna rannsókna.

Þá er þess getið í 30. lið formála reglugerðarinnar að m.a. ýmis tæki og tól og forrit sem einstaklingar nota, geti tengt netauðkenni við þá. Þar eru nefnd í dæmaskyni IP-tölur (e. *internet protocol addresses*), vefkökuauðkenni (e. *cookie identifiers*) og fjarskiptatíðniauðkenningar. Kemur fram að fyrir tilstilli slíkra auðkenna geta orðið eftir spor sem hægt er að nota til að útbúa persónusnið um einstaklinga og bera kennsl á þá, einkum þegar sporunum er bætt við einkvæm auðkenni og aðrar upplýsingar sem berast netþjónum.

3. *Viðkvæmar persónuupplýsingar.* Í þessu ákvæði eru taldar upp persónuupplýsingar sem fjallað er um í 1. mgr. 9. gr. reglugerðarinnar undir heitinu sérstakir flokkar persónuupplýsinga. Þessar persónuupplýsingar eru háðar sérstökum skilyrðum og útgangspunkturinn er að vinnsla þeirra sé óheimil nema að einhverjum þessara skilyrða uppfylltum en þau ganga lengra en skilyrði fyrir vinnslu annarra persónuupplýsinga. Þessi skilyrði eru rakin í 11. gr. frumvarpsins og 2.-4. mgr. 9. gr. reglugerðarinnar og verður nánar vikið að þeim í skýringum á því frumvarpsákvæði. Ákvæðið svarar að mestu til skilgreiningar í 8. tölul. 2. gr. núgildandi laga en þó eru nokkrar breytingar gerðar á. Annars vegar bætast hér við ný atriði sem talin eru í 1. mgr. 9. gr. reglugerðarinnar en það eru erfðafræðilegar upplýsingar og lífkennaupplýsingar í því skyni að persónugreina einstakling með einkvæmum hætti. Í gildandi lögum hafa þessir þættir verið taldir falla undir upplýsingar um heilsuhagi. Hins vegar verður sú breyting að upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað teljast ekki lengur til viðkvæmra upplýsinga og er það í samræmi við upptalningu 1. mgr. 9. gr. reglugerðarinnar. Hins vegar gilda ákveðnar reglur um vinnslu persónuupplýsinga sem varða sakfellingar í refsímálum og refsiverð brot skv. 10. gr. reglugerðarinnar sem verður nánar fjallað um í 12. gr. frumvarpsins.

Ýmis atriði sem talin eru upp í ákvæðinu eru skilgreind sérstaklega í 4. gr. reglugerðarinnar. Samkvæmt 13. tölul. þess ákvæðis eru „erfðafræðilegar upplýsingar“ 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. Í 14. tölul. segir að með „lífkennaupplýsingum“ sé átt við persónuupplýsingar sem fást með sérstakri tæknivinnslu og tengjast líkamlegum, lífeðlisfræðilegum eða atferlisfræðilegum eiginleikum einstaklings og gera það kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti, svo sem andlitsmyndir eða gögn um fingraför. Þá er hugtakið „heilsufarsupplýsingar“ skilgreint í 15. tölul. sem persónuupplýsingar sem varða líkamlegt eða andlegt heilbrigði einstaklings, þ.m.t. heilbrigðisþjónustu sem hann hefur fengið, og sem gefa upplýsingar um heilsufar. Er þannig ljóst að undir heilsufarsupplýsingar falla atriði sem í núgildandi lögum eru talin í dæmaskyni um það sem falli undir hugtakið „heilsuhagir“, þ.e. lyfja-, áfengis- og vímuefnanotkun.

Ákvæðið skýrir hvað teljast vera viðkvæmar persónuupplýsingar og hefur það fyrst og fremst þýðingu við afmörkun á því hvenær hin sérstöku skilyrði þurfa að vera uppfyllt fyrir vinnslu persónuupplýsinga. Í formála reglugerðarinnar er vikið nánar að markmiðum sérstakrar verndar og hvernig skuli skýra einstök atriði í þessari talningu. Samkvæmt 51. lið eiga persónuupplýsingar, sem eru í eðli sínu sérlega viðkvæmar að því er varðar grundvallarréttindi og mannfrelsi, að njóta sérstakrar verndar þar sem vinnsla þeirra gæti haft í för með sér umtalsverða áhættu fyrir grundvallarréttindi og mannfrelsi. Til þessara persónuupplýsinga teljist m.a. upplýsingar um kynþátt og þjóðernislegan uppruna, en ekki beri að skilja notkun hugtaksins „kynþáttur“ sem viðurkenningu á kenningum sem reyna að sanna tilvist mismunandi kynþátta manna. Einnig er tekið fram að ekki ætti kerfisbundið að telja vinnslu ljósmynda til vinnslu sérstakra flokka persónuupplýsinga þar sem þær falla eingöngu undir skilgreiningu á

lífkennaupplýsingum þegar vinnsla þeirra fer fram með sérstakri tæknilegri aðferð sem gerir kleift að greina eða staðfesta deili á einstaklingi með ótvíræðum hætti.

Ljóst er að oft geta aðrar upplýsingar en þær sem hér eru taldar upp verið viðkvæmar fyrir hlutaðeigandi. Í framkvæmd verður að taka tillit til slíks, jafnvel þótt ekki sé um að ræða upplýsingar sem teljast viðkvæmar samkvæmt upptalningu þessa ákvæðis.

4. *Vinnsla.* Orðið vinnsla er eitt af lykilhugtökum regluverksins um persónuvernd og ber að túlka rúmt. Með því er átt við 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.

Í skilgreiningu ákvæðisins á vinnslu er tekið beint upp orðalag 2. tölul. 4. gr. reglugerðarinnar. Efnislega er um að ræða sömu skilgreininguna og fram kemur í 1. mgr. 3. gr. tilskipunarinnar og 2. tölul. 2. gr. núgildandi laga. Reglugerðin telur þó upp fleiri tilvik í dæmaskyni sem fallið geta undir vinnslu án þess að um tæmandi talningu sé að ræða.

Rétt er að taka fram að hingað til hafa orðin „automatic processing“ í tilskipuninni, sbr. á móta orðalag í reglugerðinni, „automated processing, verið þýdd í íslenskum lagatexta sem „rafræn vinnsla“. Var þar m.a. fylgt danskri fyrirmynd en í núgildandi dönskum lögum um persónuvernd frá árinu 2000 er notast við orðin „elektronisk databehandling“. Hér er hins vegar leitast við að fara sem næst orðunum „automated processing“ með því að notast við orðalagið „sjálfvirk vinnsla“. Með því er átt við vélknúna/rafræna vinnslu og er ekki stefnt að neinni efnisbreytingu frá því sem er í gildandi lögum þótt þýðingu umrædds orðalags að þessu leyti sé nú breytt. Þar sem minnst er á sjálfvirka vinnslu er í samræmi við þetta átt við það sama og fram að þessu hefur verið nefnt rafræn vinnsla. Þess má geta að í 1. gr. danska lagafrumvarpsins til nýrra persónuverndarlaga sem nú er til meðferðar á danska þinginu hefur orðalagi verið breytt með sama hætti og í frumvarpi þessu, þ.e. úr „elektronisk databehandling“ í „automatisk databehandling“. Í skýringum með því frumvarpsákvæði segir að merking þessara orða sé að öllu leyti hliðstæð. Þá má geta þess að í núgildandi lögum eru orðin „meðferð“ og „vinnsla“ notuð jöfnum höndum sem þýðing á hugtakinu „processing“ og merking þeirra er hin sama. Það sama gildir þegar orðið kemur fyrir í frumvarpi þessu, þótt megináhersla sé hér á að nota orðið „vinnsla“ eins og m.a. sést af heiti frumvarpsins sem vísar til persónuverndar og vinnslu persónuupplýsinga gagnstætt því sem á við um heiti núgildandi laga sem vísar til meðferðar slíkra upplýsinga.

Sem fyrr segir er vinnsluhugtakið vítt og tekur til hvers konar meðferðar á persónuupplýsingum, óháð þeirri aðferð sem notuð er og óháð því hvort gagnagrunnur er miðlægur eða dreifður. Af því er m.a. ljóst að handvirk vinnsla persónuupplýsinga fellur undir gildissviðið þegar þær eru eða eiga að verða hluti af skrá eins og nánar er lýst í 4. gr. sem fjallar um efnislegt gildissvið. Þegar um annars konar vinnslu er að ræða er hins vegar ekki lögð áhersla á skrár og skráningu, enda er skráning aðeins ein tegund vinnslu. Með vinnslu er t.d. átt við söfnun og skráningu og þar undir fellur m.a. rafræn vöktun, flokkun, varðveisla, breyting, leit, miðlun, samtenging eða hver sú aðferð sem nota má til að gera upplýsingar tiltækar. Sama á við um lokun og eyðingu upplýsinga. Í reglugerðinni bættist við orðið „kerfisbinding“ (e. *structuring*).

5. *Skrá.* Hér er átt við gagnasafn eða upptalningu þar sem persónuupplýsingum er komið fyrir á þann hátt að þar má finna upplýsingar um einstaka menn. Ákvæðið á við hvort sem upplýsingar eru miðlægur eða dreifðar. Nánar er fjallað um hugtakið í athugasemdum við 4. gr. frumvarpsins um efnislegt gildissvið ákvæða laganna og reglugerðarinnar. Orðið „skrá“ hefur unnið sér hefð í íslensku lagamáli á sviði persónuverndar sem þýðing á hugtakinu „filing system“ í ESB-tilskipuninni og reglugerðinni. Í íslenskri þýðingu reglugerðarinnar er hins vegar notað orðið „skráningarkerfi“. Það byggist á framkvæmd þýðingarmiðstöðvar utanríkisráðuneytisins sem hefur einnig við þýðingu á ESB-gerðum notað orðið skráningarkerfi í alls óskyldu samhengi, t.d. sem þýðing á „system of registries“ sem starfrækja skal samkvæmt ESB-gerðum um loftslagsmál, sbr. lög nr. 70/2012. Til að fyrirbyggja óvissu um þetta lykilhugtak í persónuvernd er í frumvarpinu áfram notað orðið „skrá“ og er þar ótvírætt átt við sama hugtak og fram kemur í 6. tölul. 4. gr. reglugerðarinnar.

6. *Ábyrgðaraðili.* Ákvæðið er samhljóða fyrri málslíð skilgreiningar 4. tölul. 4. gr. reglugerðarinnar sem er efnislega hliðstæð d-lið 2. gr. tilskipunarinnar og 4. tölul. 2. gr.

núgildandi laga. Seinni málsl. reglugerðarákvæðisins tilgreinir einnig, að sé tilgangur og aðferðir við slíka vinnslu ákveðin í lögum Sambandsins eða aðildarríkis sé heimilt að tilgreina þar ábyrgðaraðila eða sérstakar viðmiðanir fyrir tilnefningu hans. Ábyrgðaraðili er sá sem hefur ákvörðunarvald um vinnslu persónuupplýsinga, aðferð við vinnsluna, tilganginn með vinnslu þeirra og hvað sá hugbúnaður sem notaður er á að gera, svo og um að aðra ráðstöfun upplýsinganna.

Jafnvel þótt slíkur aðili feli öðrum meðferð upplýsinganna ber hann ábyrgðina, svo fremi sem hann hafi áfram ákvörðunarvaldið. Sá sem vinnur með upplýsingarnar á vegum ábyrgðaraðila er hins vegar nefndur vinnsluaðili eins og fjallað er um í næsta tölulið þessa frumvarpsákvæðis. Skilyrði þess að geta talist ábyrgðaraðili er að hafa aðildarhæfi og að geta svarað til saka vegna tiltekinnar vinnslu persónuupplýsinga fyrir dómstólum, ef svo ber undir. Bæði einstaklingar og lögpersónur geta haft aðildarhæfi í þeim skilningi sem hér er vísað til. Hópur getur ekki haft aðildarhæfi nema um sé að ræða einhvers konar samtök eða félagsskap, en krafan um aðildarhæfi er m.a. byggð á því að nauðsynlegt getur verið að leita réttarráða til að fullnægja kröfum gagnvart ábyrgðaraðila. Tilgangur með vinnslu persónuupplýsinga kann að vera skilgreindur í sérlögum og þar afmarkað nákvæmlega hvað megi gera við þær. Að því marki sem slík lög gera það hins vegar ekki fer um það samkvæmt frumvarpi þessu. Ábyrgðaraðili getur í mörgum tilvikum verið lögaðili, enda tekur frumvarpið til vinnslu af hálfu atvinnurekenda, fyrirtækja, félaga, stofnana og opinberra aðila. Rísið geta vafatilvik um hver sé persónulega ábyrgur í slíkum tilvikum, en benda má á að verði ábyrgðaraðili gjaldþrota telst þrotabú hans vera ábyrgðaraðili. Þá kemur fram í 26. gr. reglugerðarinnar að ef tveir eða fleiri ábyrgðaraðilar ákveða sameiginlega tilgang vinnslunnar og aðferðir við hana skulu þeir teljast vera sameiginlegir ábyrgðaraðilar. Þeim ber á gagnsæjan hátt, að ákveða ábyrgð hvers um sig á því að skuldbindingar samkvæmt reglugerðinni séu uppfylltar en nánari skilyrði þar um eru talin upp í reglugerðarákvæðinu. Nánari reglur um ábyrgð og skyldur ábyrgðaraðila er að finna í 23. og 24. gr. frumvarpsins.

7. *Vinnsluaðili.* Hugtakið er óbreytt frá gildandi lögum, sbr. 5. tölul. 2. gr. þeirra laga og e-lið 2. gr. tilskipunarinnar og samhljóða skilgreiningu 8. tölul. 4. gr. reglugerðarinnar. Vinnsluaðili er sá sem vinnur með persónuupplýsingar á vegum ábyrgðaraðila og er í 25. gr. frumvarpsins að finna almennar reglur varðandi þær kröfur sem hann þarf að uppfylla svo og reglur um gerð vinnslusamninga. Vinnsluaðili getur t.d. verið aðili sem sér um að þróa upplýsingakerfi eða gera við og viðhalda tölvuhugbúnaði, enda sér slíkur aðili oft jafnframt um að varðveita upplýsingarnar eða hefur með öðrum hætti aðgang að þeim. Skilyrði er að vinnslan fari fram fyrir hönd ábyrgðaraðila og byggist á ósk eða fyrirmælum hans.

8. *Samþykki skráðs einstaklings.* Skilgreining ákvæðisins á samþykki er samhljóða 11. tölul. 4. gr. reglugerðarinnar. Nokkrar orðalagsbreytingar eru gerðar frá h-lið 2. gr. tilskipunarinnar og 7. tölul. 2. gr. núgildandi laga. Þær miða að því að setja fram strangari kröfur til þess að hinn skráði hafi veitt ótvírætt og afdráttarlaust samþykki sitt, þar sem krafa er gerð um samþykki hins skráða fyrir vinnslu persónuupplýsinga. Þannig bætist við að slík viljayfirlýsing skuli vera „ótvíræð“ og birtast í „yfirlýsingu eða ótvíræðri staðfestingu hans“. Í núgildandi lögum er skilgreiningin ítarlegri en ákvæði tilskipunarinnar og tekið fram að um ræði yfirlýsingu hins skráða um að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fari fram, hvernig persónuvernd verði tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv. Þá er rétt að hafa í huga að eftir því sem persónuupplýsingar eru viðkvæmari, þeim mun ríkari kröfur eru gerðar til þess að samþykki teljist ótvírætt.

Samþykkishugtak reglugerðarinnar og frumvarpsins nær til allra þessara atriða og verður að skoðast í ljósi nýrrar sérreglu um skilyrði fyrir samþykki sem lýst er í 10. gr. frumvarpsins og 7. gr. reglugerðarinnar. Í þessum ákvæðum endurspeglast eitt af meginmarkmiðum reglugerðarinnar að auka vernd einstaklinga með setningu strangari skilyrða fyrir því að hin skráði teljist hafa gefið samþykki sitt. Þannig er fyrirtækjum skylt að setja beiðni um samþykki fram á þann hátt að hún sé auðgreinanleg frá öðrum málefnum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli. Þá er lýst rétti hins skráða til að draga samþykki sitt til baka hvenær sem er og settar fram viðmiðunarreglur um mat á því hvort samþykki sé gefið af fúsum og frjálsum vilja.

Um þetta gildir því sem fyrr sú grundvallarregla að þögn verður ekki talin jafngilda samþykki. Þá verður samþykkið að vera „upplýst“ en með því er átt við að hinn skráði viti hvað hann er

að samþykkja og hvaða afleiðingar meðferð upplýsinganna hefur eða getur haft fyrir hann. Loks þarf samþykkið að vera persónubundið en í því felst að enginn getur gefið samþykki fyrir annars hönd nema hafa til þess sérstaka heimild. Samkvæmt þessu myndi t.d. samþykki forsvarsmanna tiltekinna samtaka fyrir hönd allra félagsmanna almennt ekki vera talið gilt nema mjög sérstaklega stæði á, svo sem ef telja mætti inngöngu í slík samtök jafngilda samþykki. Þá myndi almennt verða litið svo á að samþykki lögráðamanns þurfi fyrir hönd ólögráða einstaklings. Sérreglu um þetta er þó að finna í 5. mgr. 10. gr. frumvarpsins þess efnis að þegar barni er boðin þjónusta í upplýsingasamfélaginu með beinum hætti og vinnsla persónuupplýsinga byggist á samþykki þess teljist vinnslan því aðeins lögmæt ef barnið hefur náð 13 ára aldri. Sé barnið undir 13 ára aldri telst vinnslan því aðeins lögmæt og því marki sem forsjáraðili þess heimilar samþykki. Nánar verður fjallað um þessi nýmæli tengd samþykki barna í skýringum við 10. gr. frumvarpsins.

9. *Rafræn vöktun.* Hér er byggt á sömu skilgreiningu og fram kemur í 6. tölul. 2. gr. núgildandi laga, en með lögum nr. 46/2003 voru ákvæði laga nr. 77/2000 um efnið endurskoðuð og rafræn vöktun skilgreind með nákvæmari hætti. Skýringar hér á eftir eru því að hluta árétting á þeim skýringum sem birtust með lögum nr. 46/2003. Með rafrænni vöktun er bæði átt við sjónvarpsvöktun og aðra rafræna vöktun. Undir hugtakið fellur öll rafræn upptaka mynda og hljóða, hvort sem upptökur eru varðveittar á stafrænu formi eða ekki. Hugtakið nær hins vegar ekki til allrar vöktunar, t.d. ekki þeirrar þegar hljóð eða mynd er aðeins flutt í hátalara eða á skjá en ekki varðveitt. Engu síður gilda um slíka vöktun sérstakar reglur. Samkvæmt ákvæðinu tekur hugtakið rafræn vöktun í fyrsta lagi til vöktunar sem leiðir, á að leiða eða getur leitt til vinnslu persónuupplýsinga. Til dæmis er hér átt við það þegar myndefni er safnað með aðferðum sem gera kleift að finna upplýsingar um tiltekna einstaklinga með skjótvirkum hætti. Það gæti átt við ef skráð er með kerfisbundnum hætti hvar í myndbandasafni sé að finna myndir af tilteknum einstaklingum. Með þessu er einnig átt við vöktun, sem í eðli sínu getur leitt til vinnslu persónuupplýsinga, t.d. þegar myndefni er safnað með stafrænni aðferð. Til þess að skýra þann mun sem er á sjónvarpsvöktun og annarri rafrænni vöktun má nefna það dæmi, að maður setji upp vefmyndavél og birti það sem ber fyrir linsu vélarinnar beint á vefsíðu án þess að safna myndefninu, en slíkt er dæmi um sjónvarpsvöktun. Ef einhver annar hleður hins vegar slíku myndefni á geymslumiðil, t.d. tölvudisk, getur hann talist hafa framkvæmt vinnslu persónuupplýsinga. Slíkt hlýtur þó að velta á atvikum hverju sinni, einkum því hvort unnt sé að bera kennsl á þá sem birtast á myndunum. Til rafrænnar vöktunar telst einnig tölvupóstsvöktun sem fer fram með sjálfvirkri og viðvarandi skráningu á upplýsingum um tölvupósta og tölvupóstkerfisnotkun einstakra starfsmanna.

Í 14. gr. frumvarpsins er að finna sérreglur um rafræna vöktun, samhljóða núgildandi reglum um efnið og verður nánar fjallað um skilyrði slíkrar vöktunar í skýringum um það frumvarpsákvæði.

Reglugerð ESB hefur ekki að geyma sérstök ákvæði um sjónvarpsvöktun. Slík vöktun fellur þó undir gildissvið hennar ef hún telst til rafrænnar meðferðar persónuupplýsinga, t.d. vegna varðveislu á stafrænu formi. Þá er getið um vöktun í formála hennar, en í 24. lið formálans segir að til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga ætti að ganga úr skugga um hvort slóð einstaklinga sé rakin á Netinu, m.a. hvort í kjölfarið séu notaðar vinnsluáðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf.

10. *Gerð persónusniðs.* Hugtakið er nýmæli í talningu meðal helstu hugtaka í 4. gr. reglugerðarinnar, en hefur þegar þýðingu í ýmsu tilliti í gildandi persónuverndarlöggjöf. Er m.a. fjallað um ákveðin réttindi hins skráða í 23. gr. núgildandi laga sem lýtur að viðvörunum til hins skráða við notkun persónusniða. Skilgreining frumvarpsins á gerð persónusniðs (e. *profiling*) nær til hvers kyns sjálfvirkar vinnslu 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. Skýringar á núgildandi 23. gr. lýsa nánar inntaki hugtaksins sem þar er þýtt sem „persónumynstur“. Undir hugakið fellur þannig sú aðstaða að ýmiss konar persónuupplýsingum er steipt saman til að finna hóp manna sem fellur inn í sameiginlegt mynstur að því er varðar háðurni, smekk, þarfir, hæfileika o.fl. Slíkar upplýsingar geta t.d. verið rafræn spor, svo sem persónuupplýsingar sem safnað er reglulega í

kerfi fyrir greiðslumiðlun, rafræna upplýsingaþjónustu á Netinu og þess háttar. Þá geta persónusnið orðið til úr ýmiss konar upplýsingum sem koma fram á samfélagsmiðlum á borð við Facebook, svo sem um hvar menn versla, hvað þeir kaupa og hvenær, tekjuflokka þeirra, menntun, búsetu, tómstundir, áhugamál og aldur. Ef t.d. er safnað saman upplýsingum um menn sem vinna eftir kl. 19.00, oftast en þrisvar í viku, hafa yfir 500.000 kr. í mánaðarlaun og búa í tilteknu hverfi verður til hópur sem fellur inn í mynstur sem gefur til kynna tilteknar þarfir. Mynstrið gerir t.d. líklegt að einstaklingar í hópnum vilji skipta við tiltekna þöntunarþjónustu. Þá má einnig hugsa sér notkun persónusniða við söfnun meðlima í ýmiss konar samtök, söfnun nýliða í hóp þeirra sem styrkja ýmiss konar hugsjónastarfsemi eða fyrir pólitíska áróðurs- og áhrifastarfsemi. Persónusnið eru einkum notuð við greiningu í markhópa en þau eru og notuð víðar, svo sem við töku sértækra ákvarðana, t.d. um lánveitingar.

Reglugerðin geymir ýmsar sérreglur um réttindi skráðs einstaklings í tengslum við gerð persónusniðs, þar á meðal tengslum við sjálfvirka, einstaklingsmiðaða ákvarðanatöku í 22. gr. Þá er víðað vikið að gerð persónusniða og vinnslu slíkra upplýsinga í formála reglugerðarinnar. Í 24. lið hans er tekið fram að til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga ætti að ganga úr skugga um hvort slóð einstaklinga sé rakin á Netinu, m.a. hvort í kjölfarið séu notaðar vinnsluáðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf. Þá koma fram varúðarorð í 30. lið formálans þar sem bent er á að ýmis tæki, forrit og samskiptareglur, sem einstaklingar nota, geta tengt Netauðkenni við þá, s.s. IP-tölur og svokölluð vefkökuauðkenni eða önnur auðkenni, s.s. fjarskiptatíðniauðkenningar. Þessi notkun getur skilið eftir spor sem hægt er að nota til að útbúa persónusnið um einstaklinga og bera kennsl á þá, einkum þegar sporunum er bætt við einkvæm auðkenni og aðrar upplýsingar sem berast netþjónum.

Nánnar er fjallað um réttindi skráðra samkvæmt reglugerðinni, þ.á m. andmælarétt í skýringum við það í 21. og 22. gr. frumvarpsins.

11. *Öryggisbrot við meðferð persónuupplýsinga.* Hér er tekin upp skilgreining 12. tölul. reglugerðarinnar, en nýmæli er frá gildandi tilskipun og lögum að telja öryggisbrot (e. *personal data breach*) til lykilhugtaka. Öryggisbrot hefur veigamikla þýðingu fyrir eftirlit með framkvæmd reglugerðarinnar og hefur sérstakar afleiðingar m.a. tengdar tilkynningarskyldu ábyrgðaraðila skv. 33. og 34. gr. reglugerðarinnar. Þannig tengist það sérstökum áherslum reglugerðarinnar á að leggja ríkari skyldur en tilskipunin á ábyrgðaraðila við vinnslu persónuupplýsinga og hina nýju meginreglu, öryggisregluna, sem bætist við þær fimm meginreglur sem tilskipunin hefur byggst á, og kemur fram í f-lið 1. mgr. 5. gr. reglugerðarinnar.

Samkvæmt skilgreiningunni telst öryggisbrot vera brot á öryggi sem leiðir til óviljandi eða ólögðmætrar eyðingar persónuupplýsinga eða að þær glattist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi. Í formála reglugerðarinnar er m.a. skýrður út tilgangur þess að veita þessu hugtaki sérstök réttaráhrif sem skapar sérstakar skyldur fyrir ábyrgðaraðila. Í 85. lið formálans segir m.a. að öryggisbrot við meðferð persónuupplýsinga geti, ef ekki er brugðist við því á réttan hátt og tímanlega, valdið einstaklingum efnislegu tjóni, eignatjóni eða óefnislegu tjóni, s.s. missi yfirráða yfir persónuupplýsingum um þá eða takmörkun réttinda þeirra, mismunun, auðkennisþjófnaði eða svikum, fjárhagstjóni, að notkun gerviauðkenna sé aflétt í leyfisleysi, skaða á orðstír, töpuðum trúnaði gagnvart persónuupplýsingum sem njóta verndar samkvæmt þagnarskyldu eða öðru umtalsverðu efnahagslegu eða félagslegu óhagræði fyrir viðkomandi einstakling.

Nánnar er fjallað um afleiðingar öryggisbrots í 32.-34. gr. reglugerðarinnar sem fyrr segir svo og í 27. gr. frumvarpsins og verður nánar vikið að þeim í skýringum við það frumvarpsákvæði.

Um 4. gr.

Frumvarpsákvæði þessu er ekki ætlað að breyta almennu efnislegu gildissviði laganna frá núgildandi lögum en nokkrar nýjar sérreglur hafa þó bæst við sem taka mið af ákvæðum reglugerðarinnar. Í 1. mgr. 3. gr. núgildandi laga sem byggist á 3. gr. tilskipunar ESB er mælt fyrir um að gildissviðið taki til meðferðar persónuupplýsinga sem sé rafræn í heild eða að hluta, svo og til handunninnar meðferðar ef persónuupplýsingarnar eru eða eiga að verða hluti af skrá. Er 1. mgr. þessa frumvarpsákvæðis samhljóða 1. mgr. 2. gr. reglugerðarinnar en samkvæmt því nær efnislegt gildissvið til 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. Hér hefur verið tekið upp hugtakið „sjálfvirk“ í staðinn fyrir „rafræn“ í núgildandi lögum, sem þýðing á orðinu „automated“ en því er ekki ætlað að breyta í neinu tilliti efnislegri merkingu. Þetta ber að hafa í huga þegar vísað til rafrænnar eða eftir atvikum vélrænnar vinnslu persónuupplýsinga í frumvarpi þessu eða reglum byggðum á persónuverndarlögum.

Í 1. mgr. birtist sú meginregla að öll sjálfvirk vinnsla persónuupplýsinga hvort heldur að hluta eða í heild fellur undir gildissvið laganna. Þegar aðrar aðferðir en sjálfvirk vinnsla, m.ö.o. handvirk vinnsla er notuð, er gerð krafa um að persónuupplýsingar séu eða eigi að verða hluti af skrá. Þetta er áréttað í 14. lið formála reglugerðarinnar sem mælir fyrir um að vernd einstaklinga skuli eiga við um sjálfvirka jafnt sem handvirka vinnslu persónuupplýsinga ef upplýsingarnar eru varðveittar eða ráðgert er að varðveita þær í skrá. Eins og fram kom í skýringum við 3. gr. að framan er með skrá átt við gagnasafn eða upptalningu þar sem persónuupplýsingum er komið fyrir á þann hátt að þar má á ný finna upplýsingar um einstaka menn.

Augljóst er að þegar persónuupplýsingar eru að öllu leyti varðveittar eða unnar í tölvu er vinnslan sjálfvirk. Út frá persónuverndarsjónarmiðum er mikill munur á því hvort vinnsla er sjálfvirk eða handvirk enda gefur auga leið að mun meiri vinnslumöguleikar eru með tölvutækni, sem telst sjálfvirk vinnsla í þessu samhengi. Það á t.d. við um möguleika til samtengingar, dreifingar og endurvinnslu varðveittra upplýsinga. Sú viðmiðun að meðferð persónuupplýsinga verði annaðhvort að vera sjálfvirk eða tengjast handvinnslu skrár snertir öll ákvæði frumvarpsins. Vinnsla sem aðeins er sjálfvirk að hluta til er lögð að jöfnu við vinnslu sem er sjálfvirk að öllu leyti. Því myndi vinnsla sem er að hluta til handvirk en að hluta til unnin í tölvu falla undir gildissviðið. Reglugerðin, líkt og tilskipunin veitir aðeins takmarkaða leiðsögn um mörkin milli handvirkrar vinnslu og sjálfvirkrar. Þó er tekið fram í 15. lið formálans að til að komast hjá því að alvarleg hætta skapist á því að reglur verði sniðgengnar ætti vernd einstaklinga að vera tæknilega hlutlaus og ekki háð þeim aðferðum sem notaðar eru.

Sérstakt álitaefni er að hvaða marki hljóð- og myndbandsupptökur teljast til sjálfvirkrar vinnslu. Hér eru ekki ráðgerðar breytingar frá núgildandi skipan um að hljóð- og myndbandsupptökur myndu falla undir gildissvið laganna. Sama á við um sjónvarpsvöktun ef hvorki mynd né hljóð er varðveitt heldur birtist aðeins á skjá. Í núgildandi lögum er þó byggt á því að vinnsla efnis á myndbandi eða hljóðsnældu falli ekki undir gildissvið þeirra nema hún eigi sér stað með sjálfvirkum hætti eða ef upplýsingar um efnið eru varðveittar í skrá þannig að án mikillar fyrirhafnar megi finna aftur upplýsingar um tiltekinn einstakling. Um það hvort vinnsla sé sjálfvirk er sú viðmiðun almennt lögð til grundvallar að hún geri kleift að finna í safni gagna, án mikillar fyrirhafnar, upplýsingar um tiltekinn einstakling.

Gildissvið laganna tekur til skráningar af hálfu atvinnurekenda, fyrirtækja, félaga, stofnana og til skráningar á vegum opinberra aðila. Þótt þetta sé ekki orðað í frumvarpinu eða reglugerðinni er miðað við óbreytta skipan að þessu leyti og að sama eigi við óháð því hver á í hlut. Undantekningu frá þessu er að finna í 2. mgr. 4. gr. frumvarpsins sem tilgreinir að lögin og frumvarpið gildi ekki um vinnslu einstaklings á persónuupplýsingum sem eingöngu varða einkahagi hans eða fjölskyldu hans og eru aðeins til persónulegra nota. Þessi lýsing á gildissviði kemur fram í c-lið 2. mgr. 2. gr. reglugerðarinnar og hefur 18. liður formála hennar að geyma nánari skýringar. Þar segir að reglugerðin eigi ekki við um vinnslu einstaklings á persónuupplýsingum ef hún er einungis í þágu hans sjálfs eða fjölskyldu hans og hefur þannig engin tengsl við atvinnu- eða viðskiptastarfsemi. Vinnsla, sem er einungis í þágu einstaklings eða fjölskyldu hans, getur t.d. tekið til bréfaskrifta og þess að halda skrár yfir heimilisföng, notkunar samfélagsmiðla og netnotkunar sem fram fer í tengslum við slíka vinnslu. Hins vegar er tekið fram að reglugerðin á við um ábyrgðaraðila eða vinnsluaðila sem setja fram leiðir til að vinna persónuupplýsingar í þágu einstaklings eða fjölskyldu hans.

Af þessu er ljóst að t.d. einkabréfaskipti, færsla skráa með heimilisföngum vina, ættingja o.s.frv., færsla dagbókar og meðferð upplýsinga sem tengjast tómstundamálum fellur utan gildissviðsins. Það sem úrslitum ræður er hvort vinnslan varðar aðeins hreina einkahagi eða ekki. Skilyrði er að um sé að ræða venjulegar og lögmætar athafnir, en það er nauðsynleg viðmiðun til að ákvæðið verði ekki notað til að fara í kringum önnur ákvæði laganna. Þegar vinnsla persónuupplýsinga fer fram í þágu tiltekinnar einkastarfsemi eiga ákvæði laganna hins

vegar við, jafnvel þótt hún sé ekki atvinnustarfsemi. Á það t.d. við um rannsóknarvinnu vísindamanns.

Í 3. mgr. 4. gr. frumvarpsins er sérregla um vernd persónuupplýsinga látinna manna. Í 27. lið formála reglugerðarinnar er tekið fram að hún eigi ekki við um persónuupplýsingar látinna einstaklinga en aðildarríkjunum sé heimilt að kveða á um reglur um vinnslu persónuupplýsinga þeirra. Þá er vísað til þess í 158. lið formálans í umfjöllun um vinnslu persónuupplýsinga vegna skjalavistunar að reglugerðin eigi ekki við um látna einstaklinga og í 160 gr. formálans að þótt reglugerðin nái til sagnfræðirannsókna og rannsókna í erfðafræðilegum tilgangi gildi hún ekki um látna einstaklinga.

Eins og lýst var í skýringum með 3. gr. frumvarpsins er sú leið farin að fella niður tilvísun til þess að lögin gildi jafn um persónuupplýsingar lifandi og látinna einstaklinga. Í framkvæmd laganna hefur sjaldan reynt á ágreiningsmál um vinnslu persónuupplýsinga um látna menn. Ljóst er jafnframt að ekki er unnt að uppfylla kröfur laganna um réttindi hins skráða þegar hann er látinn, s.s. um samþykki, fræðsluskyldu, andmælarétt og aðrar skyldur sem hvíla á ábyrgðaraðila. Í frumvarpi til nýrra persónuverndarlaga í Noregi sem ætlað er að innleiða reglugerðina þar í landi, eru engar sérreglur að finna um vernd persónuupplýsinga látinna manna en vísað til þess að þegar unnt er að tengja slíkar upplýsingar lifandi einstaklingum falli þær undir persónuupplýsingar hinna síðarnefndu. Í dönsku frumvarpi sama efnis er hins vegar farin sú leið að leggja til að lögin gildi í 10 ár eftir andlát hins skráða. Þá er ráðherra veitt heimild til að mæla nánar fyrir í reglugerð um lengri eða styttri tíma frá andláti.

Í frumvarpi þessu er lagt til stað að þess að falla að öllu leyti frá núgildandi skipan þar sem persónuupplýsingar látinna einstaklinga njóta verndar verði hér miðað við 5 ára tímamark eftir andlát. Áfram er ótvírætt að lögin ná til persónuupplýsinga um látna einstaklinga þegar þær tengjast lifandi einstaklingum beint eða óbeint, svo sem gæti átt við um arfgenga sjúkdóma. Hins vegar er lagt til sem fyrr segir að lögin gildi um persónuupplýsingar látinna einstaklinga í 5 eftir andlát og lengur þegar um ræðir persónuupplýsingar sem sanngarnt og eðlilegt má telja að leynt fari. Þá er til þess að líta að þegar upplýsingar um látna eru varðveittar innan um upplýsingar um lifandi einstaklinga verður oft talið óhjákvæmilegt að upplýsingar um báða hópa, hina látnu og hina lifandi, falli undir sömu öryggisráðstafanir, t.d. notkun gerviauðkenna. Hins vegar er ljóst að persónubundin réttindi einstaklings skv. III. kafla frumvarpsins falla niður við andlát, s.s. upplýsingaréttur og aðgangsréttur.

Í 4. mgr. 4. gr. frumvarpsins er lagt til að lögin og reglugerðin gildi ekki um vinnslu persónuupplýsinga sem fer fram þegar dómstólar fara með dómssvald sitt. Þótt vernd reglugerðarinnar gildi almennt m.a. um vinnslu persónuupplýsinga í starfsemi dómstóla er gert ráð fyrir því í 20. lið formála hennar að aðildarríki hafi talsvert svigrúm til að tilgreina vinnsluaðgerðir og verklagsreglur í tengslum við slíka vinnslu. Þá er tekið fram að til að standa vörð um sjálfstæði dómskerfisins við framkvæmd verkefna þess á sviði dómsmála, m.a. ákvarðanatöku, ætti valdsvið eftirlitsstjórnvalda ekki að ná til vinnslu dómstóla á persónuupplýsingum þegar þeir fara með dómssvald sitt. Mögulegt ætti að vera að fela eftirlit með slíkri vinnslu persónuupplýsinga sérstökum aðilum innan dómskerfis aðildarríkisins sem ættu einkum að tryggja að farið sé að reglum þessarar reglugerðar, efla vitund dómara um skyldur sínar samkvæmt henni og annast meðferð kvartana í tengslum við slíka gagnavinnslu.

Gildandi persónuverndarlög hafa verið túlkuð með þeim hætti að með vísan til ákvæða stjórnarskrár um þrískiptingu ríkisvalds séu því takmörk sett að hvaða marki Persónuvernd geti, sem stjórnvald, hlutast til um mál sem eru á forræði annarra sjálfstæðra handhafa ríkisvaldsins, Alþingis og dómstóla þegar þeir beita dómssvaldi sínu. Tilvísun til dómssvaldshugtaksins hér þýðir að reglan á ekki við um starfsemi dómstóla sem fellur ekki beint undir dómssvald þeirra, þar á meðal þegar um ræðir birtingu dóma á Netinu. Í úrskurði Persónuverndar frá 16. júní 2017 í máli nr. 2016/1783 varð það niðurstaðan að nafnbirting aðila dómsmáls ásamt ýmsum viðkvæmum persónuupplýsingum um hann í dómi sem birtur var á heimasíðu héraðsdómstólanna væri vinnsla persónuupplýsinga sem heyrði undir eftirlitsheimildir Persónuverndar. Vék stofnunin þá frá fyrri framkvæmd sinni um að það félli utan heimilda hennar að fjalla efnislega um ákvarðanir sem teknar væru af hálfu dómstólaráðs eða dómara um birtingu dóma. Var það rökstutt með því að þótt valdsvið stofnunarinnar gæti ekki náð til eftirlits með vinnslu dómstóla á persónuupplýsingum þegar þeir færu með dómssvald við meðferð mála fyrir dómstólunum fæli birting dóma á Netinu skv. þágildandi 22. gr. a laga nr. 15/1998 um dómstóla ekki í sér dómsathöfn sem tengdist meðferð máls. Ætti það jafnframt við þótt

ákvörðun um nafnleynd og úrfellingu persónuupplýsinga væri tekin af dómara. Slík ákvörðun lyti enda ekki að efni dómsins sjálfs heldur einungis að því hvaða upplýsingar skyldi birtar á Netinu.

Í núgildandi lögum um dómstóla nr. 50/2016 eru ákvæði um útgáfu dóma á öllum dómstigum, 20. gr. um dóma Hæstaréttar, 28. gr. um dóma Landsréttar og 38. gr. um héraðsdóma. Í öllum þessum ákvæðum eru ákvæði um að taka þurfi tillit til persónuverndarsjónarmiða, þar á meðal að héraðsdómar um viðkvæm persónuleg málefni skuli ekki gefnir út og að gæta skuli nafnleyndar í ákveðnum tilvikum í dómum á öllum dómstigum. Þá skal dómstólasýslan setja nánari reglur um útgáfu dóma og úrskurða héraðsdómstóla og Landsréttur og Hæstiréttur skulu hafa samráð við dómstólasýsluna um tilhögun dómaútgáfu.

Í 5. mgr. er ákvæði sem byggir á sambærilegum sjónarmiðum og 4. mgr. um gildissvið laganna og reglugerðarinnar gagnvart öðrum handhöfum ríkisvalds en framkvæmdarvaldshöfum og er því ætlað að festa í lög óskráðar reglur sem gilda í þessu tilliti. Þannig er lagt til að lögin nái ekki til vinnslu upplýsinga sem fer fram í tengslum við lögbundin verkefni Alþingis. Fyrirmynd að sérreglu um þetta er m.a. sótt til 3. gr. danska frumvarpsins til nýrra persónuverndarlaga. Hér er þá fyrst og fremst litið til verkefna Alþingis sem leidd eru af stjórnarskrá og eru útfærð frekar í ákvæðum laga um þingsköp nr. 55/1991. Meginverkefni Alþingis í þessu tilliti eru lagasetning, fjárstjórnarvald og eftirlit með framkvæmdarvaldinu, en þó aðeins að því leyti sem þingið sjálft og nefndir þess sinna eftirlitsstarfinu. Af ákvæðinu verður þannig ályktað að vinnsla persónuupplýsinga sem fellur undir þá starfsemi Alþingis sem ekki lýtur beint að þessum verkefnum falli undir gildissvið laganna, þar með talin birting gagna á vef Alþingis. Á slík álitamál hefur m.a. reynt í framkvæmd núgildandi laga sbr. úrskurð Persónuverndar frá 25. apríl 2017 í máli nr. 2016/1133. Þá nær gildissvið lagana og reglugerðarinnar einnig til stofnana á vegum Alþingis svo sem ríkisendurskoðunar og umboðsmanns Alþingis.

Í 6. mgr. 4. gr. er ráðgert að lögin og reglugerðin gildi 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 almannaoðryggi. Í 2. mgr. 3. gr. núgildandi laga er að finna áþekkt ákvæði sem undanskilur tilgreind ákvæði laganna frá vinnslu persónuupplýsinga sem varða almannaoðryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu. Frumvarpsákvæðið tilgreinir ekki sérstaklega landvarnir og öryggi ríkisins og er þar fylgt orðalagi d-liðar 2. mgr. 2. gr. reglugerðarinnar. Hins vegar er hér um að ræða þætti sem falla undir almannaoðryggi og er því hér ekki um efnisbreytingu að ræða.

Umrætt ákvæði reglugerðarinnar er lýst nánar í 19. lið formála hennar og m.a. vísað til þess að um vinnslu á sviði refsivörslu og í þágu almannaoðryggis skuli gilda sértækari gerð Sambandsins, nánar tiltekið 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 með öðrum lögum.

Í lokamálsgrein 4. gr. frumvarpsins er lagt til að ákvæði laganna og reglugerðarinnar skuli gilda án tillits til þess hvort starfsemi falli undir gildissvið EES-samningsins. Regla þessi er sett sem sérregla sem vikur frá a-lið 2. mgr. 2. gr. reglugerðarinnar um að hún gildi ekki um vinnslu persónuupplýsinga í starfsemi sem fellur utan gildissviðs laga Sambandsins. Ekki er talin ástæða hér til að undanskilja gildi laganna og reglugerðarinnar starfsemi sem ekki fellur undir gildissvið EES-samningsins. Auk þess er það líklegt til að skapa réttaróvissu að skera þurfi úr um hvort starfsemi heyrir undir málefnavið EES-samningsins áður en ljóst sé hvort persónuverndarlög taka til hennar. Reglugerðin hindrar ekki að veitt sé betri vernd að þessu leyti og er umrædd leið því farin hér en sami háttur er hafður á í 1. mgr. 2. gr. norska frumvarpsins til nýrra persónuverndarlaga. Jafnframt er tekið af skarið um að VII. kafli reglugerðarinnar sem fjallar um samræmt eftirlit með reglugerðinni á svæðinu og hlutverk og valdheimildir Evrópska persónuverndarráðsins geti þó ekki átt við um starfsemi sem fellur utan EES-samningsins. Þannig geta lögin eðli máls samkvæmt ekki felld undir persónuverndarráðið verkefni og valdheimildir sem lúta að vinnslu upplýsinga í slíkri starfsemi.

Um 5. gr.

Í þessari grein frumvarpsins er kveðið á um tengsl ákvæða þess og ákvæða reglugerðarinnar við önnur lög. Í 44. gr. núgildandi laga um persónuvernd og meðferð persónuupplýsinga eru áþekkar reglur og fram koma í 1. og 2. mgr. þessarar frumvarpsgreinar.

Í 1. mgr. er kveðið á um gildissvið þess gagnvart öðrum lögum. Ákvæði frumvarpsins eru viðtæk og almenns eðlis í þeim skilningi að þau taka til hvers kyns vinnslu persónuupplýsinga hvar og hvernig sem hún fer fram, með þeim frávikum sem fram koma í frumvarpinu. Af þeim sökum þykir rétt að taka fram að frumvarpið taki jafnframt til meðferðar og vinnslu slíkra upplýsinga sem fram fer samkvæmt öðrum lögum nema þau lög tilgreini annað sérstaklega. Þannig geta sérákvæði annarra laga gengið framar þessum reglum á grundvelli almennra sjónarmiða um *lex specialis*. Þó er tekið fram að sérlög verði að vera innan þess ramma sem reglugerð ESB setur, þ.e. að þau fari ekki gegn ákvæðum hennar.

Í 2. mgr. ákvæðisins er kveðið á um samspil við upplýsingalög og stjórnsýslulög. Í IV. kafla stjórnsýslulaga nr. 37/1993 er að finna sérákvæði um rétt aðila máls til aðgangs að þeim gögnum er mál hans varða. Samkvæmt þessu frumvarpsákvæði halda þessi ákvæði stjórnsýslulaga gildi sínu óháð frumvarpinu. Þá verður að ætla að gildissvið frumvarpsins taki að hluta til sömu gagna og upplýsingalög, nr. 140/2012. Grunnreglur þeirra laga eru tvenns konar. Önnur mælir fyrir um aðgang almennings að upplýsingum í vörslu stjórnvalda en hin um aðgang aðila að upplýsingum um hann sjálfan í öðrum tilvikum en þeim sem falla undir stjórnsýslulögin. Af þessu ákvæði frumvarpsins leiðir að því er ekki ætlað að takmarka rétt einstaklinga til aðgangs að gögnum samkvæmt upplýsingalögum, enda eru réttindi einstaklinga til aðgangs að persónuupplýsingum hjá stjórnvöldum almennt meiri. Þá verður einnig að líta svo á að reglur upplýsingalaga um rétt almennings til aðgangs að gögnum í vörslu stjórnvalda feli almennt í sér næga heimild til vinnslu persónugreinanlegra upplýsinga skv. 9. og 11. gr. frumvarpsins.

Í reglugerðinni er gert ráð fyrir því að í landslögum sé kveðið á um rétt almennings til aðgangs að upplýsingum í vörslu stjórnvalda. Yfirskrift 86. gr. reglugerðarinnar er vinnsla og aðgangur almennings að opinberum skjölum. Samkvæmt ákvæðinu er opinberu stjórnvaldi, opinberri stofnun eða einkaaðila heimilt að afhenda persónuupplýsingar úr opinberum skjölum, sem þau hafa í sinni vörslu vegna framkvæmdar verkefnis í þágu almannahagsmuna, í samræmi við lög aðildarríkis sem stjórnvaldið heyrir undir, til þess að samræma aðgang almennings að opinberum skjölum og réttinn til verndar persónuupplýsinga samkvæmt reglugerðinni. Frekari skýringar á samspili ákvæða hennar við löggjöf aðildarríkja um aðgang almennings að opinberum skjölum er að finna í 154. lið formála reglugerðarinnar. Þar er tekið fram að reglugerðin heimili að tekið sé mið af meginreglunni um aðgang almennings að opinberum skjölum við beitingu hennar. Telja megi að aðgangur almennings að opinberum skjölum sé í þágu almannahagsmuna. Opinberu yfirvaldi eða opinberri stofnun ætti að vera heimilt að birta almenningi persónuupplýsingar í skjölum í vörslu sinni ef kveðið er á um birtinguna í lögum aðildarríkis sem opinbera stjórnvaldið eða opinbera stofnunin heyrir undir. Slík lög ættu að samræma aðgang almennings að opinberum skjölum og endurnotkun upplýsinga frá hinu opinbera annars vegar og réttinn til verndar persónuupplýsinga hins vegar og geti því kveðið á um nauðsynlega samræmingu við réttinn til verndar persónuupplýsinga samkvæmt reglugerðinni. Tilvísunin til opinberra yfirvalda og stofnana ætti í því samhengi að taka til allra yfirvalda eða annarra stofnana sem heyra undir lög aðildarríkis um aðgang almennings að skjölum. Bent er á að tilskipun 2003/98/EB um endurnotkun upplýsinga frá hinu opinbera skerði ekki og hafi á engan hátt áhrif á umfang verndar einstaklinga með tilliti til vinnslu persónuupplýsinga samkvæmt ákvæðum laga um persónuvernd og einkum breyti hún ekki þeim skyldum og réttindum sem sett eru fram í reglugerðinni. Þá er tekið fram að sú tilskipun ætti ekki að gilda um gögn, sem enginn eða takmarkaður aðgangur er að samkvæmt reglum um aðgangsrétt til verndar persónuupplýsingum, og um hluta úr skjölum, sem eru aðgengilegir samkvæmt slíkum reglum, þegar skjalshlutarnir innihalda persónuupplýsingar og kveðið hefur verið á um í lögum að endurnotkun þeirra sé ósamrýmanleg lögum um vernd einstaklinga að því er varðar vinnslu persónuupplýsinga. Umrædd tilskipun hefur verið leidd inn í íslenskan rétt, sbr. VII. kafla upplýsingalaga.

Í 3. mgr. 5. gr. frumvarpsins er tekið fram að ákvæði reglugerðarinnar gangi framar ákvæðum laga þessara. Eins og lýst var í almennum athugasemdum hvílir þjóðréttarleg skylda á íslenska ríkinu skv. 7. gr. EES-samningsins til að innleiða texta reglugerðarinnar í heild sinni inn í íslensk lög og ekki er svigrúm til að endurskrifa ákvæði hennar eða aðlaga þau að íslenskum lögum nema þar sem reglugerðin sjálf veitir heimild til þess að ríki útfæri nánar

tiltekin ákvæði eða víki frá þeim. Þar sem nokkur lykilákvæði reglugerðarinnar eru tekin upp í frumvarpið, samhengisins vegna og til að veita ákveðna heildarmynd er mikilvægt að hafa í huga að texti reglugerðarinnar í heild sinni verður einnig gild lög og frumvarpinu er ekki ætlað að breyta ákvæðum hennar. Þannig er í raun um tvær jafnréttáár réttarheimildir að ræða, þ.e. tveir textar sem báðir eru festir í almennum lögum. Markmið ákvæðisins er að tryggja að ef svo færi að ósamræmi sé á milli ákvæða þessa frumvarps og ákvæða reglugerðarinnar eða vafi um ólíkan skilning, þá verði tryggt að ákvæði reglugerðarinnar gangi fram. Það er einnig ákveðnu í samræmi við túlkunarreglu sem gildir um stöðu þjóðréttarsamninga gagnvart almennum lögum, þ.e. að túlka beri landsrétt í samræmi við þjóðréttarskuldbindingar, þó frábrugðið að því leyti að reglugerðin sjálf er gildur lagatexti en ekki aðeins þjóðréttarskuldbinding.

Um 6. gr.

Ákvæði þetta er efnislega hliðstætt því sem stendur í 5. gr. núgildandi laga sem ber yfirskriftina tengsl við tjáningarfrelsi. Ekki er stefnt að breytingum á gildissviði þess en eins og vænta má eru tilvísanir til lagagreina og reglugerðarinnar aðrar en í núgildandi lögum. Ákvæðið sækir stoð í 85. gr. reglugerðarinnar. Þar er gert ráð fyrir skyldu aðildarríkja til að samræma samkvæmt lögum réttinn til verndar persónuupplýsinga og réttinn til tjáningar- og upplýsingafrelsis, þ.m.t. vinnslu vegna fréttamennsku og starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar. Þá er í 2. mgr. þessa reglugerðarákvæðis tekið fram að þegar um ræðir vinnslu í þágu fréttamennsku eða starfsemi fræðimanna eða listrænnar eða bókmenntalegrar tjáningar skuli aðildarríkin kveða á um undanþágur eða frávik frá II. kafla um meginreglur, III. kafla um réttindi skráðs einstaklings, IV. kafla um ábyrgðaraðila og vinnsluaðila, V. kafla um miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, VI. kafla um sjálfstæð eftirlitsyfirvöld, VII. kafla um samstarf og samræmingu og IX. kafla um vinnslu persónuupplýsinga við tilteknar aðstæður ef það er nauðsynlegt til þess að samræma réttinn til verndar persónuupplýsingum og réttinn til tjáningar- og upplýsingafrelsis. Aðildarríki hafa samkvæmt þessu ákveðið svigrúm til að víkja frá ákvæðum tiltekinna kafla og það svigrúm er nýtt eftir því sem fram kemur í frumvarpsákvæðinu. Í 53. lið formála reglugerðarinnar er varpað frekara ljósi á hvernig er rétt að háttá reglusetningu. Þar er m.a. bent á að slík undantekning ætti einkum að gilda um vinnslu persónuupplýsinga á sviði hljóð- og myndmiðlunar og í gagna- og bókasöfnum fréttamiðla. Því þurfi að setja í lög undanþágur og frávik varðandi almennar meginreglur, réttindi skráðra einstaklinga, ábyrgðaraðila og vinnsluaðila, miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana, sjálfstæð eftirlitsyfirvöld, samstarf og samræmi og gagnavinnslu við tilteknar aðstæður. Jafnframt er tilgreint að þar sem undanþágur og frávik eru mismunandi milli aðildarríkja gildi lög aðildarríkisins sem ábyrgðaraðili heyrir undir. Með tilliti til mikilvægis réttarins til tjáningarfrelsis í hverju lýðræðisþjóðfélagi sé nauðsynlegt að túlka hugtök vítt í tengslum við það frelsi, s.s. fréttamennsku.

Um rök að baki þessum undantekningum má m.a. vísa til skýringa í greinargerð með núgildandi ákvæði. Samkvæmt því er ljóst er að ýmis ákvæði frumvarpsins og reglugerðarinnar samrýmast ekki að öllu leyti sjónarmiðum um tjáningarfrelsi sem varið er í 73. gr. stjórnskrárinna og 10. gr. mannréttindasáttmála Evrópu. Markmið ákvæðisins er að vera almenn vísiregla sem felur í sér að hvenær sem á þetta reynir þarf að meta hvernig sjónarmið um persónuvernd og sjónarmið um tjáningarfrelsi vegast á og komast að niðurstöðu sem byggð er á eðlilegu jafnvægi þessara sjónarmiða. Til þess að ná slíku jafnvægi mun í framkvæmd verða að víkja að nokkru frá tilteknum ákvæðum laganna vegna þeirrar starfsemi sem hér um ræðir. Eðlilegt er að sú spurning vakni hvernig leyst verður úr slíkum árekstrum. Í því sambandi er í fyrsta lagi lögð á það áhersla að aðilar vegi slíkt og meti að nokkru sjálfir og hlýtur mikil ábyrgð að hvíla á þeim í þeim efnum. Í öðru lagi verður til leiðbeiningar afstaða Persónuverndar í einstökum málum sem undir hana eru borin eða hún tekur upp að eigin frumkvæði. Í gildistið núgildandi laga hefur Persónuvernd alloft þurft að skera úr um það hvort undanþáguákvæði 5. gr. laganna eigi við. Auk þess hefur Persónuvernd gefið út almennt álit frá 4. júlí 2005 um umfjöllun fjölmiðla um einkamálefni sem hægt er að styðjast við í slíku mati.

Þau ákvæði reglugerðarinnar sem vísað er til að gildi um persónuupplýsingar sem einvörðungu eru unnar í þágu fréttamennsku eða bókmenntalegrar eða listrænnar starfsemi eru að mestu hin sömu og lögð eru til í 3. gr. norska frumvarpsins til nýrra persónuverndarlaga, þ.e. 24. gr. um ábyrgð ábyrgðaraðila, 26. gr. um sameiginlega ábyrgðaraðila, 28. gr. um

vinnsluaðila, 29. gr. um vinnslu í umboði ábyrgðar- eða vinnsluaðila, 32. gr. um öryggi, 40. gr. um hátternisreglur, 41. gr. um eftirlit með hátternisreglum, 42. gr. um vottun, 43. gr. um vottunaraðila og 82. gr. um bætur. Einnig er tilgreint að 48. gr. frumvarpsins um refsingar og 51. gr. þess um bætur gildi um slíka vinnslu og hér um ræðir en í þeim efnum er farin sama leið og í 5. gr. gildandi laga nr. 77/2000. Þá er tilgreint, eins og í gildandi lögum, að um umrædda vinnslu gildi grunnreglurnar um að persónuupplýsingar skulu unnar með lögmætum, sanngjörnum og gagnsæjum hætti, sem og um áreiðanleika persónuupplýsinga, sbr. a- og d-liði 1. mgr. 5. gr. reglugerðarinnar. Ljóst er að 85. gr. reglugerðarinnar veitir aðildarríkjum talsvert svigrúm til að kveða á um undanþágur frá ákvæðum reglugerðarinnar. Er nokkuð breytilegt hvernig þær heimildir eru nýttar t.d. í norrænum frumvörpum um efnið, en sem fyrr segir er þetta frumvarpsákvæði áþekkt þeirri leið sem farin er í Noregi og felur ekki í sér verulegar breytingar frá núgildandi lögum.

Tiltekin ákvæði frumvarpsins um aðgang að upplýsingum geta vakið spurningar um skörun við rétt blaðamanna til að leyna því hvaðan upplýsingar eru fengnar. Staðfest er í framkvæmd íslenskra dómstóla og Mannréttindadómstóls Evrópu að blaðamenn þurfi ekki að gefa upp heimildamenn sína nema sérstaklega standi á, sbr. einkum ákvæði 119. gr. laga um meðferð sakamála nr. 88/2008. Því verður upplýsingarétti hins skráða ekki beitt ef það skerðir þessi réttindi nema alveg sérstaklega standi á. Sú skylda sem ábyrgðaraðila er lögð á herðar til að láta í té almenna vitneskju um vinnslu persónuupplýsinga er hins vegar svo almenn og takmörkuð að hún veldur ekki vandkvæðum í þessu sambandi.

Varðandi ákvæði um flutning persónuupplýsinga úr landi verður að hafa í huga að slíkt getur t.d. gerst á netinu eða í gegnum aðrar alþjóðlegar upplýsingaveitur, eins og með því að þær eru birtar opinberlega, svo sem í ævisögu, í kvikmynd eða í tímariti sem keypt er hér á landi og tekið með til annars lands. Öll þessi tilvik eiga það sammerkt að tengjast starfi fjölmiðla eða bókmenntalegri og/eða listrænni tjáningu.

Um 7. gr.

Frumvarpsákvæðið kemur í stað 6. gr. gildandi laga um landfræðilegt gildissvið sem er byggt á samsvarandi ákvæði 7. gr. tilskipunarinnar. Reglugerðin breytir reglum um landfræðilegt gildissvið frá tilskipuninni. Felst meginbreytingin í því að gildissviðið er víkkað og nær nú til fyrirtækja með staðfestu utan sambandsins þegar vinnsla lýtur að boði um vörur eða þjónustu til borgara innan sambandsins, án tillits til þess hvort ábyrgðaraðili notar tæki og búnað sem er í einhverju sambandsríkjanna. Í 3. gr. reglugerðarinnar er fjallað um landfræðilegt gildissvið og er 7. gr. frumvarpsins hliðstæð því ákvæði nema að því leyti að vísað er til Evrópska efnahagssvæðisins.

Almenna reglan um landfræðilegt gildissvið birtist í 1. mgr. 3. gr. um að lögin gildi um vinnslu persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila á svæðinu óháð því hvort vinnslan sjálf fer fram þar. Hið rýmkaða gildissvið birtist í 2. mgr. ákvæðisins sem mælir fyrir um að lögin gildi um vinnslu ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu á svæðinu, á persónuupplýsingum um skráða einstaklinga innan svæðisins þegar vinnslustarfsemin tengist því annars vegar að bjóða þessum skráðu einstaklingum á svæðinu vöru eða þjónustu, án tillits til þess hvort það er gert gegn greiðslu, og hins vegar því að hafa eftirlit með hegðun einstaklinga að svo miklu leyti sem hún á sér stað innan Sambandsins. Þegar aðstæður skv. 2. mgr. eru uppi skal ábyrgðaraðili eða vinnsluaðili tilnefna fulltrúa sinn innan Evrópska efnahagssvæðisins eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu, með þeim undantekningum sem leiða af 27. gr. reglugerðarinnar. Gilda þá ákvæði laganna varðandi ábyrgðaraðila eða vinnsluaðila um þann fulltrúa samkvæmt nánari fyrirmælum 27. gr. reglugerðarinnar.

Í 22.-24. lið formála reglugerðarinnar er að finna frekari skýringar á ákvæði 3. gr. hennar um landfræðilegt gildissvið. Er áréttað í 22. lið formálans að hvers kyns vinnsla persónuupplýsinga í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila sem hefur staðfestu í Sambandinu ætti að fara fram í samræmi við ákvæði reglugerðarinnar án tillits til þess hvort vinnslan sjálf fer fram í Sambandinu. Með staðfestu er átt við virka og raunverulega starfsemi með föstu fyrirkomulagi. Lögákveðið rekstrarform slíks fyrirkomulags, hvort sem um er að ræða útibú eða dótturfélag með réttarstöðu lögaðila, ræður ekki úrslitum að því er þetta varðar.

Þá er vikið að markmiði þess að víkka gildissvið reglugerðarinnar í 23. lið, en það er að tryggja að einstaklingar séu ekki sviptir þeirri vernd sem þeir njóta samkvæmt reglugerðinni með vísan til þess að ábyrgðaraðilinn sé utan svæðisins. Á þeirri forsendu hvílir því það nýmæli að vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga þar fellur undir reglugerðina ef vinnslustarfsemin tengist því að bjóða hinum skráðu vörur eða þjónustu, án tillits til þess hvort það er gegn greiðslu. Álitamál geta vaknað um það hvenær sú aðstaða er uppi. Til að ákvarða hvort slíkur ábyrgðaraðili eða vinnsluaðili bjóði skráðum einstaklingum á svæðinu vörur og þjónustu segir í þessum lið formálans að ganga þurfi úr skugga um hvort ljóst sé að ábyrgðaraðilinn eða vinnsluaðilinn hafi í hyggju að bjóða skráðum einstaklingum þjónustu í einu eða fleiri af aðildarríkjum Sambandsins. Aðgangurinn einn og sér að vefsetri ábyrgðaraðila, vinnsluaðila eða milliliðar í Sambandinu, netfangi hans eða öðrum upplýsingum um hvernig megi nálgast viðkomandi, eða notkun tungumáls, sem almennt er notað í þriðja landinu þar sem ábyrgðaraðili hefur staðfestu, nægir almennt ekki til að staðfesta að um slíka fyrirætlan sé að ræða. Því geta þættir eins og að nota tungumál eða gjaldmiðil, sem er almennt notaður í einu eða fleiri aðildarríkjum, möguleikinn á að panta vörur og þjónustu á því tungumáli og að nefna viðskiptavinum eða notendum í Sambandinu gert það ljóst að ábyrgðaraðili hafi í hyggju að bjóða skráðum einstaklingum þar vörur eða þjónustu.

Í 24. lið formála reglugerðarinnar er varpað ljósi á hvernig vinnsla ábyrgðaraðila eða vinnsluaðila, sem ekki hefur staðfestu í Sambandinu, á persónuupplýsingum um skráða einstaklinga, sem þar eru staddir, fellur undir reglugerðina ef hún tengist því að vakta hegðun hinna skráðu, að því marki sem slík hegðun á sér stað innan Sambandsins. Til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga þarf að ganga úr skugga um hvort slóð einstaklinga sé rakin á Netinu, m.a. hvort í kjölfarið séu notaðar vinnsluaðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf.

Í 3. mgr. 7. gr. frumvarpsins er lýst áhrifum þess að ábyrgðaraðili eða vinnsluaðili eigi ekki staðfestu hér á landi, Evrópska efnahagssvæðinu eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu en þá skal hann tilnefna fulltrúa sinn innan svæðisins. Gilda þá ákvæði laganna og reglugerðarinnar um ábyrgðaraðila eða vinnsluaðila um þann fulltrúa samkvæmt nánari fyrirmælum sem lýst er í 27. gr. reglugerðarinnar.

Loks má geta niðurlagsákvæðis 3. gr. reglugerðarinnar sem mælir fyrir um að hún skuli gilda um vinnslu persónuupplýsinga af hálfu ábyrgðaraðila sem ekki hefur staðfestu innan Sambandsins en þó á stað þar sem lög aðildarríkis gilda samkvæmt þjóðarétti. Í 25. lið formálans eru tekin dæmi af því sem hér gæti fallið undir. Þar er tekið fram að þegar lög aðildarríkis gilda í krafti þjóðaréttar ætti reglugerðin einnig að gilda um ábyrgðaraðila sem hefur ekki staðfestu í Sambandinu, svo sem í sendiskrifstofu eða ræðisstofnun aðildarríkis.

Um 8. gr.

Þessi grein er lykilákvæði um þær meginreglur sem gilda um vinnslu persónuupplýsinga. Hún kemur í stað 7. gr. núgildandi laga sem er efnislega samsvarandi 6. gr. tilskipunar ESB. Frumvarpsákvæðið á beina fyrirmynd í 5. gr. reglugerðarinnar og vísar einnig til þeirrar greinar til að undirstrika að full efnisleg samsvörun sé hér á milli.

Í ákvæðinu birtast þær meginreglur sem hafa um langt skeið verið hornsteinar persónuverndarlöggjafarinnar í tengslum við vinnslu persónuupplýsinga. Þetta eru nánar tiltekið lögmætisreglan, tilgangsreglan, meðalhöfsreglan, áreiðanleikareglan og varðveislureglan. Þau nýmæli sem fólgin eru í reglugerðinni og frumvarpsákvæði þessu lúta einkum að 6. tölul. 1. mgr. sem festir í sessi svokallaða öryggisreglu svo og 2. mgr. ákvæðisins sem mælir fyrir um svokallaða ábyrgðarskyldu ábyrgðaraðila.

Verður nú nánar lýst inntaki hverrar meginreglu, eins og þeim hefur verið beitt í framkvæmda núgildandi laga og þar á eftir vikið að nýmælum ákvæðisins.

Í 1. tölul. er mælt fyrir um að persónuupplýsingar skuli unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart hinum skráða. Í 39. lið formála reglugerðarinnar er tekið fram til frekari skýringar að einstaklingum ætti að vera ljóst þegar persónuupplýsingum um þá er safnað, þær notaðar, skoðaðar eða unnar á annan hátt að hvaða marki upplýsingarnar séu eða muni verða unnar. Meginreglan um gagnsæi krefjist þess að hvers kyns upplýsingar og

samskipti, sem tengjast vinnslu þessara persónuupplýsinga, séu auðveldlega aðgengileg og auðskiljanleg og á skýru og einföldu máli. Sú meginregla eigi einkum við um upplýsingar til skráðra einstaklinga um það hver ábyrgðaraðilinn er og tilganginn með vinnslunni, frekari upplýsingar til að tryggja sanngjarna og gagnsæja vinnslu gagnvart viðkomandi einstaklingum og rétt þeirra til að fá staðfestingu og tilkynningu um vinnslu á persónuupplýsingum um sig. Samkvæmt þessu birtist umrædd meginregla í ákvæðum frumvarpsins um upplýsinga- og aðgangsrétt einstaklinga. Í því sambandi segir í fyrirnefndu ákvæði formálans að gera ætti einstaklingum ljósa áhættu, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga og hvernig þeir geta neytt réttar síns í tengslum við slíka vinnslu. Þá er í 40. lið formálans tekið fram að til að vinnsla persónuupplýsinga teljist lögmæt verði hún að fara fram með samþykki hlutaðeigandi skráðs einstaklings eða á einhverjum öðrum lögmætum grundvelli, sem mælt er fyrir um í reglugerðinni þ. á m. þegar hún er nauðsynleg til að fara að ákvæðum um lagaskyldu sem hvílir á ábyrgðaraðilanum eða vegna framkvæmdar samnings sem hinn skráði á aðild að eða með hliðsjón af ráðstöfunum sem eru gerðar að beiðni hans áður en samningur er gerður. Áskilnaður um lögmæti vinnslu felur ekki einungis í sér skírskotun til skráðra lagareglna heldur einnig til óskráðra grundvallarreglna um persónuvernd og friðhelgi einkalífs. Vinnsla telst ólögmæt ef tilgangur hennar fær ekki samrýmst almennum sjónarmiðum um persónuvernd. Í þessu sambandi má benda á 41. lið formála reglugerðarinnar þar sem tekið er fram að þegar vísað er til lagaheimildar í reglugerðinni sé ekki endilega gerð sú krafa að um ræði sett lög sett af þjóðþingi hlutaðeigandi aðildarríkis. Slíkur lagagrundvöllur eigi þó að vera skýr og nákvæmur og beitingin fyrirsjáanleg þeim sem falla þar undir, eins og krafist er í dómaframkvæmd Evrópuðómstólsins og Mannréttindadómstóls Evrópu. Hér ber að hafa í huga að í íslenskum rétti hafa á grundvelli lögmætisreglu verið gerðar allstrangar kröfur til þess að takmarkanir á réttindum manna, þar með talin friðhelgi einkalífs, verði að eiga stoð í settum lögum en ekki t.d. stjórnvaldsfyrirmælum, sbr. til dæmis dóm Hæstaréttar frá 27. nóvember 2003, nr. 151/2003 (gagnagrunnsmál).

Tilgangsreglan í 2. tölul. 1. mgr. þessa frumvarpsákvæðis felur í sér að persónuupplýsingar séu fengnar í skýrt tilgreindum, lögmætum og málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Með áskilnaði um að tilgangurinn sé skýr er átt við að hann skuli vera nægjanlega vel skilgreindur og afmarkaður til að vinnslan sé gagnsæ og auðskilin og komið í veg fyrir svo víðtæka tilgreiningu tilgangs að undir hann megi fella næstum hvað sem er, enda samrýmst slíkt ekki sjónarmiðum um persónuvernd. Því viðkvæmari persónuupplýsingar sem unnið er með og því meiri afleiðingar sem notkun þeirra getur haft í för með sér þeim mun mikilvægara er að tilgangurinn sé skýrt afmarkaður. Auk þess er líklegra að hinn skráði veiti réttar og viðeigandi upplýsingar ef hann þekkir tilgang vinnslunnar. Jafnframt verður auðveldara fyrir hann að gæta eigin hagsmuna, t.d. að krefjast þess að upplýsingum verði eytt. Þá ber að hafa í huga að varla er unnt að ákveða hvaða lágmarksupplýsingar vinna þarf með fyrr en tilgangurinn er skýr og hlýtur val persónuupplýsinga að ráðast af því í hvaða samhengi á að nota þær. Loks skal tilgangur vinnslu vera málefnalegur. Með því er átt við að ekki má vinna með upplýsingar í hvaða tilgangi sem er, jafnvel þótt hann sé yfirlýstur og skýr. Við mat á þessu verður m.a. að skoða hvort markmiðið sé í samræmi við eðli þeirrar starfsemi sem ábyrgðaraðili hefur með höndum. Samkvæmt þessu ákvæði má ekki vinna með persónuupplýsingar í tilgangi sem er ósamrýmanlegur þeim tilgangi sem var með söfnun þeirra. Sérsjónarmið gilda þó um frekari vinnslu í sagnfræðilegum, tölfraðilegum eða vísindalegum tilgangi sem telst ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt. Slíkar rannsóknir eru tíðum þess eðlis að rökstyðja má að ávinningurinn af nýrri vinnslu geti verið meiri en óhagræðið fyrir þá einstaklinga sem í hlut eiga. Niðurstaða slíks hagsmunamats hlýtur þó að verða önnur þegar tillit til hins skráða telst af einhverjum ástæðum vega þyngra en hagsmunir samfélagsins af því að fá niðurstöðu rannsóknar. Er og ljóst að því viðkvæmari sem þær upplýsingar eru sem unnið er með þeim mun meiri kröfur verður að gera til mikilvægis almannahagsmuna. Við slíkt hagsmunamat vega þungt þær ráðstafanir sem gerðar eru til að draga úr hugsanlegu óhagræði fyrir hinn skráða. Dæmi um slíkar ráðstafanir geta verið ýmsar öryggisráðstafanir, t.d. dulkóðun upplýsinga.

Meðalhöfsreglan endurspeglar í 3. tölu. 1. mgr. þessa ákvæðis frumvarpsins og skarast nokkuð við tilgangsregluna. Hún miðast það sem kallað er „lágmarkun gagna“ og felur í sér að persónuupplýsingar ættu að vera nægilegar, viðeigandi og takmarkaðar við það sem nauðsynlegt er miðað við tilganginn með vinnslunni. Þetta krefst þess einkum að geymslutími

persónuupplýsinganna sé takmarkaður við algjört lágmark, eins og lýst er í 39. lið formála reglugerðarinnar. Því aðeins ætti að vinna persónuupplýsingar að ekki sé unnt að ná tilganginum með vinnslunni á annan aðgengilegan hátt. Í 39. lið formála reglugerðarinnar kemur fram að til að tryggja að persónuupplýsingar séu ekki varðveittar lengur en nauðsynlegt er ætti ábyrgðaraðilinn að setja tímafresti varðandi eyðingu eða reglulega endurskoðun þeirra. Með því að áskilja að upplýsingarnar séu nægjanlegar og viðeigandi er átt við að eðli þeirra og efni skuli þjóna yfirlýstum tilgangi. Ákvæðið mælir í raun fyrir um að vinnsla ábyrgðaraðila sé háð hlutfallssjónarmiði, sem er kjarni meðalhófsreglunnar, en með því er átt við að hún megi ekki ganga lengra en þörf krefur til að ná því markmiði sem ábyrgðaraðila er heimilt að ná.

Í 4. tölul. 1. mgr. frumvarpsins birtist áreiðanleikareglan sem gerir þá kröfu að persónuupplýsingar séu áreiðanlegar og uppfærðar eftir þörfum. Persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal eyða eða leiðrétta án tafar. Í 39. lið formála reglugerðarinnar er áréttað að gera verði hóflegar ráðstafanir til að tryggja að óáreiðanlegar persónuupplýsingar verði leiðréttaðar eða þeim eytt. Skylda til að uppfæra upplýsingar á að tryggja að leiðréttaðar séu upplýsingar sem reynast úreltar, sé þess þörf. Í vissum tilvikum mun ábyrgðaraðili geta frestað leiðréttingu. Hversu fljótt leiðrétting þarf að eiga sér stað ræðst bæði af efni þeirra upplýsinga sem unnið er með og því hvernig þær eru notaðar. Stundum má fresta leiðréttingu en sé t.d. um að ræða vinnslu rangra upplýsinga sem geta leitt til tjóns fyrir hinn skráða skal leiðrétting eiga sér stað tafarlaust.

Í 5. tölul. er kveðið á um varðveisluregluna sem vísar til sérstaklega til þess á hvaða formi persónuupplýsingar eru varðveittar. Mælt er fyrir um að þær skuli varðveittar í því formi að ekki sé unnt að bera kennsl á skráða einstaklinga lengur en þörf krefur miðað við tilgang vinnslu. Upplýsingar má með öðrum orðum ekki varðveita í persónugreinanlegu formi lengur en nauðsyn krefur í ljósi þess tilgangs sem var með söfnun þeirra og vinnslu. Ekki verður gefið einhlítt svar við því hversu lengi varðveita megi upplýsingar í persónugreinanlegu formi þar sem slíkt hlýtur að ráðast af aðstæðum hverju sinni. Persónuvernd getur sett almennar reglur og gefið leiðbeiningar um það hve lengi ábyrgðaraðili skuli að jafnaði varðveita persónugreinanlegar upplýsingar miðað við tegund vinnslu. Sá fyrirvari er hér gerður að 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. Í 50. lið formála reglugerðarinnar er tekið fram að frekari vinnsla í þessum tilgangi teljist til samrýmanlegra og lögmætra vinnsluaðgerða.

Loks er kveðið á um þá almennu meginreglu í 6. tölul. að persónuupplýsingar skuli unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt. Eins og gildir um aðrar meginreglur endurspeglar þessi krafa víða í ákvæðum frumvarpsins og reglugerðarinnar. Þannig er í 39. lið formálans áréttað að vinnsla persónuupplýsinga ætti að vera með þeim hætti að viðeigandi öryggi sé til staðar og trúnaður um upplýsingarnar sé tryggður, m.a. að komið sé í veg fyrir óheimilan aðgang eða notkun á persónuupplýsingum og þeim búnaði sem notaður er við vinnsluna.

Í 2. mgr. 8. gr. frumvarpsins birtist reglan um ábyrgðarskyldu en í henni er áréttað að ábyrgðaraðili beri ábyrgð á því að vinnsla persónuupplýsinga uppfylli þær kröfur sem leiða af meginreglum 1. mgr. sömu greinar eins og þær eru útfærðar í ákvæðum reglugerðarinnar. Þá er tekið af skarið um að hann þarf að geta sýnt fram á að þessi skilyrði séu uppfyllt. Þessi regla endurspeglar þá áherslu reglugerðarinnar umfram það sem ráðið verður af tilskipun ESB að hún leggur almennt ríkari skyldur á þá sem vinna með persónuupplýsingar, einkum um ráðstafanir til að tryggja öryggi við vinnsluna og tæknilegar ráðstafanir sem gera þarf í því skyni. Þessi skylda birtist skýrt í 24. -26. gr. reglugerðarinnar og 23. og 24. gr. frumvarpsins. Þá hvílir skylda ábyrgðaraðilans til að tilkynna um öryggisbrot til Persónuverndar skv. 32. gr. reglugerðarinnar og 27. gr. frumvarpsins á þessari frumforsendu, sbr. einnig 85. lið í formála reglugerðarinnar. Verður nánar vikið að þeirri skyldu í skýringum með 27. gr. frumvarpsins.

Um 9. gr.

Þessi grein frumvarpsins geymir almennar reglur um heimildir fyrir vinnslu persónuupplýsinga og er samhljóða 1. mgr. 6. gr. reglugerðarinnar. Reglugerðinni er ekki ætlað að breyta efnislega reglum 7. gr. tilskipunar ESB og 8. gr. núgildandi laga um heimildir til vinnslu almennra persónuupplýsinga. Því eiga þær skýringar sem birtust í greinargerð með 8.

gr. nógildandi laga við að mestu og verður kjarni þeirra dreginn saman hér, auk tilvísana til formála reglugerðarinnar eftir því sem við á. Í því sambandi skal þess getið að framsetningu heimildanna hefur verið breytt en tveimur liðum í upptalningu gildandi laga á þeim hefur verið steipt saman eins og nánar er rakið hér á eftir

Fyrst má áréttá að af ákvæðinu leiðir að vinnsla er óheimil nema uppfyllt sé eitthvert þeirra sex skilyrða sem þar eru talin upp. Að undanskilinni reglu 1. tölul. eiga reglurnar allar það sameiginlegt að vinnsla er óheimil nema hún sé *nauðsynleg* vegna nánar tilgreindra hagsmuna, en það endurspeglar meginregluna um meðalhóf sem lýst var í skýringum á 8. gr. frumvarpsins. Það ræðst hins vegar af aðstæðum hverju sinni hvort tiltekin vinnsla persónuupplýsinga teljist nauðsynleg og er ábyrgðaraðila falið visst mat í þeim efnum. Mat á nauðsyn vinnslu ræðst af eðli hennar, en meta þarf hvern áfanga vinnslunnar sjálfstætt. Þannig þarf að meta sjálfstætt hvort nauðsynlegt sé að safna upplýsingum, skrá þær, miðla þeim, samkeyra þær o.s.frv. Matið ræðst og af eðli og efni þeirra upplýsinga sem unnið er með. Meðal annars skiptir máli hvort um sé að ræða upplýsingar um hrein einkamálefni einstaklinga, svo sem um félagsleg vandamál, hjónaskilnaði og samvistarslit, ættleiðingar og annað sem sanngjarnt er og eðlilegt að fari leynt, en þá ber að gera ríkar kröfur að því er varðar nauðsyn vinnslunnar. Hafa ber í huga að auknar kröfur eru gerðar til vinnslu viðkvæmra persónuupplýsinga eins og nánar verður fjallað um í skýringum við 11. gr. frumvarpsins.

Í 1. tölul. segir að vinna megi með persónuupplýsingar ef hinn skráði hafi gefið samþykki sitt fyrir vinnslunni í þágu eins eða fleiri tiltekinna markmiða. Hér er átt við samþykki í skilningi 8. tölul. 3. gr. frumvarpsins. Sú breyting er hér á orðalagi frá gildandi lögum að ekki er tekið fram að samþykki skuli vera „ótvírætt“. Ekki er stefnt að því að slaka á kröfum að þessu leyti. Þvert á móti er það þáttur í skilgreiningu reglugerðarinnar og frumvarpsins á samþykkishugtakinu að það skuli vera ótvírætt. Það á ávallt við og því ekki þörf á að tilgreina það hér sérstaklega. Þá setur reglugerðin fram ítarlegri reglur og strangari kröfur til þess hvernig samþykki er fengið, auk þess sem fyrirtækjum er skylt samkvæmt henni að gera skilmála fyrir samþykki gegnsæri og aðgengilegri og hafa þá á skiljanlegu máli, eins og nánar verður rakið í skýringum með 10. gr. frumvarpsins. Vinnsla byggð á samþykki verður meðal annars, eins og ávallt á við þegar unnið er með persónuupplýsingar, að samrýmast vönduðum vinnsluháttum, fara fram í yfirlýstum, skýrum og málefnalegum tilgangi og má ekki ganga lengra en nauðsyn krefur. Þegar Persónuvernd metur hvort kröfunum til samþykkis sé fullnægt tekur hún bæði mið af þeirri vinnsluáðferð sem viðhöfð er og eðli þeirra upplýsinga sem unnið er með. Samþykki þarf að vera frjálst og óháð og myndi ekki teljast vera það þegar einstaklingur þarf að samþykkja tiltekna vinnslu um sig til að geta fengið þjónustu. Dæmi af þeim toga væri ef einstaklingur þarf að samþykkja að fá sendan markaðssetningarpóst til að geta keypt vöru, enda ljóst að markaðssetningarpósturinn er ekki nauðsynlegur til að geta veitt þjónustuna. Þá er vert að benda á að stjórnvöld geta sjaldnast byggt á samþykki, nema í undantekningartilvikum þegar samþykki hefur engin áhrif á veitingu þjónustu eða réttindi manna.

Í 2. tölul. kemur fram að vinnsla er heimil sé hún 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. Af þessu ákvæði leiðir að í tengslum við efndir samnings við hinn skráða má viðhafa nauðsynlega vinnslu, svo sem á pöntunum, reikningum, kvittunum o.s.frv. Það er skilyrði að hinn skráði sé aðili samnings. Samningur milli ábyrgðaraðila og t.d. vinnuveitanda hins skráða getur þar með ekki orðið grundvöllur vinnslu upplýsinga um hinn skráða. Undir ákvæðið fellur einnig sú aðstaða þegar vinnsla er nauðsynleg til að undirbúa gerð samnings.

Samkvæmt 3. tölul. er vinnsla persónuupplýsinga heimil sé hún nauðsynleg til að fullnægja lagaskyldu sem hvílir á ábyrgðaraðila. Með lagaskyldu er átt við hvers konar skyldu sem leiðir af lögum í rúmri merkingu, þ.e. bæði lögum og stjórnvaldsfyrirmælum settum á grundvelli þeirra. Undir hugtakið falla einnig skyldur samkvæmt dómi eða stjórnvaldsúrskurði. Hins vegar falla samningsskyldur ekki hér undir.

Samkvæmt 4. tölul. er vinnsla persónuupplýsinga heimil sé hún nauðsynleg til að vernda brýna hagsmuna hins skráða eða annars einstaklings. Um slíkt getur t.d. verið að ræða sé hinn skráði, vegna sjúkdóms, fjarveru eða af öðrum samsvarandi ástæðum, ófær um að veita samþykki sitt. Sama á við sé vinnsla upplýsinga um hinn skráða svo áriðandi að hún geti ekki beðið þann tíma sem það tekur að afla slíks samþykkis. Af skírskotun til brýnna hagsmuna leiðir að vinnslan verður að tengjast hagsmunum sem hafa grundvallarþýðingu fyrir hinn skráða. Það gæti t.d. átt við þegar hinn skráði getur, vegna sjúkdóms eða fjarveru, ekki samþykkt vinnslu

sem mundi forða honum frá verulegu fjárhagstjóni eða öðrum skaða. Í nágildandi ákvæði er aðeins vísað til hins skráða, en hér bætist við tilvísun til annars einstaklings. Í 46. lið formála reglugerðarinnar er bent á að vinnsla persónuupplýsinga sé lögmæta ef hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir líf skráðs einstaklings eða annars einstaklings. Vinnsla persónuupplýsinga á grundvelli brýnna hagsmuna annars einstaklings ætti að meginreglu til aðeins að fara fram þegar greinilegt er að hún getur ekki byggst á öðrum lagagrundvelli. Sumar tegundir vinnslu geta bæði þjónað mikilvægum almannahagsmunum og brýnum hagsmunum skráðs einstaklings, t.d. þegar vinnsla er nauðsynleg í mannúðarskyni, s.s. við að fylgjast með farsóttum og útbreiðslu þeirra eða bregðast við neyðarástandi sem kallar á mannúðaraðstoð, einkum þegar um er að ræða náttúruhamfarir eða stóráföll af mannavöldum.

Í 5. tölul. kemur fram að vinnsla persónuupplýsinga er heimil sé hún nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds. Í þessum lið sameinast tveir töluliðir sem standa í 5. og 6. tölul. 1. mgr. 8. gr. nágildandi laga. Um fyrra atriðið gildir að viðkomandi verkefni þarf að vera unnið í almannabágu, þ.e. hafa þýðingu fyrir breiðan hóp manna. Þetta gæti t.d. átt við um vinnslu sem á sér stað í sagnfræðilegum, tölfræðilegum eða vísindalegum tilgangi. Sama á við um vinnslu sem á sér stað í upplýsingakerfi réttarkerfisins sem ætlað er að veita almenningi upplýsingar um löggjöf, dómaframkvæmd o.s.frv. Vinnsla getur talist fara fram í þágu almannahagsmuna þótt hún fram ekki fram á vegum hins opinbera svo fremi hún þjóni hagsmunum breiðs hóps manna. Þótt vinnsla eigi sér stað í fjárhagslegu augnamiði útilokar það ekki að hún geti verið í þágu almannahagsmuna. Í síðara atriðinu er vísað til þess að vinnsla sé nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili fer með. Ákvæðið tekur meðal annars til vinnslu upplýsinga á vegum stjórnvalda sem tengist meðferð opinbers valds. Með því er fyrst og fremst átt við töku stjórnvaldsákvæðana. Jafnframt mundi önnur vinnsla sem telst til stjórnsýslu, svo sem við opinbera þjónustustarfsemi, alla jafna falla hér undir. Hafi meðferð opinbers valds verið falin þriðja manni með þjónustusamningi eða lögheimiluðu ytra valdframsali, leiðir af ákvæðinu að þessi þriðji maður getur viðhaft nauðsynlega vinnslu á upplýsingum við framkvæmd þeirrar stjórnsýslu.

Loks er tilgreint í 6. tölul. þessa frumvarpsákvæðis að vinnsla persónuupplýsinga sé heimil sé hún 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. Hér er vikið nokkuð frá orðalagi 7. tölul. 1. mgr. 8. gr. nágildandi laga og m.a. vísað til sérstakra sjónarmiða þegar barn á í hlut. Ákvæðið á ekki við nema ábyrgðaraðili hafi viðhaft ákveðið mat, þ.e. á því hvort hagsmunir hins skráða af því að vinnslan fari ekki fram vegi þyngra en þeir hagsmunir sem mæla með vinnslunni. Ekki er nauðsynlegt að um sé að ræða hagsmuni ábyrgðaraðila eða þess þriðja manns sem tekur við upplýsingunum og því getur ákvæðið átt við þótt um hagsmuni annarra sé að ræða. Í 47. lið formála reglugerðarinnar er því lýst að lögmætir hagsmunir ábyrgðaraðila, þ.m.t. hagsmunir ábyrgðaraðila sem fá persónuupplýsingarnar í hendur, eða þriðja aðila geta verið gild vinnsluheimild að því tilskildu að hagsmunir eða grundvallarréttindi og frelsi hins skráða vegi ekki þyngra, að teknu tilliti til eðlilegra væntinga skráðra einstaklinga á grundvelli tengsla þeirra við ábyrgðaraðilann. Nefnt er það dæmi um lögmæta hagsmuni ábyrgðaraðila að tiltekin tengsl sem máli skipta séu milli skráðs einstaklings og ábyrgðaraðilans svo sem í tilvikum þar sem hinn skráði er viðskiptavinur ábyrgðaraðilans eða í þjónustu hans. Hvað sem öðru líði þurfi að meta af kostgæfni hvort um lögmæta hagsmuni sé að ræða, m.a. hvort skráður einstaklingur geti, þegar söfnun persónuupplýsinga fer fram og í samhengi við hana, haft gilda ástæðu til að ætla að vinnsla muni fara fram í þeim tilgangi. Hagsmunir hins skráða og grundvallarréttindi hans gætu einkum gengið framar hagsmunum ábyrgðaraðila af vinnslu persónuupplýsinga þegar hún fer fram við aðstæður þar sem skráðir einstaklingar hafa ekki ástæðu til að ætla að um frekari vinnslu verði að ræða. Auk þess segir í umræddum lið formála reglugerðarinnar að vinnsla persónuupplýsinga, sem er beinlínis nauðsynleg í þeim tilgangi að koma í veg fyrir svik, teljist einnig til lögmætra hagsmuna hlutaðeigandi ábyrgðaraðila gagna. Þá megi líta svo á að vinnsla persónuupplýsinga vegna beinnar markaðssetningar sé í þágu lögmætra hagsmuna.

Nýmæli er að vísa til þess að það hafi áhrif á hagsmunamatið ef hinn skráði sé barn. Reglugerðin skilgreinir ekki á einum stað hvar eða hvernig eigi að líta sérstaklega til réttinda barna, né heldur hverjir teljast börn í skilningi hennar en ákvæði um börn er að finna á nokkrum stöðum í formála og ákvæðum hennar. Í 6. tölul. 9. gr. frumvarpsins er byggt á f-lið 1. mgr. 6. gr. reglugerðarinnar. Hér birtast áherslur á að taka tillit til réttinda barna sem oftast en ekki eru

ófær um að gefa samþykki eða nýta sér þau réttindi sem skráðir einstaklingar njóta samkvæmt reglugerðinni. Í þessu ljósi þurfa hagsmunir af vinnslu að vera enn meira knýjandi þegar skráðir einstaklingar eru börn. Í 38. lið formála reglugerðarinnar er bent á að persónuupplýsingar barna eigi að njóta sérstakrar verndar þar sem þau kunna að vera síður meðvituð um áhættu, afleiðingar og viðkomandi verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga. Þessi sérstaka vernd ætti samkvæmt umræddum lið formálans einkum að eiga við um notkun persónuupplýsinga barna í markaðssetningarskyni, þá aðstöðu þegar búin eru til persónu- eða notendasnið og um söfnun persónuupplýsinga er varða börn þegar þau nota þjónustu sem börnum eru boðin beint. Samþykki þeirra sem fara með forsjá barns ætti þó ekki að vera nauðsynlegt þegar um er að ræða forvarnar- eða ráðgjafarþjónustu sem barni er boðin beint. Reglugerðin geymir sérreglur um samþykki barna gagnvart þjónustu í upplýsingasamfélaginu sem nánar verður lýst í umfjöllun um 10. gr. frumvarpsins hér á eftir.

Að auki er það nýmæli að stjórnvöld geta ekki grundvallað vinnslu á sínum vegum á lögmætum hagsmunum eins og tekið er fram í niðurlagi 1. mgr. 6. gr. reglugerðarinnar. Í 47. lið formála hennar er í þessu sambandi vísað til þess hlutverks löggjafans að kveða á um lagagrundvöll fyrir vinnslu stjórnvalda á persónuupplýsingum.

Í 2. mgr. 6. gr. reglugerðarinnar er tekið fram að aðildarríkjunum sé heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglna um vinnslu þannig að samrýmist c-lið 1. mgr. sömu greinar (vinnsla nauðsynleg til að uppfylla lagaskyldu) og e-lið sömu málsgreinar (vinnsla nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með). Þannig geta ríki sett fram með ítarlegri hætti sértækar kröfur til vinnslunnar og aðrar ráðstafanir til að tryggja lögmæta og sanngjarna vinnslu, þ.m.t. varðandi vinnslu ákveðinna tegunda upplýsinga eða á ákveðnum sviðum eins og kveðið er á um í IX. kafla (um sérstakar vinnsluheimildir í tengslum við tjáningarfrelsi, aðgang að opinberum skjölum, kennitölur, atvinnutengt samhengi, undanþágur vegna vísindarannsókna, sagnfræði, tölfraði eða skjalavistunar í þágu almannahagsmuna).

Sérreglur af þessum toga er að finna ú nokkrum ákvæðum frumvarpsins, s.s. 6. gr. um tengsl við tjáningarfrelsi og 18. gr. þess um verndarráðstafanir og undanþágur varðandi vinnslu vegna vísindarannsókna, sagnfræði, tölfraði eða skjalavistunar í þágu almannahagsmuna. Þá er heimilt samkvæmt þessu reglugerðarákvæði að setja sértækari ákvæði um vinnslu í sérlög þar sem fram koma heimildir til vinnslu persónuupplýsinga.

Um 10. gr.

Þessi grein frumvarpsins er nýmæli og byggist á 7. og 8. gr. reglugerðarinnar sem fjalla um almenn skilyrði fyrir samþykki svo og sérstök skilyrði sem gilda um samþykki barns í tengslum við þjónustu í upplýsingasamfélaginu. Eru 1.-3. mgr. samhljóða 7. gr. reglugerðarinnar og 4. mgr. er sérregla sem byggir á ákvæði 8. gr. hennar. Í formála reglugerðarinnar er nánar fjallað um hvernig skýra beri þessar greinar hennar. Þá hefur starfshópur skv. 29. gr. tilskipunar ESB fjallað um samþykkishugtakið samkvæmt ákvæðum reglugerðarinnar og gefið út ítarlegar leiðbeiningar um efnið (Guidelines on Consent under Regulation 2016/679) frá 28. nóvember 2017.

Eins og lýst var í 1. tölul. 9. gr. frumvarpsins er samþykki skráðs einstaklings ein algengasta heimildin sem vinnsla persónuupplýsinga hvílir á. Í 8. tölul. 3. gr. frumvarpsins er samþykki skilgreint sem óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um sig. Með því að setja fram enn frekari skilyrði fyrir því að einstaklingur teljist hafa veitt samþykki sitt, birtist það markmið reglugerðarinnar að tryggja betur en áður réttindi skráðra einstaklinga. Þetta endurspeglast m.a. í auknum skyldum ábyrgðaraðila tengdum öflun samþykkis og að hann þurfi jafnframt að færa sönnur á að hann hafi uppfyllt uppfyllt þær.

Í þessu ljósi er mælt fyrir um það 1. mgr. þessarar frumvarpsgreinar að þegar vinnsla sé byggð á samþykki skráðs einstaklings skuli ábyrgðaraðilinn geta sýnt fram á að einstaklingur hafi samþykkt vinnslu persónuupplýsinga um sig. Víkið er að skilyrðum samþykkis í nokkrum liðum formála reglugerðarinnar. Þannig kemur fram í 32. lið hennar að samþykki skuli veitt með skýrri staðfestingu, t.d. skriflegri yfirlýsingu, þar á meðal með rafrænum hætti, eða munnlegri yfirlýsingu, á því að fyrir liggi óþvinguð, afmörkuð, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki vinnslu persónuupplýsinga sem varða hann sjálfan. Dæmi af þessum toga gæti falið í sér að haka við reit þegar farið er inn á vefsetur á

Netinu, velja tæknilegar stillingar fyrir þjónustu í upplýsingasamfélaginu eða aðra yfirlýsingu eða athöfn sem gefur skýrt til kynna í þessu samhengi að skráður einstaklingur samþykki fyrirhugaða vinnslu á persónuupplýsingum um sig. Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi eiga samkvæmt þessu ekki að geta falið í sér samþykki. Þá segir í umræddum lið formálans að samþykki ætti að ná til allrar vinnslustarfsemi sem fram fer í þágu sama markmiðs, eins eða fleiri. Þegar vinnslan sé í margvíslegum tilgangi ætti að gefa samþykki fyrir hverjum og einum þeirra. Sé um að ræða samþykki við rafrænni beiðni verði beiðnin að vera skýr og skilmerkileg og megi ekki raska óþarflega notkun þjónustunnar sem samþykkið er veitt fyrir. Þá er í 42. lið formálans áréttuð skylda ábyrgðaraðila til að geta sýnt fram á samþykki og tekið fram að hann þurfi að tryggja, einkum í tengslum við skriflega yfirlýsingu um annað málefni, að hinum skráða sé kunnugt um að samþykki hafi verið veitt og að hvaða marki. Í þessu sambandi er vísað til tilskipunar ráðsins 93/13/EB frá 5. apríl 1993 um óréttmæta skilmála í neytendasamningum. Hún hefur verið innleidd hér á landi með breytingum á ákvæðum laga um samningsgerð, umboð og ógilda löggæringa nr. 7/1936, svo og lögum nr. 56/2007 um samvinnu stjórnvalda á Evrópska efnahagssvæðinu um neytendavernd.

Í 2. mgr. þessa frumvarpsákvæðis er gerð krafa um að hafi hinn skráði gefið samþykki sitt með skriflegri yfirlýsingu, sem einnig varðar önnur málefni, skuli beiðnin um samþykki sett fram á þann hátt að hún sé auðgreinanleg frá hinum málefnum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli. Þá segir í 42. lið formála reglugerðarinnar að ábyrgðaraðili þurfi að setja fram yfirlýsingu um samþykki á skiljanlegu og aðgengilegu formi og á skýru og einföldu máli sem ætti ekki að fela í sér óréttmæta skilmála. Til þess að samþykki teljist upplýst ætti skráður einstaklingur að vita deili á a.m.k. ábyrgðaraðilanum og vera kunnugt um tilgang þeirrar vinnslu sem persónuupplýsingunum er ætlað að þjóna.

Í 3. mgr. er mælt fyrir um að skráður einstaklingur eigi rétt á að draga samþykki sitt til baka hvenær sem er. Þó hefur slík afturköllun samþykkis ekki áhrif á lögmæti vinnslu á grundvelli samþykkisins fram að afturkölluninni. Um afturköllun segir m.a. í leiðbeiningum 29. gr. starfshópsins um samþykki, bls. 21, að í sumum tilvikum eigi að beita sambærilegum aðferðum við afturköllun samþykkis og við veitingu þess. Það eigi án vafa við þegar samþykkis sé aflað með einföldum, rafrænum hætti, s.s. með því að haka við reit á vefsíðu, en þá eigi hinn skráði að geta afturkallað samþykki sitt með jafn einföldum hætti. Hinn skráði verði auk þess að eiga þess kost að afturkalla samþykki sitt án þess að hafa af því neitt óhagræði, s.s. kostnað eða aðrar afleiðingar. Þá kemur einnig fram í leiðbeiningum 29. gr. starfshópsins, bls. 22, að þegar vinnsluheimild byggist á samþykki, sem síðar er afturkallað, getur ábyrgðaraðilinn ekki haldið áfram vinnslunni með því að vísa til annarrar vinnsluheimildar t.d. almannahagsmuna eða annarra atriða sem talin eru upp í 9. gr. frumvarpsins.

Í 4. mgr. er fjallað um atriði sem skal líta til þegar metið er hvort samþykki sé gefið af fúsum og frjálsum vilja. Þannig 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. Í fyrrgreindum 42. lið formála reglugerðarinnar er tekið fram að ekki eigi að telja að samþykki hafi verið veitt af fúsum og frjálsum vilja ef hinn skráði hefur ekki raunverulegt eða frjálst val eða getur ekki neita eða dregið til baka samþykki án þess að verða fyrir tjóni. Þá kemur fram í 43. lið formálans að til þess að tryggja að samþykki sé veitt af fúsum og frjálsum vilja ætti það ekki að teljast gildur lagagrundvöllur fyrir vinnslu persónuupplýsinga í tilteknu tilviki þar sem skýr aðstöðumunur er milli hins skráða og ábyrgðaraðilans, einkum þegar ábyrgðaraðilinn er stjórnvald og því ólíklegt að samþykki hafi verið veitt af fúsum og frjálsum vilja í ljósi allra aðstæðna í því tiltekna tilviki. Samþykki telst ekki veitt af fúsum og frjálsum vilja ef ekki er hægt að veita sérstakt samþykki fyrir einstökum, aðskildum aðgerðum við vinnslu persónuupplýsinga eða ef framkvæmd samnings, m.a. veiting þjónustu, er komin undir samþykkinu þótt samþykkið sé ekki nauðsynlegt vegna framkvæmdar samningsins.

Þótt þess sé ekki getið í frumvarpsákvæðinu er ljóst að samþykki þarf að vera persónubundið, en í því felst að hinn skráði sjálfur verður að gefa það. Þannig getur enginn gefið samþykki fyrir annars hönd nema hafa til þess sérstaka heimild. Samkvæmt þessu mundi t.d. samþykki forsvarsmanna tiltekinna samtaka fyrir hönd allra félagsmanna almennt ekki vera talið gilt nema mjög sérstaklega standi á, svo sem ef telja má inngöngu í slík samtök jafngilda samþykki. Þá myndi almennt verða litið svo á að samþykki þeirra sem fara með forsjá barns, sem eru lögráðamenn barnsins, þurfti til að gefa samþykki fyrir hönd barnsins svo og lögráðamanna fullorðinna einstaklinga sem ekki eru lögráða.

Í 5. mgr. koma fram sérreglur um samþykki barna í upplýsingasamfélaginu. Tilvísun til hugtaksins „þjónusta í upplýsingasamfélaginu“ er ætlað að ná til samninga sem gerðir eru um þjónustu sem veitt er á netinu. Þegar í þjónustu eru fölgirnir tveir aðgreindir þættir, þ.e. annars vegar upplýsingagjöf um vöru eða þjónustu sem fer að öllu leyti fram rafrænt, m.a. í markaðssetningarskyni, og hins vegar bein afhending vöru, t.d. vegna kaupa sem fram fara á Netinu, þá nær umrætt hugtak aðeins til fyrrgreindu aðstöðunnar.

Ljóst er að börn og unglingar nýta sér margvíslega þjónustu í upplýsingasamfélaginu svo sem á samskiptamiðlum af ýmsum toga án þess að ábyrgðaraðilum hafi verið gert skylt að kanna hvort samþykki forsjáraðila fyrir hönd barnanna liggi fyrir. Ákvæðið gerir bæði tillögu um lægri aldursmörk heldur en þegar 18 ára lögráðaldri er náð, en gerir jafnframt kröfu til ábyrgðaraðila um að 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.

Í 1. mgr. 8. gr. reglugerðarinnar er gert ráð fyrir því að barn þurfi að hafa náð 16 ára aldri til að veita samþykki eins og hér um ræðir, en jafnframt er kveðið á um að aðildarríkin geti í lögum kveðið á um lægri aldur en þó ekki lægri en 13 ár. Í 5. mgr. þessa frumvarpsákvæðis er lagt til að fara sömu leið og valin hefur verið í danska, norska og sænska frumvarpinu til nýrra persónuverndarlaga, þ.e. að miða við 13 ára samþykkisaldur barna. Hafa allmörg aðildarríki sem reglugerðin bindur nýtt sér svigrúm hennar til að áskilja lægri aldur en 16 ár í þessu tilliti, og miða þá við hvort heldur er 13, 14 eða 15 ár. Ljóst er að íslenskir unglingar sem náð hafa þessum aldri hafa flestir nýtt sér þjónustu upplýsingasamfélagsins í ríkum mæli án aðkomu forsjáraðila. Má því telja að þeir geti tekið upplýsta afstöðu til þess hvort þeir veiti slíkt samþykki. Viða í lögum er gert ráð fyrir því að börn undir 18 ára aldri geti tekið ákvörðun um persónuleg réttindi sín þótt lögræði sé ekki náð og þannig er tekið tillit til þess að þau njóti ákveðins sjálfsákvörðunarréttar um slík málefni. Hér ber þó að ávallt að hafa í huga þau varnaðarorð sem fram koma í 38. lið formála reglugerðarinnar að börn kunna að vera síður meðvituð um áhættu, afleiðingar, verndarráðstafanir og réttindi sín í tengslum við vinnslu persónuupplýsinga.

Í fyrrgreindum leiðbeiningum 29. gr. starfshópsins, bls. 23-27, koma fram ítarlegar skýringar á skilyrðum þess að leita samþykkis barna. Þar er bent á að ábyrgðaraðilum verði að vera ljóst að samþykkisaldur barna kann að vera mismunandi milli ríkja. Þá liggur fyrir að til þess að samþykki barns teljist vera „upplýst“ verður ábyrgðaraðili að huga sérstaklega að því að upplýsingar séu á skýru og skiljanlegu máli fyrir börn. Loks er ætlast til þess í niðurlagsorðum þessa ákvæðis frumvarpsins að ábyrgðaraðili geri það sem sanngjarnt má telja til að sannreyna í slíkum tilvikum og hér um ræðir að samþykkið sé gefið eða heimilað af hálfu forsjáraðila barnsins, að teknu tilliti til þeirrar tækni sem fyrir hendi er. Hér eru því ekki settar fram tilteknar reglur um hvernig ábyrgðaraðili skuli sannreyna það, en það kann að taka mið af aðstæðum hvaða ráðstafana má telja sanngjarnt að ábyrgðaraðili grípi til. Nánari útfærslu á því miðað við ólíkar aðstæður má m.a. sjá í fyrrgreindum leiðbeiningum 29. gr. starfshópsins um samþykki.

Um 11. gr.

Í þessu ákvæði er tæmandi upptalning á því hvenær má vinna með viðkvæmar persónuupplýsingar eins og það hugtak er skilgreint í 3. tölul. 3. gr. frumvarpsins. Í 9. gr. gildandi laga kemur fram sú meginregla að vinnsla viðkvæmra persónuupplýsinga sé óheimil nema uppfyllt sé eitthvert þeirra skilyrða sem þar eru talin upp, auk einhvers hinna almennu skilyrða fyrir vinnslu samkvæmt 8. gr. laganna. Frumvarpsákvæði þetta byggist á 9. gr. reglugerðarinnar sem skilgreinir tilteknar upplýsingar svo að þær falli undir „sérstaka flokka persónuupplýsinga“ með sama hætti og gert er í 8. gr. gildandi ESB-tilskipunar.

Í skýringum við 3. tölul. 3. gr. frumvarpsins kom fram að reglugerðin breytir upptalningu á þeim persónuupplýsingum sem falla hér undir í tvenns konar tilliti. Í fyrsta lagi falla nú ekki lengur í þennan flokk upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað eins og er samkvæmt gildandi lögum. Sérreglur um persónuupplýsingar af þessum toga koma nú fram í 10. gr. reglugerðarinnar og 12. gr. frumvarps þessa sem nánar verður fjallað um í skýringum við það ákvæði. Í öðru lagi bætir reglugerðin við tveimur flokkum upplýsinga sem í gildandi lögum eru ekki taldar upp í

skilgreiningu viðkvæmra upplýsinga. Þetta eru annars vegar erfðafræðiupplýsingar og hins vegar lífkennaupplýsingar í því skyni að persónugreina einstakling með einkvæmum hætti.

Eins og fram kemur í 51. lið formála reglugerðarinnar eiga persónuupplýsingar, sem eru í eðli sínu sérlega viðkvæmar að því er varðar grundvallarréttindi og mannfrelsi, að njóta sérstakrar verndar þar sem vinnsla þeirra gæti haft í för með sér umtalsverða áhættu fyrir þessi réttindi. Meginmarkmið 11. gr. frumvarpsins er að skilgreina með tæmandi hætti hvenær heimilt er að víkja frá banni við vinnslu viðkvæmra persónuupplýsinga. Er hér byggt á talningu atriða sem réttlæta frávík og fram koma í 2. mgr. 9. gr. reglugerðarinnar. Þessi frávík eru nokkuð fleiri og ítarlegri en þau sem talin eru upp í núgildandi lögum og tilskipun ESB. Hér má benda á að 2. mgr. 9. gr. reglugerðarinnar veitir aðildarríkjum heimild til að útfæra nánar hvernig þessum undantekningum er háttað í landslögum, m.ö.o. ber aðildarríkjum ekki skylda samkvæmt reglugerðinni til að heimila þær. Í þessu frumvarpi er sú leið valin að heimila slíkar undantekningar, líkt og gert hefur verið í norska og danska frumvarpinu til nýrra persónuverndarlaga.

Verður nú nánar vikið að skýringu á sérreglum 1. mgr. 11. gr. frumvarpsins m.a. í ljósi athugasemda sem koma fram í formála reglugerðarinnar en sem fyrr segir er hún byggð á talningu sömu atriða í 2. mgr. 9. gr. reglugerðarinnar.

Samkvæmt 1. tölul. má vinna með viðkvæmar persónuupplýsingar hafi hinn skráði afdráttarlaust samþykkt vinnsluna fyrir sitt leyti. Má ætla að á þetta geti reynt við gerð ýmiss konar samninga, svo sem váttryggingarsamninga, samninga um að njóta félagslegrar þjónustu o.s.frv. Við öflun samþykkis verður að uppfylla þær kröfur sem fram koma í skilgreiningu á samþykki samkvæmt 8. tölul. 3. gr. frumvarpsins, svo og þau sérstöku skilyrði 10. gr. frumvarpsins sem lýst var framan, þar á meðal um skyldu ábyrgðaraðila til að gera beiðni um samþykki skýra og auðskiljanlega til að tryggja að það sé gefið af fúsum og frjálsum vilja. Skilyrði um samþykki hins skráða er ákjósanlegt frá sjónarhóli persónuverndar en það getur þó ekki alltaf ráðið úrslitum um hvort vinnsla fari fram eða ekki. Því er lagt til að vinnsla viðkvæmra persónuupplýsinga geti verið heimil í öðrum tilvikum og er um þau fjallað í 2.–11. tölul. 1. mgr.

Í 2. tölul. er lagt til að vinna megi með viðkvæmar persónuupplýsingar sé vinnslan 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. Skilyrðið er efnislega áþekkt gildandi lögum. Hér á landi byggjast réttindi og skyldur á vinnumarkaði ekki síður á frjálsum samningum en lagafyrirmælum og því er lögð til sú viðmiðun að ábyrgðaraðili geti byggt vinnslu á samningi aðila á vinnumarkaði, en með því er m.a. átt við ákvæði í ráðningarsamningi og/eða heildarkjarasamningi. Hér sem endranær gildir einnig að því meiri íhlutun í einkalíf hins skráða sem vinnslan hefur í för með sér þeim mun ótvíræðara verður slíkt ákvæði að vera.

Í 3. tölul. er lýst heimild til vinnslu viðkvæmra persónuupplýsinga sé hún nauðsynleg til að verja brýna hagsmuni hins skráða eða annars einstaklings sem ekki er sjálfur fær um að gefa samþykki sitt. Ákvæðið er óbreytt frá gildandi reglu. Hin ströngu skilyrði með vísun til nauðsynjar og brýnna hagsmuna gefa til kynna að ákvæðið beri að túlka þröngt. Átt er við að hinn skráði sé ófær af líkamlegum ástæðum eða í lagalegum skilningi, t.d. vegna lögræðissviptingar, um að veita samþykki sitt. Í skýringu gildandi laga um ákvæðið er áréttað að vinnsla viðkvæmra persónuupplýsinga má ekki fara fram þegar hinn skráði gefur ekki samþykki sitt þótt hann geti það, jafnvel þótt hann tefli eigin hagsmunum þar með í tvísýnu. Hafi hinn skráði gerhæfi og skilji þá áhættu sem hann tekur á hann ákvörðunarvald í þeim efnum. Öðru máli gegnir ef neitun hefur þær afleiðingar að ekki verður unnt að verja verulega hagsmuni þriðja manns og getur þá reynt á þessa undanþágu. Hún hvílir m.a. á þeim almennu sjónarmiðum sem koma fram í 112. lið formála reglugerðarinnar að miðlun persónuupplýsinga teljist lögmæt þegar hún er nauðsynleg til að vernda hagsmuni sem skipta sköpum fyrir brýna hagsmuni skráðs einstaklings eða annars einstaklings, þar á meðal líkamlega friðhelgi eða líf, ef hinn skráði er ekki fær um að veita samþykki sitt.

Í 4. tölul. er lýst heimild til vinnslu fari hún fram sem liður í lögmætri starfsemi stofnunar, samtaka eða annars aðila sem starfar ekki í hagnaðarskyni og hefur stjórnmalaleg, 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. Ákvæðið er efnislega hið sama og í gildandi lögum. Það hefur verið skýrt á þann veg að það hafi ekki sjálfstæða þýðingu gagnvart einstökum meðlimum hafi þeir þegar samþykkt vinnsluna með samþykki skv. 1. tölul. Varðandi aðra einstaklinga kann að vera um einhvers konar þjónustusamband að ræða, sbr. t.d. ef hjálparamtök útbúa lista yfir heimilislausa menn sem gist hafa í húsnæði samtakanna. Í slíkum tilvikum ber að túlka ákvæði 4. tölul. þannig að hið reglubundna samband, sem er forsenda vinnslunnar, byggist á fúsum og frjálsum vilja hins skráða. Þess vegna geta samtök t.d. ekki rekið kerfisbundna leitarstarfsemi og þannig öðlast rétt til að vinna með viðkvæmar upplýsingar um þá sem leitað er að en vilja e.t.v. ekki vera leitaðir uppi. Í ákvæðinu eru talin upp þau markmið samtaka sem falla undir umrætt ákvæði og það gert að skilyrði að um sé að ræða samtök með lögmæta starfsemi. Í því felst ekki aðeins að samtökin skuli vera lögleg í þröngum skilningi (þ.e. ekki bönnuð) heldur skuli vinnsla persónuupplýsinganna þjóna málefnalegum tilgangi vinnslunnar, sbr. meginreglur 8. gr. frumvarpsins, og taka viðhlítandi tillit til persónuverndar, en með því er m.a. átt við nauðsynlegar öryggis- og verndarráðstafanir. Af því leiðir að sé ekki tekið viðhlítandi tillit til persónuverndarsjónarmiða, með þeim afleiðingum að starfsemin telst vera ólögmæt, getur Persónuvernd skv. 42. gr. frumvarpsins bannað viðkomandi samtökum að vinna með viðkvæmar persónuupplýsingar eða mælt fyrir um ráðstafanir til að tryggja öryggi og persónuvernd. Þá skal áréttað að ákvæði 4. tölul. tekur ekki til allrar vinnslu persónuupplýsinga, enda beinlínis tekið fram að það heimili ekki birtingu (miðlun) upplýsinganna til óviðkomandi aðila. Samkvæmt því er ekki sjálfgefið að félagsamtök megi láta frá sér lista með nöfnum félagsmanna án þess að hafa til þess samþykki hvers og eins félagsmanns. Að öðru leyti skal tekið fram að það hvaða vinnsla sé heimil hverju sinni samkvæmt ákvæðinu hlýtur m.a. að ráðast af eðli viðkomandi samtaka. Í formála reglugerðarinnar er vikið að aðstæðum sem gætu átt undir ákvæðið þegar stjórnmalaflokkar eiga í hlut. Samkvæmt 56. lið formálans má, þegar nauðsynlegt reynist fyrir starfsemi lýðræðislegs stjórnkerfis í aðildarríki, í tengslum við kosningar, heimila að stjórnmalaflokkar taki saman persónuupplýsingar um stjórnmalaskoðanir fólks í þágu almannahagsmuna, að því tilskildu að gerðar séu viðeigandi verndarráðstafanir. Þá er tekið fram í 55. lið formálans að vinnsla persónuupplýsinga af hálfu opinberra yfirvalda í þeim tilgangi að vinna að markmiðum opinberlega viðurkenndra trúarsamtaka, eins og mælt er fyrir um í stjórnarskrá eða samkvæmt þjóðarétti, fari einnig fram með vísan til almannahagsmuna.

Í 5. tölul. er lagt til að vinna megi með viðkvæmar persónuupplýsingar sem hinn skráði hefur augljóslega sjálfur gert opinberar. Ákvæðið er óbreytt frá gildandi lögum, en bætt er við tilvísun um að hinn skráði hafi „augljóslega“ gert upplýsingarnar opinberar. Með þessu er undirstrikað að vafi í þessum efnunum yrði túlkaður hinum skráða í hag. Með því að upplýsingar hafi verið gerðar opinberar er átt við að þær hafi verið kunngjörðar ótilgreindum hópi manna, t.d. með ritun ævisögu eða í sjónvarpsviðtali. Síðari vinnsla slíkra upplýsinga er því heimil án sérstaks samþykkis hins skráða, en tekið skal fram að hér sem endranær gildir að gæta skuli að þeim meginreglum sem fram koma í 8. gr. frumvarpsins. um meðferð persónuupplýsinga.

Samkvæmt 6. tölul. má vinna með viðkvæmar persónuupplýsingar til að unnt sé að stofna, hafa uppi eða verja réttarkröfur. Ákvæðið er efnislega hliðstætt gildandi lögum þar sem mælt er fyrir um vinnslu í því skyni að afmarka, setja fram og verja tiltekna kröfu vegna dómsmáls eða annarra slíkra laganauðsynja. Vinnuveitanda getur t.d. verið nauðsynlegt að vinna upplýsingar um heilsufar starfsmanns til að geta sýnt fram á lögmætar forsendur fyrir uppsögn. Það er ekki skilyrði að málið verði lagt fyrir dómstóla heldur nægir að vinnslan sé nauðsynleg til að styðja kröfu fullnægjandi rökum. Vinnsla viðkvæmra persónuupplýsinga í þessum tilgangi telst hins vegar því aðeins vera lögleg að krafan verði hvorki afmörkuð né staðreynd með öðrum hætti. Í niðurlagi 52. liðar formála reglugerðarinnar er vísað til þess að vinnsla upplýsinga vegna slíkra krafna getur farið fram hvort heldur er á vegum dómstóls, við stjórnsýslumeðferð eða við málsmeðferð utan réttar.

Samkvæmt 7. tölul. má vinna með viðkvæmar persónuupplýsingar sé vinnslan nauðsynleg af ástæðum sem varða verulega almannahagsmuni og fyrir henni sé sérstök lagaheimild. Ákvæði þetta á beina fyrirmynd í g-lið 2. mgr. 9. gr. reglugerðarinnar. Auk þess verður að skoða 7. tölul. 1. mgr. frumvarpsákvæðisins í ljósi annarra ákvæða frumvarpsins og reglugerðarinnar. Þannig er fjallað um leyfisskylda vinnslu í 31. gr. frumvarpsins. Ákvæðið mælir fyrir um að ef vinnsla persónuupplýsinga fari fram vegna verkefnis í þágu almannahagsmuna sem geti falið í sér sérstaka hættu á að farið verði í bága við réttindi og frelsi skráðra einstaklinga geti Persónuvernd

ákveðið að vinnslan megi ekki hefjast fyrr en hún hafi verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar. Nánar verður fjallað um slík leyfi og skilyrði þeirra þegar viðkvæmar persónuupplýsingar eru annars vegar í skýringum með 31. og 32. gr. frumvarpsins. Í 52. lið formála reglugerðarinnar er m.a. fjallað um dæmi um almannahagsmuni sem hér gætu fallið undir, en sumra þeirra einnig getið í öðrum tölulíðum 8.–11. tölul. 1. mgr. 11. gr. frumvarpsins og 2. mgr. 9. gr. reglugerðarinnar. Er þar m.a. bent á vinnslu persónuupplýsinga á sviði vinnulöggjafar og löggjafar um félagslega vernd, m.a. lífeyri, og með hliðsjón af heilbrigðisöryggi, vöktun og viðvörðunum, forvörnum og vörnum gegn smitsjúkdómum og annarri alvarlegri heilsufarsógn. Að auki er mælt fyrir um að vinnslu megi heimila af heilbrigðisástæðum, s.s. vegna lýðheilsu og stjórnunar heilbrigðisþjónustu, einkum til að tryggja gæði og kostnaðarhagkvæmni þess verklags sem notað er við uppgjör á kröfum um bætur og þjónustu sjúkratryggingakerfisins, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Þá er rakið í 53. lið formála reglugerðarinnar að vinnsla viðkvæmra persónuupplýsinga, sem þurfa að njóta aukinnar verndar, ætti aðeins að fara fram í þágu heilsutengdra markmiða þegar það er nauðsynlegt til að ná þessum markmiðum í þágu einstaklinga og samfélagsins alls, einkum í tengslum við stjórnun heilbrigðis- eða félagsþjónustu og -kerfa. Í því sambandi er tilgreind vinnsla slíkra upplýsinga á vegum stjórnsýslunnar og miðlægra landsbundinna heilbrigðisýfirvalda í þágu gæðastýringar, gagnaumsýslu stjórnsýslunnar og almenns eftirlits með heilbrigðis- og félagsþjónustu á lands- og staðarvísu og til að tryggja samfellu í heilbrigðis- og félagsþjónustu og heilbrigðisþjónustu eða heilbrigðisöryggi yfir landamæri, vegna vöktunar og viðvörðunar, eða vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Ljóst er að vinnsla viðkvæmra persónuupplýsinga í þágu mikilvægra samfélagshagsmuna af þeim toga sem taldir eru upp í þessum liðum formálans er iðulega heimiluð í sérlögum.

Samkvæmt 8. tölul. má vinna með viðkvæmar persónuupplýsingar sé vinnslan 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. Þetta ákvæði skiptir einkum máli í tengslum við vinnslu upplýsinga um sjúklinga innan heilbrigðiskerfisins en um þá vinnslu er einnig fjallað í sérlögum á því sviði, sbr. m.a. lög nr. 55/2009 um sjúkraskrár. Þá skiptir ákvæðið máli í tengslum við vinnslu upplýsinga um starfsmenn sem fram fer á vegum trúnaðarlækna á vinnustöðum.

Í 9. tölul. er lýst heimild til vinnslu viðkvæmra persónuupplýsinga sé vinnslan nauðsynleg af ástæðum er varða almannahagsmuni á sviði lýðheilsu, svo sem til að verjast alvarlegum heilsufarsögnum sem ná yfir landamæri eða tryggja gæði og öryggi heilbrigðisþjónustu og lyfja eða lækningatækja en að því var einnig vikið fyrr. Um lýðheilsuhugtakið er fjallað í 54. gr. formála reglugerðarinnar. Tekið er fram að vinnsla viðkvæmra persónuupplýsinga vegna almannahagsmuna á sviði lýðheilsu án samþykkis skráðs einstaklings kunni að vera nauðsynleg. Slík vinnsla ætti að vera með fyrirvara um viðeigandi og sértækar ráðstafanir til að standa vörð um réttindi og frelsi einstaklinga. Í þessu samhengi ætti að túlka hugtakið „lýðheilsa“ eins og það er skilgreint í reglugerð Evrópuþingsins og ráðsins (EB) nr. 1338/2008, þ.e. sem alla heilsufarstengda þætti, nánar tiltekið heilsufar, m.a. sjúkdómstilvik og fötlun, ákvarðandi þætti sem hafa áhrif á heilsufar, þörf fyrir heilbrigðisþjónustu, fjármagn sem veitt er til heilbrigðisþjónustu, veitingu og almennan aðgang að heilbrigðisþjónustu og kostnað og fjármögnun heilbrigðisþjónustu, auk dánarorsakar. Slík vinnsla heilsufarsupplýsinga í þágu almannahagsmuna ætti ekki að leiða til vinnslu persónuupplýsinga í öðrum tilgangi af hálfu þriðju aðila, s.s. vinnuveitenda eða tryggingafélaga og bankastofnana. Hefur fyrrgreind reglugerð verið tekin upp í EES-samninginn.

Í 10. tölul. eru taldir upp heimildir til vinnslu viðkvæmra persónuupplýsinga sé vinnslan nauðsynleg vegna tölfraði-, sagnfræði- eða vísindarannsókna enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á í samræmi við lögin. Með tilteknum ráðstöfunum í 10. tölul. er vísað til aðgerða á borð við dulkóðun eða eyðingu persónuauðkenna, sem og annarra nauðsynlegra öryggisráðstafana sem viðhafa ber.

Í 11. tölul. eru veittar heimildir til vinnslu viðkvæmra persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna enda fari hún fram á grundvelli laga sem kveða á um viðeigandi og sértækar ráðstafanir til að vernda grundvallarréttindi og hagsmuni hins skráða,

einkum þagnarskyldu. Þetta ákvæði skiptir fyrst og fremst máli í tengslum við Þjóðskjalasafn Íslands og önnur opinber skjalasöfn, sbr. lög nr. 77/2014 um slík söfn.

Hafa ber í huga að ýmsar sérreglur gilda samkvæmt framangreindum ákvæðum 10. og 11. tölul. um undanþágur varðandi vinnslu vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, sbr. einkum 89. gr. reglugerðarinnar og 18. gr. frumvarpsins. Verður nánar vikið að þeim í skýringum við það frumvarpsákvæði.

Í 2. mgr. 11. gr. frumvarpsins er kveðið á um að Persónuvernd leysi úr ágreiningi um hvort persónuupplýsingar skuli teljast viðkvæmar eða ekki. Er hér í raun áréttað það sem leiðir af almennum reglum 39. og 40. gr. frumvarpsins um verkefni og valdheimildir Persónuverndar sem eftirlitsstjórnvalds samkvæmt VI. kafla reglugerðarinnar. Leiki vafi á um það hvort tilteknar upplýsingar teljist viðkvæmar er Persónuvernd þannig lögbært stjórnvald til að skera úr um það. Það útilokar þó ekki að dómstólar geti skorið úr slíku álitaefni ef aðilar máls sem lýtur að beitingu ákvæða persónuverndarlöggjafarinnar kjósa að leggja ágreining sinn fyrir dómstóla með venjubundnum hætti, svo sem nánar er vikið að í skýringum með 38. gr. frumvarpsins.

Um 12. gr.

Sem fyrr var lýst er sú breyting ráðgerð með frumvarpinu frá gildandi lögum að upplýsingar um hvort maður hafi verið grunaður, kærður, ákærður eða dæmdur fyrir refsiverðan verknað falli ekki lengur undir hugtakið viðkvæmar persónuupplýsingar, sbr. b-lið 8. tölul. 2. gr. laganna, sem háðar eru sérreglum um vinnslu, sbr. 9. gr. laganna.

Í reglugerðinni eru upplýsingar af þessum toga ekki taldar til sérstakra flokka persónuupplýsinga, en í 10. gr. hennar er þó að finna sérákvæði um efnið. Ljóst er að um slíkar upplýsingar gilda um margt sérstök sjónarmið, t.d. almannahagsmunir af því að hafa vitneskju um sakaferil manna í tengslum við ráðningu í störf og að starfrækt sé sakaskrá, að kæra til lögreglu getur verið nauðsynleg til að vekja athygli á refsiverðri háttsemi o.s.frv.

Samkvæmt 10. gr. reglugerðarinnar skal vinnsla persónuupplýsinga, sem varða sakfellingar í refsímálum og refsiverð brot eða tengdar öryggisráðstafanir á grundvelli 1. mgr. 6. gr. reglugerðarinnar, einungis fara fram undir eftirliti opinbers yfirvalds eða þegar vinnsla er heimiluð samkvæmt lögum Sambandsins eða lögum aðildarríkis þar sem kveðið er á um viðeigandi verndarráðstafanir í tengslum við réttindi og frelsi skráðra einstaklinga. Þá segir að ítarlega skrá yfir refsidóma skuli varðveita undir eftirliti opinbers yfirvalds. Þannig er gert ráð fyrir því að í lögum aðildarríkis sé að finna nánari útfærslur á tilhögun við vinnslu slíkra upplýsinga. Frumvarpsákvæði þetta sem er nýmæli frá gildandi lögum er ætlað að setja fram slíkar reglur en það sækir að nokkru leyti fyrirmynd til 8. gr. danska frumvarpsins til nýrra persónuverndarlaga. Markmið þess er tvíþætt og lýtur annars vegar að setningu sérreglna um skyldur stjórnvalda í 1. og 2. mgr. og hins vegar að skyldum einkaaðila. Ljóst er að reglur 9. gr. frumvarpsins og 6. gr. reglugerðarinnar um almennar heimildir til vinnslu eiga hér við sem endranær og ákvæðið felur ekki í sér undantekningar á því heldur áréttar nokkur atriði sem vinnslan verður að byggjast á og setur í sumu tilliti strangari skilyrði þótt þau séu ekki jafn ströng og þau sem gilda um vinnslu viðkvæmra persónuupplýsinga. Reglugerðin vísar berum orðum til upplýsinga um „sakfellingu“ í refsímáli og verður að álykta af því að hún gildi ekki um vinnslu upplýsinga tengslum við sýknudóma. Ekki er skilgreint í texta hennar hvað felst í tilvísun til refsiverðs brots og tengdra öryggisráðstafana. Þessi hugtök verða skýrð rúmt og ná til upplýsinga um það einnig hvort maður hafi verið grunaður, kærður eða ákærður fyrir refsiverðan verknað. Hugtakið öryggisráðstafanir yrði einnig að túlka rúmt og má geta þess að skýringum í norska frumvarpinu til nýrra persónuverndarlaga er litið svo á að það nái til ráðstafana sem byggðar eru á heimildum sakamála í tengslum við rannsókn sakamála.

Hvað varðar skyldur stjórnvalda samkvæmt þessu frumvarpsákvæði birtist sú meginregla í 1. mgr. að stjórnvöld mega ekki vinna með upplýsingar um refsiverða háttsemi nema það sé nauðsynlegt í þágu lögbundinna verkefna þeirra. Þá er gert ráð fyrir ákveðnum sérreglum um miðlun slíkra upplýsinga í 2. mgr. ákvæðisins, en eitthvert þeirra skilyrða þarf að vera uppfyllt. Þeim má því ekki miðla nema *í fyrsta lagi* að hinn skráði hafi gefið ótvírætt samþykki sitt fyrir miðluninni eftir þeim reglum sem gilda samkvæmt lögum um samþykki, *í öðru lagi* að 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, *í þriðja lagi* að miðlunin sé nauðsynleg í þágu lögbundinna verkefna viðkomandi stjórnvalds eða til að unnt sé að taka stjórnvaldsákvörðun eða *í fjórða lagi* að miðlunin sé nauðsynleg vegna verkefnis í þágu hins opinbera sem einkaaðila hefur verið falið á lögmætan hátt. Hér ber að hafa í huga að víða í lögum er að finna heimildir til þess að stjórnvöld vinni með upplýsingar um hvort maður hafi hlotið refsidóm. Dæmi af þeim toga má sjá í 36. gr. barnaverndarlaga nr. 80/2002 sem fjallar um rétt Barnaverndarstofu til upplýsinga úr sakaskrá og miðlun upplýsinga til barnaverndarnefnda. Þá er ljóst að ríkissaksóknara er skylt að halda sakaskrá fyrir landið allt þar sem skráðar eru niðurstöður sakamála og samræmist það áskilnaði 10. gr. reglugerðarinnar um að aðildarríki skuli halda ítarlega skrá yfir refsidóma undir eftirliti opinbers yfirvalds. Eins gilda heimildir í sérlögum um vinnslu persónuupplýsinga hjá lögreglu, sbr. t.d. i-lið 1. mgr. 5. gr. lögreglulaga nr. 90/1996 um að ríkislögreglustjóri haldi málaskrá um kærur sem berast lögreglu, dagbók lögreglu, skrá yfir handtekna menn o.fl. og lög um erfðaeftnissskrá lögreglu nr. 88/2001 o.fl. Þá er ljóst að tilskipun ESB nr. 2016/680 um vinnslu persónuupplýsinga á sviði lögreglumála geymir sérreglur um vinnslu persónuupplýsinga í þágu lögreglu, sem innleiddar verða hér á landi með sérstökum lögum eftir að gerðin hefur verið tekin upp í EES-samninginn.

Seinni hluti frumvarpsákvæðisins lýtur að möguleikum á því að einkaaðilar vinni með persónuupplýsingar um refsiverða háttsemi. Slík vinnsla er aðeins heimil skv. 3. mgr. án samþykkis hins skráða sé hún nauðsynleg í þágu lögmætra hagsmuna sem auðsýnilega vega þyngra en einkalífsréttur hins skráða. Þá eru frekari fyrirvarar gerðir um miðlun slíkra upplýsinga í 4. mgr. ákvæðisins um að ábyrgðaraðili megi ekki miðla upplýsingunum nema hinn skráði veiti til þess ótvírætt samþykki sitt. Einnig er þar að finna undantekningu um að miðla megi 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. Dæmi um aðstæður þar sem lögmætir hagsmunir réttlæta vinnslu einkaaðila skv. 3. mgr. og miðlun upplýsinga skv. 4. mgr. gæti verið þegar fyrirtæki skráir upplýsingar um grun um refsiverða háttsemi manna, t.d. þjófnað í verslun, með það í huga að tilkynna lögreglu um meint brot. Þá má nefna varðveislu á upptökum úr eftirlitsmyndavélum í sama skyni.

Í lokamálsgrein þessa frumvarpsákvæðis er mælt fyrir um að vinnsla upplýsinga samkvæmt greininni skuli ávallt eiga stoð í einhverri af heimildum 1. mgr. 9. gr. laga þessara, sbr. 1. mgr. 6. gr. reglugerðarinnar. Af þessu er ljóst að skilyrði um almennar vinnsluheimildir verða að vera uppfyllt til að frumvarpsákvæðið eigi við, það skapar m.ö.o. ekki sjálfstæðar vinnsluheimildir fyrir ábyrgðaraðila.

Um 13. gr.

Í 10. gr. gildandi laga er að finna sérreglu um notkun kennitalna, sem byggir á ákvæði 7. mgr. 8. gr. tilskipunar ESB sem mælir fyrir um að aðildarríkin skuli setja reglur um efnið. Í 87. gr. reglugerðarinnar er fjallað um vinnslu landsbundins auðkennisnúmera. Samkvæmt því er aðildarríkjum heimilt að ákvarða frekar hvaða sértæku skilyrði gilda um vinnslu landsbundinna auðkennisnúmera eða annarra almennra auðkenna. Í því tilviki skal því aðeins nota landsbundið auðkennisnúmer eða annað almennt auðkenni að gerðar séu viðeigandi verndarráðstafanir varðandi réttindi og frelsi skráðs einstaklings samkvæmt þessari reglugerð.

Ljóst er að notkun kennitölu getur aukið áreiðanleika persónuupplýsinga með því að stuðla að öruggari persónugreiningu en ella, þ.e. að tveimur eða fleiri einstaklingum sé ekki ruglað saman. Jafnframt getur hún hins vegar falið í sér skerðingu á friðhelgi einkalífs þar sem hún er fremur einfaldur lykill að persónugreiningu upplýsinga og gerir það að verkum að auðveldara er en ella að samkeyra persónuupplýsingar sem fengnar eru úr mismunandi skráum og mynda úr þeim eina skrá. Tilgangurinn með notkun kennitölu er fyrst og fremst sá að stuðla að öruggri persónugreiningu þegar það á við, þ.e. að tengja tiltekna upplýsingar við þann sem upplýsingarnar varða.

Í frumvarpinu er nýtt heimild til að viðhalda ákvæði um kennitölur inni í landslögum og eru ekki ráðgerðar breytingar frá 10. gr. gildandi laga. Samkvæmt ákvæðinu þarf notkun kennitölu að eiga sér málefnalegan tilgang og vera nauðsynleg til að tryggja örugga persónugreiningu upplýsinga. Kröfunni um málefnalegan tilgang verður ekki fullnægt nema önnur auðkenni, svo sem nafn, heimilisfang eða viðskiptanúmer, séu ófullnægjandi. Við mat á málefnalegum

tilgangi ber m.a. að líta til þess hvort örugg persónugreining sé mikilvæg fyrir hinn skráða, fyrir ábyrgðaraðila eða vegna almannahagsmuna.

Að öðru leyti er ekki lagt til að setja fram ítarlega eða tæmandi talningu á því hvenær notkun kennitölu sé heimil enda getur hún átt við í fjölbreytilegum aðstæðum. Krafan um viðhlítandi gæði og öryggi tekur m.a. til þess að upplýsingar séu uppfærðar reglulega og að persónuupplýsingarnar séu réttar og fullnægjandi. Persónuvernd getur gefið út frekari leiðbeiningar um notkun kennitalna og skorið úr ágreiningi um það hvort notkun kennitölu sé heimil. Í úrskurðum Persónuverndar um gildandi lagaákvæði um kennitölur hefur m.a. komið fram að ákvæði 10. gr. er til fyllingar ákvæði 8. gr. um vinnsluheimildir en í því felst að til vinna megi með almennar persónuupplýsingar verður ávallt að vera fullnægt einhverju skilyrðanna í 1. mgr. síðarnefnda ákvæðisins. Það sama gildir um samspil þessarar sérreglu frumvarpsins um kennitölur við almennar vinnsluheimildir samkvæmt 1. mgr. 9. gr. þess. Þannig þarf ábyrgðaraðili bæði að uppfylla einhverja þeirra og haga vinnslu kennitalna í samræmi við 13. gr.

Um 14. gr.

Í þessari grein er að finna sérreglur um skilyrði rafrænnar vöktunar, vinnslu persónuupplýsinga sem verða til við slíka vöktun, varðveislutíma þeirra o.fl. Hér er safnað á einn stað ákvæðum gildandi laga um efnið, sbr. 4. gr. um rafræna vöktun, 24. gr. um viðvaranir um rafræna vöktun og 37. gr. um að Persónuvernd setji nánari reglur um rafræna vöktun og hvað skuli koma fram í þeim. Þá er skilgreining frumvarpsins á rafrænni vöktun skv. 9. tölul. 3. gr. samsvarandi þeirri sem er 6. tölul. 2. gr. núgildandi laga. Samkvæmt henni fellur sú vöktun undir hugtakið sem er viðvarandi eða endurtekin reglulega, 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 annars vegar til vöktunar sem leiðir, á að leiða eða getur leitt til vinnslu persónuupplýsinga og hins vegar 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.

Frumvarpinu er ekki ætlað að breyta efnislega ákvæðum gildandi laga um rafræna vöktun eða reglna settra á grundvelli þeirra. Núgildandi ákvæði voru endurskoðuð og uppfærð með lögum nr. 81/2002 og 46/2003 í því skyni að leysa úr óvissu um nokkur atriði varðandi m.a. sjónvarpsvöktun án þess að fram fari söfnun myndefnis eða aðrar aðgerðir sem jafngilda vinnslu persónuupplýsinga. Þá setti Persónuvernd árið 2006 nánari reglur um rafræna vöktun og meðferð persónuupplýsinga sem verða til við slíka vöktun, nr. 837/2006, og hafa þær verið endurskoðaðar og uppfærðar á síðustu árum. Reglurnar taka til rafrænnar vöktunar á vinnustöðum, í skólum og á öðrum svæðum þar sem takmarkaður hópur fólks fer um að jafnaði. Þær gilda óháð því hvers konar tæknibúnaður er notaður, s.s. hvort notaðir eru netþjónar, búnaður til að fylgjast með símanotkun, eftirlitsmyndavélar, vefmyndavélar, ökuritar, rafrænn staðsetningarbúnaður o.s.frv. Til rafrænnar vöktunar telst meðal annars tölvupóstsvöktun sem fer fram með sjálfvirkri og viðvarandi skráningu á upplýsingum um tölvupósta og tölvupóstkerfisnotkun einstakra starfsmanna. Í reglunum er nánar lýst skilyrðum vöktunar, varðveisl, miðlun og eyðingu upplýsinga sem verða til við rafræna vöktun, sérreglum um tölvupóst og netnotkun starfsmanna á vinnustöðum og fræðslu- og upplýsingaskyldu.

Rafræn vöktun með eftirlitsmyndavélum eða öðrum tækjum hefur færst stöðugt í aukana á undanförunum áratug hvort heldur í starfsemi fyrirtækja eða hjá einstaklingum, s.s. við heimili fólks enda er rafrænn tækjabúnaður til vöktunar af margvíslegum toga í stöðugri þróun og orðinn mjög aðgengilegur almenningi. Í sumum ríkjum hefur verið sett sérstök löggjöf eða ítarlegar reglur um efnið. Má m.a. benda á að í Noregi hefur verið lagt til að samhliða frumvarpi til nýrra persónuverndarlaga verði sett sérstök lagaákvæði um eftirlitsmyndavélar á vinnustöðum. Álitafni er hvort færa ætti ákvæði um þessi efni inn í sérstök lög hér á landi en í frumvarpi þessu er sem fyrr segir gert ráð fyrir óbreyttum reglum um efnið frá gildandi lögum.

Mótast hefur talsverð framkvæmd um beitingu lagaákvæðanna um rafræna vöktun og reglna þar um og hefur Persónuvernd kveðið upp fjölmarga úrskurði um efnið. Þar hefur m.a. hefur verið leyst úr ágreiningi um uppsetningu eftirlitsmyndavéla við híbýli fólks, s.s. í fjölbýlishúsum eða við atvinnuhúsnæði innan og utan lóðamarka, birtingu myndefnis sem safnað er, vöktun með hljóðupptökum, ökuritum svo og meðferð tölvupósta starfsmanna. Þá

hefur Persónuvernd gefið út leiðbeiningar um ýmis atriði tengd framkvæmd þessara ákvæða, þar á meðal það sem þarf að hafa í huga við uppsetningu eftirlitsmyndavéla á vinnustað.

Reglugerð ESB hefur ekki að geyma nein sérákvæði um rafræna vöktun en aðildarríki geta sett sérreglur þar um innan þess ramma sem reglugerðin setur. Á einum stað í reglugerðinni er vísað til þess hvernig túlka beri ákvæði hennar í tengslum við vöktun með eftirlitsmyndavélum. Nánar tiltekið segir í 91. lið formálans, sem fjallar um það hvenær mat á áhrifum á persónuvernd ætti að fara fram skv. 35. gr. reglugerðarinnar, að slíkt mat ætti að framkvæma þegar um sé að ræða umfangsmikið eftirlit með svæðum sem eru aðgengileg almenningi, einkum þegar notaður sé ljósrafeindabúnaður (e. *optic-electronic devices*) eða eða um ræði aðrar aðgerðir sem eftirlitsstjórnvald telji líklega hafa í för með sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum vegna þess að þær komi í veg fyrir að hinir skráðu geti neytt réttar síns, notað þjónustu eða byggt á samningi, eða vegna þess að þær séu umfangsmiklar og framkvæmdar kerfisbundið. Ákvæði reglugerðarinnar gilda að öðru leyti almennt um vinnslu persónuupplýsinga sem fást með rafrænni vöktun. Þó ber að hafa í huga að slík vöktun, sem eingöngu þjónar einstaklingi persónulega eða fjölskyldu hans fellur utan gildissviðs reglugerðarinnar, sbr. c-lið 2. mgr. 2. gr. hennar, svo og 2. mgr. 4. gr. frumvarps þessa. Þannig myndi eftirlitsmyndavél sem eingöngu vaktar einkaheimili, þ.e. íbúð þess sem viðhefur vöktunina eða t.d. einkagarð eða bilskúr viðkomandi, ekki falla hér undir. Óheimil er hins vegar uppsetning eftirlitsmyndavéla sé þeim gagnert beint að hóbýlum nágretta. Vöktun annarra svæða, svo sem sameignar fjöleignarhúss, fellur undir lögum. Oft eru slík svæði vöktuð í þeim tilgangi að hindra innbrot og skemmdarverk, og getur slíkt talist til málefnalegs tilgangs. Eigi vöktunin sér stað á svæði sem fáir fara um, svo sem við inngang í fjölbýlishús eða í bílastæðahús, leiðir af ákvæðinu að uppfylla þarf skilyrði um sérstaka nauðsyn. Þá getur ákvörðun um uppsetningu eftirlitsmyndavéla í eða við fjöleignarhús verið bundin öðrum reglum, t.d. ákvæðum fjöleignarhúsalaga nr. 26/1994 sem lúta að ákvörðunum sem tengjast sameign í slíkum húsum.

Ákvæði reglugerðarinnar gera víða ráð fyrir því að aðildarríki setji sérreglur. Þar undir geta fallið sérreglur um rafræna vöktun og má þar benda á 88. gr. reglugerðarinnar sem fjallar um vinnslu í atvinnutengdu samhengi. Þar er tekið fram að í lögum megi kveða á um sértækar reglur til að tryggja vernd réttinda og frelsis við vinnslu persónuupplýsinga starfsmanns í atvinnutengdu samhengi, einkum að því er varðar ráðningu, framkvæmd ráðningarsamnings, stjórnun, undirbúning og skipulagningu vinnu, jafnrétti og fjölbreytileika á vinnustað, heilbrigði og öryggi, vernd eigna vinnuveitanda eða viðskiptavinar og það að vinnutengd réttindi og fríðindi séu nýtt. Rennir þetta ákvæði viðhlítandi stöðum undir að settar séu sérstakar reglur um eftirlitsmyndavélar á vinnustöðum. Samhliða því verður að viðhafa viðeigandi verndar- og öryggisráðstafanir gagnvart hinum skráða, enda ljóst að stöðug vöktun með starfsmönnum á vinnustað felur í sér talsvert inngrip í fríðhelgi einkalífs þeirra. Því skiptir máli að einkalífsréttur þeirra sem sæta vöktun sé virtur eins og kostur er og forðast ber alla óþarfa íhlutun í einkalíf þeirra, en í því felst m.a. að gengið skal úr skugga um hvort markmiðinu með vöktun sé unnt að ná með öðrum og vægari raunhæfum úrræðum.

Sérreglur hafa lengi verið í lögum um rafræna vöktun á vegum þeirra sem sinna öryggisþjónustu í atvinnuskyni, sbr. lög nr. 58/1997 um öryggisþjónustu og reglugerð um sama efni nr. 340/1997. Samkvæmt þeim getur starf þeirra sem fá leyfi ríkislögreglustjóra til að reka öryggisþjónustu m.a. falist í notkun myndavéla við eftirlit með fólki, bæði á lokuðum svæðum og svæðum opnum almenningi. Í starfsleyfum sem ríkislögreglustjóri veitir samkvæmt þessu kemur fram að leyfishafi skuli gæta þess í starfi sínu að safna hvorki né skrá upplýsingar sem óheimilt er að meðhöndla samkvæmt lögum um skráningu og meðferð persónuupplýsinga og að í því felist m.a. að upptaka á myndefni og í kjölfarið skráning á persónuupplýsingum sé óheimil án samþykkis Persónuverndar. Þá hefur lögreglan um árabíl rekið eftirlitsmyndavélar á almannafæri, t.d. í miðbæ Reykjavíkur og víðar. Heimild lögreglunnar til slíks byggist á almennum reglum persónuverndarlaga og reglum settum samkvæmt þeim, sbr. 2. mgr. 45. gr. laganna og reglugerð nr. 322/2001 um meðferð persónuupplýsinga hjá lögreglu. Þá má í þessu sambandi líta til 2. mgr. 82. gr. laga nr. 88/2008 um meðferð sakamála.

Ákvæði 1. mgr. þessarar greinar er samhljóða 1. mgr. 4. gr. nógildandi laga, en þar eru sett fram þau almennu skilyrði fyrir rafrænni vöktun að hún fari fram í málefnalegum tilgangi og þegar um ræðir vöktun svæðis þar sem takmarkaður hópur fer um að jafnaði að hennar sé

sérstök þörf vegna eðlis þeirra starfsemi sem þar fer fram. Hér er um matskennda ákvörðun að ræða en ljóst er að Persónuvernd getur endurskoðað hvort þessum áskilnaði sé fullnægt.

Markmið 2. mgr. ákvæðisins er að árétta að vinnsla persónuupplýsinga sem á sér stað í tengslum við rafræna vöktun skal uppfylla ákvæði þess. Er þá til dæmis átt við að skilyrðum 9. gr. um almennar heimildir til vinnslu og eftir atvikum 11. gr. um sérstök skilyrði fyrir vinnslu viðkvæmra upplýsinga þarf að vera fullnægt.

Í 3. mgr. er nánar vikið að heimildum í tengslum við framkvæmd rafrænnar vöktunar og skilyrði þess að safna efni eða sem verður til við vöktunina, svo sem hljóð- og myndefni, með viðkvæmum persónuupplýsingum. Eru skilyrði þessi m.a. nánar útfærð í fyrirnefndum reglum Persónuverndar um efnið. Þar er áréttað að rafræn vöktun verður að fara fram í yfirlýstum, skýrum og málefnalegum tilgangi, s.s. í þágu öryggis eða eignavörslu. Einnig er áréttað að óheimilt er að varðveita persónuupplýsingar sem til verða við rafræna vöktun nema það sé nauðsynlegt í ljósi tilgangs vöktunarinnar. Málefnaleg ástæða til að varðveita upplýsingar getur m.a. byggst á fyrirmælum í lögum eða því að ábyrgðaraðili vinni enn með þær í samræmi við upphaflegan tilgang með öflun þeirra. Upplýsingar sem verða til við rafræna vöktun má þó ekki varðveita lengur en í 90 daga nema lög heimili. Þetta á ekki við um persónuupplýsingar sem verða til við atburðaskráningu eða eru geymdar á öryggisafritum. Sama á við um upplýsingar sem nauðsynlegar eru til að krafa verði afmörkuð, sett fram eða varin vegna dómsmáls eða annarra slíkra laganauðsynja. Ákvæðið leggur bann við því að efni sem verður til við vöktun verði afhent öðrum eða unnið frekar nema með samþykki viðkomandi eða á grundvelli sérstakra reglna sem Persónuvernd kann að setja skv. 5. mgr. Frá því er gerð sú undantekning, byggð á réttaröryggissjónarmiðum, að heimilt er að afhenda lögreglu upplýsingar um slys eða meintan refsiverðan verknað.

Í 4. mgr. er að finna ákvæði samhljóða 24. gr. gildandi laga sem fjallar um viðvaranir um rafræna vöktun. Samkvæmt því er skylt, þegar rafræn vöktun fer fram á vinnustað eða á almannafæri, að gera glögglega viðvart um vöktunina og hver sé ábyrgðaraðili með merki eða á annan áberandi. Greinin hefur að geyma sérákvæði um viðvörðunarskyldu þegar um rafræna vöktun er að ræða. Hafa almenn viðvörðunarákvæði reglugerðarinnar og frumvarpsins ekki þótt eiga vel við þessa tegund vinnslu persónuupplýsinga og því er talin þörf fyrir sérstakt ákvæði um hana. Hér verða oft engin bein tengsl milli ábyrgðaraðila og hins skráða og ábyrgðaraðila verður e.t.v. ekki kunnugt um nafn eða heimili hins skráða. Af því leiðir að almenna reglan um einstaklingsbundnar viðvaranir á ekki við. Þetta leysir hins vegar ekki ábyrgðaraðila sem er í beinu sambandi við hinn skráða, t.d. í vinnuréttarsambandi, undan þeirri skyldu að fræða hann um þá vinnslu persónuupplýsinga sem fer fram hjá honum. Vöktun með leynd er óheimil nema hún styðjist við lagaheimild eða úrskurð dómara, sbr. einnig 3. gr. reglna Persónuverndar um rafræna vöktun. Sérreglur um þess háttar vöktun koma m.a. fram í ákvæðum um rannsóknarheimildir lögreglu í XI. kafla laga um meðferð sakamála nr. 88/2008.

Lokaákvæðið í 5. mgr. frumvarpsgreinarinnar lýtur að heimild Persónuverndar til að setja reglur og gefa fyrirmæli um rafræna vöktun og vinnslu efnis sem verður til við vöktunina, svo sem hljóð- og myndefni, 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. Eins og fyrr var nefnt voru slíkar reglur settar árið 2006 og hafa tekið ýmsum breytingum. Þess má geta að ásamt 2. tölul. 3. mgr. frumvarpsins veitir umrætt ákvæði svigrúm til að heimila afhendingu myndefnis með viðkvæmum persónuupplýsingum til fleiri aðila en eingöngu lögreglu en slíkt kann að styðjast við málefnaleg rök. Má þar nefna að afhending til tryggingafélags á myndefni af slysi, sem hefur að geyma slíkar upplýsingar, kann að þjóna hagsmunum einstaklinga af skjótri úrlausn um váttryggingarábyrgð og flýta fyrir greiðslu bóta til þeirra.

Um 15. gr.

Ákvæði þetta er samsvarandi 2. mgr. 45. gr. núgildandi laga, sbr. einnig 1. mgr. sömu greinar, um vinnslu upplýsinga um fjárhagsmálefni og lánstraust. Segir í 2. mgr. 45. gr. laganna að í reglugerð skuli mælt fyrir um heimild til skráningar upplýsinga sem verða fjárhagsmálefni og lánstraust fyrirtækja, svo og annarra lögaðila, í því skyni að miðla til annarra upplýsingum um það efni. Á grundvelli 1. mgr. sömu greinar, þess efnis að með reglugerð megi mæla fyrir um meðferð persónuupplýsinga í tiltekinni starfsemi og hjá einstökum starfsstéttum, hefur auk þess verið litið svo á að fjalla megi um vinnslu slíkra upplýsinga um einstaklinga í reglugerð.

Hér er hins vegar lagt til að tekið sé skýrt fram að reglugerð um vinnslu upplýsinga um fjárhagsmálefni og lánstraust taki bæði til þess háttar upplýsinga um einstaklinga og lögaðila. Það að reglugerðin taki til upplýsinga um lögaðila felur í sér undantekningu frá þeirri meginreglu að lögaðilar falli ekki undir gildissvið laganna og hefur sú skipan verið allt frá setningu fyrstu laganna á sviði persónuverndar frá 1981. Rétt þykir að lögpersónum verði áfram tryggð sú vernd sem mælt er fyrir um í gildandi lögum og er gert ráð fyrir að hún verði ekki lakari ef frumvarp þetta verður að lögum en hafa ber meðal annars í huga að atvinnufyrirtæki geta verið grundvöllur fyrir lífsviðurværi einstaklinga og er sanngirni í því fólgin að meðal annars skráning fyrirtækja á vanskilalista sé háð einhverjum reglum, samfara því sem hagsmunir atvinnulífsins af ábyrgum lánveitingum og annars konar fyrirgreiðslum séu tryggðir. Hins vegar er lögð áhersla að eingöngu er gert ráð fyrir að tiltekin ákvæði frumvarpsins gildi um lögaðila og er þar um að ræða sömu efnisákvæði og samkvæmt gildandi lögum. Um einstaklinga gilda hins vegar almennar reglur laganna án sérstakrar tilgreiningar.

Reglugerð ESB geymir engin ákvæði sem lúta að vinnslu upplýsinga um fjárhagsmálefni. Hafa aðildarríki því svigrúm til að setja sérreglur um þau efni innan ramma reglugerðarinnar. Í sumum ríkjum hafa verið settar ítarlegar reglur um vinnslu upplýsinga um fjárhagsmálefni hvort heldur í sér lögum eða inni í ákvæðum almennrar persónuverndarlöggjafar. Dæmi um hið síðarnefnda má sjá í danskri persónuverndarlöggjöf en í gildandi lögum frá árinu 2000 eru tveir kaflar (15.-26. gr.) helgaðir ákvæðum um vinnslu upplýsinga hjá fjárhagsupplýsingastofum. Í fyrirbyggjandi frumvarpi til nýrra persónuverndarlaga í Danmörku, standa ákvæði þessi að miklu leyti óbreytt, þar á meðal áskilnaður um að starfræksla fjárhagsupplýsingastofa sé háð leyfi frá dönsku persónuverndarstofnuninni. Í skýringum með frumvarpinu er vísað til þess að setning sérreglna um þessi efni eigi stoð í 2. mgr. 6. gr. reglugerðar ESB sem kveður á um að aðildarríkjum sé heimilt að viðhalda eða innleiða sértækari ákvæði til að aðlaga beitingu reglugerðarinnar að því er varðar tiltekna vinnslu þannig að samrýmist c- og e-lið 1. mgr. sama ákvæðis með því að setja fram með ítarlegri hætti sértækar kröfur til vinnslunnar.

Í frumvarpsákvæði þessu er ákvæði um vinnslu upplýsinga um fjárhagsmálefni flutt úr lokaákvæði um reglugerðarheimildir í II. kafla um almennar reglur um vinnslu. Kveðið er skýrt á um að starfræksla fjárhagsupplýsingastofa og vinnsla upplýsinga um fjárhagsmálefni og lánstraust bæði einstaklinga og lögaðila sé leyfisskyld. Þó gilda aðeins tilteknar greinar frumvarpsins þegar um lögaðila er að ræða eins og fyrr greinir. Þá kemur meðal annars fram að ákvæðið tekur til vanskilaskráningar en á vinnslu slíkra upplýsinga hefur einkum reynt í gildistíð núgildandi laga. Hafa allmargir úrskurðir gengið hjá Persónuvernd vegna ágreinings um heimildir samkvæmt lögum, reglum og skilmálum í starfsleyfi fjárhagsupplýsingastofu, sem er aðeins ein hér á landi, Creditinfo Lánstraust hf. Hefur því mótast nokkuð föst framkvæmd um túlkun gildandi laga um persónuvernd þegar um er að ræða vanskilaskráningu.

Ítarlega útfærslu á reglum um um söfnun og miðlun upplýsinga um fjárhagsmálefni og lánstraust er að finna í reglugerð nr. 246/2001. Samkvæmt 1. gr. hennar er markmið hennar að tryggja öryggi, áreiðanleika og gæði vinnslu upplýsinga sem varða fjárhagsmálefni og lánstraust einstaklinga, fyrirtækja og annarra lögaðila. Í 1. mgr. 1. gr. er einnig tekið fram að reglugerðin taki ekki til starfsemi sem felst í útgáfu skýrslna um lánshæfi, en um lánshæfismat verður nánar fjallað hér á eftir. Samkvæmt 2. mgr. 1. gr. á fyrrgreind reglugerð einvörðungu við um vinnslu í því skyni að miðla upplýsingum til annarra um fjárhagsmálefni og lánstraust. Ef ekki er stofnað til vinnslu í slíkum tilgangi fellur hún utan gildissviðs reglugerðarinnar. Það á t.d. við um vinnslu banka á slíkum upplýsingum sem einvörðungu er til eigin nota. Í reglugerðinni er nánar lýst skyldum fjárhagsupplýsingastofa sem ábyrgðaraðila og hvaða upplýsingar þeim er heimilt að vinna með. Sérákvæði eru um rétt hins skráða m.a. í 7. og 8. gr. reglugerðarinnar um upplýsingarétt, aðvaranir og andmælarétt. Þá er mælt fyrir um í 5. gr. að eyða skuli upplýsingum jafnharðan þegar þær verða fjögurra ára gamlar, nema annað sé sérstaklega heimilað í starfsleyfi frá Persónuvernd.

Nýmæli í þessu frumvarpsákvæði er að vísa sérstaklega til vinnslu upplýsinga sem lýtur að gerð lánshæfismats og taka fram að sú vinnsla þurfi að byggjast á leyfi Persónuverndar. Á undanförunum árum hefur vinnsla persónuupplýsinga sem fer fram við gerð lánshæfismats haft æ meiri þýðingu sem skilyrði fyrir lánveitingum. Í k-lið 5. gr. laga um neytendalán nr. 33/2013 er lánshæfismat skilgreint sem mat lánveitanda byggt á upplýsingum sem eru til þess fallnar að veita áreiðanlegar vísbendingar um líkindi þess hvort lántaki geti efnt lánssamning. Lánshæfismat skal byggt á viðskiptasögu aðila á milli og/eða upplýsingum úr gagnagrunnum

um fjárhagsmálefni og lánstraust. Þá er í 10. gr. laganna nánar fjallað um hvernig lánshæfismat er gert að skilyrði fyrir gerð samnings um neytendalán. Áþekk ákvæði er að finna í 15. tölul. 4. gr. og 20. gr. laga um fasteignalán til neytenda nr. 118/2016. Loks er að finna sérstök lög um lánshæfismatsfyrirtæki nr. 50/2017 sem byggjast á ESB-reglugerðum sem teknar hafa verið upp í EES-samninginn. Lögin lúta fyrst og fremst að eftirliti Eftirlitsstofnunar EFTA og Fjármálaeftirlitsins með lánshæfismatsfyrirtækjum en lítil reynsla er komin á framkvæmd laganna.

Á síðustu árum hefur Persónuvernd fjallað um kvartanir sem lúta að vinnslu persónuupplýsinga við gerð lánshæfismats þar sem m.a. er byggt á vanskilaupplýsingum. Fyrirgreind reglugerð, nr. 246/2001, tekur ekki til starfsemi sem felst í útgáfu skýrsla um lánshæfi og gilda því hér eingöngu almennar reglur persónuverndarlaga um vinnsluheimildir og réttindi hins skráða. Samkvæmt því þarf vinnsla upplýsinga um fjárhagsmálefni og lánstraust að eiga sér stoð í einhverjum af tölulögum 1. mgr. 8. gr. gildandi laga. Hefur Persónuvernd tekið fram í úrskurðum sínum að sú aðgerð að afla upplýsinga um lánshæfismat hjá Creditinfo, geti einkum stuðst við 2. tölul. 1. mgr. 8. gr. laga nr. 77/2000, þar sem fram kemur að vinnsla sé heimil ef hún er nauðsynleg til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður, sem og 7. tölul. sama ákvæðis, þess efnis að vinna megi með persónuupplýsingar sé það nauðsynlegt til að gæta lögmætra hagsmuna ábyrgðaraðila, þriðja aðila eða þess aðila sem upplýsingum er miðlað til nema grundvallarréttindi og frelsi hins skráða vegi þyngra. Þá hefur vinnsla í tengslum við gerð lánshæfismats einkum verið talin styðjast við síðarnefnda tölulögin. Við mat á því hvort vinnsla sé heimil samkvæmt honum verður að líta til þess hvort hagsmunir ábyrgðaraðila af því að vinnslan fari fram skuli vega þyngra en hagsmunir hins skráða af því að vinnslan fari ekki fram. Þá verður vinnslan einnig að vera nauðsynleg. Verður því að meta í hverju tilviki hvort umrædd skilyrði séu uppfyllt þegar afla á upplýsinga um lánshæfismat.

Eðlilegt væri að setja sérstakar reglur eða frekari ákvæði um framkvæmd persónuverndarreglna í tengslum við gerð og öflun upplýsinga um lánshæfismat inn í fyrirgreinda reglugerð um söfnun og miðlun upplýsinga um fjárhagsmálefni og lánstraust einstaklinga. Þá er álitamál hvort rétt væri að setja sérstök lög um efnið í ljósi þessa mikla umfangs sem er á vinnslu persónuupplýsinga um fjárhagsmálefni og lánstraust og margvíslegra áhrifa sem slík vinnsla hefur á stöðu einstaklinga, einkum gagnvart fjármálaþyrirtækjum.

Um 16. gr.

Í þessu frumvarpsákvæði er fjallað um miðlun persónuupplýsinga úr landi. Það leysir af hólmi þau ákvæði sem standa í V. kafla núgildandi laga í 29. og 30. gr. um það efni. Markmið þessa ákvæðis er fyrst og fremst að taka af skarið um að ákvarðanir framkvæmdastjórnarinnar um miðlun upplýsinga til þriðja lands eða alþjóðastofnunar samkvæmt 45. gr. reglugerðarinnar gildi hér á landi í samræmi við ákvörðun sameiginlegu EES nefndarinnar. Þá er gert ráð fyrir að ráðherra staðfesti slíkar ákvarðanir og birti auglýsingu þar um í Stjórnartíðindum, en til þessa hefur Persónuvernd auglýst ákvarðanir framkvæmdastjórnarinnar í þessum efnum í Stjórnartíðindum. Auk þessa frumvarpsákvæðis munu með lögfestingu ESB-reglugerðarinnar taka gildi ákvæði V. kafla, 44.-50. gr. hennar, sem fjalla um miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana og verður nánar vikið að efni þeirri hér á eftir.

Meginreglan samkvæmt 29. gr. núgildandi laga byggist á 25. gr. ESB-tilskipunarinnar og mælir fyrir um að flutningur persónuupplýsinga til annars ríkis sé heimill ef lög þess veita persónuupplýsingum fullnægjandi vernd. Hvorki tilskipunin né núgildandi lög skilgreina hvað felst í flutningi en í framkvæmdinni er miðað við flutning á eða aðgang að persónuupplýsingum yfir landamæri tveggja eða fleiri ríkja. Rétt er að taka fram að flutningur getur átt sér stað innan sama fyrirtækis eða fyrirtækjasamsteypu sem hefur starfsemi í mörgum löndum. Þannig felur flutningur ekki alltaf í sér miðlun persónuupplýsinga milli tveggja óskyldra aðila. Í 29. gr. núgildandi laga felst að frjálst er að miðla upplýsingum innan Evrópska efnahagssvæðisins enda eru öll ríkin þar bundin af tilskipuninni. Samkvæmt 2. mgr. 29. gr. laganna getur ríki sem framfylgir tilskipuninni talist fullnægja skilyrðum 1. mgr. Það sama gildir um lönd eða staði sem Persónuvernd auglýsir í Stjórnartíðindum að virtum ákvörðunum framkvæmdastjórnar ESB. Í auglýsingum Persónuverndar eru talin upp þau ríki sem viðurkennd hafa verið af framkvæmdastjórninni og eru þau á annan tug þegar þetta er ritað. Framkvæmdastjórnin getur einnig tekið slíkar ákvarðanir varðandi einstaka staði eða viðtökuðila. Þótt það ríki, þar sem

viðtökuaðili er staddur, þyki almennt ekki veita næga vernd er samkvæmt þessu unnt að koma á fyrirkomulagi þar sem tilteknir aðilar innan þess eru taldir öruggir viðtakendur persónuupplýsinga. Var slíku fyrirkomulagi komið á varðandi Bandaríkin en þarlend fyrirtæki gátu fengið viðurkenningu á að þau væru svonefndar „öruggar hafnir“ (e. *safe harbour*). Til öruggra hafna töldust nánar tiltekið fyrirtæki sem ákveðið höfðu að fara að reglum bandaríska viðskiptaráðuneytisins um vernd friðhelgi einkalífs og hélt bandaríska ráðuneytið lista yfir þessi fyrirtæki. Um öruggar hafnir og þau viðmið sem byggt er á var fjallað í ákvörðun framkvæmdastjórnarinnar nr. 2000/520/EB frá 26. júlí 2000. Þá ákvörðun dæmdi Evrópudómstóllinn ógilda með dómi sínum hinn 6. október 2015 (mál nr. C-362/14) þar sem vernd persónuupplýsinga var ekki talin nægilega vel tryggð. Höfust í framhaldinu viðræður milli ESB og Bandaríkjanna um nýtt fyrirkomulag og lyktaði því ferli meðákvörðun framkvæmdastjórnarinnar (ESB) 2016/1250 um heimild til að flytja persónuupplýsingar til aðila í Bandaríkjunum sem falla undir reglur um svokallaðan „friðhelgis skjöld“ (e. *privacy shield*). Með auglýsingu nr. 953/2016 breytti Persónuvernd auglýsingu nr. 228/2010 um flutning persónuupplýsinga til annarra landa þannig að fram kæmi að miðla mætti persónuupplýsingum til bandarískra fyrirtækja sem færu að þeim reglum.

Reglugerð ESB breytir ekki í meginatriðum gildandi rétti um miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana. Ákvæði um efnið í V. kafla hennar eru þó mun ítarlegri en þau sem er að finna í tilskipun ESB um efnið og setja fram með skýrari hætti viðmið til að tryggja persónuvernd við flutning upplýsinga úr landi og undantekningar frá meginreglunni. Í 45. gr. eru birtar almennar meginreglur um miðlun upplýsinga, 46. gr. fjallar um viðeigandi verndarráðstafanir og þá er nýmæli að ítarlegt ákvæði er um bindandi fyrirtækjareglur í 47. gr. reglugerðarinnar, en samkvæmt henni skulu lögbær eftirlitsstjórnvöld, Persónuvernd hér á landi, samþykkja bindandi fyrirtækjareglur í samræmi við samræmingarkerfið sem fjallað er um í 63. gr. reglugerðarinnar. Um skilyrði fyrir setningu slíkra reglna og efni þeirra er nánar fjallað í 1. og 2. mgr. 47. gr. reglugerðarinnar. Tekin er afstaða til skilyrða um miðlun eða birtingu sem ekki er heimil samkvæmt lögum Sambandsins þegar um ræðir dóma og ákvarðanir stjórnvalda í þriðja landi í 48. gr. Loks er að finna ítarlegar reglur um undanþágur frá framangreindum ákvæðum vegna sérstakra aðstæðna í 49. gr. reglugerðarinnar. Í 5. mgr. þess ákvæðis er sérstaklega tilgreint að þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geti lög aðildarríkis takmarkað með ótvíræðum hætti miðlun sérstakra flokka persónuupplýsinga til þriðja lands eða alþjóðastofnunar á grundvelli mikilvægra almannahagsmuna. Aðildarríkin skulu tilkynna framkvæmdastjórninni um slík ákvæði. Hér er aðildarríkjum því veitt svigrúm til strangari reglusetningar varðandi miðlun persónuupplýsinga til þriðju landa eða alþjóðastofnana sé um viðkvæmar persónuupplýsingar að ræða. Ekki er gerð tillaga í frumvarpi þessu, frekar en í danska eða norska frumvarpinu til nýrra persónuverndarlaga, um að nýta þessa heimild sérstaklega með tilgreindu ákvæði um efnið. Er ekki sýnt fram á raunhæfa þörf á slíku ákvæði, a.m.k. ekki að svo stöddu en auk þess ber að hafa í huga að framkvæmdastjórnin getur ákveðið skv. 8. mgr. 45. gr. reglugerðarinnar að falla frá ákvörðun um að þriðja ríki eða alþjóðastofnun veiti fullnægjandi vernd. Lokaákvæði V. kafla reglugerðarinnar, 50. gr. mælir fyrir um alþjóðlega samvinnu um vernd persónuupplýsinga og viðeigandi ráðstafanir sem taldar eru upp í ákvæðinu sem framkvæmdastjórnin og eftirlitsstjórnvöld aðildarríkja gera í samvinnu við þriðju lönd eða alþjóðastofnanir.

Í formála reglugerðarinnar koma fram ítarlegar skýringar á markmiðum hennar í þessum efnunum og á einstaka ákvæðum varðandi miðlun persónuupplýsinga til þriðju landa, einkum í 101.-116. lið, svo og 169. lið, sem hafa ber í huga við framkvæmd þeirra. Þannig er áréttað í 101. lið að flæði persónuupplýsinga til og frá löndum utan Sambandsins og alþjóðastofnunum sé nauðsynlegt vegna vaxandi alþjóðaviðskipta og alþjóðlegrar samvinnu. Aukið flæði af þessu tagi hafi skapað ný viðfangsefni og vanda í tengslum við vernd persónuupplýsinga. Þegar persónuupplýsingum sé miðlað frá Sambandinu til ábyrgðaraðila, vinnsluaðila eða annarra viðtakenda í þriðju löndum eða til alþjóðastofnana ætti það ekki að grafa undan þeirri vernd sem reglugerðin tryggir einstaklingum í Sambandinu, þ.m.t. við framsendingu persónuupplýsinga frá viðkomandi þriðja landi eða alþjóðastofnun til ábyrgðaraðila eða vinnsluaðila í sama eða öðru þriðja landi eða hjá annarri alþjóðastofnun. Miðlun til þriðju landa eða alþjóðastofnana megi þó því aðeins fara fram að reglugerðinni sé fylgt í einu og öllu. Upplýsingunum megi því aðeins miðla, með fyrirvara um önnur ákvæði reglugerðar, að ábyrgðaraðili eða vinnsluaðili hafi farið að skilyrðunum sem mælt er fyrir um í ákvæðum

hennar. Þá er tekið fram í 103. lið formálans að framkvæmdastjórnin geti ákveðið, þannig að gildi hafi alls staðar í Sambandinu, að þriðja land, yfirráðasvæði eða tilgreindur geiri innan þriðja lands eða alþjóðastofnun veiti fullnægjandi persónuvernd, og þannig skapað réttarvissu og einsleitni á öllu svæðinu að því er varðar þriðja land eða alþjóðastofnun sem talin er veita slíka vernd. Í þeim tilvikum sé leyfilegt að miðla persónuupplýsingum til viðkomandi þriðja lands eða alþjóðastofnunar án þess að afla frekari heimildar. Framkvæmdastjórnin geti einnig ákveðið að afturkalla slíka ákvörðun eftir að hún hefur tilkynnt þriðja landinu eða alþjóðastofnuninni um það og upplýst að fullu um ástæður. Um þessar ákvarðanir framkvæmdastjórnarinnar er fjallað í þessu frumvarpsákvæði og mælt fyrir um auglýsingar á þeim.

Í 104. lið formálans er nánar rætt um hvað framkvæmdastjórnin leggur til grundvallar mati sínu á þriðja landi eða á yfirráðasvæði eða tilgreindum geira innan þriðja lands. Henni ber í samræmi við þau grundvallargildi sem Sambandið er byggt á, einkum vernd mannréttinda, að taka tillit til þess hvernig viðkomandi þriðja land virðir grunnreglur réttaríkisins, tryggir aðgang að réttarkerfinu og fer að alþjóðlegum reglum og viðmiðunum um mannréttindi, og til almennra laga og sérlaga, þar á meðal löggjafar um almannaoðryggi, landvarnir og öryggi ríkisins, auk allsherjarreglu og refsiréttar. Við samþykkt ákvörðunar um það hvort vernd sé fullnægjandi að því er varðar yfirráðasvæði eða tilgreindan geira innan þriðja lands á framkvæmdastjórnin að taka tillit til skýrra og hlutlægra viðmiðana, s.s. tiltekinna vinnsluáðgerða og gildissviðs viðkomandi lagareglna og löggjafar sem eru í gildi í þriðja landinu. Þriðja landið á að ábyrgjast að tryggð sé fullnægjandi vernd sem er í meginatriðum sambærileg þeirri sem er tryggð í Sambandinu, einkum þegar vinnsla persónuupplýsinga fer fram í einum eða fleiri tilgreindum geirum. Þriðja landið ætti einkum að tryggja skilvirkt og sjálfstætt eftirlit með persónuvernd og móta verklag vegna samstarfs við persónuverndaryfirvöld í aðildarríkjunum og skráðir einstaklingar eiga að njóta skilvirkra og framfylgjanlegra réttinda og geta leitað réttar síns fyrir stjórnsluvaldi og dómstólum með skilvirkum hætti.

Í 107. lið formálans er áréttað það sem einnig kemur fram í 45. gr. reglugerðarinnar að framkvæmdastjórnin getur staðfest að þriðja land, yfirráðasvæði eða tilgreindur geiri í þriðja landi eða alþjóðastofnun tryggi ekki lengur fullnægjandi persónuvernd. Af þessum sökum á að banna miðlun persónuupplýsinga til viðkomandi þriðja lands eða alþjóðastofnunar nema fullnægt sé kröfum reglugerðarinnar um miðlun með fyrirvara um viðeigandi verndarráðstafanir, þ.m.t. bindandi fyrirtækjareglur, og undanþágur vegna sérstakra aðstæðna. Í því tilviki á að gera ráð fyrir samráði milli framkvæmdastjórnarinnar og umræddra þriðju landa eða alþjóðastofnana. Framkvæmdastjórnin á að tilkynna þriðja landinu eða alþjóðastofnuninni tímanlega um ástæðurnar og hefja viðræður við það eða hana til þess að ráða bót á ástandinu.

Þegar ekki liggur fyrir hvort fullnægjandi vernd er fyrir hendi á ábyrgðaraðili eða vinnsluadili að gera ráðstafanir til að bæta upp skort á persónuvernd í þriðja landi með viðeigandi verndarráðstöfunum í þágu skráðs einstaklings. Þetta er nánar útfært 46. gr. reglugerðarinnar og 108. lið formálans. Viðeigandi verndarráðstafanir geta m.a. falist í því að nota bindandi fyrirtækjareglur, stöðluð ákvæði um persónuvernd sem framkvæmdastjórnin hefur samþykkt, stöðluð ákvæði um persónuvernd sem eftirlitsyfirvald hefur samþykkt eða samningsákvæði sem eftirlitsyfirvald hefur heimilað. Þessar verndarráðstafanir eiga að tryggja að farið sé að kröfum um persónuvernd og að virt séu réttindi skráðra einstaklinga sem varða vinnslu innan Sambandsins, þ.m.t. að fyrir liggi framfylgjanleg réttindi skráðra einstaklinga og skilvirk lagaleg úrræði, m.a. að hægt sé að leita réttar síns fyrir stjórnsluvaldi eða dómstólum með skilvirkum hætti og að krefjast bóta, í Sambandinu eða í þriðja landi. Þær eiga einkum að varða fylgni við almennar meginreglur um vinnslu persónuupplýsinga og meginreglur um innbyggða og sjálfgefna persónuvernd. Opinber yfirvöld eða stofnanir geta einnig miðlað upplýsingum til opinberra yfirvalda eða stofnana í þriðju löndum eða til alþjóðastofnana sem hafa samsvarandi skyldur eða hlutverk, m.a. á grundvelli ákvæða sem eru felld inn í stjórnvaldsráðstafanir sem veita skráðum einstaklingum framfylgjanleg og skilvirk réttindi. Afla ætti heimildar eftirlitsstjórnvalds ef gert er ráð fyrir verndarráðstöfunum í stjórnvaldsráðstöfunum sem eru ekki lagalega bindandi.

Í 111. lið formálans koma fram frekari skýringar á ákvæði 49. gr. reglugerðarinnar um undanþágur vegna sérstakra aðstæðna, en slíkar undanþágur eru taldar upp í sjö staflaðum í 1.

mgr. 49. gr. Í framangreindum formálslið er bent á að setja ætti ákvæði um möguleika á miðlun við sérstakar aðstæður þegar skráður einstaklingur hefur veitt ótvírætt samþykki sitt og miðlunin er tilfallandi og nauðsynleg í tengslum við samning eða réttarkröfu, hvort heldur er við dómsmeðferð eða stjórnáðferð eða aðra málsmeðferð utan dómstóla, þ.m.t. málsmeðferð hjá eftirlitsaðilum. Einnig ætti að gera ráð fyrir möguleika á miðlun þegar brýnir almannahagsmunir, sem mælt er fyrir um í lögum Sambandsins eða lögum aðildarríkis, krefjast þess eða þegar miðlunin er úr skrá sem komið var á fót samkvæmt lögum og ætluð er til þess að almenningur eða þeir sem hafa lögmætra hagsmuna að gæta geti skoðað hana. Í síðarnefnda tilvikinu ætti miðlunin ekki að ná til persónuupplýsinganna í heild sinni eða heilla flokka upplýsinga í skránni og miðlunin ætti, þegar gert er ráð fyrir að þeir sem hafa lögmætra hagsmuna að gæta geti skoðað skrána, aðeins að fara fram að beiðni þeirra eða, ef þeir eiga að vera viðtakendur upplýsinganna, að teknu fullu tilliti til hagsmuna og grundvallarréttinda viðkomandi skráðs einstaklings. Þá er tekið fram í 112. lið formálans að undanþágurnar ættu einkum að gilda um miðlun upplýsinga sem eru nauðsynlegar vegna mikilvægra almannahagsmuna. Tekin eru dæmi um alþjóðleg upplýsingaskipti milli samkeppnisyrvalda, skatta- eða tolfyrvalda, milli fjármálaeftirlitsstofnana, milli stofnana sem starfa á sviði almannatrygginga eða lýðheilsu, t.d. við að rekja smitleiðir vegna smitsjúkdóma eða í þeim tilgangi að draga úr og/eða útrýma lyfjamisnotkun í íþróttum. Einnig ætti miðlun persónuupplýsinga að teljast lögmæt þegar hún er nauðsynleg til verndar þáttum sem skipta sköpum fyrir brýna hagsmuni skráðs einstaklings eða annars einstaklings, þ.m.t. líkamlega friðhelgi eða líf, ef hinn skráði er ekki fær um að veita samþykki sitt

Þegar ekki hefur verið tekin ákvörðun um hvort fullnægjandi vernd er fyrir hendi geta lög aðildarríkis sérstaklega takmarkað, í ljósi mikilvægra almannahagsmuna, miðlun tiltekinna flokka upplýsinga til þriðja lands eða alþjóðastofnunar, sbr. það sem fyrr sagði um 5. mgr. 49. gr. reglugerðarinnar Aðildarríkin eiga að tilkynna framkvæmdastjórninni um slík ákvæði. Telja mætti miðlun persónuupplýsinga um skráðan einstakling, sem er líkamlega eða í lagalegum skilningi ófær um að veita samþykki sitt, til alþjóðlegrar stofnunar á sviði mannúðarmála vegna framkvæmdar verkefnis samkvæmt Genfarsamningunum eða til að framfylgja alþjóðlegum mannúðarlögum sem gilda um vopnuð átök, nauðsynlega í ljósi mikilvægra almannahagsmuna eða þess að hún varði brýna hagsmuni hins skráða.

Þá er bent á það í 113. lið formála reglugerðarinnar að miðlun, sem telja má að verði ekki endurtekin og sem aðeins varðar takmarkaðan fjölda skráðra einstaklinga, gæti einnig verið möguleg með tilliti til mikilvægra lögmætra hagsmuna sem ábyrgðaraðili gætir þegar hagsmunir eða réttindi og frelsi skráðs einstaklings ganga þeim ekki framar og ef ábyrgðaraðilinn hefur kannað allar aðstæður í tengslum við miðlun upplýsinganna. Ábyrgðaraðilinn ætti einkum að skoða eðli persónuupplýsinganna, tilgang og tímalengd fyrirhugaðrar vinnsluáðgerðar eða -aðgerða, svo og aðstæður í upprunalandinu, þriðja landinu og endanlegu viðtökulandi og ætti að gera viðeigandi verndarráðstafanir til að vernda grundvallarréttindi og frelsi einstaklinga með tilliti til vinnslu persónuupplýsinga þeirra. Slík miðlun ætti aðeins að vera möguleg í einstaka tilvikum þegar engin annarra nefndra ástæðna til miðlunar á við. Taka ætti tillit til lögmætra væntinga samfélagsins um aukna þekkingu þegar um er að ræða vísindalegar eða sagnfræðilegar rannsóknir eða tölfræðilegan tilgang. Ábyrgðaraðilinn ætti að tilkynna eftirlitsyfirlindinu og hinum skráða um miðlunina.

Loks skal vikið að skýringum á 50. gr. reglugerðarinnar um alþjóðlega samvinnu um vernd persónuupplýsinga í 116. lið formálans. Tekið er fram að þegar persónuupplýsingar fara yfir landamæri utan Sambandsins geti það leitt til aukinnar áhættu fyrir getu einstaklinga til að neyta réttar síns til persónuverndar, einkum verja sig gegn ólögmætri notkun eða birtingu upplýsinganna. Jafnframt geti eftirlitsstjórnvöld komist að þeirri niðurstöðu að þau geti ekki fylgt eftir kvörtunum eða sinnt rannsóknum í tengslum við starfsemi utan landamæra sinna. Ófullnægjandi valdheimildir til forvarna eða úrbóta, misræmi milli lagareglna og hindranir sem lúta að framkvæmd á borð við takmarkað fjármagn geti staðið í vegi fyrir viðleitni þeirra til að vinna saman yfir landamæri. Þess vegna er hvatt til nánara samstarfs meðal eftirlitsstjórnvalda á sviði persónuverndar til að hjálpa þeim við að skiptast á upplýsingum og vinna að rannsóknum með samsvarandi alþjóðlegum aðilum. Í þeim tilgangi að móta fyrirkomulag alþjóðlegrar samvinnu til að greiða fyrir og veita gagnkvæma aðstoð á alþjóðavettvangi við framkvæmd löggjafar um vernd persónuupplýsinga ættu framkvæmdastjórnin og eftirlitsstjórnvöld að skiptast á upplýsingum og starfa með lögbærum yfirlindum þriðju landa að verkefnum sem

tengjast beitingu valdheimilda þeirra, á gagnkvæmum grundvelli og í samræmi við reglugerðina.

Um 17. gr.

Þetta frumvarpsákvæði er fyrsta ákvæði III. kafla sem fjallar um réttindi hins skráða og takmarkanir á þeim. Kaflinn kemur í stað III. kafla núgildandi laga sem fjallar um upplýsingarétt og upplýsingaskyldu, fræðslu- og viðvörunarskyldu og rétt til rökstuðnings. Stærsti hluti ákvæða þessa kafla byggist á tilvísunum til mun ítarlegri ákvæða reglugerðarinnar um sama efni, en markmið þess að bæta þeim í frumvarpið er að lögin veiti yfirsýn á einum stað yfir réttindi hins skráða, í stað þess að aðeins sé fjallað um sérreglur og undantekningar sem aðildarríkjum er heimilt að gera á ákvæðum reglugerðarinnar. Fjallað er um réttindi hins skráða í III. kafla reglugerðarinnar. Ákvæði kaflans endurspeglar að stóru leyti reglur og framkvæmd um efnið sem þegar gilda samkvæmt ESB-tilskipuninni og gildandi lögum. Reglugerðin setur þó fram ítarlegri reglur um réttindi hins skráða og nokkur ný réttindi bætast við. Þá ber að hafa í huga að réttindi þessi ber ávallt að skoða í ljósi meginreglnanna sem fram koma í 8. gr. frumvarpsins og II. kafla reglugerðarinnar. Þá fjallar hluti ákvæða þessa kafla, 17.-19.gr. frumvarpsins um undantekningar sem reglugerðin heimilar aðildarríkjum að gera frá ákvæðum hennar um réttindi hins skráða.

Í 16. gr. núgildandi laga er fjallað um skyldu ábyrgðaraðila til að veita almenna vitneskju um þá vinnslu persónuupplýsinga sem fram fer á hans vegum og byggist það á 2. mgr. 21. gr. tilskipunar ESB. Samkvæmt því er ábyrgðaraðila skylt, sé þess óskað, að veita almenna vitneskju um þá vinnslu persónuupplýsinga sem fram fer á hans vegum. Markmið ákvæðisins er í fyrsta lagi að veita hverjum sem er færi á að ganga úr skugga um hvort honum þyki vinnslan áhugaverð og ástæða til að fá um hana gleggri upplýsingar. Þá var markmið með setningu ákvæðisins í öðru lagi að skapa hinum skráða forsendur til að meta hvort hann kærði sig um að viðkomandi ábyrgðaraðili ynni með upplýsingar um sig eða ekki. Sambærilegt ákvæði er ekki að finna í reglugerðinni heldur er aukin áhersla lögð á að ábyrgðaraðilinn sýni frumkvæði að auknu gagnsæi, t.a.m. með setningu persónuverndarstefnu. Er það í samræmi við meginregluna um ábyrgðarskyldu.

Framsetning þessarar frumvarpsgreinar er með þeim hætti að í 1. mgr. er fjallað um meginreglur um gagnsæi upplýsinga, einkum tilkynningar til hins skráða svo hann geti neytt upplýsingarréttar síns og réttar til aðgangs. Í 2. mgr. er fjallað um rétt hins skráða til upplýsinga um vinnslu og rétt til aðgangs að upplýsingum um sig. 3. mgr. geymir undantekningar frá réttindum hins skráða í þessu tilliti. 4. mgr. geymir sérreglu um aðgang að málum sem eru til meðferðar hjá stjórnvöldum og 5. gr. geymir sérreglu með undanþágu frá skyldu til að tilkynna hinum skráða um öryggisbrot. Verður nú nánar vikið að hverri þessara málsgreina.

Fyrirmæli 1. mgr. um að ábyrgðaraðili skuli gera viðeigandi ráðstafanir til að tryggja gagnsæi, eru byggð á 12. gr. reglugerðarinnar sem lýsir í ítarlegu máli kröfum sem eru gerðar til gagnsæis upplýsinga, tilkynninga og nánari reglna til að skráður einstaklingur geti neytt réttar síns. Í 58. lið formála reglugerðarinnar er nánar lýst inntaki meginreglunnar um gagnsæi. Í henni felst að hvers kyns upplýsingar, sem ætlaðar eru almenningi eða skráðum einstaklingi, skulu vera gagnorðar, aðgengilegar og auðskiljanlegar og á skýru og einföldu máli, auk þess sem beita á sjónrænum aðferðum eftir því sem við á. Bent er á að veita má upplýsingar um vinnslu á rafrænu formi, t.d. á vefsetri, þegar þær eru ætlaðar almenningi. Þetta á einkum við í tilvikum þar sem erfitt er fyrir skráðan einstakling að vita og skilja, vegna hins mikla fjölda aðila sem koma að máli og flókinar tækni sem notuð er, hvort, af hverjum og í hvaða tilgangi upplýsingum er safnað um hann, s.s. þegar um er að ræða auglýsingar á netinu. Þar sem börn þurfa að njóta sérstakrar verndar ættu hvers kyns upplýsingar og tilkynningar, þegar vinnsla beinist að barni, að vera á skýru og einföldu máli sem barnið getur auðveldlega skilið. Þá er því lýst í 59. lið formálans að koma ætti á nánari reglum til að greiða fyrir því að skráður einstaklingur geti neytt réttar síns til upplýsinga og aðgangs, m.a. gera ráðstafanir sem gera honum kleift að fara fram á og, ef við á, fá því endurgjaldslaust framgengt að honum sé veittur aðgangur að persónuupplýsingum, að þær séu leiðréttar eða þeim eytt, sem og að hann geti neytt andmælaréttar síns. Ábyrgðaraðili ætti einnig að sjá til þess að hægt sé að leggja fram beiðnir rafrænt, einkum þegar vinnsla persónuupplýsinga fer fram með rafrænum hætti. Ábyrgðaraðila ber að svara beiðnum skráðs einstaklings án ótilhlýðilegrar tafar og innan eins mánaðar hið

mesta, sbr. 4. mgr. 12. gr. reglugerðarinnar og færa fram rök ef hann hyggst ekki taka beiðnir til greina.

Í 2. mgr. frumvarpsákvæðisins er mælt fyrir um rétt manns til upplýsinga um vinnslu og gildir sá réttur án tillits til þess hvort persónuupplýsinga hefur verið aflað hjá honum sjálfum eða ekki. Þá er mælt fyrir um rétt manns til aðgangs að persónuupplýsingum um sig samkvæmt fyrirmælum 13.-15. gr. reglugerðarinnar með þeim undantekningum sem greinir í 3. mgr. þessa frumvarpsákvæðis. Ákvæðið felur bæði í sér að hinum skráða er veittur réttur til upplýsinga en að sama skapi er sú skylda lögð á ábyrgðaraðila að fræða hinn skráða um vinnsluna, sk. fræðsluskylda.

Í 13. gr. reglugerðarinnar er fjallað um upplýsingar sem ber að veita við öflun persónuupplýsinga hjá skráðum einstaklingi. Ákvæðið felur að stóru leyti í sér þær reglur og framkvæmd sem leidd verður af 20. gr. gildandi laga en bætir einnig við nýjum réttindum s.s. að ábyrgðaraðili sem hyggst vinna persónuupplýsingar frekar í öðrum tilgang en þeim sem lá að baki söfnun þeirra skuli láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en frekari vinnsla hefst, sbr. 3. mgr. 13. gr. Þá er sú undantekning gerð í 4. mgr. að réttur samkvæmt 13. gr. gildir ekki hafi hinn skráði þegar fengið vitneskju um vinnsluna.

Í 14. gr. reglugerðarinnar er fjallað um upplýsingar sem ber að veita þegar persónuupplýsingar hafa ekki fengist hjá skráðum einstaklingi. Einnig hér geymir reglugerðin nokkuð ítarlegri reglur en gilda samkvæmt 21. gr. núgildandi laga. Þá er getið undantekninga frá þessum rétti í 5. mgr. 14. gr. sem eru áþekkar þeim sem nú gilda og eiga við ef hinn skráði hefur þegar fengið upplýsingarnar (a-liður), ekki er unnt að veita upplýsingarnar eða það kostar óhóflega fyrirhöfn (b-liður), skýrt er mælt fyrir um öflun eða miðlun upplýsinganna í lögum (c-liður) eða persónuupplýsingar eru bundnar trúnaði á grundvelli þagnarskyldu (d-liður).

Í 15. gr. reglugerðarinnar er fjallað um rétt skráðs einstaklings til aðgangs. Þær breytingar eru ráðgerðar frá 16. gr. núgildandi laga að ekki er lengur rætt um rétt til almennrar vitneskju um vinnslu persónuupplýsinga, þ.e. að ábyrgðaraðila sé skylt að veita hverjum sem þess óskar almenna vitneskju um þá vinnslu persónuupplýsinga sem fer fram á hans vegum. Þess í stað kveður 1. mgr. 15. gr. reglugerðarinnar á um rétt skráðs einstaklings til að fá staðfestingu á því frá ábyrgðaraðila hvort unnið sé með persónuupplýsingar um hann sjálfan, og ef svo er rétt til aðgangs að persónuupplýsingum og upplýsingum um eftirtalin atriði; tilgang vinnslunnar (a-liður), viðkomandi flokka persónuupplýsinga (b-liður) viðtakendur eða flokka viðtakenda sem fengið hafa eða munu fá persónuupplýsingarnar í hendur, einkum viðtakendur í þriðju löndum eða alþjóðastofnanir (c-liður), ef mögulegt er, hversu lengi fyrirhugað er að varðveita persónuupplýsingarnar eða, ef það reynist ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða það (d-liður), að fyrir liggi réttur til að fara fram á það við ábyrgðaraðila að láta leiðrétta persónuupplýsingar, eyða þeim eða takmarka vinnslu þeirra hvað hinn skráða varðar eða til að andmæla slíkri vinnslu (e-liður), réttinn til að leggja fram kvörtun hjá eftirlitsyfirlaldi (f-liður), ef persónuupplýsinganna er ekki aflað hjá hinum skráða, allar fyrirliggjandi upplýsingar um uppruna þeirra (g-liður) og hvort fram fari sjálfvirk ákvarðanatataka, þ.m.t. gerð persónusniðs og þá marktækar upplýsingar um þau rök sem þar liggja að baki og einnig þýðingu og fyrirhugaðar afleiðingar vinnslu fyrir hinn skráða (h-liður). Almennt eru aðgangsreglur 15. gr. reglugerðarinnar um rétt hins skráða strangari en þær sem nú gilda.

Ákvæði 13.-15. gr. reglugerðarinnar og 2. mgr. þessa ákvæðis um rétt hins skráða til upplýsinga og aðgangs ber að skýra í ljósi 60. -64. liða formála hennar. Í 60. lið formálans er bent á að meginreglurnar um sanngirni og gagnsæi við vinnslu krefjast þess að skráðum einstaklingi sé tilkynnt um að vinnsluáðgerð standi yfir og hver sé tilgangur hennar. Ábyrgðaraðila beri að veita hinum skráða frekari upplýsingar sem nauðsynlegar séu til að tryggja að gætt sé sanngirni og gagnsæi við vinnslu persónuupplýsinga með tilliti til þeirra sérstöku aðstæðna og samhengis sem eiga við um vinnslu þeirra. Enn fremur ætti að upplýsa hinn skráða um að gert hafi verið persónusnið og um afleiðingar þess. Þegar persónuupplýsingar séu fengnar hjá skráðum einstaklingi ætti einnig að upplýsa hann um hvort honum sé skylt að láta persónuupplýsingarnar í té og um það hvaða afleiðingar það hafi að veita þær ekki. Hægt sé að láta staðlaðar tákmyndir fylgja þessum upplýsingum til að veita greinargott yfirlit yfir fyrirhugaða vinnslu á auðsýnilegan, skiljanlegan og auðlæsilegan hátt. Táknmyndirnar ættu að vera á tölvulesanlegu sniði þegar þær séu settar fram rafrænt. Nánar er fjallað um tímamörk í þessu tilliti í 61. gr. formálans og tekið fram að veita eigi skráðum einstaklingi upplýsingar í tengslum við vinnslu persónuupplýsinga um hann á þeim tíma þegar upplýsinganna er aflað hjá

honum eða, þegar persónuupplýsinganna er aflað frá öðrum heimildum, innan hæfilegs tíma, með hliðsjón af aðstæðum í hverju tilviki fyrir sig. Ef fá megi öðrum viðtakanda persónuupplýsingar í hendur með lögmætum hætti ætti að tilkynna það hinum skráða þegar viðtakandinn fái persónuupplýsingarnar í fyrsta sinn. Hyggist ábyrgðaraðili vinna með persónuupplýsingarnar í öðrum tilgangi en þeim sem lá að baki söfnun þeirra ætti hann að láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum nauðsynlegum upplýsingum. Ef ekki sé hægt að skýra hinum skráða frá uppruna persónuupplýsinganna vegna þess að þær komi frá mismunandi heimildum ætti að veita almennar upplýsingar. Undantekningar frá þessu eru nánar útskýrðar í 62. lið formálans, m.a. hvernig megi líta svo á að upplýsingagjöf geti falið í sér óhóflega fyrirhöfn. Það gæti einkum átt við þegar vinnslan fari fram vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi. Í því sambandi ætti að taka tillit til fjölda skráðra einstaklinga, þess hversu gamlar upplýsingarnar séu og viðeigandi verndarráðstafana sem gerðar hafi verið. Rétturinn til aðgangs er nánar útfærður í 63. lið formálans. Þar er áréttað að skráðum einstaklingi eigi að vera auðveldað að neyta réttar síns til aðgangs til þess að hann geti gert sér grein fyrir því hvort vinnslan fari fram með lögmætum hætti og sannreynt það. Þetta feli m.a. í sér rétt skráðra einstaklinga til aðgangs að upplýsingum sem varða heilsufar þeirra, t.d. upplýsingum í sjúkraskrá á borð við sjúkdómsgreiningu, niðurstöður rannsókna, mat meðhöndlandi lækna og hvers kyns meðferðir eða inn grip. Sérhver skráður einstaklingur ætti því einkum að hafa rétt til að fá vitneskju og tilkynningu um tilganginn með vinnslu persónuupplýsinganna, vinnslutímabil upplýsinganna ef unnt sé, viðtakendur þeirra, hvaða rök liggi að baki sjálfvirkri vinnslu persónuupplýsinga og afleiðingar slíkrar vinnslu, einkum þegar hún sé byggð á gerð persónusniðs. Ábyrgðaraðili ætti, ef mögulegt sé, að vera fær um að veita hinum skráða fjaraðgang að öruggu kerfi sem veiti honum beinan aðgang að persónuupplýsingum um sig. Sá réttur ætti ekki að hafa neikvæð áhrif á réttindi eða frelsi annarra, þ.m.t. viðskiptaleyndarmál eða hugverkaréttindi og þá einkum höfundarrétt til verndar hugbúnaðinum. Niðurstaða þessara atriða ætti þó ekki að vera sú að skráðum einstaklingi sé neitað um allar upplýsingar. Þegar ábyrgðaraðili vinni með mikið magn upplýsinga sem varða skráðan einstakling ætti hann að geta óskað eftir því að hinn skráði tilgreini nánar um hvaða upplýsingar eða vinnsluáðgerðir beiðnin snúist, áður en upplýsingarnar séu veittar. Þá er tekið fram í 64. lið formálans að ábyrgðaraðili ætti að gera allar eðlilegar ráðstafanir til að sannreyna deili á skráðum einstaklingi sem óski eftir aðgangi, einkum í tengslum við þjónustu á Netinu og netauðkenni..

Í 3. og 4. mgr. frumvarpsákvæðisins er mælt fyrir um undantekningar sem gerðar eru frá réttindum hins skráða samkvæmt 13.-15. gr. reglugerðarinnar. Þessar undantekningar byggjast á heimildum sem fram koma í 1. mgr. 23. gr. reglugerðarinnar. Þar kemur m.a. fram að í lögum aðildarríkis, sem ábyrgðaraðili eða vinnsluadili gagna heyrir undir, er heimilt að takmarka með löggjafarráðstöfun gildissvið þeirra skyldna og réttinda, sem um getur í 12.-22. gr. ef slík takmörkun virðir eðli grundvallarréttinda og mannfrelsis og telst nauðsynleg og hófleg ráðstöfun í lýðræðisþjóðfélagi með hliðsjón af 10 nánar tilgreindum atriðum.

3. og 4. mgr. frumvarpsákvæðisins eiga aðeins við ef tilvik geta ekki fallið undir undantekningarákvæði 4. mgr. 13. gr., 5. mgr. 14. gr. og 4. mgr. 15. gr. Ljóst er að ef beita á undantekningarákvæði 3. mgr. þarf að fara fram mat á þeim hagsmunum sem nefndir eru í ákvæðinu ef víkja á frá rétti hins skráða til upplýsinga eða aðgangs. Þannig verður að vega hagsmuni hins skráða af því að fá upplýsingar eða aðgang andspænis hagsmunum annarra einstaklinga, t.d. vegna tillits til viðskiptaleyndarmála einkaaðila, ólöggráða barns hins skráða eða vitna í dómsmáli. Þá er mikilvægt að hafa í huga að gerð er krafa um „brýna“ hagsmuni einstaklinga sem þarf að sýna fram á til að réttlæta undantekningu frá rétti hins skráða til upplýsinga og aðgangs. Markmið 3. mgr. skarast að nokkru leyti við 6. tölul. 4. mgr. frumvarpsákvæðisins sem einnig vísar til réttinda annarra einstaklinga.

Þau atriði, sem vísað er til í 4. mgr. 17. gr. frumvarpsins um takmarkanir á réttindum hins skráða skv. 13.-15. gr. reglugerðarinnar, byggjast á 23. gr. reglugerðarinnar. Í 2. mgr. eru talin upp eftirfarandi atriði sem geta verið grundvöllur takmörkunar: 1) þjóðaröryggi 2) landvarnir 3) almannaröryggi 4) þörf á að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsivíðurlögum, 5) önnur mikilvæg markmið sem þjóna almannahagsmunum, einkum efnahagslegum eða fjárhagslegum, þ.m.t. vegna gjaldeyrismála, fjárlaga og skattamála, lýðheilsu og almannatrygginga, 6) vernd skráðs einstaklings, brýnir

almannahagsmunir eða grundvallarréttindi annarra, 7) það að einkaréttarlegum kröfum sé fullnægt og 8) lagaákvæði um þagnarskyldu.

Um heimildir ríkja til að beita takmörkunum samkvæmt 23. gr. reglugerðarinnar er nánar fjallað í 73. lið formála hennar. Er þar áréttað að aðildarríki geta sett í landslög takmarkanir í tengslum við rétt til upplýsinga, aðgangs að persónuupplýsingum og leiðréttingar á þeim eða eyðingar þeirra, rétt til að flytja eigin gögn, rétt til andmæla, ákvarðanir sem byggjast á gerð persónusniðs, ásamt tilkynningum til skráðs einstaklings um öryggisbrot við meðferð persónuupplýsinga og tilteknum tengdum skyldum ábyrgðaraðila, að því marki sem nauðsynlegt er og hóflegt í lýðræðisþjóðfélagi til að vernda almannaoöryggi. Í tengslum við þau atriði sem talin eru upp í 1. mgr. 23. reglugerðarinnar er vísað til verndunar mannlífa, einkum vegna viðbragða við náttúruhamförum og hamförum af mannavöldum, vegna forvarna, rannsókna og saksóknar í refsímálum eða fullnustu refsiviðurlaga, m.a. til að vernda gegn og koma í veg fyrir ógnir við almannaoöryggi eða brot á siðareglum í lögvernduðum atvinnugreinum, vegna annarra mikilvægra markmiða sem þjóna almannahagsmunum aðildarríkis, einkum mikilvægum efnahagslegum eða fjárhagslegum hagsmunum, vegna færslu opinberra skráa í þágu almannahagsmuna, frekari vinnslu persónuupplýsinga í skjalasöfnum til að útvega sérstaka vitneskju um stjórn málahegðun undir stjórnnum fyrrverandi einræðisríkja eða til að vernda hinn skráða eða réttindi og frelsi annarra, m.a. til að njóta félagslegrar verndar, lýðheilsu og mannúðar. Þessar takmarkanir ættu að vera í samræmi við kröfurnar sem settar eru fram í sáttmála ESB um grundvallarréttindi og mannréttindasáttmála Evrópu.

Í 5. mgr. 17. gr. frumvarpsins er sérregla sem kveður á um að upplýsingar í málum sem eru til meðferðar hjá stjórnvöldum megi undanþiggja réttinum til aðgangs samkvæmt 1. mgr. 15. gr. reglugerðarinnar að sama marki og gildir um undantekningar á upplýsingarétti samkvæmt upplýsingalögum og stjórnsýslulögum. Er þetta sambærileg regla við á sem nú er að finna í 3. mgr. 19. gr. gildandi laga. Með þessu eru mörkuð skil upplýsingaréttar samkvæmt stjórnsýslulögum nr. 97/1993 og upplýsingalögum nr. 140/2012 annars vegar og persónuupplýsingalögum hins vegar. Miðað er við að réttur til aðgangs samkvæmt persónuupplýsingalögum verði sambærilegur við rétt aðila máls skv. 15. gr. stjórnsýslulaga og rétt almennings skv. 5. gr. upplýsingalaga. Af því leiðir að aðili getur ekki á grundvelli persónuupplýsingalaga krafist aðgangs að skjölum eða öðrum gögnum sem undanþegin eru aðgangi samkvæmt stjórnsýslu- eða upplýsingalögunum. Með vísun til þess að hjá einkaaðilum getur reynt á svipaða hagsmuni og hjá stjórnvöldum gerir frumvarpsákvæðið ráð fyrir því að sömu reglur gildi um aðgang að gögnum þeirra og gilda um aðgang að gögnum stjórnvalda, þ.e. varðandi innanhússkjöl og vinnugögn.

Í 6. mgr., sem er lokamálsgrein þessa frumvarpsákvæðis er tekið fram að 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, en í þessum tölulíðum er fjallað um þjóðaröryggi og þörf á því að koma í veg fyrir, rannsaka, koma upp um eða saksækja fyrir refsiverð brot eða fullnægja refsiviðurlögum. Þessi heimild byggist einnig á 23. gr. reglugerðarinnar um takmarkanir sem aðilar geta sett í landslög og er þar beinlínis vísað til 34. gr. reglugerðarinnar. Nánar verður fjallað um öryggisbrot og skyldu til að tilkynna um þau í 27. gr. frumvarpsins og skýringum við þá grein.

Um 18. gr.

Þetta frumvarpsákvæði geymir sérreglur um vinnslu vegna rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi og skjalavistunar í þágu almannahagsmuna, þar á meðal undantekningar frá ákveðnum ákvæðum þegar vinnsla í slíkum tilgangi á sér stað. Í núgildandi lögum og tilskipun ESB er ekki að finna sambærilegt ákvæði þótt vikið sé að vinnslu í þessum tilgangi á nokkrum stöðum. Í 2. tölul. 7. gr. laganna sem endurspeglar svokallaða tilgangsreglu er tekið fram að frekari vinnsla persónuupplýsinga í sagnfræðilegum, tölfraðilegum eða vísindalegum tilgangi teljist ekki ósamrýmanleg að því tilskildu að viðeigandi öryggis sé gætt, en samsvarandi ákvæði er að finna í 5. tölul. 8. gr. frumvarps þessa sem lýst var að framan. Í reglum um almennar vinnsluheimildir í 8. gr. núgildandi laga er vísað til þess í 5. tölul. að vinnsla er heimil sé hún nauðsynleg vegna verks sem er unnið í þágu almannahagsmuna. Hefur þetta ákvæði verið skýrt svo að átt sé við verkefni í almannaðágu, þ.e. sem hefur þýðingu fyrir breiðan hóp manna, t.d. vinnslu í sagnfræðilegum, tölfraðilegum eða vísindalegum tilgangi. Samsvarandi ákvæði er nú í 5. tölul. 9. gr. frumvarps þessa. Í 9. tölul. 1. mgr. 9. gr. núgildandi

laga er veitt heimild til vinnslu viðkvæmra persónuupplýsinga vegna tölfraði- eða vísindarannsókna enda sé persónuvernd tryggð með tilteknum ráðstöfunum eftir því sem við á. Samsvarandi ákvæði er að finna í 10. tölul. 1. mgr. 11. gr. frumvarps þessa. Þá er tekið fram í 1. mgr. 19. gr. núgildandi laga að upplýsingaréttur hins skráða nær ekki til upplýsinga sem einvörðungu eru notaðar til tölfraðivinnslu eða vísindarannsókna, enda geti vinnsla þeirra ekki haft bein áhrif á hagsmuni hans. Eins og kemur fram í 25. gr. núgildandi laga að reglur á skyldan til að leiðrétta, eyða, bæta við eða stöðva vinnslu á röngum, villandi eða ófullkomnum persónuupplýsingum ekki við ef viðkomandi annmarki hefur ekki áhrif á hagsmuni hins skráða. Hefur verið litið svo á að sögulegar upplýsingar og upplýsingar sem safnað er í vísindaskyni eða til tölfraðivinnslu mundu að öllu jöfnu ekki falla undir 25. gr. þar sem annmarki á upplýsingum mundi þá sjaldnast geta haft beinar afleiðingar fyrir hinn skráða.

18. gr. frumvarpsins byggist á 89. gr. reglugerðarinnar. Nýmæli er að sérreglur um vinnslu vegna rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi eða skjalavistunar í þágu almannahagsmuna og undanþágur frá ýmsum reglum við slíka vinnslu er að finna á einum stað. Reglugerðin ráðgerir hins vegar ekki breytingar á þeim efnisreglum og framkvæmd þeirra sem gilda um vinnslu af þessum toga og þeim undantekningum sem leiddar verða af núgildandi lögum og tilskipun ESB.

Er 1. mgr. þessa frumvarpsákvæðis samsvarandi 1. mgr. 89. gr. reglugerðarákvæðisins og áskilur að vinnsla vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi skuli vera háð viðeigandi ráðstöfunum til verndar réttindum og frelsi skráðra einstaklinga í samræmi við reglugerðina. Þessar verndarráðstafanir skulu tryggja að tæknilegar og skipulagslegar ráðstafanir séu gerðar, einkum til þess að tryggja að farið sé að meginreglunni um lágmörkun gagna. Notkun gerviauðkenna getur verið á meðal þessara ráðstafana, sem og að upplýsingar séu varðveittar á ónettengdri tölvu. Sé hægt að ná umræddum markmiðum með frekari vinnslu sem leyfir ekki, eða leyfir ekki lengur, persónugreiningu skráðra einstaklinga skal þessum markmiðum náð með þeim hætti. Í 156. lið formálans er varpað ljósi á markmið sérstakra verndarráðstafana. Þar er meðal annars áréttað það sem fyrr greinir um að þær skuli tryggja lágmörkun gagna. Í því felst að frekari vinnsla persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi skal eingöngu fram þegar ábyrgðaraðili hefur metið hvort framkvæmanlegt sé að ná þeim tilgangi án þess að bera kennsl á skráða einstaklinga, að því tilskildu að viðeigandi verndarráðstafanir séu fyrir hendi (s.s. notkun gerviauðkenna fyrir upplýsingarnar).

Ákvæði um sérstakar verndarráðstafanir sem taka mið af eðli og umfangi vinnslu á þeim sviðum sem talin eru upp í frumvarpsákvæðinu er að finna í sérlöggjöf. Hér á landi gilda nokkuð ítarleg sérlög um sum þessi svið. Helstu lög sem hér hafa þýðingu eru fremur nýlega endurskoðuð og tekið hefur verið tillit til persónuverndarreglna. Um skjalavistun hjá stjórnvöldum fjalla lög um opinber skjalasöfn, nr. 77/2014, um vinnslu í tölfraðilegum tilgangi vegna hagskýrslugerðar fjalla lög um Hagstofu Íslands og opinbera hagsýslugerð, nr. 163/2007, og meginlöggjöfin um rannsóknir á sviði vísinda eru lög um vísindarannsóknir á heilbrigðissviði, nr. 44/2014 sem fjalla um skilyrði fyrir því að slíkar rannsóknir verði gerðar.

Í 2. og 3. mgr. þessa frumvarpsákvæðis er nýtt heimild 89. gr. reglugerðarinnar til að gera undanþágur að því er varðar kröfur um upplýsingar og réttinn til leiðréttingar, eyðingar, til að gleymast, til takmörkunar á vinnslu, til að flytja eigin gögn og til að andmæla vinnslu persónuupplýsinga vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi.

Undanþágur samkvæmt 2. mgr. lúta að vinnslu persónuupplýsinga sem fer aðeins fram í þágu vísinda eða sagnfræði eða í tölfraðilegum tilgangi. Í gildandi lögum er einnig að finna slíkar undantekningar, sbr. einkum 1. mgr. 19. gr. um takmarkanir á upplýsingarétti hins skráða við þær aðstæður enda geti vinnsla ekki haft bein áhrif á hagsmuni hins skráða. Af því leiðir að hinn skráði hefur rétt til aðgangs að umræddum upplýsingum ef ætla má að vinnsla þeirra geti haft réttaráhrif eða beinar afleiðingar gagnvart honum. Frumvarpsákvæðið gerir ráð fyrir því að þegar um ræðir vinnslu í þágu vísinda eða sagnfræði eða í tölfraðilegum tilgangi verði heimilt að víkja frá réttindum sem um getur í 15. gr. (réttur til aðgangs), 16. gr. (réttur til leiðréttingar), 18. gr. (réttur til takmörkunar á vinnslu) og 21. gr. (andmælaréttur), með fyrirvara um skilyrði og verndarráðstafanir sem um getur í 1. mgr. þessarar greinar, að svo miklu leyti sem telja má

að slík réttindi geri það ómögulegt eða hamli því verulega að unnt sé að ná viðkomandi markmiðum og undanþágur séu nauðsynlegar til að þeim verði náð.

Í formála reglugerðarinnar er varpað ljósi á rök að baki sérreglum um og mikilvægi vinnslu persónuupplýsinga á þessum sviðum. í 162. og 163. lið er fjallað um hvað fellur undir um vinnslu persónuupplýsinga í tölfraðilegum tilgangi og stöðu hagskýrslufirvalda. Samkvæmt því telst tölfraðilegur tilgangur vera hver sú aðgerð sem felst í söfnun og vinnslu persónuupplýsinga sem nauðsynlegar eru vegna tölfraðilegra kannana eða til að ná fram tölfraðilegum niðurstöðum. Þessar tölfraðilegu niðurstöður má nota frekar í ýmiss konar tilgangi, þ.m.t. til vísindarannsókna. Tölfraðilegur tilgangur þýðir að niðurstöður vinnslu í tölfraðilegum tilgangi eru ekki persónuupplýsingar heldur samantekin gögn og að þessar niðurstöður eða persónuupplýsingarnar eru ekki notaðar til stuðnings ráðstöfunum eða ákvörðunum viðvíkjandi tilteknum einstaklingi. Þá er tekið fram að vernda ætti trúnaðarupplýsingar sem hagskýrslufirvöld aðildarríkjanna safna til að gera opinberar hagskýrslur og jafnframt ætti gerð innlendra hagskýrslna að byggjast á lögum.

Dæmi um það sem félli hér undir er vinnsla upplýsinga á grundvelli laga um Hagstofu Íslands og opinbera hagskýrslugerð. Samkvæmt þeim lögum er Hagstofan miðstöð opinberrar hagsýslugerðar sem ætlað er að nýta stjórnsýslugögn í því skyni og til þess hefur hún heimild til að tengja saman gagnaskrár með einstaklingsauðkennum. Þá veita lögin heimildir til þess að sækja gögn til einstaklinga og lögaðila sé þess þörf að teknu tilliti til hófsemi og svarbyrði. Að lokinni frumvinnslu persónugagna til tölfraðigreininga tekur við umbreyting frumgagna í tölfraðigögn sem felur í sér stöðlun, flokkun, tilreiknun og vigtun þannig að áreiðanlegar tölfraðilegar niðurstöður fái við greiningu. Við lokaúrvinnslu er þess gætt að niðurstöður séu með öllu ópersónugreinanlegar. Af þessu má vera ljóst að réttur einstaklings til aðgangs að og leiðréttinga á upplýsingum, svo og til takmörkunar á vinnslu þeirra eða andmælaréttur, gætu gert það ómögulegt eða hamlað því verulega að lög um hagsýslugerð Hagstofunnar næðu markmiði sínu og eru þessar undanþágur því nauðsynlegar í því ljósi.

Um sérstök sjónarmið sem gilda um vísindarannsóknir er m.a. fjallað í 157. lið formálans. Þar er tekið fram að með því að tengja saman upplýsingar úr mismunandi skrár geti vísindamenn öðlast nýja og afar verðmæta þekkingu á útbreiddu heilsufarsástandi á borð við hjarta- og æðasjúkdóma, krabbamein og þunglyndi. Með notkun skráa sé hægt að efla rannsóknaniðurstöður þar sem þær byggist á stærra þýði. Í félagsvísindum geri rannsóknir á grundvelli skráa vísindamönnum kleift að öðlast mikilvæga þekkingu á langtímafylgni milli félagslegra aðstæðna af ýmsum toga, s.s. atvinnuleysis og menntunar, og annarra aðstæðna í lífi fólks. Rannsóknaniðurstöður, sem fáið með notkun skráa, gefi trausta og vandaða þekkingu sem nota megir til grundvallar við mótun og framkvæmd þekkingarstefnu, til að bæta lífsgæði margra og bæta skilvirkni félagsþjónustunnar. Þá er tekið fram í 159. lið að skilgreina beri vinnslu persónuupplýsinga í þágu vísindarannsókna vítt þannig að undir hana falli t.d. tækniþróun og tilraunaverkefni, grunnrannsóknir, hagnýtar rannsóknir og rannsóknir sem einkaaðilar fjármagna. Rannsóknir í þágu almannahagsmuna á sviði lýðheilsu ættu einnig að teljast þjóna vísindalegum tilgangi. Til að uppfylla þær sérstöku kröfur sem gerðar eru til vinnslu persónuupplýsinga í þágu vísindarannsókna ættu sérstök skilyrði að gilda, einkum að því er varðar útgáfu eða aðra birtingu persónuupplýsinga í þágu vísindarannsókna. Um sagnfræðirannsóknir er sérstaklega tekið fram í 160. lið formálans að reglugerðin nái bæði til sagnfræðirannsókna og rannsókna í erfðafræðilegum tilgangi en þó ætti að hafa í huga að reglugerðin gildi ekki um látna einstaklinga. Eins og rakið er í athugasemdum við 4. gr. er ríkjum hins vegar heimilt að fella upplýsingar um látna einstaklinga undir gildissvið reglugerðarinnar og er það svigrúm nýtt í frumvarpi að takmörkuðu leyti, þ.e. aðeins í 5 ár eftir andlát, m.a. með það í huga að óeðlilegt væri að setja því takmörk að upplýsingar um löngu látna einstaklinga séu nýttar í þágu sagnfræðirannsókna.

Í 3. mgr. frumvarpsákvæðisins er regla, áþekk 2. mgr., um undantekningar frá réttindum hins skráða þegar unnið er með persónuupplýsingar vegna skjalavistunar í þágu almannahagsmuna. Þar bætist þó við tilvísun til undanþágu frá 19. gr. reglugerðarinnar (skylda til að tilkynna um leiðréttingu og eyðingu persónuupplýsinga og takmörkun á vinnslu) og 20. gr. hennar (réttur til að flytja eigin gögn.) Hér á einnig við sá fyrirvari að undanþágum verði beitt að svo miklu leyti sem telja má þessi réttindi gera það ómögulegt eða hamla því verulega að unnt sé að ná markmiðum reglna um skjalavistun í þágu almannahagsmuna. Meginlagaheimildin sem geymir sérreglur um skjalavistun í því skyni er sem fyrr segir lög um

opinber skjalasöfn nr. 77/2014. Markmið þeirra er að tryggja myndun, vörslu og örugga meðferð opinberra skjala með réttindi borgaranna, hag stjórnsýslunnar og varðveislu sögu íslensku þjóðarinnar að leiðarljósi. Af þessu er ljóst að veigamikil samfélagssjónarmið geta mælt gegn eyðingu persónuupplýsinga sem vistuð eru í skjalasöfnun, þar á meðal tillit til sagnfræðirannsókna. Sú sérregla kemur fram í niðurlagi 3. mgr. að hinn skráði á rétt á að leggja fram yfirlýsingu til varðveislu í gögnum með persónuupplýsingum um hann. Það breytir hins vegar engu um varðveislu viðkomandi skjals eða gagna vilji einstaklingur koma að athugasemdum sínum þar sem upplýsingar séu rangar eða villandi. Í 158. lið formála reglugerðarinnar er varpað ljósi á hvernig beri að skýra reglur um vinnslu persónuupplýsinga vegna skjalavistunar. Þar segir m.a. að opinber yfirvöld, opinberir aðilar og einkaaðilar, sem halda skrár sem tengjast almannahagsmunum, ættu að vera þjónustuaðilar sem hafa samkvæmt lögum aðildarríkis lagaskyldu til að afla, varðveita, meta, skipuleggja, lýsa, veita upplýsingar um, kynna, dreifa og veita aðgang að skráum sem hafa varanlegt gildi fyrir almannahagsmunum. Aðildarríkin ættu einnig að hafa heimild til að kveða á um frekari vinnslu persónuupplýsinga vegna skjalavistunar. Eru lög um opinber skjalasöfn dæmi um löggjöf sem ætlað er að ná framangreindum markmiðum.

Í 4. mgr. frumvarpsákvæðisins er hnykkð á sérstöðu afhendingu upplýsinga til opinberra skjalasafna, en ákvæði þessa efnis er að finna í 15. gr. a í gildandi lögum. Reglunni var bætt í lög nr. 77/2000 með lögum um opinber skjalasöfn nr. 77/2014 og þykir ekki ástæða til að fella hana niður.

Um 19. gr.

Ákvæði þetta mælir fyrir um að upplýsingaskylda ábyrgðaraðila skv. 3. mgr. 13. gr. og 4. mgr. 14. gr. reglugerðarinnar gildi 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. Eins og fyrr er lýst kemur fram í þessum ákvæðum reglugerðarinnar að hyggist ábyrgðaraðili vinna persónuupplýsingarnar frekar í öðrum tilgangi en þeim sem lá að baki söfnun þeirra skuli hann láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst og gildir þetta án tillits til þess hvort upplýsinga hefur upprunalega verið aflað hjá hinum skráða eða ekki.

Frumvarpsákvæðið sækir m.a. fyrirmynd til 23. gr. danska frumvarpsins til nýrra persónuverndarlaga og er sett innan þess ramma sem 23. gr. reglugerðarinnar ráðgerir um takmarkanir á réttindum hins skráða. Ákvæðið byggist á sjónarmiðum um að umrædd upplýsingaskyldi kunni að fela í sér óþarfa stjórnsýslulega byrði fyrir stjórnvöld í ljósi þess að önnur ákvæði laga tryggja sérstaklega vernd einstaklinga í samskiptum við þau. Þannig má benda á að um starfsemi opinberra aðila gilda auk ákvæða frumvarpsins, ef að lögum verður, ákvæði annarra laga sem tryggja vernd einstaklingsins í skiptum sínum við ríkisvaldið, t.d. bæði ákvæði stjórnsýslu- og upplýsingalaga.

Um 20. gr.

Ákvæði þetta endurspeglar þau réttindi hins skráða sem talin upp eru í 16.-20. gr. reglugerðarinnar og er ekki ætlað að víkja frá þeim reglum eða setja fram frekari útfærslur. Þau eru fest í þennan kafla frumvarpsins til að gefa yfirlit yfir réttindi hins skráða, og vísast um inntak réttindanna til ítarlegri lýsingar í þessum ákvæðum. Þessi reglugerðarákvæði mæla fyrir um rétt hins skráða til leiðréttingar á óáreiðanlegum upplýsingum um hann (16. gr.), rétt til eyðingar persónuupplýsinga, sem einnig kallast „réttur til að gleymast“ (17. gr.), réttur til takmörkunar á vinnslu (18. gr.), skyldu til að tilkynna um leiðréttingu og eyðingu persónuupplýsinga, takmörkun á vinnslu (19. gr.) og rétt til að flytja eigin gögn (20. gr.). Í þessum ákvæðum felast ýmis nýmæli, en áður en þeim er lýst verður varpað stuttlega ljósi á efni gildandi laga um sama efni.

Réttur skráðra einstaklinga til að fá að gögn leiðrétt eða þeim eytt, svo og andmælaréttur hefur lengi verið ein grunnreglna persónuverndarlaga og birtist m.a. í 14. gr. tilskipunar ESB. Í greininni eru reglur um rétt hins skráða til að mótmæla tiltekinni vinnslu persónuupplýsinga um sjálfan sig. Ákvæði um efnið koma fram í 25. og 26. gr. gildandi laga. Annars vegar er um að ræða ákvæði um leiðréttingu og eyðingu rangra og villandi persónuupplýsinga og hins vegar um eyðingu og bann við notkun persónuupplýsinga sem hvorki eru rangar né villandi. Þá er í

27. gr. fjallað um rétt til að fá ákvörðun sem byggist á handvirkri vinnslu upplýsinga eytt. Það ákvæði og 25. gr. teljast gjarnan innihalda svokallaðar leiðréttingarreglur og endurspeglar einkum þá meginreglu að persónuupplýsingar skulu vera áreiðanlegar og uppfærðar eftir þörfum og að persónuupplýsingum sem eru óáreiðanlegar eða ófullkomnar, miðað við tilgang vinnslu þeirra, skal eyða eða leiðrétta án tafar, auk þess sem Persónuvernd getur bannað notkun upplýsinga sé breyting þeirra eða eyðing óheimil samkvæmt ákvæðum annarra laga eins og fram kemur í 3. mgr. 25. gr. Ákvæði 26. gr. endurspeglar hins vegar þær meginreglur að vinnsla persónuupplýsinga skal vera lögmæt, og ekki umfram það sem nauðsynlegt er vegna tilgangs vinnslunnar, sem og að upplýsingar skulu varðveittar á því formi að ekki sé unnt að bera kennsl á hina skráðu lengur en þörf krefur miðað við þann tilgang. Hafi þessar meginreglur í för með sér að ekki megi lengur varðveita persónuupplýsingar ber að eyða þeim. Þar sem eyðing getur eftir atvikum verið óheimil, einkum á grundvelli löggjafar um opinber skjalasöfn, getur Persónuvernd auk þess bannað notkun upplýsinga eins og fram kemur í 3. mgr. 26. gr.

Fyrirgreind ákvæði reglugerðarinnar eru mun ítarlegri en ákvæði ESB-tilskipunarinnar um efnið. Að hluta til festa þau í sessi gildandi framkvæmd með nánari útfærslum. Samkvæmt 16. gr. á skráður einstaklingur rétt á að fá óáreiðanlegar persónuupplýsingar er varða hann sjálfan leiðrétta af ábyrgðaraðila án ótilhlýðilegrar tafar. Að teknu tilliti til tilgangsins með vinnslunni skal hinn skráði eiga rétt á að láta fullgera ófullkomnar persónuupplýsingar, m.a. með því að leggja fram yfirlýsingu með upplýsingunum.

Rétturinn til eyðingar upplýsinga, þar með talinn rétturinn til að gleymast samkvæmt 17. gr., felst í því að hinn skráði á við ákveðnar aðstæður rétt á því að ábyrgðaraðilinn eyði persónuupplýsingum sem hann varða án ótilhlýðilegrar tafar og skal ábyrgðaraðilanum skylt að gera svo ef ein eftirtalinna ástæða á við: a) persónuupplýsingarnar eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun þeirra eða annarri vinnslu þeirra, b) hinn skráði dregur til baka samþykkið sem vinnslan byggist á og ekki er annar lagagrundvöllur fyrir vinnslunni, c) hinn skráði andmælir vinnslunni og ekki eru fyrir hendi lögmætastæður fyrir vinnslunni d) vinnsla persónuupplýsinganna var ólögmæt, e) eyða þarf persónuupplýsingunum til að uppfylla lagaskyldu sem hvílir á ábyrgðaraðila eða f) persónuupplýsingunum var safnað í tengslum við boð um þjónustu í upplýsingasamfélaginu. Þá er nánar mælt fyrir um ráðstafanir sem ábyrgðaraðila ber að grípa til hafi hann gert persónuupplýsingar opinberar. Frá þessu eru síðan gerðar undantekningar í 3. mgr. 17. gr. sem að nokkru marki hefur verið fjallað um fyrr í frumvarpi þessu. Samkvæmt því gildir fyrirgreindur réttur ekki að því marki sem vinnsla er nauðsynleg til að neyta réttarins til tjáningar- og upplýsingafrelsis, til að rækja skyldu sem hvílir á ábyrgðaraðilanum samkvæmt lögum og krefst þess að unnið sé með persónuupplýsingar, vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, vegna almannahagsmuna á sviði lýðheilsu, vegna skjalavistunar í þágu almannahagsmuna og rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi, sem og til að stofna, hafa uppi eða verja réttarkröfur.

Frekari skýringar á réttinum til leiðréttingar og eyðingar gagna er að finna í formálsorðum reglugerðarinnar. Í 65. lið formálans er m.a. bent á að réttur til leiðréttingar og til að gleymast á einkum við þegar hinn skráði hefur veitt samþykki sitt sem barn og gerir sér ekki fulla grein fyrir áhættunni sem vinnslan felur í sér og óskar eftir því síðar að persónuupplýsingunum verði eytt, einkum á netinu. Skráður einstaklingur á að geta neytt þessa réttar þrátt fyrir að hann sé ekki lengur barn. Þó er bent á á undantekningu að frekari varðveisla persónuupplýsinganna kann að vera lögmæt sé hún nauðsynleg til að neyta réttar til tjáningar- og upplýsingafrelsis, til að uppfylla lagaskyldu, vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, í þágu almannahagsmuna á sviði lýðheilsu, vegna skjalavistunar í þágu almannahagsmuna, rannsókna á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi eða til að unnt sé að stofna, hafa uppi eða verja réttarkröfur. Í 66. lið formálans er tekið fram að til að efla megi réttinn til að gleymast í netumhverfinu ætti einnig að víkka réttinn til eyðingar þannig að ábyrgðaraðila, sem gerði persónuupplýsingarnar opinberar, sé skylt að upplýsa þá ábyrgðaraðila sem vinna með upplýsingarnar um að afmá beri alla tengla á þær, þar á meðal afrit af þeim eða endurgerðir þeirra. Í því sambandi ætti viðkomandi ábyrgðaraðili að gera eðlilegar ráðstafanir með tilliti til þeirrar tækni sem er fyrir hendi og aðferða sem honum eru aðgengilegar, þ.m.t. tæknilegar ráðstafanir til að upplýsa ábyrgðaraðilana, sem vinna með persónuupplýsingar um hinn skráða, um beiðni hans.

Dótt rétturinn til að gleymast sé ekki orðaður sem slíkur í tilskipun ESB og gildandi lögum, hefur hann verið talin efnislega fölginn í þessum reglum. Það var m.a. staðfest í dómi Evrópudómstólsins frá 13. maí 2014 í máli Google Spain (C-131/12). Með dóminum var veittur forúrskurður um tiltekin álitæfni tengd dómsmáli á Spáni þar sem til úrlausnar var krafa manns um að niðurstöður á leitarsíðu Google sem tengdust fjárnámi í eignum hans skyldu fjarlægðar. Eitt helsta álitæfnið var hvort leggja mætti fyrir Google að fjarlægja leitarniðurstöður á grundvelli persónuverndarregla og varð niðurstaða dómsins sú að þegar við ættu b-liður 1. mgr. 12. gr. tilskipunar ESB (um rétt til meðal annars eyðingar upplýsinga ef vinnsla þeirra fullnægir ekki kröfum hennar) og a-liður 1. mgr. 14. gr. tilskipunarinnar (andmælaréttur á grundvelli lögmætra og knýjandi ástæðna vegna sérstakra aðstæðna) væri rekanda vefleitarvélar það skylt. Dómurinn hefur þó ekki í för með sér að sjálfu efninu, sem um ræðir hverju sinni, skuli eyða heldur aðeins leitarniðurstöðunum sjálfum á vefsíðu viðkomandi vefleitarvélar. Einnig kemur fram í dóminum að það hvort leitarniðurstöðum skuli eytt fer eftir mati á hagsmunum af annars vegar því að þær séu aðgengilegar og hins vegar hagsmunum viðkomandi einstaklings af að svo sé ekki þá var í dóminum litið til þess að Google hefur starfsstöðvar innan ESB, í þessu tilviki á Spáni, og bar samkvæmt því að virða ákvæði laga í einstökum aðildarríkjum sem sett eru á grundvelli ESB-tilskipunarinnar.

Dómur Evrópudómstólsins setti mikilvægt fordæmi um viðmið sem leggja ber til grundvallar. Persónuvernd hefur þegar litið til þeirra við meðferð á kvörtunum einstaklinga um að Google hafi neitað að fjarlægja niðurstöðu leitar á vefleitarvél sinni þar sem nöfn einstaklinga koma upp. Í framkvæmd Persónuverndar hefur þannig komið fram að líta verður til sjónarmiða um hagsmuni af frjálsri fjölmiðlun að því marki sem það er nauðsynlegt til að samrýma sjónarmið um rétt til einkalífs annars vegar og tjáningarfrelsis hins vegar. Hefur verið horft til þess að það tilheyrir nútímafjölmiðlun að fréttir séu gerðar aðgengilegar og leitarbærar á netinu og því litið svo á að meta verði í hvert og eitt skipti hvort undantekning sem fram kemur í 5. gr. gildandi laga, sbr. einnig 6. gr. frumvarpsins um tengsl við tjáningarfrelsi og a-lið 3. mgr. 17. gr. reglugerðarinnar, eigi við. Verður því að líta til ákvæða 73. gr. stjórnarskrárinnar og 10. gr. mannréttindasáttmála Evrópu, þ.e. til þess hvort sú takmörkun á tjáningar- og upplýsingafrelsi, sem skylda til að eyða upplýsingum felur í sér, teljist nauðsynleg í lýðræðisþjóðfélagi.

Í 18. gr. reglugerðarinnar eru sett fram ný regla um rétt hins skráða til takmörkunar á vinnslu. Skráður einstaklingur skal þannig hafa rétt til þess að ábyrgðaraðili takmarki vinnslu þegar eitt af eftirfarandi á við; a) hinn skráði vefengi að persónuupplýsingar séu réttar og ábyrgðaraðilinn hafi ekki fengið tækifæri til að fá staðfest hvort svo sé, b) vinnslan sé ólögmæt og hinn skráði andmæli því að persónuupplýsingunum sé eytt og fari fram á takmörkun á notkun þeirra í staðinn, c) ábyrgðaraðilinn þurfi ekki lengur á persónuupplýsingunum að halda fyrir vinnsluna en hinn skráði þarfnist þeirra til þess að stofna, hafa uppi eða verja réttarkröfur eða d) hinn skráði hafi andmælt vinnslunni á meðan beðið er sannprófunar á því hvort hagsmunir ábyrgðaraðila gangi framar lögmætum hagsmunum hins skráða. Þá er mælt fyrir um það í 2. mgr. 18. gr. að þegar vinnsla hefur verið takmörkuð skuli einungis vinna með viðkomandi persónuupplýsingar, að varðveislunni undanskilinni, með samþykki hins skráða, til að stofna, hafa uppi eða verja réttarkröfur, til að vernda réttindi annars einstaklings eða lögaðila eða á grundvelli brýnna almannahagsmuna. Í 67. lið formála reglugerðarinnar kemur fram að aðferðir til að takmarka vinnslu persónuupplýsinga gætu m.a. falið í sér að færa valdar upplýsingar tímabundið í annað vinnslukerfi, gera valdar persónuupplýsingar óaðgengilegar notendum eða fjarlægja birtar upplýsingar tímabundið af vefsetri. Í sjálfvirkum skráningarkerfum ætti að jafnaði að tryggja takmörkun vinnslu með tæknilegum aðferðum á þann hátt að ekki verði um frekari vinnslu persónuupplýsinganna að ræða og ekki sé hægt að breyta þeim. Tilgreina ætti með skýrum hætti í kerfinu að vinnsla persónuupplýsinga sé takmörkuð.

Í 2. mgr. frumvarpsákvæðisins er kveðið á um rétt skráðs einstaklings til að fá persónuupplýsingar um sig, sem hann hefur sjálfur látið ábyrgðaraðila í té, á skipulegu, algengu, tölvulesanlegu sniði og jafnframt til að senda þessar upplýsingar til annars ábyrgðaraðila. Ákvæðið er byggt á 20. gr. reglugerðarinnar þar sem einnig er að finna nánari útfærslur á þessum rétti. Þar kemur fram að réttindi þessi verða virk þegar vinnsla persónuupplýsinga byggir á samþykki hins skráða eða samningi og vinnslan er sjálfvirk. Þá kemur fram í reglugerðarákvæðinu að þegar hinn skráði neytir réttar síns til þess að flytja eigin gögn skal hann eiga rétt á að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars ef

það er tæknilega framkvæmanlegt. Eins er tekið fram að þegar einstaklingur nýtir sér umræddan rétt skal það ekki hafa áhrif á rétt hans til eyðingar gagna. Loks er ljóst af ákvæðinu að rétturinn gildir ekki um vinnslu opinberra aðila eða ef hann skerðir réttindi og frelsi annarra.

Réttur þessi, sem einnig er kallaður flutningsréttur (e. *data portability*) er nýmæli í reglugerðinni og á sér enga beina hliðstæðu í ESB-tilskipuninni eða gildandi lögum. Hann er náskyldur réttinum til aðgangs en þó ólíkur í mörgu tilliti. Hann er í reynd tvíþættur, annars vegar hefur hinn skráði rétt til að fá í hendur gögn sem varða hann sjálfan og hins vegar hefur hann rétt til að láta flytja eigin gögn frá einum ábyrgðaraðila til annars.

Markmið þessa nýja ákvæðis er að tryggja hinum skráða meiri stjórn yfir vinnslu upplýsinga sem varða hann. Þar sem flutningsrétturinn tryggir rétt manns til að flytja persónuupplýsingar frá einum ábyrgðaraðila til annars, er þessi skipan einnig til þess fallin að tryggja frjálst flæði upplýsinga milli ríkja og stuðla þannig að samkeppni milli ábyrgðaraðila. Í 68. lið formálans er varpað ljósi á hvernig og hvenær rétturinn gildir og hvernig hann á að verða framkvæmanlegur. Nánar tiltekið kemur fram að hann á við þegar hinn skráði hefur látið persónuupplýsingar í té á grundvelli samþykkis eða ef vinnslan er nauðsynleg vegna framkvæmdar samnings, en hins vegar ekki þegar vinnslan byggist á öðrum lagagrundvelli en samþykki eða samningi. Þá segir að eðli málsins samkvæmt eigi ekki að beita þessum rétti gagnvart ábyrgðaraðilum sem vinna með persónuupplýsingar við opinber skyldustörf sín. Hann gildi því ekki þegar vinnsla persónuupplýsinga er nauðsynleg til að rækja skyldu sem hvílir á ábyrgðaraðilanum samkvæmt lögum eða vegna verkefnis sem er unnið í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með.

Bent er á að ábyrgðaraðili ætti að þróa samvirkandi snið sem geri það mögulegt að flytja eigin gögn. Réttur skráðs einstaklings til að senda eða taka á móti persónuupplýsingum ætti þó ekki að verða til þess að ábyrgðaraðilum sé skylt að taka upp eða viðhalda vinnslukerfum sem eru tæknilega samhæfð. Ef tiltekið mengi persónuupplýsinga varði fleiri en einn skráðan einstakling ætti réttur þeirra til að fá persónuupplýsingarnar að vera með fyrirvara um réttindi og frelsi annarra skráðra einstaklinga í samræmi við reglugerðina. Loks er áréttað í 68. lið formálans að flutningsrétturinn ætti ekki að hafa áhrif á rétt skráðs einstaklings til að láta eyða persónuupplýsingum og takmarkanir á þeim rétti eins og mælt er fyrir um í reglugerðinni. Nánar segir að einkum ætti hann ekki að hafa í för með sér að persónuupplýsingum, sem varða hinn skráða, sem hann hefur látið af hendi vegna efnda á samningi, verði eytt, að því marki og svo lengi sem persónuupplýsingarnar eru nauðsynlegar til að efna samninginn. Sé það tæknilega gerlegt ætti skráður einstaklingur að hafa rétt til að láta senda persónuupplýsingarnar beint frá einum ábyrgðaraðila til annars.

Þess má geta að starfshópur skv. 29. gr. tilskipunar ESB hefur fjallað um samþykkishugtakið samkvæmt ákvæðum reglugerðarinnar og gefið út leiðbeiningar um flutningsrétt (Guidelines on the right to data portability) frá 13. desember 2016 með breytingum frá 5. apríl 2017. Þar er því lýst í ítarlegu máli hvað felist í inntaki flutningsréttarins, hvenær hann eigi við og hvert sé samspil hans við almenn réttindaákvæði reglugerðarinnar. Þá koma þar fram ítarlegar leiðbeiningar til ábyrgðaraðila um hvaða tæknilegu ráðstafanir þeir geti gert til þess að réttur hins skráða verði virkur.

Um 21. gr.

Í þessari grein er annars vegar að finna almenn fyrirmæli um andmælarétt hins skráða og hins vegar sérreglur um bannskrá Þjóðskrár Íslands um þá sem kjósa að nöfn þeirra séu ekki notuð í markaðssetningarstarfsemi. Hér er um að ræða réttindi sem þegar eru tryggð í 28. gr. gildandi laga, sem innleiddi m.a. ákvæði 14. gr. ESB-tilskipunarinnar, og stefnir frumvarpið ekki að efnislegum breytingum á því.

Fyrirmæli 1. mgr. um andmælarétt hins skráða byggjast á 21. gr. reglugerðarinnar sem er nokkuð ítarlegri en 14. gr. tilskipunarinnar og tekur m.a. tillit til þess hvernig andmælarétti verður komið við í upplýsingasamfélaginu. Samkvæmt 21. gr. reglugerðarinnar skal skráður einstaklingur eiga rétt á að andmæla hvenær sem er, vegna sérstakra aðstæðna sinna, vinnslu persónuupplýsinga er varða hann sjálfan, þ.m.t. gerð persónusniðs, þegar vinnslan byggist á e- eða f-lið 1. mgr. 6. gr. reglugerðarinnar, þ.e. á almannahagsmunum eða lögmætum hagsmunum. Ábyrgðaraðili skal ekki vinna með persónuupplýsingarnar frekar nema hann geti sýnt fram á mikilvægar lögmætar ástæður fyrir vinnslunni sem gangi framar hagsmunum, réttindum og frelsi hins skráða eða því að stofna, hafa uppi eða verja réttarkröfur. Þá er í 2. og 3. mgr. 21. gr.

reglugerðarinnar tryggður réttur einstaklinga í tengslum við markaðssetningu og kveðið á um að þegar persónuupplýsingar eru unnar í þágu beinnar markaðssetningar skuli einstaklingurinn hvenær sem er eiga rétt á að andmæla vinnslu persónuupplýsinga sem varða hann sjálfan, þ.m.t. gerð persónusniðs að því marki sem hún tengist markaðssetningunni. Andmæli hinn skráði vinnslu í þágu beinnar markaðssetningar skal ekki vinna með persónuupplýsingarnar frekar í slíkum tilgangi. Sé um að ræða þjónustu í upplýsingasamfélaginu skuli hinum skráða vera heimilt að neyta andmælaréttar síns rafrænt með notkun tækniforskrifta, eins og segir í 5. mgr. Loks er tekið fram í 6. mgr. 21. reglugerðarinnar að þegar unnið er með persónuupplýsingar í þágu rannsókna á sviði vísinda eða sagnfræði eða í tölfraðilegum tilgangi, skuli hinn skráði eiga rétt á, vegna sérstakra aðstæðna sinna, að andmæla vinnslu persónuupplýsinga er varða hann sjálfan nema vinnslan sé nauðsynleg vegna verkefnis sem unnið er í þágu almannahagsmuna. Um undantekningar af þessum toga var fjallað í skýringum við 18. gr. frumvarpsins. Í 69. og 70. lið formála reglugerðarinnar eru fyrirmæli 21. nánar skýrð. Er m.a. bent á að það ætti að vera á hendi ábyrgðaraðila að sýna fram á að mikilvægir lögmætir hagsmunir hans gangi framar hagsmunum eða grundvallarréttindum og frelsi hins skráða í tengslum við andmælarétt hins síðarnefnda.

Sérreglurnar um bannskrá Þjóðskrár Íslands í 2.-4. mgr. frumvarpsins stefna að því að ná markmiðum reglugerðarinnar um andmælarétt hins skráða í tengslum við beina markaðssetningu en ganga jafnframt lengra en reglugerðin, m.a. þar sem ekki er gert ráð fyrir að andmæli þurfi að byggjast á sérstökum aðstæðum. Reglurnar eru færðar svo til óbreyttar úr 2.-7. mgr. 28. gr. núgildandi laga en höfðu sætt nokkrum efnislegum breytingum með lögum nr. 90/2001. Lagt er til að Þjóðskrá haldi eftir sem áður skrá yfir þá sem andmæla því að nöfn þeirra séu notuð í markaðssetningarstarfsemi. Nánar tiltekið segir í 2. mgr. ákvæðisins að þeir sem nota slíkar skrár, s.s. eigin viðskiptamannaskrár, í tengslum við markaðssetningarstarfsemi, skuli bera þær saman við bannskrá Þjóðskrár áður en þær eru notaðar í slíkum tilgangi, til að koma í veg fyrir að markpóstur verði sendur eða hringt verði til einstaklinga sem hafa andmælt slíku. Nánari útfærslu lagareglna um bannskrá Þjóðskrár og andmæli einstaklinga við markaðssetningarstarfsemi er að finna í reglum nr. 36/2005 sem settar voru af dómsmálaráðherra þann 5. janúar 2005. Í 4. gr. reglnanna segir að þeim sem stunda markaðssetningarstarfsemi sé skylt að beita bannskrá Þjóðskrár við starfsemi sína, en þar er m.a. átt við útsendingu dreifibréfa, happdrættismiða, giróseðla, auglýsinga og kynningarefnis, símhringingar, útsendingu tölvupósts eða beitingu hliðstæðra aðferða, sem varða kaup eða leigu á vöru eða þjónustu eða þátttöku í tiltekinni starfsemi, hvort sem hún er viðskiptalegs eðlis eða varðar tómstundir, afþreyingu, námskeið eða sambærilegt atferli, sbr. 2. mgr. 2. gr. reglnanna. Rétt er að taka fram að í 5. mgr. 46. gr. laga um fjarskipti nr. 81/2003 er mælt fyrir um að þeir sem nota almenna tal- og farsímaþjónustu sem lið í markaðssetningu skuli virða merkingu í símaskrá sem gefur til kynna að viðkomandi áskrifandi vilji ekki slíkar símhringingar í símanúmer sitt. Áskrifandi á rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja úthringingu til grundvallar. Mál varða framangreinda bannmerkingu í símaskrá falla þannig ekki undir valdssvið Persónuverndar heldur Póst- og fjarskiptastofnunar, ólíkt því sem gildir um bannskrá Þjóðskrár.

Í 3. mgr. er tekið fram til áréttingar að öll notkun bannskrár sé óheimil í öðrum tilvikum en þar er lýst.

Samkvæmt 4. mgr. er skylt að á markpósti komi fram á áberandi stað eftir hvaða skrá efninu er dreift og í vörslu hvaða ábyrgðaraðila skráin er. Með markpósti er átt við allan auglýsingapóst sem er með límmiðaráritun eða annars konar áritun nafns og heimilisfangs viðtakanda. Falla þar undir venjulegur póstur, símbréf og tölvupóstur sem notaður er í beinni markaðssókn. Með beinni markaðssókn er átt við beina sókn að einstaklingnum í því skyni að selja honum vöru eða þjónustu. Samkvæmt þessu falla dreifirit sem borin eru út í hús án áritunar ekki þar undir. Ákvæðið tekur jafnframt til símasölu eftir því sem við á. Samkvæmt því á sá sem stundar markaðssókn í gegnum síma að greina þeim sem hann setur sig í samband við frá því hvaðan upplýsingarnar sem hann notar eru fengnar. Þá er í niðurlagi 4. mgr. kveðið á um að unnt skuli vera að bera kennsl á markpóst sem sendur er með rafrænum hætti á skýran og ótvíræðan hátt um leið og viðtakandinn fær hann í hendur, en slík skylda byggist á fyrirmælum Evrópureglna um rafræn viðskipti.

Í 5. mgr. kemur fram að ábyrgðaraðili getur afhent félaga-, nemenda-, starfsmanna- eða viðskiptamannaskrár til nota við beina markaðssetningu ef hann hefur áður gefið hinum skráðu

kost á að andmæla því að nafn viðkomandi verði á hinni afhentu skrá. Þá ber ábyrgðaraðila enn fremur að kanna hvort viðkomandi einstaklingur hafi með tilkynningu til Þjóðskrár andmælt notkun á nafni sínu við markaðssetningu, auk þess sem afhendingin má ekki fara gegn félagssamþykktum eða starfsreglum sem í gildi eru hjá viðkomandi ábyrgðaraðila. Þetta hefur ekki þótt varhugavert með tilliti til persónuverndar en bein markaðssetning hefur viðgengist lengi hér á landi og í öðrum löndum. Tekið skal fram í því sambandi að afhending samkvæmt 5. mgr. er óheimil sé um að ræða viðkvæmar persónuupplýsingar en af því leiðir til dæmis að óheimilt væri að afhenda lista yfir meðlimi stjórnmalaflokks, stéttarfélags eða samtaka fólks með tiltekinn sjúkdóm í þágu markaðssetningar. Þá er vakin athygli á að skýrt er samkvæmt 5. mgr. að hún taki til afhendingar á skráum yfir nemendur. Í 5. mgr. 28. gr. gildandi laga, sem er fyrirmyndin að þessu frumvarpsákvæði, er slíkra skráa ekki getið. Persónuvernd hefur litið svo á að þær séu fyllilega sambærilegar við félaga-, starfsmanna- eða viðskiptamannaskrár og falli því samkvæmt eðli sínu undir ákvæðið. Við afhendingu skráa yfir nemendur í þágu beinnar markaðssetningar verði því að fara að kröfum umrædds ákvæðis laganna.

Tekið er fram í 6. mgr. að skilyrði 5. mgr. gildi ekki ef afhending félaga-, starfsmanna- eða viðskiptamannaskrár til nota við beina markaðssetningu byggist á samþykki hins skráða og er í því sambandi vísað til almennrar vinnsluheimildar samkvæmt 1. tölul. 1. mgr. 9. gr. frumvarpsins þegar aflað er samþykkis.

Loks kemur fram í 7. mgr. þessa frumvarpsákvæðis að ákvæði greinarinnar taka, eftir því sem við á, einnig til markaðs- neyslu- og skoðanakannanna. Framkvæmd þeirra á margt sameiginlegt með markaðssókn og því er eðlilegt að sömu reglur gildi um notkun persónuupplýsinga í þeirri starfsemi.

Um 22. gr.

Í þessari grein er að finna reglur um réttindi hins skráða sem tengjast einstaklingsmiðuðum ákvörðunum sem byggjast á sjálfvirkri gagnavinnslu, þar með talinni gerð persónusniðs. Eins og fram kom í skilgreiningu 10. tölul. 3. gr. frumvarpsins er með gerð persónusniðs átt við hvers kyns sjálfvirka vinnslu 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. Reglur um þessi efni er nú að finna í 22. og 23. gr. gildandi laga en þær byggjast á 15. gr. tilskipunar ESB um rétt einstaklingsins til þess að neita því að teknar séu um hann ákvarðanir með réttaráhrif gagnvart honum sem grundvallast eingöngu á sjálfvirkri vinnslu upplýsinga. Þá stefnir 12. gr. tilskipunar ESB um réttinn til aðgangs að því að tryggja að sérhver einstaklingur eigi rétt til þess að fá vitneskju um fyrirkomulag rafrænnar vinnslu um sig, að minnsta kosti þegar um er að ræða gagnavinnslu eins og nefnd er í 15. gr.

Samkvæmt frumvarpsgreininni er óheimilt að taka ákvörðun eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerðar persónusniðs, sem hefur réttaráhrif gagnvart skráðum einstaklingi varðar eða snertir hann á sambærilegan hátt að verulegu leyti samkvæmt nánari fyrirmælum 22. gr. reglugerðarinnar, með þeim undantekningum sem þar getur. Er 22. gr. reglugerðarinnar nokkuð nákvæmari en ákvæði tilskipunarinnar um efnið. Þar má finna einnig undantekningar frá meginreglunni. Þannig gildir hún ekki ef ákvörðun er forsenda þess að unnt sé að gera eða efna samning milli hins skráða og ábyrgðaraðila, ef hún er heimiluð í lögum sem gilda gagnvart ábyrgðaraðila þar sem einnig er kveðið á um víðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða, sem og ef hún byggist á afdráttarlausu samþykki hins skráða. Sé vinnslan byggð á framkvæmd samnings eða samþykki, skal ábyrgðaraðili á vinnslu persónuupplýsinga gera víðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða, a.m.k. réttinn til mannlegrar íhlutunar af hálfu ábyrgðaraðilans, til að láta skoðun sína í ljós og til að vefengja ákvörðun. Þá segir í ákvæði 22. gr. reglugerðarinnar að þegar um er að ræða sjálfvirka ákvarðanatöku sem byggir á viðkvæmum persónuupplýsingum sé slíkt eingöngu heimilt á grundvelli samþykkis eða lagaheimildar.

Auk skilgreiningar á því hvað felst í gerð persónusniða og ákvæða 22. gr. má finna ýmis varúðarorð um efnið í formála reglugerðarinnar. Í 24. lið formálans er tekið fram að til að ákvarða hvort vinnslustarfsemi geti talist vera vöktun á hegðun skráðra einstaklinga ætti að ganga úr skugga um hvort slóð einstaklinga sé rakin á netinu, m.a. hvort í kjölfarið séu notaðar aðferðir við vinnslu á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um

smekk hans, hegðun og viðhorf. Þá koma frekari varnaðarorð fram í 30. lið formálans þar sem bent er á að ýmis tæki, forrit og samskiptareglur, sem einstaklingar nota, geta tengt netauðkenni við þá, s.s. IP-tölur. Þessi notkun geti skilið eftir spor sem hægt sé að nota til að útbúa persónusnið um einstaklinga og bera kennsl á þá, einkum þegar sporunum sé bætt við einkvæm auðkenni og aðrar upplýsingar sem berast netþjónum.

Í 71. lið formálans er varpað ljósi á inntak 22. gr. reglugerðarinnar. Áréttað er að skráður einstaklingur á rétt á því að sæta ekki ákvörðun sem kann að fela í sér ráðstöfun þar sem persónulegir þættir hans eru metnir eingöngu á grundvelli sjálfvirkrar gagnavinnslu og hefur réttaráhrif gagnvart honum sjálfum eða veruleg sambærileg áhrif. Dæmi sem tekin eru um slíkar aðstæður eru sjálfvirk höfnun lánsúmsóknar á netinu eða rafrænt ráðningarferli án mannlegrar íhlutunar. Ákvarðanatöku, sem byggist á slíkri vinnslu, þ.m.t. gerð persónusniðs, ætti að vera leyfileg samkvæmt sérstakri heimild í lögum sem ábyrgðaraðilinn fellur undir. Gætt slík heimild verði sett í þeim tilgangi að fylgjast með og koma í veg fyrir svindl og skattsvik í samræmi við reglur, staðla og tilmæli eftirlitsstofnana og til að tryggja öryggi og áreiðanleika þjónustu sem ábyrgðaraðili veitir eða, þegar nauðsyn krefur, vegna gerðar eða framkvæmdar samnings milli skráðs einstaklings og ábyrgðaraðila eða þegar hinn skráði hefur veitt ótvírátt samþykki sitt. Hvað sem öðru líður ætti vinnslan að falla undir viðeigandi verndarráðstafanir, þ. á m. að hinum skráða séu veittar skilmerkilegar upplýsingar og að hann njóti réttar til mannlegrar íhlutunar, að láta skoðun sína í ljós, fá útskýringar á ákvörðun sem tekin er að mannlegri íhlutun lokinni og vefengja ákvörðunina. Sérstaklega er bent á að slík vinnsla og hér um ræðir ætti ekki að varða barn.

Þá er tekið fram í sama formálalið að til að tryggja að vinnslan sé sanngjörn og gagnsæ gagnvart skráðum einstaklingi, að teknu tilliti til sérstakra aðstæðna og samhengis við vinnslu persónuupplýsinganna, ætti ábyrgðaraðilinn að nota viðeigandi stærðfræðilegar eða tölfræðilegar aðferðir við gerð persónusniðs, gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, einkum til að tryggja að þættir sem gera persónuupplýsingar óáreiðanlegar séu leiðréttir og dregið sé úr hættu á mistökum, sem og að tryggja öryggi persónuupplýsinga þannig að tekið sé tillit til mögulegrar áhættu fyrir hagsmuni og réttindi hins skráða og m.a. komið í veg fyrir að einstaklingum sé mismunað á grundvelli kynþáttar eða þjóðernislegs uppruna, stjórnmálaskoðana, trúarbragða eða trúar, stéttarfélagsaðildar, erfðaeiginleika eða heilsuhaga eða kynhneigðar, eða að gerðar verði ráðstafanir sem hafa samsvarandi áhrif. Sjálfvirka ákvarðanatöku og gerð persónusniðs, sem byggist á sérstökum flokkum persónuupplýsinga, ætti einungis að heimila með sérstökum skilyrðum.

Í 72. lið formálans er bent á að gerð persónusniðs fellur undir reglurnar um vinnslu persónuupplýsinga samkvæmt reglugerðinni, m.a. hvað varðar lagagrundvöll vinnslu og meginreglur um persónuvernd. Þá segir að Evrópska persónuverndarráðið, sem er sett á fót með reglugerðinni, ætti að geta gefið út leiðbeiningar í því tilliti. Ráðið tekur ekki til starfa fyrr enn reglugerðin kemur til framkvæmda. Í þessu sambandi má benda á að starfshópur skv. 29. gr. tilskipunar ESB hefur þegar gefið út leiðbeiningar þar sem fjallað er um samþykkishugtakið samkvæmt ákvæðum reglugerðarinnar og gefið út leiðbeiningar um einstaklingsmiðaðar ákvarðanir og gerð persónusniðs samkvæmt henni (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679) frá 3. október 2017, með breytingum frá 6. febrúar 2018, WP251rev.01. Þar kemur fram ítarleg greining á nánara inntaki 22. gr. reglugerðarinnar og einstökum hugtökum greinarinnar eins og þau eru túlkuð á grundvelli almennra reglna reglugerðarinnar um vinnsluheimildir, réttindi hins skráða og skyldur ábyrgðaraðila og má þar nefna hugtakið „ákvörðun [sem] eingöngu [er tekin] á grundvelli sjálfvirkrar gagnavinnslu“. Þá er að finna í leiðbeiningunum sérstaka umfjöllun um að börn skuli njóta sérstakrar verndar fyrir gerð persónusniða, m.a. með vísan til formálsorðanna í 71. lið formálans.

Um 23. gr.

Þessi grein er upphafsákvæði IV. kafla sem geymir almennar reglur um skyldur ábyrgðaraðila og vinnsluaðila og öryggi persónuupplýsinga. Öll ákvæði þessa kafla endurspeglar samsvarandi ákvæði reglugerðarinnar um sama efni og þar er ekki að finna neinar sérreglur eða undantekningar enda veitir reglugerðin ekki heimild þess. Í ljósi þess lykilhlutverks sem ábyrgðaraðili og vinnsluaðili hafa í tengslum við vinnslu persónuupplýsinga þykir þó rétt samhengisins vegna að safna helstu kjarnaatriðum IV. kafla reglugerðarinnar um

það efni á einn stað í frumvarpinu, og varpa ljósi á hvernig ber að skýra þau, m.a. með hliðsjón af formálsorðum reglugerðarinnar. Það er líka mikilvægt í ljósi þess að einmitt í þessum efnum felur reglugerðin í sér margvísleg nýmæli, einkum auknar skyldur á ábyrgðaraðila en einnig á vinnsluaðila og nýjar kröfur til öryggis við vinnslu persónuupplýsinga. Helstu nýmælin birtast í hinni nýju meginreglu um ábyrgðarskyldu, því að auknar kröfur eru gerðar um gagnsæi og fræðslu gagnvart hinum skráða, að gerð er krafa um tæknilegar og skipulagslegar ráðstafanir til að tryggja innbyggða og sjálfgefna persónuvernd, að í sumum tilvikum er lögð sjálfstæð ábyrgð á vinnsluaðila, að skylt er að halda skrá yfir vinnslustarfsemi, að auknar kröfur eru gerðar til öryggis við vinnslu, að skylt er eða tilkynna um öryggisbresti og að í ákveðnum tilvikum þarf að láta fara fram mat á áhrifum á persónuvernd við tiltekna vinnslu. Verður fjallað nánar um þessi atriði og hvaða breytingar eru gerðar frá núverandi skipan í skýringum við einstök. Gildandi lög og persónuverndartilskipun ESB hafa ekki að geyma sérstakan kafla um skyldur ábyrgðaraðila og vinnsluaðila en þær birtast í dreifðum ákvæðum í löggjöfinni.

Skilgreining á hugtakinu „ábyrgðaraðili“ kemur fram í 6. tölul. 3. gr. frumvarpsins, þ.e. að um ræðir þann einstakling, lögaðila, stjórnvald eða annan aðila sem ákveður einn eða í samvinnu við aðra tilgang og aðferðir við vinnslu persónuupplýsinga. Vísað er til nánari skýringa með áður nefndu frumvarpsákvæði, en áréttá má að skilgreiningin er efnislega óbreytt frá núgildandi reglum.

Í 23. gr. frumvarpsins er mælt fyrir um þá skyldu ábyrgðaraðila að 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. Í 24. gr. reglugerðarinnar er til viðbótar því sem segir í frumvarpsákvæðinu tekið fram að ráðstafanirnar, sem vísað er til skuli m.a. fela í sér að ábyrgðaraðili innleiði viðeigandi persónuverndarstefnur. Samkvæmt þessu er ætlast til að upplýsingar um hvernig unnið er með persónuupplýsingar í starfsemi ábyrgðaraðila séu á aðgengilegu og auðskiljanlegu formi. Nýja löggjöfin gerir strangari kröfur til framsetningar og innihalds fræðslu en núgildandi löggjöf, enda er meginreglan um gagnsæi ein af hornsteinum reglugerðarinnar, eins og birtist víða í ákvæðum hennar.

Þá er tekið fram að sé samþykktum háttarnisreglum fylgt, eins og um getur í 40. gr. reglugerðarinnar, eða samþykktu vottunarfyrirkomulagi, eins og um getur í 42. gr. hennar, megi nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar. Þessar skyldur ábyrgðaraðila verður að skoða í ljósi þeirrar nýju meginreglu í 2. mgr. 8. gr. frumvarpsins að ábyrgðaraðili verður að geta sýnt fram á að vinnsla persónuupplýsinga sé í samræmi við meginreglur um lögmæti, tilgang, meðalhóf, áreiðanleika og varðveislu. Í formála reglugerðarinnar, 74. lið, eru þessi sjónarmið áréttuð og tekið fram að ábyrgðaraðilanum ætti einkum að vera skylt að gera viðeigandi og skilvirkar ráðstafanir og að hann ætti að vera fær um að sýna fram á að vinnslan fari fram í samræmi við reglugerðina, þ.m.t. að því er varðar skilvirkni umræddra ráðstafana. Ættu þær að taka mið af eðli, umfangi, samhengi og tilgangi vinnslunnar og áhættu fyrir réttindi og frelsi einstaklinga. Þá er í 75. lið formálans varpað frekara ljósi á hvernig ber að meta áhættu einstaklings. Vísað er þar til þess að vinnsla kann að leiða til misjafnlega líklegar og alvarlegrar áhættu fyrir réttindi og frelsi einstaklinga sem getur leitt af sér efnislegt tjón, eignatjón og óefnislegt tjón, einkum þegar vinnslan getur haft í för með sér mismunun, auðkennisþjófnað eða svik, fjárhagstjón, skaða á orðstír, tapaðan trúnað um persónuupplýsingar sem njóta verndar á grundvelli þagnarskyldu, að notkun gerviauðkenna sé aflétt í leyfisleysi eða annað umtalsvert efnahagslegt eða félagslegt óhagræði. Nánar er í dæmaskyni nefnt það þegar skráðir einstaklingar gætu misst réttindi sín og frelsi eða verið hindraðir í að stjórna eigin persónuupplýsingum og þegar persónuupplýsingar eru unnar sem leiða í ljós kynþátt eða þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð, heimspekilega sannfæringu eða stéttarfélagsaðild. Einnig er í þessu sambandi sérstaklega tilgreind vinnsla erfðafræðilegra upplýsinga, upplýsinga sem varða heilsu, upplýsinga um kynlíf og upplýsinga um sakfellingar í refsímálum, refsiverð brot og tengdar öryggisráðstafanir. Þá er það sérstaklega nefnt þegar lagt er mat á persónulega þætti, einkum við að greina eða spá fyrir um atriði er varða frammistöðu í starfi, fjárhagsstöðu, heilsuhagi, smekk eða áhugamál, áreiðanleika eða hegðun, staðsetningu eða hreyfanleika í því skyni að útbúa eða nota persónusnið, sem og það þegar persónuupplýsingar berskjaldaðra einstaklinga, einkum barna, eru unnar og þegar vinnsla tekur til mikils magns persónuupplýsinga og hefur áhrif á marga skráða einstaklinga.

Í 77. lið formálans er lagt til að ábyrgðaraðilum og vinnsluaðilum verði veittar leiðbeiningar um framkvæmd viðeigandi ráðstafana og um það hvernig sýna skuli fram á fylgni við reglur, einkum að því er varðar greiningu á áhættu í tengslum við vinnslu, mat þeirra að því er varðar orsök áhættunnar, eðli hennar, hversu líkleg og alvarleg hún er og greiningu á bestu starfsvenjum til að draga úr henni, einkum með því að nota viðurkenndar háttæknireglur og viðurkennda vottun. Mun Persónuvernd vinna að því að gefa út slíkar leiðbeiningar og hér um ræðir og einnig er stefnt að því að Evrópska persónuverndarráðið gefi út viðmiðunarreglur um vinnsluaðgerðir sem ólíklegt er að leiði af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga og bendi þá á ráðstafanir sem geta verið nægilegar í slíkum tilvikum til að bregðast við áhættuþáttum. Þá ber að hafa í huga að sérreglur gilda um 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, sbr. 29. gr. frumvarpsins og 35. gr. reglugerðarinnar, en nánari umfjöllun um það er að finna í skýringum við þau ákvæði.

Í seinni málslið 23. gr. frumvarpsins er vísað til þess að þegar tveir eða fleiri eru sameiginlegir ábyrgðaraðilar fer um skyldur þeirra eftir 26. gr. reglugerðarinnar. Í því reglugerðarákvæði er nánar útfært hvenær beri að líta svo á að ábyrgðaraðilar séu fleiri en einn en það á við ef tveir eða fleiri ábyrgðaraðilar ákveða sameiginlega tilgang vinnslu og aðferðir við hana. Sé ábyrgð hvers ábyrgðaraðila um sig ekki ákveðin í lögum er þeim skylt að ákveða á gagnsæjan hátt með samkomulagi sín í milli ábyrgð hvers um sig á því að skuldbindingar samkvæmt reglugerðinni séu uppfylltar, einkum hvað snertir beitingu réttinda hinna skráðu, og skyldur hvers um sig til að láta í té upplýsingarnar sem um getur í 13. og 14. gr. Í samkomulaginu má tilnefna tengilið fyrir skráða einstaklinga. Þá segir að samkomulagið skuli endurspegla með tilhlýðilegum hætti hlutverk og tengsl hvers hinna sameiginlegu ábyrgðaraðila gagnvart skráðum einstaklingum, sem og að megininntak þess skuli gert aðgengilegt skráðum einstaklingi. Í 79. lið formála reglugerðarinnar er áréttað mikilvægi þess að skipting ábyrgðarsviða sé skýr þegar fleiri en einn ábyrgðaraðili ákveða tilgang og aðferðir við vinnslu.

Um 24. gr.

Í þessu ákvæði birtast nýmæli sem fram koma í 25. gr. reglugerðarinnar um svokallaða innbyggða og sjálfgefna persónuvernd. Reglur um þetta efni endurspegla jafnframt áherslur reglugerðarinnar á ríkari kröfur sem almennt eru gerðar til ábyrgðaraðila. Samkvæmt því skal ábyrgðaraðili, bæði þegar ákveðnar eru aðferðir við vinnsluna og þegar vinnslan sjálf fer fram, gera viðeigandi tæknilegar ráðstafanir, sem hannaðar eru til að framfylgja með skilvirkum hætti meginreglum um persónuvernd, þar á meðal lágmörkun gagna, og fella nauðsynlegar verndarráðstafanir inn í vinnsluna til að uppfylla kröfur reglugerðarinnar og vernda réttindi skráðra einstaklinga, eins og fram kemur í 1. mgr. 25. gr. reglugerðarinnar..

Í 2. mgr. þessa frumvarpsákvæðis er mælt fyrir um að ábyrgðaraðili skuli 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. Í tilvitnuðu ákvæði er tekið fram að þessi skylda gildi um það hversu miklum persónuupplýsingum er safnað, að hvaða marki unnið er með þær, hversu lengi þær eru varðveittar og aðgang að þeim. Einkum skal tryggja með ráðstöfunum samkvæmt því að það sé sjálfgefið að persónuupplýsingar verði ekki gerðar aðgengilegar ótakmörkuðum fjölda fólks án ihlutunar viðkomandi einstaklings.

Í 78. lið formálans er varpað frekar ljósi á úrræði og ráðstafanir til að ná markmiðum 25. gr. reglugerðarinnar og þar með frumvarpsákvæðisins. Áréttað er að slíkar ráðstafanir geti m.a. falið í sér að draga sem mest úr vinnslu persónuupplýsinga, færa persónuupplýsingar undir gerviaudkenni eins skjótt og unnt er, gagnsæi að því er varðar eiginleika persónuupplýsinga og vinnslu þeirra, að gera skráðum einstaklingi kleift að fylgjast með vinnslu upplýsinganna og gera ábyrgðaraðila kleift að taka upp og bæta öryggisþætti. Einnig segir að þegar framleiðendur vöru, þjónustu og hugbúnaðar þróa, hanni, velji og noti hugbúnað, vöru og þjónustu, sem er byggð á vinnslu persónuupplýsinga, eða vinni með persónuupplýsingar í störfum sínum, ætti að hvetja þá til að taka tillit til réttarins til persónuverndar við þróun og hönnun á slíkum vörum, þjónustu og hugbúnaði og ganga úr skugga um, að teknu tilhlýðilegu tilliti til nýjustu tækniþekkingar, að ábyrgðaraðilar og vinnsluaðilar geti uppfyllt skyldur sínar um persónuvernd. Einnig ætti að taka tillit til meginreglnanna um innbyggða og sjálfgefna persónuvernd í tengslum við opinber útboð.

Af þessu sést að hönnuðir upplýsingakerfa eru hvattir til þess að hanna hugbúnað sinn og þjónustu frá upphafi með vernd persónuupplýsinga í huga, t.d. með innbyggðum eða sjálfgefnum persónuverndarstillingum. Þetta er gert í þeim tilgangi að ábyrgðaraðilar geti í kjölfarið mætt þeim kröfum sem lög og reglur gera til þeirra. Nýju ákvæðin um innbyggða og sjálfgefna persónuvernd munu því hafa mikil áhrif á upplýsingatækni, hönnun og endurhönnun hugbúnaðar í framtíðinni. Innbyggð persónuvernd gerir ráð fyrir því sem fyrr segir að vernd persónuupplýsinga sé innbyggð í vörur og þjónustu, t.d. hugbúnað og upplýsingakerfi, strax frá upphafi, með því að draga úr líkum á að öryggisbrot verði. Sjálfgefin persónuvernd miðast við að persónuupplýsingar verði ekki sjálfkrafa gerðar aðgengilegar almenningi, nema á grundvelli mannlegrar ihlutunar. Sem dæmi um sjálfgefnar persónuverndarstillingar má nefna að við birtingu ljósmynda á vefsíðu eða samfélagsmiðli verði persónuverndarstillingar í upphafi stilltar þannig að tiltekin mynd sé einungis sýnileg eiganda en ekki opin almenningi, þannig að viðkomandi þurfi ekki sjálfur að grípa til aðgerða til að vernda upplýsingar sínar gegn óviðkomandi.

Þetta felur m.a. í sér að þau fyrirtæki sem starfa við hönnun og þróun upplýsingakerfa þurfa að hafa í huga hvernig vernd þeirra persónuupplýsinga, sem unnið er með í kerfum þeirra, skuli vera tryggð. Ný tækni, vara og þjónusta ætti því að vera þannig úr garði gerð að hún uppfylli skilyrði hinnar nýju persónuverndarlöggjafar. Reglan um innbyggða og sjálfgefna persónuvernd er þó ekki eingöngu bundin við þá sem þróa nýjan hugbúnað eða vöru heldur þurfa ábyrgðaraðilar að vinnslu persónuupplýsinga einnig að huga að reglunni við alla vinnslu persónuupplýsinga, líkt og segir í ákvæði frumvarpsins.

Af þeirri ástæðu þurfa þau fyrirtæki og einstaklingar sem hanna og þróa hugbúnað eða upplýsingakerfi að kynna sér vel þær kröfur sem löggjöfin gerir til vinnslu persónuupplýsinga. Það þarf því að huga að því hvort upplýsingavinnsla byggist á heimild einstaklings eða lagaskyldu, sem og hvort þeim meginreglum sem ávallt ber að fylgja, um gæði gagna og vinnslu, sé fylgt. Þessar meginreglur lúta t.d. að því að upplýsingar skuli vera áreiðanlegar og réttar, að þær séu unnar í skýrum og málefnalegum tilgangi og að meðalhöfs sé gætt.

Um 25. gr.

Þetta frumvarpsákvæði byggist á 28. gr. reglugerðarinnar. Eins og í núgildandi lögum og reglugerð ESB er ráðgert í reglugerðinni að ábyrgðaraðilum sé heimilt að fela vinnsluaðila að vinna persónuupplýsingar fyrir sig að hluta eða í heild að tilteknum skilyrðum uppfylltum. Er skilgreining á vinnsluaðila efnislega óbreytt í frumvarpi þessu og reglugerðinni frá því sem í gildandi lögum og tilskipun ESB, þ.e. að átt sé við einstakling, lögaðila, stjórnvald eða annan aðila sem vinnur með persónuupplýsingar á vegum ábyrgðaraðila, sbr. 7. tölul. 3. gr. frumvarpsins. Sem dæmi um vinnsluaðila má nefna upplýsingatæknifyrirtæki sem veita tölvuþjónustu, s.s. hýsingu, umsjón, viðhald o.fl., netöryggisfyrirtæki eða fyrirtæki sem veita ráðgjöf á sviði upplýsingatækni og hafa aðgang að persónuupplýsingum, markaðs- eða samskiptafyrirtæki sem vinna persónuupplýsingar fyrir hönd viðskiptavina og hvers konar stofnanir eða fyrirtæki sem sinna þjónustu er felur í sér vinnslu persónuupplýsinga fyrir hönd annarra stofnana eða fyrirtækja.

Í 1. mgr. frumvarpsákvæðisins er tekið fram að ábyrgðaraðili megi aðeins leita til vinnsluaðila sem veita nægilegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnsla uppfylli kröfur reglugerðarinnar og réttindi skráðra einstaklinga séu tryggð. Þá er nánar tryggt í 2. mgr. frumvarpsins að vinnsluaðili geti ekki leitað til annars vinnsluaðila, þ.e. svonefnds undirvinnsluaðila (e. *sub-processor*), nema hafa til þess sértæka eða almenna skriflega heimild ábyrgðaraðila. Er þessi áskilnaður um hvenær leita má til undirvinnsluaðila nýmæli sem ekki er að finna í gildandi lögum eða ESB-tilskipuninni.

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.

Samkvæmt 3. mgr. frumvarpsákvæðisins er það skilyrði þess að ábyrgðaraðili feli öðrum að vinna með persónuupplýsingar á sínum vegum að vinnslusamningur liggi fyrir eða önnur 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. Í 3. mgr. 28. gr. reglugerðarinnar eru talin upp í ítarlegu máli frekari atriði sem skulu koma fram í slíkum

samningi. Þá er í 4. mgr. 28. gr. reglugerðarinnar mælt fyrir um hvernig skyldur samkvæmt vinnslusamningi yfirfærast á undirvinnsluaðila.

Í 81. lið formála reglugerðarinnar eru frekari skýringar á því hvaða kröfur reglugerðin gerir til vinnsluaðila og á atriðum sem ábyrgðaraðila ber að gæta að. Mikilvægt er að vinnslusamningur sé skriflegur, þ.m.t. á rafrænu formi, sbr. 9. mgr. 28. gr. reglugerðarinnar, og geta ábyrgðaraðili og vinnsluaðili valið að nota stakan samning eða föst samningsákvæði sem annaðhvort framkvæmdastjórnin samþykkir beint eða eftirlitsstofnun í aðildarríkinu samþykkir í samræmi við samræmingarkerfið og framkvæmdastjórnin samþykkir síðan. Persónuvernd hefur nú þegar gefið út leiðbeiningar þar sem finna má drög að föstum samningsákvæðum í vinnslusamningi og má því ætla að slík samningsákvæði verði til staðar fyrir fyrirtæki og stofnanir.

Loks er ljóst að sú meginregla gildir skv. 10. mgr. 28. gr. reglugerðarinnar að brjótí vinnsluaðili í bága við reglugerðina þegar hann ákveður tilgang og aðferðir við vinnslu, telst hann vera ábyrgðaraðili varðandi þá vinnslu. Um það hvernig bótaábyrgð og viðurlög vegna brota ábyrgðaraðila og vinnsluaðila á ákvæðum reglugerðarinnar er komið fram gagnvart þeim er nánar fjallað í 46., 48. og 51. gr. frumvarpsins og 82., 83. og 84. gr. reglugerðarinnar.

Um 26. gr.

Þessi frumvarpsgrein er nýmæli í persónuverndarlöggjöfinni og byggist á 30. gr. reglugerðarinnar. Hér er mælt fyrir um nýjar skyldur bæði ábyrgðaraðila og vinnsluaðila til að halda skrá yfir þá starfsemi sína þar sem vinnsla persónuupplýsinga fer fram. Þetta ákvæði endurspeglar áherslur reglugerðarinnar á auknar skyldur þeirra sem vinna með persónuupplýsingar og á að þeir hafi yfirsýn á hverjum tíma yfir það hvaða vinnsla fer fram á hverjum tíma í starfsemi þeirra. Í 1. mgr. 30. gr. reglugerðarinnar er talið upp í ítarlegu máli í sjö stafliðum hvaða upplýsingar eiga að koma fram í skrá samkvæmt ákvæðinu. Samantekið eru helstu atriði sem þar þurfa að koma fram heiti og samskiptaupplýsingar ábyrgðaraðila, eftir atvikum sameiginlegs ábyrgðaraðila, fulltrúa hans eða persónuverndarfulltrúa, af hverju persónuupplýsingar eru unnar, að hvaða einstaklingum þær lúta, hvenær þær eru unnar, af hverjum og hversu lengi, hvar og hversu lengi þær eru varðveittar og ef mögulegt er almenn lýsing á tæknilegum og skipulagslegum öryggisráðstöfunum. Þá eru sérreglur um skrár sem vinnsluaðili heldur í 2. mgr. 30. gr. Atriði sem þurfa að koma fram þar eru áþekkt því sem gildir um ábyrgðaraðila en lúta þó fyrst og fremst að því hvaða flokkar vinnslu fara fram fyrir þann síðarnefnda. Áskilið er í 3. mgr. 30. gr. reglugerðarinnar að skrár yfir vinnslustarfsemi séu skriflegar og einnig á rafrænu formi. Þá ber ábyrgðaraðilum og vinnsluaðilum að hafa slíkar skrár aðgengilegar fyrir Persónuvernd á hverjum tíma, sbr. einnig 4. mgr. 30. gr. reglugerðarinnar.

Í 2. mgr. þessa frumvarpsákvæðis er fjallað um undantekningar frá því að halda vinnsluskrá og byggist hún á 5. mgr. 30. gr. reglugerðarinnar. Samkvæmt þessu á skyldan ekki við um fyrirtæki og stofnanir sem hafa færri en 250 starfsmenn. Þó eru gerðir fyrirvarar við það í sama ákvæði því að undantekningin á ekki við ef vinnslan, sem innt er af af hendi hjá viðkomandi aðila er 1) líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, 2) er ekki tilfallandi, 3) tekur til viðkvæmra persónuupplýsinga eða 4) persónuupplýsinga sem varða sakfellingar í refsímálum og refsiverð brot. Af þessu sést, einkum af öðrum fyrirvaranum, að undantekningin frá skyldunni virðist mun þrengri en orð 5. mgr. gefa til kynna við fyrstu sýn. Ljóst er að nær öll fyrirtæki eða stofnanir hafa með höndum vinnslu persónuupplýsinga sem er meira en „tilfallandi“ en er regluleg og kerfisbundin. Sem dæmi um slíkt má nefna vinnslu persónuupplýsinga um launamál starfsmanna og mánaðarlegar keyrslur slíkra upplýsinga, jafnt á fámönnum sem fjölmönnum vinnustöðum. Af þessu verður ályktað að skylda til að halda vinnsluskrár sé allvíðtæk og hvíli á nær öllum fyrirtækjum og stofnunum. Á móti þessu koma hins vegar skýringar í 13. lið formála reglugerðarinnar sem taka fram að með hliðsjón af sérstökum aðstæðum örfyrirtækja og lítilla og meðalstórra fyrirtækja sé sett undanþága í reglugerðina varðandi skráhald fyrirtækja með færri en 250 starfsmenn. Enn fremur eru stofnanir og aðilar Sambandsins og aðildarríkin og eftirlitsyfyrirvöld þeirra hvött til að taka tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja við beitingu reglugerðarinnar. Af þessu verður ályktað að þegar vinnsla persónuupplýsinga er smá í sniðum sé a.m.k. ekki ætlast til jafn ítarlegra vinnsluskráa örfyrirtækja og lítilla og meðalstórra fyrirtækja og raunin væri ella

Í formála reglugerðarinnar er að öðru leyti lítt varpað ljósi á hvernig beri að skýra 30. gr. hennar um vinnsluskrár og undantekningar frá meginreglunni um að halda beri slíkar skrár. Um þetta ákvæði segir aðeins í 82. lið formálans að til þess að sýna fram á að farið sé að reglugerðinni ætti ábyrgðaraðilinn eða vinnsluaðilinn að halda skrár um vinnsluaðgerðir sem eru á hans ábyrgð. Hverjum ábyrgðaraðila og vinnsluaðila eigi jafnframt að vera skylt að vinna með eftirlitsyfirvaldi og gera þessar skrár, að fenginni beiðni, aðgengilegar eftirlitsyfirvaldinu svo að nýta megi þær í þágu eftirlits með þessum vinnsluaðgerðum.

Starfshópur skv. 29. gr. tilskipunar ESB undirbýr nú útgáfu á nánari leiðbeiningum um hvernig túlka skuli undantekningarákvæði 5. mgr. 30. gr. reglugerðarinnar. Þá má ætla að frekari leiðbeiningar um gerð vinnsluskráa, hugsanlega með hliðsjón af stöðluðum formum um framsetningu þeirra, sem fyrirtæki hér á landi geti stuðst við verði gefnar út hjá Persónuvernd þar verður litið til viðmiða og leiðbeininga 29. gr. starfshópsins svo og ráðgjafar eða tilmæla sem væntanlega kemur frá Evrópska persónuverndarráðinu um samræmda framkvæmd í þessu tilliti.

Um 27. gr.

Þessi grein frumvarpsins byggist á 32.-34. gr. reglugerðarinnar og er efni hennar tvíþætt, annars vegar um skyldur ábyrgðaraðila og vinnsluaðila til að gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja viðunandi öryggi persónuupplýsinga og hins vegar um viðbrögð við því að öryggisbrot eigi sér stað. Í 11. og 12. gr. núgildandi laga er að finna fyrirmæli um skyldur ábyrgðaraðila til að gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda persónuupplýsingar, svo og til að viðhafa innra eftirlit með vinnslu persónuupplýsinga til að ganga úr skugga um að unnið sé í samræmi við gildandi lög og reglur og þær öryggisráðstafanir sem ákveðnar hafa verið.

Ákvæði 32.-34. gr. reglugerðarinnar um öryggi við vinnslu eru talsvert ítarlegri en samsvarandi ákvæði ESB-tilskipunarinnar. Þannig leggur 32. gr. þá skyldu á bæði ábyrgðaraðila og vinnsluaðila að 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. Er síðan tekin dæmi um ráðstafanir sem átt gætu við, s.s. að notuð séu gerviaudkenni og að persónuupplýsingar séu dulkóðaðar; að tryggður sé viðvarandi trúnaður, auk samfellu, tiltækileika og álagspóls vinnslukerfa og -þjónustu; að tryggt sé að tímanlega megi gera persónuupplýsingar tiltækilegar að nýju og endurheimta aðgang að þeim ef til efnislegs eða tæknilegs atviks komi; og að til staðar sé ferli til að prófa og meta reglulega skilvirkni tæknilegra og skipulagslegra ráðstafana til að tryggja öryggi vinnslunnar. Er þessi atriði áréttuð frekar í 83. lið formála reglugerðarinnar. Hér er einkum verið að vísa til þess sem jafnan er kallað gerð öryggisstefnu, framkvæmd áhættumats og ákvarðanir um öryggisráðstafanir.

Þá kemur fram í 2. mgr. 32. gr. reglugerðarinnar að þegar metið er hvort öryggi sé viðunandi skal einkum hafa hliðsjón af þeirri áhættu sem vinnslan hefur í för með sér, sérstaklega hvað varðar óviljandi eða ólögmæta eyðingu persónuupplýsinga, sem eru sendar, geymdar eða unnar á annan hátt, eða það að þær glattist, breytist, verði birtar eða að aðgangur verði veittur að þeim í leyfisleysi. Í 3. og 4. mgr. 32. gr. reglugerðarinnar er nánar rakið að hægt sé að sýna fram á að öryggiskröfur séu uppfylltar með því að vísa til samþykkttra háttarnisreglna skv. 40. gr. reglugerðarinnar eða samþykktts vottunarfyrirkomulags skv. 42. gr. hennar,

Í 2. mgr. þessa frumvarpsákvæðis er fjallað um viðbrögð við öryggisbroti. Eins og fram kom í 11. tölul. 3. gr. frumvarpsins er með því átt við brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga eða að þær glattist, breytist, verði birtar eða að aðgangur verði veittur að þeim í leyfisleysi. Fyrirmæli um þetta koma fram í 33. gr. reglugerðarinnar og eru nýmæli. Þar kemur fram sú meginregla að ábyrgðaraðili skuli, án ótilhlýðilegrar tafar, og, ef mögulegt er, eigi síðar en 72 klst. eftir að hann verður brotsins var, tilkynna það til Persónuverndar. Sá fyrirvari er þó gerður að tilkynningarskyldan eigi ekki við ef ólíklegt þygi að brotið leiði til áhættu fyrir réttindi og frelsi einstaklinga. Hér er vissulega um matskennt atriði að ræða, en rétt er í vafatilvikum að sinna tilkynningarskyldunni. Dragist að tilkynna Persónuvernd um öryggisbrot fram yfir 72 klst. skulu ástæður fyrir töfinni fylgja tilkynningunni. Þá er tekið fram í 2. mgr. að vinnsluaðili skal tilkynna ábyrgðaraðila um það án ótilhlýðilegrar tafar ef hann verður var við öryggisbrot við meðferð persónuupplýsinga.

Nánari leiðbeiningar um efni tilkynningar til Persónuverndar koma fram í 3. mgr. 33. gr. reglugerðarinnar. Samkvæmt því ákvæði skal í fyrsta lagi lýsa eðli öryggisbrotsins, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem það varðar og flokkum og áætluðum fjölda færslna með persónuupplýsingum sem um er að ræða, í öðru lagi að gefa upp nafn og samskiptaupplýsingar persónuverndarfulltrúa eða annars tengiliðar þar sem hægt er að fá frekari upplýsingar, í þriðja lagi að lýsa líklegum afleiðingum öryggisbrotsins og loks í fjórða lagi að lýsa þeim ráðstöfunum sem ábyrgðaraðili hefur gert eða fyrirhugar að gera vegna þess, þ.m.t., eftir því sem við á, ráðstöfunum til að milda hugsanleg skaðleg áhrif þess. Þá er sú skylda lögð á ábyrgðaraðila í 5. mgr. 33. gr. að skrá niður hvers kyns öryggisbrot við meðferð persónuupplýsinga og tilgreina málsatvik í tengslum við viðkomandi brot, áhrif þess og aðgerðir til úrbóta sem gripið var til. Þessi skráning gerir Persónuvernd kleift að sannreyna að farið sé að framangreindum förmælum um viðbrögð við öryggisbroti. Í 85. lið formála reglugerðarinnar koma fram frekari skýringar á markmiðinu að baki tilkynningarskyldu með vísan til þeirra afleiðinga sem öryggisbrot getur haft í för með sér fyrir einstakling. Bent er á að öryggisbrot við meðferð persónuupplýsinga getur, ef ekki er brugðist við því á réttan hátt og tímanlega, valdið einstaklingum efnislegu tjóni, eignatjóni eða óefnislegu tjóni, s.s. missi yfirráða yfir persónuupplýsingum um sig eða takmörkun réttinda sinna, mismunun, auðkennisþjófnaði eða svikum, fjárhagstjóni, að notkun gerviauðkenna sé aflétt í leyfisleysi, skaða á orðstír, töpuðum trúnaði gagnvart persónuupplýsingum sem njóta verndar samkvæmt þagnarskyldu eða öðru umtalsverðu efnahagslegu eða félagslegu óhagræði.

Í 3. mgr. þessa frumvarpsákvæðis er mælt fyrir um tilkynningarskyldu ábyrgðaraðila til skráðs einstaklings sem persónuupplýsingarnar varða, um öryggisbrot án ótilhlýðilegrar tafar ef líklegt er að brotið leiði af sér mikla áhættu fyrir réttindi og frelsi einstaklinga. Ákvæði þetta er byggt á 34. gr. reglugerðarinnar sem kveður nánar á um efni slíkrar tilkynningar. Þar skal lýsa á skýru og einföldu máli eðli öryggisbrots og skal tilkynningin innihalda a.m.k. þær upplýsingar sem um getur í tilkynningu til Persónuverndar skv. 33. gr. Samkvæmt 86. lið formála reglugerðarinnar er markmið tilkynningarskyldu í þessum tilvikum einkum að gefa viðkomandi einstaklingi færi á að gera nauðsynlegar varúðarráðstafanir. Í tilkynningunni ætti að koma fram eðli öryggisbrotsins, auk tilmæla til viðkomandi einstaklings um að draga úr mögulegum skaðlegum áhrifum. Slíkar tilkynningar til skráðra einstaklinga ætti að senda eins fljótt og mögulegt sé og í nánú samstarfi við Persónuvernd, í samræmi við leiðbeiningar frá henni. Þörf á að draga úr bráðri hættu á tjóni kalli eftir skjótum samskiptum við skráða einstaklinga.

Undantekningar frá tilkynningarskyldu til skráðs einstaklings er að finna í 2. mgr. 34. gr. reglugerðarinnar. Hún á í fyrsta lagi ekki við hafi ábyrgðaraðilinn gert viðeigandi tæknilegar og skipulagslegar verndarráðstafanir og þessar ráðstafanir voru gerðar varðandi þær persónuupplýsingar sem öryggisbrotið varðaði, einkum ráðstafanir til að gera persónuupplýsingar ólæsilegar hverjum þeim sem ekki hefur aðgangsheimild að þeim, s.s. með dulkóðun. Í öðru lagi á tilkynningarskyldan ekki við hafi ábyrgðaraðilinn gert ráðstafanir í kjölfar öryggisbrots sem tryggja að ólíklegt sé að aftur komi til jafnmikillar áhættu fyrir réttindi og frelsi skráðra einstaklinga og um getur í 1. mgr. 34. gr. Loks á hún í þriðja lagi ekki við ef hún myndi hafa í för með sér óhóflega fyrirhöfn. Í því tilviki skal í stað tilkynningar til skráðs einstaklings birta almenna tilkynningu eða grípa til svipaðrar ráðstöfunar þar sem hinum skráðu er gert viðvart um brot með jafnáhrifaríkum hætti.

Í 87. og 88. lið formála reglugerðarinnar koma fram frekari skýringar á því hvernig á að bera sig að við tilkynningu til Persónuverndar, þar á meðal við undirbúning hennar. Nánar segir að ábyrgðaraðila beri að ganga úr skugga um hvort allar viðeigandi tæknilegar verndarráðstafanir og skipulagsráðstafanir hafi verið gerðar til að staðfesta tafarlaust hvort öryggisbrot við meðferð persónuupplýsinga hafi átt sér stað og til að upplýsa Persónuvernd og hinn skráða þegar í stað um það. Gangi ætti úr skugga um að tilkynningin hafi verið send án ótilhlýðilegrar tafar, einkum með tilliti til eðlis og alvarleika öryggisbrots við meðferð persónuupplýsinga, afleiðinga þess og skaðlegra áhrifa þess fyrir hinn skráða. Slík tilkynning geti leitt til inngrípa af hálfu Persónuverndar í samræmi við verkefni hennar og valdsvið.

Þegar settar eru ítarlegar reglur um viðeigandi framsetningu og verklag við tilkynningu öryggisbrots við meðferð persónuupplýsinga ætti að taka tilhlýðilegt tillit til aðstæðna þegar viðkomandi brot átti sér stað, m.a. hvort persónuupplýsingar hafi verið varðar með viðeigandi

tæknilegum ráðstöfunum sem takmarki í reynd líkur á auðkennasvikum eða annars konar misnotkun.

Þess má loks geta að starfshópur skv. 29. gr. tilskipunar ESB hefur gefið út leiðbeiningar um öryggisbrot við vinnslu á persónuupplýsingum samkvæmt þeim nýju ákvæðum reglugerðarinnar um efnið sem rakin eru að framan (Guidelines on Personal data breach notification under Regulation 2016/679) frá 3. október 2017, endurskoðuð og breytt 6. febrúar 2018, WP350rev.01. Þar eru gefnar ítarlegar leiðbeiningar, s.s. um hvenær tilkynningarskyldan verður virk og hvenær undantekningar frá henni eiga við, og hugtök í 32.-34. gr. reglugerðarinnar skýrð. Persónuvernd hefur jafnframt gefið út leiðbeiningar um tilkynningar vegna öryggisbrota, en þær eru byggðar á framangreindum leiðbeiningum 29. gr. hópsins.

Um 28. gr.

Í þessari grein er áréttuð sú regla sem fram kemur í 31. gr. reglugerðarinnar að ábyrgðaraðili og vinnsluaðili og, eftir atvikum, fulltrúar þeirra skulu, að fenginni beiðni Persónuverndar, hafa samvinnu við stofnunina við framkvæmd verkefna hennar. Er hér undirstrikað mikilvægi þess að þeir sem vinna með persónuupplýsingar bregðist við athugunum og eftirliti Persónuverndar þegar hún óskar slíkrar samvinnu. Ákvæðið er í raun ákveðin speglun á verkefnum og valdheimildum Persónuverndar sem lýst er í 41. og 42. gr. frumvarpsins. Þar er mælt fyrir um ýmsar heimildir stofnunarinnar til að hafa afskipti af starfsemi ábyrgðaraðila og vinnsluaðila, m.a. til að fyrirskipa að þeir veiti hverjar þær upplýsingar sem hún þarfnast vegna reglna frumvarpsins og reglugerðarinnar. Verður nánar vikið að þeim valdheimildum í umfjöllun um ákvæði VII. kafla frumvarpsins.

Í þessu sambandi má einnig benda á 47. gr. frumvarpsins þar sem fjallað er um atriði sem áhrif hafa á ákvörðun um stjórnvaldssektir vegna brota á reglum frumvarpsins og reglugerðinni. Í 6. og 8. tölul. 1. mgr. er sérstaklega tilgreint að taka skuli tilhlýðilegt tillit til umfangs samvinnu við Persónuvernd til að bæta úr brotinu, svo og með hvaða hætti ábyrgðaraðili eða vinnsluaðili tilkynnti um brotið.

Um 29. gr.

Þessi grein er upphafsgrein V. kafla frumvarpsins sem fjallar um mat á áhrifum á persónuvernd, fyrirframsamráð, leyfisfiskyldu, skilmála Persónuverndar við leyfisveitingu o.fl. Byggjast 29. og 30. gr. frumvarpsins á ákvæðum 35. og 36. gr. reglugerðarinnar en 31.-34. gr. frumvarpsins fjalla um sérreglur sem reglugerðin heimilar varðandi skilyrði um leyfisveitingar í tengslum við ákveðna vinnslu.

Í 1. mgr. 29. gr. frumvarpsins er fjallað um mat á áhrifum á persónuvernd. Markmið þess er að tryggja að þegar vinnsluaðferðir skapa mikla hættu fyrir friðhelgi einstaklinga meti ábyrgðaraðili þá hættu og mögulegar afleiðingar hennar áður en vinnslan hefst. Komi í ljós að áhættan sé mikil og að honum sé sjálfum ekki fært að draga úr henni verður að leita fyrirfram álits Persónuverndar á vinnslunni. Ákvæðið er nýmæli og á sér því ekki beina hliðstæðu í ESB-tilskipuninni, þar sem ekki er vikið sérstaklega að skyldu til að gera áhættumat, né heldur í gildandi lögum. Þess er þó að geta að ákvæði 11. gr. núgildandi laga, eins og þeim var breytt með lögum nr. 90/2001, fjallar um áhættumat, öryggi og gæði persónuupplýsinga og gildir að hluta til um áþekkt efni og hér um ræðir, en þó frá þrengra sjónarhorni. Á grundvelli umrædds ákvæðis laganna hafa verið settar reglur nr. 299/2001 um öryggi persónuupplýsinga sem lúta fyrst og fremst að skilyrðum sem gerð eru til öryggiskerfa. Bæði þar og í lögnum er byggt á þeirri forsendu að skriflegt áhættumat sé gert.

Reglur 35. gr. reglugerðarinnar um mat á áhrifum á persónuvernd fela í sér sérstakar skyldur til að láta fara fram slíkt mat við þær aðstæður sem lýst er að ofan og er í 2. mgr. greinarinnar jafnframt mælt fyrir um að leita skuli ráða hjá persónuverndarfulltrúa um efnið, sé hann til staðar. Þá er nánar rakið í 3. mgr. 35. gr. hvenær sérlega ríkar ástæður eru til að láta fara fram umrætt mat, en þrenns konar aðstæður eru þar nefndar. Í fyrsta lagi þegar um er að ræða kerfisbundið og umfangsmikið mat, byggt á sjálfvirkri vinnslu, á persónulegum þáttum sem tengjast einstaklingum, þ.m.t. gerð persónusniðs, og sem leiðir til töku ákvarðana sem hafa réttaráhrif fyrir einstaklinginn eða snerta hann verulega; í öðru lagi ef um er að ræða umfangsmikla vinnslu viðkvæmra persónuupplýsinga eða persónuupplýsinga um sakfellingar í refsímálum og refsiverð brot eins og um getur í 10. gr. reglugerðarinnar; og í þriðja lagi ef um er að ræða kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi.

Í 84. og 91. lið formála reglugerðarinnar eru þessi fyrirmæli skýrð nánar og dæmi tekin um hvenær ákvæðið á við. Kemur þar m.a. fram að sérstaklega eigi að láta fara fram mat á áhrifum á persónuvernd þegar um er að ræða umfangsmiklar vinnsluaðgerðir sem miða að því að vinna verulegt magn persónuupplýsinga á alþjóðlegum vettvangi, sem gætu haft áhrif á mikinn fjölda skráðra einstaklinga og sem líklegt má telja að leiði af sér mikla áhættu, t.d. vegna þess hversu viðkvæmar upplýsingarnar eru. Einnig þegar notuð er ný tækni í miklum mæli, svo og þegar viðhafðar eru aðrar vinnsluaðgerðir sem leiða af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum þegar þessar aðgerðir gera hinum skráðu erfiðara fyrir með að neyta réttar síns. Þá er tekið fram í 91. lið að framkvæma ætti mat á áhrifum á persónuvernd þegar unnið er með persónuupplýsingar vegna ákvarðana sem varða tiltekna einstaklinga í kjölfar kerfisbundins og umfangsmikils mats á persónubundnum þáttum sem tengjast þeim og byggt er á gerð persónusniðs úr þessum upplýsingum, sem og þegar ákvarðanirnar fylgja í kjölfar vinnslu viðkvæmra upplýsinga, lífkennaupplýsinga eða upplýsinga um sakfellingar í refsímálum og refsiverð brot eða tengdar öryggisráðstafanir. Um skýringu á því hvað geti falist í umfangsmiklu eftirliti með svæðum sem eru aðgengileg almenningi er einkum vísað til þess þegar notaður er ljósrafeindabúnaður eða aðrar aðgerðir viðhafðar sem Persónuvernd telur að leiði líklega af sér mikla áhættu fyrir réttindi og frelsi skráðra einstaklinga, einkum vegna þess að þær komi í veg fyrir að hinir skráðu geti neytt réttar síns, notið þjónustu eða byggt á samningi, eða vegna þess að þær eru umfangsmiklar og framkvæmdar kerfisbundið. Í því sambandi er tekið fram að vinnsla persónuupplýsinga ætti ekki að teljast umfangsmikil ef hún varði persónuupplýsingar frá einstökum lækni, öðrum faglærðum heilbrigðisstarfsmanni eða lögfræðingi um sjúklinga eða viðskiptavini. Í þeim tilvikum er ekki ætlast til að mat á áhrifum á persónuvernd verði skyldubundið. Þá er bent á í 92. lið formálans að við tilteknar aðstæður kunni að vera skynsamlegt og hagkvæmt að hafa viðfangsefni mats á áhrifum á persónuvernd viðtækara en eitt verkefni. Það eigi t.d. við ef stjórnvöld eða stofnanir hafa í hyggju að koma á sameiginlegum vettvangi vegna vinnslu eða þegar margir ábyrgðaraðilar ráðgera að koma á sameiginlegu notkunar- eða vinnsluumhverfi innan atvinnugreinar eða geira í atvinnulífinu. Mikilvægt er að mat á persónuvernd fari fram áður en vinnsla hefst.

Í 2. og 3. mgr. frumvarpsákvæðisins er mælt fyrir um aðgerðir af hálfu Persónuverndar til að auðvelda ábyrgðaraðilum að greina á milli þess hvenær þörf er á að mat á persónuvernd fari fram og hvenær ekki. Er hér byggt á hliðstæðum ákvæðum 4. og 5. mgr. 35. gr. reglugerðarinnar. Þannig skal Persónuvernd birta skrá yfir þær tegundir vinnsluaðgerða þar sem krafist er mats á áhrifum á persónuvernd, en auk þess getur stofnunin ákveðið að birta skrá yfir þær tegundir vinnsluaðgerða þar sem ekki er krafist slíks mats. Við birtingu þessara upplýsinga samkvæmt framangreindu skulu a.m.k. koma fram eftirfarandi upplýsingar, sbr. 7. mgr. 35. gr. reglugerðarinnar: a) kerfisbundin lýsing á fyrirhuguðum vinnsluaðgerðum og tilganginum með vinnslunni, þ.m.t., eftir atvikum, lögmætum hagsmunum ábyrgðaraðilans, b) mat á því hvort vinnsluaðgerðirnar séu nauðsynlegar og hóflegar miðað við tilganginn með þeim, c) mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga sem í hlut eiga og d) ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu, þar á meðal verndarráðstafanir, öryggisráðstafanir og fyrirkomulag við að tryggja vernd persónuupplýsinga og sýna fram á að farið sé að reglugerðinni, að teknu tilliti til réttinda og lögmætra hagsmuna skráðra einstaklinga og annarra einstaklinga sem í hlut eiga. Í 8.-11. mgr. 35. gr. reglugerðarinnar er að finna nánari fyrirmæli um atriði sem tengjast mati á persónuvernd, þ.m.t. þýðingu þess fyrir slíkt mat að hlutaðeigandi ábyrgðar- og vinnsluaðilar fylgi samþykktum háttætnisreglum. Þá eru þar ákveðnar undantekningar á skyldu til að framkvæma mat á áhrifum á persónuvernd og fjallað um hvenær þörf sé á því að láta endurskoða slíkt mat.

Þess má loks geta að starfshópur skv. 29. gr. tilskipunar ESB hefur gefið út leiðbeiningar um mat á áhrifum á persónuvernd og ákvörðun þess hvenær vinnsla er talin líkleg til að hafa mikla áhættu í för með sér (Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679) frá 4. apríl 2017, síðast breytt 4. október 2017, WP248. Þar er að finna ítarlegar leiðbeiningar og útskýringar á inntaki 35. gr. reglugerðarinnar og bæði efnisleg og tæknileg viðmið sem ber að líta til þegar metið er hvort vinnsla sé líkleg til að skapa mikla áhættu.

Um 30. gr.

Þessi grein frumvarpsins mælir fyrir um skyldu ábyrgðaraðila til að leita fyrirframsamráðs við Persónuvernd við ákvæðnar aðstæður. Í henni birtist kjarni hliðstæðs ákvæðis með sama heiti í 36. gr. reglugerðarinnar. Ákvæðið, sem ber að skoða í ljósi undanfarandi greinar um mat á áhrifum á persónuvernd, verður virkt þegar slíkt mat leiðir í ljós að vinnsla myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðili gripi til ráðstafana til að draga úr henni, og skal hann þá hafa samráð við Persónuvernd áður en vinnslan hefst, samkvæmt nánari fyrirsmælum 36. gr. reglugerðarinnar.

Í 2. mgr. þessa frumvarpsákvæðis kemur fram að telji Persónuvernd að fyrirhuguð vinnsla myndi brjóta í bága við reglugerðina, einkum ef ábyrgðaraðili hefur ekki greint eða dregið úr áhættunni með fullnægjandi hætti, skal stofnunin, innan átta vikna frá því að henni berst beiðni um samráð, veita ábyrgðaraðila og, eftir atvikum, vinnsluaðila skriflega ráðgjöf og getur notað til þess allar þær valdheimildir sínar sem um getur í 41.–43. gr. frumvarpsins. Lengja má frestinn um sex vikur með hliðsjón af því hversu flókin fyrirhuguð vinnsla er. Persónuvernd skal tilkynna ábyrgðaraðila og, eftir atvikum, vinnsluaðila um slíka framlengingu 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.

Nánari upptalningu atriða sem ábyrgðaraðili skal greina frá þegar hann leitar samráðs hjá Persónuvernd er að finna í 3. mgr. 36. gr. reglugerðarinnar. Þessi atriði eru eftirfarandi: a) eftir atvikum, ábyrgðarsvið ábyrgðaraðila, sameiginlegra ábyrgðaraðila og vinnsluaðila, sem koma að vinnslunni, hvers um sig, einkum þegar um er að ræða vinnslu innan fyrirtækjasamstæðu, b) tilgangur fyrirhugaðrar vinnslu og aðferðir við hana, c) ráðstafanir og verndarráðstafanir sem gerðar eru til að vernda réttindi og frelsi skráðra einstaklinga samkvæmt reglugerðinni, d) ef við á, samskiptaupplýsingar persónuverndarfulltrúa, e) mat á áhrifum á persónuvernd og f) hverjar þær upplýsingar aðrar sem Persónuvernd fer fram á.

Auk þeirra aðstæðna sem fyrr er getið þar sem leita skal fyrirframsamráðs við Persónuvernd er sérregla í 4. mgr. 36. gr. reglugerðarinnar sem felur í sér að stjórnvöld skulu hafa samráð við Persónuvernd við undirbúning lagasetningar sem fjallar um vinnslu persónuupplýsinga, sbr. einnig 96. lið formála reglugerðarinnar. Það sama gildir ef stjórnvaldsráðstöfun, t.d. setning stjórnvaldsfyrirmæla sem byggist á lögum felur í sér vinnslu persónuupplýsinga. Hér er í raun fest í sessi framkvæmd sem þegar hefur verið við lýði um langt skeið á grundvelli núgildandi laga, þar sem lagafrumvörp og stjórnvaldsfyrirmæli með ákvæðum um vinnslu persónuupplýsinga hafa að jafnaði verið send Persónuvernd til umsagnar. Er einnig gert ráð fyrir slíku samráði í verkefnum Persónuverndar skv. 37. gr. núgildandi laga, svo og með nákvæmari lýsingu í 2. tölul. 3. mgr. 39. gr. frumvarps þessa. Samkvæmt því ákvæði skal Persónuvernd veita Alþingi, stjórnvöldum og öðrum aðilum ráðgjöf á sviði lagasetningar og stjórnsýslu sem tengist vernd einstaklinga við vinnslu persónuupplýsinga.

Í 94. lið formála reglugerðarinnar eru áréttaðar efnisreglur 36. gr. hennar. Þar er einnig ítrekað að eftirlitsyfirvaldið, þ.e. Persónuvernd, ætti að bregðast við beiðni um samráð innan tilgreinds tíma. Komi ekki viðbrögð frá Persónuvernd innan þess tíma ætti það þó ekki að hafa áhrif á íhlutun stofnunarinnar síðar í samræmi við verkefni hennar og valdheimildir samkvæmt frumvarpinu og reglugerðinni, þar á meðal heimildina til að banna vinnsluaðgerðir. Liður í samráðsferli þessu er að heimilt er að leggja fyrir Persónuvernd niðurstöðu mats á áhrifum á persónuvernd sem framkvæmt er með tilliti til viðkomandi vinnslu, einkum fyrirhugaðar ráðstafanir til að draga úr áhættu fyrir réttindi og frelsi einstaklinga.

Um 31. gr.

Í þessu ákvæði frumvarpsins er mælt fyrir um aðstæður þar sem heimilt er að ákveða að vinnsla persónuupplýsinga sé háð sérstöku leyfi Persónuverndar. Almennt séð felur reglugerðin í sér ákveðið fráhrif frá fyrri stefnu um að vinnsla persónuupplýsinga geti byggst á leyfum, en í ákvæði þessu felst undantekning frá því. Hér er nýtt heimild sem kemur fram í 5. mgr. 36. gr. reglugerðarinnar um að þess megi krefjast í lögum aðildarríkis að ábyrgðaraðilar hafi samráð við og fái fyrirframleyfi eftirlitsyfirvalds í tengslum við vinnslu ábyrgðaraðila sem annast framkvæmd verkefnis í þágu almannahagsmuna, þ.m.t. vinnslu sem tengist félagslegri vernd og lýðheilsu. Er hér viðhaldið heimild sem þegar er að finna í núgildandi lögum að nokkru leyti, en samkvæmt 33. gr. þeirra laga er heimilt að áskilja leyfi Persónuverndar fyrir því að fram fari

vinnsla almennra eða viðkvæmra persónuupplýsinga sem getur falið í sér sérstaka hættu á að farið verði í bága við réttindi og skyldur skráðra einstaklinga.

Í 1. mgr. frumvarpsákvæðisins er því lýst samkvæmt framangreindu að Persónuvernd geti ákveðið að vinnsla megi ekki hefjast fyrr en hún hefur verið athuguð af stofnuninni og samþykkt með útgáfu sérstakrar heimildar þegar um er 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. Þá segir að Persónuvernd geti ákveðið að slík leyfisskylda falli brott þegar settar hafa verið almennar reglur og öryggisstaðlar sem fylgja skuli við slíka vinnslu. Hafa ber í huga að hér er um heimild að ræða en ekki skyldu til að binda tiltekna vinnslustarfsemi við leyfi.

Í 2. mgr. þessa ákvæðis er mælt fyrir um að Persónuvernd skuli setja nánari reglur um leyfisskyldu. Má ætla að þar muni koma fram skýrari afmörkun á því við hvaða aðstæður ákvæðinu verður beitt. Um forsendur leyfisveitingar Persónuverndar og skilmála hennar er fjallað í 32. og 33. gr. frumvarpsins.

Um 32. gr.

Þessi grein frumvarpsins er í beinum tengslum við 31. gr. þess um leyfisskylda vinnslu og kveður á um forsendur fyrir veitingu leyfis. Fram kemur sú meginregla að þeim einum megi veita leyfi skv. 31. gr. sem líklegur er til að geta uppfyllt skyldur sínar samkvæmt reglugerðinni, lögnum eða fyrirmælum Persónuverndar. Er það Persónuvernd sem á mat í þeim efnum.

Í 2. mgr. er lýst því hagsmunamati sem viðhafa ber við ákvörðun um leyfisveitingu. Verði niðurstaðan af því mati sú að vinnslan skapi slíkt óhagræði fyrir hinn skráða að ekki sé talið hægt að bæta úr því með forsvaranlegum hætti verða hagsmunir hans taldir vega þyngra og synjað um leyfi til vinnslu. Persónuvernd ber að kanna á grundvelli m.a. þeirra atriða sem talin eru upp í 33. gr. frumvarpsins hvort hagsmunir hins skráða teljast nægilega tryggðir með setningu skilmála skv. þeirri grein.

Um 33. gr.

Í þessari grein eru tilgreind þau atriði sem Persónuvernd ber að athuga þegar ábyrgðaraðila er veitt leyfi samkvæmt 31. gr. frumvarpsins. Er hér um að ræða áþekk skilyrði leyfisveitingar og standa í 35. gr. núgildandi laga. Eins og fram kom í skýringum við það ákvæði er ekki lögð til tæmandi upptalning heldur eru í dæmaskyni nefnd atriði sem sjónarmið um persónuvernd krefjast að litið sé til. Ákvæðið er hins vegar hvorki bindandi fyrir Persónuvernd að því er varðar þau atriði sem hún byggir mat sitt á né dregur það úr valdheimildum hennar. Hins vegar er mikilvægt að ábyrgðaraðili geti að einhverju leyti áttað sig á því fyrir fram til hvaða atriða verði litið þegar Persónuvernd metur hvort veita skuli leyfi. Þannig getur Persónuvernd t.d. bundið vinnslu skilyrðum um dulkóðun eða eyðingu persónuauðkenna.

Í 3. mgr. 35. gr. núgildandi laga er ákvæði um að Persónuvernd geti ákveðið að ábyrgðaraðili og vinnsluaðili undirriti yfirlýsingu um að þeir lofi að gæta þagmælsku um viðkvæmar persónuupplýsingar sem þeir fá vitneskju um við vinnslu þeirra. Í frumvarpinu er hliðstætt ákvæði að finna í 44. gr. sem er almennt ákvæði um þagnarskyldu. Þar er tekið fram að við gerð skilmála skv. 33. gr. laganna geti 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. Þá er lögð refsing við broti á þagnarskyldu í 2. mgr. 48. gr. frumvarpsins. Verður nánar fjallað um þagnarskyldu þeirra sem vinna með persónuupplýsingar í skýringum við þessi frumvarpsákvæði síðar.

Frumvarpið geymir ekki sérstaka reglu, eins og nú er að finna í 4. mgr. gildandi laga, um að Persónuvernd geti mælt fyrir um að sérstakur tilsjónarmaður skuli skipaður til að hafa eftirlit með því að vinnsla sé í samræmi við lög og skilmála stofnunarinnar. Er það í raun fólgið í valdheimildum stofnunarinnar á grundvelli 40. gr. frumvarpsins að hún getur ákveðið að ábyrgðaraðili skuli greiða þann kostnað sem hlýst af eftirliti. Þar undir myndi falla kostnaður af starfi sérstaks tilsjónarmanns ef ákveðið er að skipa hann, svo og annar kostnaður af úttektum á starfsemi við undirbúning útgáfu vinnsluleyfis og öðrum eftirlitsaðgerðum. Um gjaldtöku vegna kostnaðar sem hlýst af eftirliti er fjallað í 40. gr. frumvarpsins.

Þá ber að hafa í huga að með tilkomu persónuverndarfulltrúa samkvæmt ákvæðum reglugerðarinnar getur dregið úr þörf á skipun tilsjónarmaður verði skipaður til þess að hafa eftirlit með því að vinnsla sé í samræmi við lög og skilmála Persónuverndar.

Um 34. gr.

Ákvæði þessarar greinar er samhljóða 35. gr. a gildandi laga, eins og hún bættist í lögum með lögum nr. 44/2014 um vísindarannsóknir á heilbrigðissviði. Með þeim lögum voru felld brott ákvæði í sérlægum, þ. á m. 3. mgr. 15. gr. laga nr. 74/1997 um réttindi sjúklinga, sem mæltu fyrir um skyldu til að afla leyfis Persónuverndar vegna upplýsingaöflunar í þágu vísindarannsókna á heilbrigðissviði en jafnframt var vísindasiðanefnd og siðanefndum heilbrigðisrannsókna falið aukið hlutverk. Samkvæmt ákvæðum laganna um vísindarannsóknir á heilbrigðissviði veitir vísindasiðanefnd eða siðanefnd heilbrigðisrannsókna á heilbrigðisstofnun leyfi fyrir vísindarannsókn á heilbrigðissviði eftir að hafa metið rannsóknaráætlun vísindarannsóknar út frá sjónarmiðum vísinda, siðfræði og mannréttinda. Nefndirnar senda Persónuvernd yfirlit yfir umsóknir um leyfi til vísindarannsókna og er heimilt að gefa út leyfi að liðnum tíu virkum dögum frá því að slíkt yfirlit berst Persónuvernd nema stofnunin hafi gert viðvart um að tiltekin rannsókn þarfnist sérstakrar skoðunar. Telji Persónuvernd að rannsókn brjóti í bága við lög um persónuvernd og meðferð persónuupplýsinga skal hún ekki leyfð.

Rétt þykir að viðhalda óbreyttu ákvæði um efnið í þessu frumvarpsákvæði enda er ljóst að Persónuvernd gegnir ákveðnu lögbundnu hlutverki í tengslum við veitingu leyfa fyrir vísindarannsóknum á heilbrigðissviði, sem lýst er í sérlægum um efnið.

Um 35. gr.

VI. kafli frumvarpsins geymir þrjú ákvæði sem fela í sér nýmæli miðað við gildandi löggjöf og ESB-tilskipun. Er meginefni kaflans um persónuverndarfulltrúa, sbr. 35. og 36. gr. og þá er fjallað um vottun og vottunaraðila í 37. gr. Ákvæðin byggjast öll á beinum fyrirmælum reglugerðarinnar en að hluta til er aðildarríkjum skylt að setja sérákvæði um þessi efni í landslög. Reglugerðin gerir ráð fyrir því að persónuverndarfulltrúar gegni lykilhlutverki til að tryggja að vinnsla persónuupplýsinga samræmist lögunum. Rétt er að taka fram að fulltrúinn er ekki persónulega ábyrgur ef reglunum er ekki fylgt. Er mælt fyrir um skyldu tiltekinna ábyrgðaraðila og vinnsluaðila til að tilnefna persónuverndarfulltrúa og fjallað nánar um stöðu þeirra og verkefni í reglugerðinni. Þótt Evrópureglur hafi ekki fjallað um persónuverndarfulltrúa hefur slíkt fyrirkomulag mótast í nokkrum Evrópuríkjum.

Fátt er um útskýringar í formála reglugerðirnar á þessum nýja hópi fagmanna sem fara með mikilvægt hlutverk samkvæmt ákvæðum 37.- 39. gr. hennar. Er kjarni þessara ákvæða þó dreginn saman í 97. lið formálans. Þar er tekið fram að þegar vinnsla persónuupplýsinga er í höndum opinbers yfirvalds, að undanskildum dómstólum eða sjálfstæðum dómsyfirvöldum þegar þau fara með dómsvald sitt, ef vinnsla í einkageiranum er í höndum ábyrgðaraðila og meginstarfsemi hans felst í vinnsluáðgerðum sem krefjast umfangsmikillar, reglubundinnar og kerfisbundinnar vöktunar á skráðum einstaklingum eða ef meginverkefni ábyrgðaraðilans eða vinnsluaðilans felast í umfangsmikilli vinnslu sérstakra flokka persónuupplýsinga og upplýsinga er varða sakfellingu í refsímálum og refsiverð brot ætti aðili með sérþekkingu á löggjöf um persónuvernd, þ.e. persónuverndarfulltrúi, að aðstoða ábyrgðaraðilann eða vinnsluaðilann við eftirlit með því að þessari reglugerð sé fylgt í starfseminni. Þá er tekið fram að ákvarða ætti nauðsynlega sérþekkingu slíks fulltrúa einkum út frá þeim vinnsluáðgerðum sem framkvæmdar eru og þeirri vernd sem nauðsynleg er vegna þeirra persónuupplýsinga sem ábyrgðaraðili eða vinnsluaðili vinnur. Loks er áréttað að persónuverndarfulltrúar, hvort sem þeir eru starfsmenn ábyrgðaraðilans eða ekki, ættu að vera í aðstöðu til að sinna skyldustörfum sínum og verkefnum óháð öðrum.

Ítarlegri skýringar á ákvæðum um efnið er að finna í leiðbeiningum um persónuverndarfulltrúa sem starfshópur skv. 29. gr. tilskipunar ESB hefur gefið út frá 16. desember 2016 með breytingum frá 5. apríl 2017 (Guidelines on Data Protection Officers), WP243 rev.01. Í febrúar 2018 gaf Persónuvernd út leiðbeiningar um persónuverndarfulltrúa sem birtar eru á heimasíðu stofnunarinnar. Þær byggja að stóru leyti á fyrrgreindum leiðbeiningum frá 29. gr. hópnum. Í umfjöllun hér á eftir verður m.a. stuðst við þær skýringar sem birtast í leiðbeiningum um persónuverndarfulltrúa um helstu hugtök ákvæða reglugerðarinnar um efnið og stöðu og hlutverk persónuverndarfulltrúa.

Í 1. mgr. þessa frumvarpsákvæðis er kveðið á um tilvik þar sem ábyrgðaraðila og vinnsluaðila er skylt að tilnefna persónuverndarfulltrúa. Í fyrsta lagi á það við, skv. 1. tölul., í öllum tilvikum þar sem vinnsla er höndum stjórnsvalds. Í 1. mgr. 37. gr. reglugerðarinnar er

vísað til opinbers yfirvalds eða stofnunar án frekari tilgreiningar, en það getur m.a. ráðist af skilgreiningu landslaga. Hér á landi verður þá einkum litið til skilgreiningar 1. gr. stjórnsýslulaga nr. 37/1993. Því er ljóst að með stjórnvöldum er vísað til allra aðila, stofnana, nefnda o.fl. sem falla undir stjórnsýslu ríkis og sveitarfélaga. Þá er hugsanlegt að tiltekin verkefni í þágu almannahagsmuna séu falin lögaðilum á sviði einkaréttar. Dæmi af þeim toga eru m.a. rakin í fyrrgreindum leiðbeiningum s.s. á sviði almenningssamgangna, vegaframkvæmda, orku- og vatnsveitna o.fl. þar sem staða skráðra einstaklinga getur verið nokkuð sambærileg og ætti við gagnvart stjórnvöldum. Þótt ekki sé um stjórnvöld að ræða í skilningi 1. tölul. og beina lagaskyldur fyrirtækja á þeim grundvelli er engu að síður talið æskilegt að þau tilnefni persónuverndarfulltrúa þegar þau vinna verkefni í þágu almannahagsmuna. Þá má vera að ákvæði 2. og 3. tölul. eigi hvort eð er við um starfsemina vegna umfangs eða eðlis vinnslunnar. Í 1. mgr. 37. gr. reglugerðarinnar eru undanskildir dómstólar þegar þeir fara með dómsveld sitt. Þar sem ljóst er að hugtakið stjórnvald í íslensku lagamáli tekur ekki til dómstóla, þarf ekki að undanskilja þá sérstaklega í þessu frumvarpsákvæði. Hins vegar er ljóst að dómstólar vinna að nokkru marki með persónuupplýsingar í starfsemi sinni sem ekki tengist beint meðferð dómssvalds, t.d. í tengslum við birtingu dóma. Getur þá verið æskilegt að þeir tilnefni persónuverndarfulltrúa þó ekki sé bein lagaskylda til þess.

Auk skyldu stjórnvalda til að tilnefna persónuverndarfulltrúa mæla eftirtaldir töluliðir fyrir um slíka skyldur í öðrum tilvikum. Það er annar vegar þegar meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í vinnsluaðgerðum sem krefjast, sakir eðlis síns, umfangs eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum (2. tölul. 1. mgr.) eða hins vegar þegar meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í umfangsmikilli vinnslu viðkvæmra persónuupplýsinga eða upplýsinga sem varða sakfellingar í refsímálum og refsiverð brot (3. tölul.). Í c-lið 1. mgr. 37. gr. reglugerðarinnar eru þessi tvö atriði 3. tölul. talin upp í röð en ótvírætt að skýra þau sem valkvæð, þ.e. nægilegt er að annað hvort eigi sér stað umfangsmikil vinnsla viðkvæmra persónuupplýsinga eða upplýsinga sem varða sakfellingar í refsímálum og refsiverð brot. Í leiðbeiningum 29. gr. hópsins um persónuverndarfulltrúa er þessi skýring á hliðstæðu ákvæði c-liðar 1. mgr. 37. gr. reglugerðarinnar áréttuð.

Þegar fyrirtæki ákveður hvort það þurfi að skipa sér persónuverndarfulltrúa þarf fyrst að leggja mat á hvað felst í hugtakinu „meginstarfsemi“. Í leiðbeiningum um persónuverndarfulltrúa segir að hér sé átt við lykilverkefni sem eru nauðsynleg fyrir starfsemi ábyrgðar- eða vinnsluaðila. Skýrt dæmi um þetta er starfsemi heilbrigðisstofnana. Þótt meginmarkmið í slíkri starfsemi sé að veita heilbrigðisþjónustu er ljóst að slíkt væri ekki unnt án þess að vinna persónuupplýsingar um einstaklinga, s.s. í sjúkraskrá, og fellur vinnsla því undir meginstarfsemi. Því er ljóst að öllum aðilum sem veita slíka þjónustu, hvort heldur opinberum (sem falla hvort eð er undir skyldu skv. 1. tölul.) og einkareknum aðilum, er skylt að tilnefna persónuverndarfulltrúa. Sem annað dæmi má nefna öryggisþjónustufyrirtæki sem starfrækir eftirlitsmyndavélar, bæði á almannafæri og einkasvæðum s.s. í verslunarmiðstöð. Er meginstarfsemi slíkra fyrirtækja fólgin í eftirliti með skráðum einstaklingum sem skapar skyldu til að tilnefna persónuverndarfulltrúa. Annað hugtak í 2. og 3. tölul. sem þarf að skýra er orðið „umfangsmikil“ vinnsla. Í leiðbeiningum um persónuverndarfulltrúa segir að þótt fjöldi þeirra sem vinnslan snertir hafi vissulega þýðingu sé ekki hægt að gefa nákvæmt mat á því t.d. um tiltekinn fjölda skráðra einstaklinga til að uppfylla þetta skilyrði heldur verði hér að taka mið af nokkrum atriðum í hverju tilviki sem eru eftirfarandi: 1) fjöldi skráðra einstaklinga 2) magn persónuupplýsinga sem vinnslan varðar 3) tímalengd vinnslustarfseminnar eða varðveislutíma upplýsinganna 4) landfræðileg mörk vinnslunnar, þ.e. hversu víðfeðm hún er. Þá eru í leiðbeiningunum talin upp dæmi um það sem myndi falla þar undir, þar á meðal vinnsla sjúkraskráupplýsinga í reglulegri starfsemi heilbrigðisstofnana, vinnsla ferðaupplýsinga einstaklinga sem ferðast með almenningssamgöngum, vinnsla persónuupplýsinga af hálfu leitarvélar um hegðun einstaklinga á Netinu í þeim tilgangi að bjóða persónusniðnar auglýsingar og vinnsla váttryggingarfélaganna og banka á persónuupplýsingum um viðskiptavinum sem eru í reglulegum samskiptum. Dæmi um það sem myndi aftur á móti ekki falla þarna undir væri vinnsla persónuupplýsinga um sjúklinga hjá sjálfstætt starfandi heilbrigðisstarfsmanni eða vinnsla upplýsinga sem varða sakfellingar í refsímálum eða refsiverð brot hjá einstaka lögmanni eða starfandi lögfræðingi. Um skýringu á hugtökunum „reglubundið“ og „kerfisbundið“ eftirlit

með einstaklingum í 2. tölul. má hafa til hliðsjónar orð 24. liðar formála reglugerðarinnar sem fjallar um vöktun á hegðun skráðra einstaklinga en undir það fellur m.a. þegar slóð einstaklinga er rakin á Netinu og í kjölfarið séu notaðar vinnsluaðferðir á persónuupplýsingum sem felast í gerð persónusniðs um einstakling, einkum í því skyni að taka ákvarðanir varðandi viðkomandi eða til að greina eða spá fyrir um smekk hans, hegðun og viðhorf. Í leiðbeiningum um persónuverndarfulltrúa er einnig tekið fram að orðið kerfisbundið taki til þess að vinnslan byggji á ákveðnu kerfi, þar sem ákveðið er fyrir fram að vinnsla fari fram eftir ákveðnu skipulagi. Dæmi um starfsemi sem getur falið í sér reglulegt og kerfisbundið eftirlit með skráðum einstaklingum er rekstur fjarskiptanets og fjarskiptaþjónustu, gerð persónusniða og áhættumats, t.d. lánshæfismats, við ákvörðun tryggingariðgjalds til að koma í veg fyrir svik eða peningabætti, eftirlit með hreyfingu einstaklings samkvæmt upplýsingum úr heilsuúrum eða annars konar heilsutækjum sem einstaklingur hefur á sér og notkun öryggismyndavéla.

Annað mikilvægt atriði í 1. mgr. er að ekki aðeins ábyrgðaraðilar heldur einnig vinnsluaðilar geta borið skyldu til að tilnefna persónuverndarfulltrúa. Í leiðbeiningum um persónuverndarfulltrúa er tekið fram að þegar vinnsluaðili vinnur upplýsingar fyrir marga ábyrgðaraðila í senn, geti þessa skylda orðið virk vegna umfangs vinnslu á upplýsingum, þótt ekki sé sjálfgefið að hver og einn ábyrgðaraðili beri skyldu til að tilnefna persónuverndarfulltrúa. Verður þannig að meta sjálfstætt í hverju og einu tilviki hvort hvor þessara aðila eða báðir uppfyllir skilyrði 2. og 3. tölul.

Samkvæmt 2. mgr. þessa frumvarpsákvæðis er fyrirtækjasamstæðu 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. Fyrri hluti ákvæðisins er hliðstæður 2. mgr. 37. gr. reglugerðarinnar. Í síðara hluta ákvæðisins er byggt á heimild í 3. mgr. 37. gr. hennar til að fleira en eitt stjórnvald geti tekið sig saman um að tilnefna einn persónuverndarfulltrúa. Um hugtakið fyrirtækjasamstæða vísast til skilgreiningar sem fram kemur í 10. tölul. 4. gr. reglugerðarinnar en þar er átt við „ráðandi fyrirtæki og undirfyrirtæki þess“. Þegar einn persónuverndarfulltrúi er tilnefndur fyrir fyrirtækjasamstæðu verður að tryggja að hver starfsstöð hafi greiðan aðgang að honum. Til að aðgengi að persónuverndarfulltrúanum sé tryggt verður hann í það minnsta að vera staðsettur innan EES-svæðisins óháð því hvort ábyrgðar- eða vinnsluaðili eru það. Þó er ekki útilokað að í afmörkuðum tilvikum geti þær aðstæður verið fyrir hendi að hvorki ábyrgðar né vinnsluaðili séu með starfsstöð innan EES-svæðisins og því sé betra fyrir persónuverndarfulltrúann að sinna starfi sínu utan þess.

Þegar fleiri en eitt stjórnvald tilnefna sameiginlegan persónuverndarfulltrúa verður að hafa hliðsjón af stjórnskipulagi þeirra og stærð. Þannig má benda á að hugsanlega gætu tvö eða fleiri sveitarfélög tekið sig saman um að tilefna sameiginlegan persónuverndarfulltrúa, en ef öll 74 sveitarfélög landsins tilnefna einn sameiginlegan fulltrúa fyrir sig öll er umfang slíks starfs hugsanlega orðið of mikið til að fulltrúinn geti sinnt skyldum sínum gagnvart þeim öllum svo vel sé.

Þess má geta að er ekkert því til fyrirstöðu samkvæmt reglugerðinni að fleira en eitt fyrirtæki, leiti þjónustu hjá sama persónuverndarfulltrúa. Ætla má að í fyrstu eftir gildistöku laganna verði ekki margir með þá sérþekkingu og faglegu hæfni sem þarf til að sinna hlutverki persónuverndarfulltrúa og aðengi að sérfræðingum efnið verði í byrjun takmarkað. Því getur verið hagfelld að t.d. fleiri en eitt smáfyrirtæki geti tilnefnt sama fulltrúa sem er ekki fastur starfsmaður neins þeirra en sinnir verkefninu sjálfstætt fyrir hvert þeirra sem verktaki.

Aðildarríkjum er veitt svigrúm í 4. mgr. reglugerðarinnar til þess að kveða á um skyldu fyrirtækja, samtaka o.fl. til að tilnefna persónuverndarfulltrúa í öðrum tilvikum en þeim sem talin eru í 1. mgr. og rakin eru að framan. Í frumvarpi þessu er ekki farin sú leið að setja ákvæði um viðtækari skyldur í þessu tilliti. Vitaskuld geta fyrirtæki tilnefnt slíka fulltrúa þó þeim sé það ekki skylt samkvæmt lögum. Í leiðbeiningum um persónuverndarfulltrúa er hvatt til þess að tilnefna persónuverndarfulltrúa þótt ekki sé um lagaskyldu að ræða.

Í 3. mgr. frumvarpsins er vísað til nánari fyrirsmála í 37.-39. gr. reglugerðarinnar um hæfni, stöðu og verkefni persónuverndarfulltrúa. Samkvæmt 5. mgr. 37. gr. skal persónuverndarfulltrúi tilnefndur á grundvelli faglegrar hæfni sinnar og einkum sérþekkingar á lögum og lagaframkvæmd á sviði persónuverndar og getu sinnar til að vinna þau verkefni sem um getur í 39. gr. reglugerðarinnar. Mikilvæg hæfni og sérþekking geta einkum falist í sérþekkingu á innlendum og evrópskum persónuverndarlögum og lagaframkvæmd á því sviði,

skilningi á þeirri vinnslu sem fer fram, skilningi á öryggis- og upplýsingatæknimálum, þekkingu á starfsemi fyrirtækis og getu til að efla persónuverndarmenningu hjá viðkomandi stofnun eða fyrirtæki. Ljóst að í litlu samfélagi eins og hér á landi búa enn sem komið er ekki mjög margir yfir sérþekkingu á lögum og lagaframkvæmd um persónuvernd, en sá hópur fer vaxandi. Í leiðbeiningum um persónuverndarfulltrúa er hvatt til þess að boðið sé upp á þjálfun og námskeið bæði af hálfu einkaaðila og stjórnvalda, þar á meðal Persónuverndar til að auka sérþekkingu á sviðinu.

Persónuverndarfulltrúi þarf sem fyrr segir ekki nauðsynlega að vera fastur starfsmaður með ráðningarsamning við ábyrgðaraðila eða vinnsluaðila. Tekið er fram í 6. mgr. 39. gr. reglugerðarinnar að hann geti sinnt verkefnum á grundvelli þjónustusamnings. Getur persónuverndarfulltrúi þannig starfað á grundvelli verktakasamnings, jafnvel hjá fleiri en einum ábyrgðar- eða vinnsluaðila eins og fyrr var lýst. Hvað sem líður vinnusambandi hans við ábyrgðar- eða vinnsluaðila, er aðalatriðið að tryggja sjálfstæði hans í starfi og jafnframt að fyrirbyggja hagsmunaárekstra starfi hann fyrir fleiri en einn aðila. Hér ber líka að hafa í huga að orðið að „tilnefna“ (e. *designate*) persónuverndarfulltrúa felur einmitt í sér að ekki sé nauðsynlega um fasta ráðningu að ræða, en ljóst sé að einstaklingi sé falið þetta hlutverk með tilnefningu og gert sé ráð fyrir aðkomu hans að ákvörðunum í starfsemi þar sem reynir á vinnslu persónuupplýsinga. Þegar utanaðkomandi verktaki gegnir starfi persónuverndarfulltrúa getur teymi á vegum verktakans gegnt starfi fulltrúans, en á ábyrgð nánar tilgreinds „stjórnanda“ gagnvart viðskiptavinum. Við þær aðstæður er mikilvægt að hver og einn starfsmaður undir stjórn persónuverndarfulltrúans uppfylli allar þær kröfur sem reglugerðin gerir til persónuverndarfulltrúa.

Um stöðu og þar með talið sjálfstæði persónuverndarfulltrúa við störf sín er fjallað í 38. gr. reglugerðarinnar. Samkvæmt 1. mgr. skulu ábyrgðaraðili og vinnsluaðili tryggja að persónuverndarfulltrúi komi, með viðeigandi hætti og tímanlega, að öllum málum sem tengjast vernd persónuupplýsinga. Þá er tekið fram í 2. mgr. sama ákvæðis að þessir aðilar skuli styðja persónuverndarfulltrúann við framkvæmd þeirra verkefna sem um getur í 39. gr. með því að láta honum í té nauðsynleg úrræði til að inna þau af hendi, auk aðgangs að persónuupplýsingum og vinnsluaðgerðum, og gera honum kleift að viðhalda sérþekkingu sinni. Þessi atriði eru öll liður í því að tilnefning persónuverndarfulltrúa nái markmiði sínu og að hann geti sinnt störfum sínum sem skyldi, einkum að hann fái tímanlega að koma að málum. Í leiðbeiningum um persónuverndarfulltrúa er bent á að meðal úrræða til að tryggja það sé að fulltrúinn hafi tök á að sitja fundi stjórnenda og millistjórnenda þar sem ákvarðanir eru undirbúnar, og þó sérstaklega fundi þar sem ákvarðanir eru teknar. Þá er tekið fram að ávallt verði að taka tillit til álits hans, og komi upp ágreiningur, væri rétt hjá ábyrgðar- eða vinnsluaðila að skjalfesta ástæður þess að ráðleggingum fulltrúans er ekki fylgt. Þá ber ávallt að gera persónuverndarfulltrúa viðvart ef öryggisbrot eiga sér stað.

Markmið 3. mgr. 38. gr. reglugerðarinnar er að stuðla að sjálfstæði persónuverndarfulltrúa við framkvæmd starfa sinna, en þar er tekið fram að ábyrgðaraðili og vinnsluaðili skuli tryggja að persónuverndarfulltrúi fái engin fyrirmæli varðandi framkvæmd þeirra. Er auk þess mælt fyrir um að þeir skuli hvorki víkja honum úr starfi né refsa honum fyrir framkvæmd verkefna sinna. Þá skal persónuverndarfulltrúi heyra beint undir æðsta stjórnunarstig hjá ábyrgðaraðila eða vinnsluaðila. Um bann við brottvísun eða viðurlög vegna starfa fulltrúans er einkum skírskotað til þess að álit eða ráðleggingar persónuverndarfulltrúa eða ágreiningur á milli hans og ábyrgðar- eða vinnsluaðila um hvernig haga beri vinnslu persónuupplýsinga megi ekki verða tilefni uppsagnar úr starfi eða á verktakasamningi.

Í 4. mgr. 38. gr. reglugerðarinnar er tekið fram að skráðir einstaklingar geti haft samband við persónuverndarfulltrúann með öll mál sem tengjast vinnslu á persónuupplýsingum þeirra og því hvernig þeir geta neytt réttar síns samkvæmt reglugerðinni. Hér er einnig undirstrikað sjálfstæði fulltrúans með því að einstaklingur þarf ekki að leita neinnar milligöngu innan stjórnvalds eða fyrirtækis til að fá ráðleggingar eða álit persónuverndarfulltrúa um réttindi sín samkvæmt reglugerðinni. Loks kemur fram í 6. mgr. að persónuverndarfulltrúi megi sinna öðrum verkefnum og skyldustörfum, en tryggja skuli að slík verkefni og skyldustörf leiði ekki til hagsmunaárekstra. Hér er m.a. haft í huga sem fyrr var nefnt að persónuverndarfulltrúi þarf ekki nauðsynlega að vera fastur starfsmaður, fyrirtækis eða stjórnvalds, þótt slík verði væntanlega algengt. En í tilvikum þar sem persónuverndarfulltrúi starfar á grundvelli verktöku og hugsanlega fyrir fleiri aðila í senn, ber að gæta sérstaklega að því að hagsmunir rekist ekki

á vegna annarra verkefna sem hann kann að fara með. Hagsmunaárekstrar geta líka skapast í tilvikum þar sem persónuverndarfulltrúi er fastur starfsmaður samkvæmt ráðningarsamningi. Það getur átt við ef hann er millistjórnandi í stofnun eða fyrirtæki (t.d. framkvæmdastjóri, öryggisstjóri, rekstrarstjóri, fjármálastjóri, markaðsstjóri, mannauðsstjóri o.fl.) en einnig í tilviki lægra settra starfsmanna ef störf þeirra fela í sér ákvarðanatöku um tilgang og aðferð við vinnslu persónuupplýsinga.

Helstu verkefnum persónuverndarfulltrúa er lýst í 39. gr. reglugerðarinnar en ekki er þó um tæmandi talningu að ræða. Megininntak starfa þeirra felst í eftirliti með reglufylgni og aðstoð við ábyrgðar- og vinnsluaðila við að fylgja ákvæðum laganna og reglugerðarinnar. Þannig skal persónuverndarfulltrúi upplýsa ábyrgðaraðila eða vinnsluaðila og starfsmenn, sem annast vinnslu, um skyldur sínar í þessum efnum og veita þeim ráðgjöf þar að lútandi, hann skal fylgjast með því að farið sé að ákvæðum laganna og reglugerðarinnar og stefnum ábyrgðaraðila eða vinnsluaðila varðandi vernd persónuupplýsinga, þ.m.t. úthlutun ábyrgðar, vitundarvakningu og þjálfun starfsfólks sem tekur þátt í vinnslustarfsemi og tilheyrandi úttektir, hann skal veita ráðgjöf, sé farið fram á það, varðandi mat á áhrifum á persónuvernd skv. 29. gr. laganna og fylgjast með framkvæmd og vinna með Persónuvernd þegar þörf krefur, t.d. vera tengiliður við Persónuvernd í samvinnu skv. 28. gr. eða í tengslum við fyrirframsamráð skv. 30. gr. laganna. Um aðkomu hans og hlutverk í tengslum við mat á áhrifum á persónuvernd og gerð skráa yfir vinnslustarfsemi er nánar fjallað í fyrrgreindum leiðbeiningum um persónuverndarfulltrúa.

Um 36. gr.

Í þessu frumvarpsákvæði er mælt fyrir um þagnarskyldu persónuverndarfulltrúa en skv. 1. mgr. er honum óheimilt að segja frá nokkru því sem hann hefur fengið vitneskju um í starfi sínu og leynt á að fara. Samkvæmt 5. mgr. 38. gr. reglugerðarinnar skal persónuverndarfulltrúi bundinn þagnarskyldu eða trúnaði um framkvæmd verkefna sinna í samræmi við lög aðildarríkis. Með þessu ákvæði er framangreindum fyrirmælum reglugerðarinnar fylgt eftir. Um lýsingu á þagnarskyldunni er sótt fyrirmynd til orðalags 18. gr. laga um réttindi og skyldur starfsmanna ríkisins nr. 70/1996. Eins og lýst var í skýringum við 35. gr. frumvarpsins er mögulegt að teymi á vegum utanaðkomandi verktaka sem gegnir starfi persónuverndarfulltrúa starfa að verkefnum undir stjórn hans. Mikilvægt er að hver og einn starfsmaður undir stjórn persónuverndarfulltrúans uppfylli allar þær kröfur sem reglugerðin gerir til persónuverndarfulltrúa og gildir þagnarskyldan því jafnt um þá.

Þá er tekið fram í 2. mgr. þessa ákvæðis að þagnarskylda gildi ekki hafi hinn skráði veitt samþykki sitt til þess að leynd sé aflétt, svo og þegar nauðsyn krefur vegna framkvæmdar starfa persónuverndarfulltrúans.

Skoða ber ákvæði um þagnarskyldu persónuverndarfulltrúa í ljósi 3. mgr. 48. gr. frumvarpsins þar sem fram kemur að brot einstaklings skv. 36. gr. varði refsingu, sem er sektir eða 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. Er hér tekið mið af sama refsiramma og kemur fram í 136. gr. almennra hegningarlaga nr. 19/1940 um brot á þagnarskyldu opinberra starfsmanna.

Um 37. gr.

Í þessu frumvarpsákvæði sem fjallar um vottun og vottunaraðila er byggt á 42. og 43. gr. reglugerðarinnar. Í 1. mgr. 42. gr. reglugerðarinnar eru aðildarríkin, innlendar persónuverndarstofnanir, Evrópska persónuverndarráðið og framkvæmdastjórnin hvött til þess að komið verði á fót vottunarfyrirkomulagi vegna persónuverndar ásamt persónuverndarinnsiglum og -merkjum til að sýna fram á að vinnsla ábyrgðaraðila og vinnsluaðila uppfylli ákvæði reglugerðarinnar. Að öðru leyti vísast til reglugerðarákvæðisins sem geymir ítarleg ákvæði um inntak vottunar, skyldur ábyrgðaraðila eða vinnsluaðila sem óska eftir vottun samkvæmt vottunarkerfinu svo og tímamörk vottunar sem skal að hámarki gefin út til þriggja ára. Markmiðinu með þessari skipan er lýst í 100. lið formála reglugerðarinnar. Þar er áréttuð áður nefnd hvatning til aðildarríkja og um leið mikilvægi þess að skráðum einstaklingum verði gert kleift að meta fljótt persónuverndarstig á vörum og þjónustu þannig að gagnsæi og fylgni við reglugerðina batni.

Í 43. gr. reglugerðarinnar er fjallað nánar um vottunaraðila og kröfur sem gerðar eru til þeirra svo þeir hljóti sérstaka faggildingu. Í 1. mgr. er mælt fyrir um að aðildarríki skuli tryggja að

þeir séu faggiltir af öðrum eða báðum eftirtalinna aðila, annars vegar eftirlitsstjórnvaldinu, þ.e. Persónuvernd, og hins vegar faggildingarstofu í aðildarríki sem tilgreind er í samræmi við reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggildingu og markaðseftirlit í tengslum við markaðssetningu á vörum, sbr. einnig Evrópustaðal EN-ISO/IE C 17065/2012. Samkvæmt lögum um faggildingu nr. 24/2006 er það Faggildingarsvið Einkaleyfastofu sem annast faggildingu fyrir hönd íslenskra stjórnvalda. Í 1. mgr. þessa frumvarpsákvæðis er lagt til að Faggildingarsviðið verði sá aðili hér á landi sem hafi heimild til að faggilda vottunaraðila sem gefur út vottun skv. 42. reglugerðarinnar. Mikilvægt er að samstarf sé á milli Persónuverndar og Faggildingarstofu við undirbúning á faggildingu vottunaraðila. Er því lagt til að Persónuvernd veiti umsögn sín áður en Faggildingarsviðið gefur út faggildingu sína á vottunaraðila.

Að öðru leyti er í 2. mgr. þessarar frumvarpsgreinar vísað til fyrirmæla 42. og 43. gr. reglugerðarinnar um fyrirkomulag og efni vottunar.

Um 38. gr.

Þessi grein um skipulag og stjórnsýslu Persónuverndar er upphafsákvæði VII. kafla frumvarpsins sem fjallar um eftirlit með framkvæmd reglugerðarinnar og laganna og viðurlög við brotum. Í núgildandi lögum er að finna samsvarandi ákvæði einnig í VII. kafla, í 36.- 43. gr. Í frumvarpinu eru lagðar til margvíslegar breytingar og nýmæli í ákvæðum um stöðu, verkefni og valdheimildir Persónuverndar og viðurlög við brotum. Í VI. kafla reglugerðarinnar, 51.-59. gr., er að finna ítarleg ákvæði um sjálfstæð eftirlitsyfirvöld, verksvið þeirra og valdheimildir og eru þar lagðar ákveðnar skyldur á aðildarríki til þess að festa í landslög ákvæði um sjálfstæða eftirlitsstofnun og sérstakar ráðstafanir til að tryggja sjálfstæði hennar. Þá eru í reglugerðinni nýmæli sem lúta að álagningu stjórnvaldssektar sem geta numið háum fjárhæðum vegna brota á ákvæðum hennar. Tekið skal fram að þegar rætt er um „eftirlitsyfirvald“ í íslenskri þýðingu reglugerðarinnar á enska hugtakinu „supervisory authority“ er í frumvarpinu rætt um „eftirlitsstjórnvald“ eða eftir atvikum „eftirlitsstofnun“ eða „persónuverndarstofnun“. Löng hefð er fyrir notkun orðsins eftirlitsstjórnvald í íslensku lagamáli, m.a. þegar rætt er um stofnanir sem hafa eftirlit með framkvæmd gerða sem teknar eru upp í EES-samninginn, t.d. eftirlitsstofnanir á fjármálamarkaði. Þá hefur hugtakið „stjórnvald“ sjálfstæða skírskotun til 1. gr. stjórnsýslulaga og þannig ótvírætt að Persónuvernd er stofnun sem er stjórnvald í skilningi laganna og fellur undir gildissvið þeirra.

Í reglugerðinni er lögð rík áhersla á að tryggja sjálfstæði eftirlitsstjórnvalda í aðildarríkjunum sem hafa eftirlit með framkvæmd hennar, þar á meðal að leysa úr kvörtunum einstaklinga telji þeir brotið á réttindum sínum. Fjallar sérstakt ákvæði hennar, 52. gr., um sjálfstæði eftirlitsstjórnvaldsins. Í 117. lið formála reglugerðarinnar kemur fram að þýðingarmikill þáttur í vernd einstaklinga varðandi vinnslu persónuupplýsinga þeirra felist í því að koma slíkum stofnunum á fót í aðildarríkjunum með umboð til að gegna störfum sínum og beita valdheimildum sínum algerlega óháð öðrum. Þá er tekið fram að aðildarríkin ættu að geta komið á fót fleiri en einu eftirlitsstjórnvaldi til að endurspegla stjórnskipan sína, stjórnunarhætti og skipulag stjórnsýslu. Tekið skal fram að í þessu frumvarpi er gert ráð fyrir að eftirlit sé á hendi einnar stofnunar, Persónuverndar. Þá kemur fram í formálanum skýr tenging á milli sjálfstæðis eftirlitsstofnunar og þeirra aðstæðna sem henni eru búnar til að sinna hlutverki með tilliti til fjármagns og innviða. Í 4. mgr. 52. gr. er tekið fram að sérhvert aðildarríki skuli tryggja að stofnunin hafi yfir að ráða þeim mannauði, tækniúræðum og fjármagni, húsakosti og innviðum sem nauðsynleg eru til að hún geti unnið störf sín og beitt valdheimildum sínum með skilvirkum hætti, þ. á m. í tengslum við gagnkvæma aðstoð, samvinnu og þátttöku í starfi persónuverndarráðsins. Einnig eru þessi fyrirmæli áréttuð í 120. lið formálans. Um þetta er vísað nánar til umfjöllunar í 9. kafla almennra athugasemda í frumvarpi þessu þar sem fjallað er um áhrif frumvarpsins á stjórnsýslu stofnana ríkisins.

Í ákvæðum þessa kafla frumvarpsins eru fest bæði þau ákvæði sem skylt er að setja í landslög samkvæmt reglugerðinni og sérreglur þar sem reglugerðin veitir aðildarríkjum svigrúm til reglusetningar. Þá eru færð inn í kaflann helstu ákvæði reglugerðarinnar um viðurlög og sjónarmið sem ber að byggja á við ákvörðun þeirra til þess að heildarmynd fái stöðugt yfir valdheimildir Persónuverndar og viðurlög.

Í þessu frumvarpsákvæði er mælt fyrir um skipulag og stjórnsýslu Persónuverndar, en það er sú stofnun hér á landi sem gegnir hlutverki eftirlitsstjórnvalds samkvæmt 51. gr.

reglugerðarinnar. Persónuvernd hefur starfað frá árinu 2001 þegar núgildandi lög tóku gildi með það hlutverk að hafa eftirlit með framkvæmd laga 77/2000 og persónuverndartilskipunar ESB, en um skipulag hennar og stjórnsýslu er fjallað í 36. gr. laganna. Í þetta ákvæði frumvarpsins um skipulag og stjórnsýslu Persónuverndar bætast nokkur atriði um stöðu stofnunarinnar og starfsmanna hennar sem annað hvort er skylt að setja í landslög eða eru til frekari skýringar á stjórnskipulagi stofnunarinnar. Verður nú nánar gerð grein fyrir helstu breytingum um efnið frá gildandi lögum.

Í 1. mgr. ákvæðisins er, auk tilgreiningar á því að Persónuvernd sé sjálfstæð stofnun með sérstaka stjórn, áréttað að hún taki ekki við fyrirmælum frá stjórnvöldum eða öðrum aðilum. Hér er m.a. tekið mið af fyrirmælum 1. og 2. mgr. 52. gr. reglugerðarinnar um að eftirlitsstjórnvald skuli vera algerlega sjálfstætt í störfum sínum og þegar það beitir valdheimildum sínum. Þar er jafnframt tekið fram að starfsmenn eftirlitsstjórnvaldsins skuli vera lausir við utanaðkomandi áhrif, jafnt bein sem óbein, og skuli hvorki leita eftir né taka við fyrirmælum frá öðrum aðilum. Í síðasta málslíð 1. mgr. þessa frumvarpsákvæðis er tekið fram að ákvörðunum Persónuverndar verði ekki skotið til annarra stjórnvalda og er þannig ekki um að ræða málskot til æðra stjórnvalds innan stjórnsýslunnar. Auk þess er áréttuð sú almenna regla sem leidd verður af 60. og 70. gr. stjórnarskrárinnar að aðilum máls sé heimilt að leggja ágreining sinn fyrir dómstóla með venjubundnum hætti, líkt og gildir um allar stjórnvaldsákvæðanir.

Í 2. mgr. er eins og í núgildandi lögum ráðgert að ráðherra sem fer með persónuverndarmálefni skipi stjórn Persónuverndar, en það er dómsmálaráðherra skv. núgildandi forsetaúrskurði um skiptingu stjórnarmálefna milli ráðuneyta í Stjórnarráði Íslands, nr. 117/2015. Þær breytingar eru lagðar til að í stað þess að sá ráðherra skipi án tilnefningar þrjá stjórnarmenn, skipi hann tvo stjórnarmenn án tilnefningar, formann og varaformann og skuli þeir vera lögfræðingar sem fullnægja hæfisskilyrðum héraðsdómara. Einnig er nýmæli að ráðherra sem fer með málefni netöryggis og fjarskipta, sem er skv. núgildandi forsetaúrskurði samgöngu- og sveitarstjórnarráðherra, tilnefni einn stjórnarmann. Það þykir rökrétt í ljósi þeirra ríku tengsla sem viðfangsefni Persónuverndar hafa við málaflokk þess ráðherra og er mikilvægt að þekking á netöryggi- og fjarskiptamálum sé til staðar í stjórninni. Þá er lagt til að ráðherra sem fer með málefni heilbrigðisþjónustu tilnefni einn stjórnarmann og samhliða því fallið frá þeirri tilhögun núgildandi laga að Hæstiréttur Íslands tilnefni einn stjórnarmann. Hefur sú venja mótast á grundvelli núgildandi laga að Hæstiréttur hefur tilnefnt fulltrúa úr heilbrigðiskerfinu. Í ljósi þess að umfangsmikil vinnsla viðkvæmra persónuupplýsinga fer fram í heilbrigðiskerfinu auk vinnslu persónuupplýsinga sem tengist vísindarannsóknum á heilbrigðissviði þykir rétt að tryggja að sérþekking á því sviði sé áfram til staðar. Loks helst óbreytt sú skipan að Skýrslutæknifélag Íslands tilnefni einn stjórnarmann og skal hann vera sérfróður á sviði tölvu- og tæknimála. Ljóst er að verkefni Persónuverndar munu í ríkari mæli beinast að tæknilegum kröfum sem gerðar eru til ábyrgðar- og vinnsluaðila þar á meðal upplýsingakerfa og upplýsingaöryggis og því mikilvægt að sérfræðiþekking um þau mál séu til staðar í stjórn. Loks er tekið fram að allir stjórnarmenn skuli hafa þekkingu á málefnum tengdum persónuvernd og menntun sem nýtist á því sviði en hér er tekið mið af fyrirmælum 2. mgr. 53. gr. reglugerðarinnar um að fulltrúi skuli búa yfir menntun og hæfi, reynslu og færni, einkum á sviði verndar persónuupplýsinga, sem honum er nauðsynleg til að hann geti sinnt skyldustörfum sínum og beitt valdheimildum sínum, sbr. einnig b-lið 1. mgr. 54. gr. reglugerðarinnar um menntun og hæfisskilyrði

Sú breyting er einnig ráðgerð í 2. mgr. að skipunartími nefndarmanna sé lengdur í fimm ár og jafnframt tekið fram að ekki sé heimilt að skipa stjórnarmenn lengur en í þrjú tímabil samfellt. Þessi breyting tekur mið af d- og e-lið 1. mgr. 54. gr. reglugerðarinnar sem mæla fyrir um að í lög aðildarríkja skuli setja reglur um skipunartíma fulltrúa sérhvers eftirlitsstjórnvalds sem ekki skuli vera skemmri en fjögur ár, að undanskilinni fyrstu skipun sem geti verið til skemmri tíma sé það er nauðsynlegt til að standa vörð um sjálfstæði stjórnvaldsins með því að nota áfangabundið skipunarferli. Þá skuli í lögum kveðið á um hvort og þá hversu oft heimilt sé að endurnýja skipun fulltrúa þess.

Í 3. mgr. er nánar rætt um hlutverk stjórnar og samspil verkefna hennar og skrifstofu Persónuverndar. Stjórnin mótar m.a. áherslur í starfsemi stofnunar í samráði við forstjóra. Í því felst að forstjóri og skrifstofa eiga frumkvæði að og undirbúa tillögur að slíkri stefnumótun og leggja fyrir stjórn. Þá er sérstaklega tilgreint að meiriháttar efnislegar eða stefnumótandi

ákvarðanir í málum sem stofnunin hefur til meðferðar séu teknar af stjórn, þar á meðal eru ákvarðanir um stjórnvaldssektir eins og fram kemur í 5. mgr. 46. gr. frumvarpsins hér síðar. Eru þessi atriði í samræmi við þau verkefni sem tilgreind eru í lögum um stjórnir sambærilegra eftirlitsstofnana á borð við Fjármálaeftirlitið skv. ákvæðum laga nr. 87/1998 um opinbert eftirlit á fjármálamarkaði og nr. 161/2002 um fjármálafyrirtæki svo og Samkeppniseftirlitið skv. lögum nr. 44/2005. Markmið þess að stjórn Persónuverndar taki þær ákvarðanir sem tilgreindar eru í ákvæðinu og undirbúnar eru af skrifstofu er að tryggja að mál af umræddum toga fái sérstaklega ítarlega og vandaða meðferð, enda kunna ákvarðanir í þeim að vera mjög íþyngjandi auk þess sem ekki er til staðar kæruréttur innan stjórnsýslunnar vegna þeirra. Þá er mikilvægt að ýmsar stefnumarkandi ákvarðanir um túlkun og framkvæmd laganna og reglugerðarinnar fái ítarlegri skoðun hjá stjórn en dagleg afgreiðslumál og ákvarðanir sem byggjast á fastri framkvæmd séu á hendi skrifstofunnar. Í ákvæðinu er mælt fyrir um að stjórn Persónuverndar setji nánari reglur um skiptingu starfa á milli stjórnar og skrifstofu stofnunarinnar og framkvæmd þeirra. Settar hafa verið reglur um það efni á grundvelli núgildandi laga, nr. 231/2012. Ljóst er að endurskoða þarf þær með hliðsjón af margvíslegum nýjum verkefnum Persónuverndar samkvæmt reglugerðinni og ákvæðum frumvarps þessa. Þá þarf jafnframt að huga þar að ítarlegri reglum um málsmeðferð, s.s. vegna álagningar stjórnvaldssekta einkum til að tryggja jafnræði í meðferð mála og gagnsæi um meðferð þeirra.

Í 4. mgr. frumvarpsákvæðis þessa er nýmæli sem ætlað er að tryggja frekar sjálfstæði fulltrúa í stjórn Persónuverndar og vernd gegn brottvikningu. Það byggist á 4. mgr. 53. gr. reglugerðarinnar sem kveður á um að fulltrúa eftirlitsstjórnvalds skuli því aðeins víkja úr starfi að um alvarlegt misferli sé að ræða eða að hann fullnægi ekki lengur þeim skilyrðum sem krafist er vegna skyldustarfa hans. Ekki er þörf á að setja sérstök skilyrði hér um lausn forstjóra Persónuverndar úr embætti enda geyma ákvæði laga nr. 70/1996 um réttindi og skyldur starfsmanna ríkisins ítarlegar reglur um skilyrði þess að embættismanni verði veitt lausn frá embætti vegna alvarlegs misferlis eða annarra ávirðinga.

Um forstjóra Persónuverndar, skipun, þátttöku í stjórnarfundum og meginverkefni er annars fjallað í 6.-8. mgr. frumvarpákvæðisins. Í 6. mgr. eru sett almenn hæfisskilyrði fyrir skipun forstjóra í embætti. Skal forstjóri hafa menntun á háskólastigi og búa yfir þekkingu og reynslu á málefnum tengdum persónuvernd. Er hér fylgt eftir fyrrgreindum fyrirmælum í 2. mgr. 53. gr. og b-lið 1. mgr. 54. gr. reglugerðarinnar um skyldu til að setja í lög skilyrði um menntun og hæfisskilyrði þeirra sem fara með stjórn eftirlitsstjórnvalds samkvæmt reglugerðinni.

Loks er í 8. mgr. frumvarpsins hnykkt frekar á starfsskyldum og ábyrgð forstjóra, frá því sem segir í gildandi lögum. Þannig er mælt fyrir um að forstjóri beri ábyrgð á og annist daglega stjórnun á starfsemi, fjárreiðum og rekstri stofnunarinnar og ráði starfsmenn hennar. Með þessu er lagt til að fest verði í lög sú framkvæmd sem gilt hefur til þessa um hlutverk og verkefni forstjóra Persónuverndar.

Um 39. gr.

Í 1. mgr. þessarar greinar er lýst hlutverki Persónuverndar, 2. og 3. mgr. fjalla sérstaklega um rétt til að bera fram kvörtun til stofnunarinnar vegna brota á lögum og reglugerðinni og um frumkvæðisathuganir hennar. Þá geymir 4. mgr. upptalningu á helstu verkefnum stofnunarinnar.

Tekið er af skarið í 1. mgr. um að Persónuvernd sé það eftirlitsstjórnvald hér á landi sem hverju aðildarríki er skylt að setja á fót samkvæmt VI. kafla reglugerðarinnar og er aðeins um eitt slíkt stjórnvald að ræða hér á landi. Þá er lýst því meginhlutverki að hún annist eftirlit með framkvæmd reglugerðarinnar, laga á grundvelli frumvarpsins, sérákvæða í lögum sem fjalla um vinnslu persónuupplýsinga og annarra reglna um efnið.

Mikilvægur þáttur í eftirlitsstörfum Persónuverndar er að fjalla um kvartanir einstaklinga sem telja að brotið hafi verið gegn réttindum sínum samkvæmt ákvæðum reglugerðarinnar eða lögum um persónuvernd. Er sérákvæði þessa efnis að finna í 2. mgr. greinarinnar um að Persónuvernd skuli úrskurða um hvort brot hafi átt sér stað. Í f-lið 1. mgr. 57. gr. reglugerðarinnar er meðferð kvartana talin til verkefna eftirlitsstjórnvalds og í 141. lið formála reglugerðarinnar er lögð áhersla á mikilvægi þessa réttar. Er þar bent á að sérhver skráður einstaklingur skuli eiga rétt á að leggja fram kvörtun hjá einu eftirlitsstjórnvaldi, einkum í aðildarríkinu þar sem hann hefur fasta búsetu. Þá er tekið fram að eftirlitsstjórnvald ætti að tilkynna hinu skráða um framvindu og niðurstöðu kvörtunarinnar innan hæfilegs tíma. Sé þörf

á frekari rannsókn málsins eða samræmingu við persónuverndarstofnun í öðru ríki ætti að veita hinum skráða í millitiðinni upplýsingar um stöðu málsins. Þá kemur fram í 2. mgr. 57. gr. að til að auðvelda framlagningu kvartana skuli eftirlitsstjórnvald bjóða upp á kvörtunareyðublað, sem einnig megi fylla út rafrænt, án þess þó að útiloka aðra samskiptamöguleika. Þess má geta að eyðublað fyrir kvörtun hafa verið aðgengileg á heimasíðu Persónuverndar um árabíl.

Það nýmæli er í þessu frumvarpsákvæði að stofnun, samtök eða félag samkvæmt 80. gr. reglugerðarinnar geti lagt fram kvörtun hjá Persónuvernd hafi þau ástæðu til að ætla að réttindi skráðs einstaklings hafi verið brotin. Er hér nýtt heimild sem fram kemur í 2. mgr. 80. gr. reglugerðarinnar um að aðildarríki geti sett í lög að stofnun, samtök eða félag, sem nánar eru skilgreind í 1. mgr. þeirrar greinar, hafi rétt, óháð því hvort hinn skráði hefur veitt umboð til þess, til að leggja fram kvörtun hjá eftirlitsstjórnvaldi hafi þau ástæðu til að ætla að réttindi skráðs einstaklings samkvæmt reglugerðinni hafi verið brotin vegna vinnslunnar. Í 142. lið formála reglugerðarinnar er varpað ljósi á heimild einstaklinga til að veita stofnun, samtökum eða félagi, sem ekki eru rekin í hagnaðarskyni og sem stofnuð eru í samræmi við lög aðildarríkis, hafa lögboðið markmið og eru virk á sviði verndar persónuupplýsinga, umboð til að leggja fram kvörtun fyrir sína hönd hjá eftirlitsstjórnvaldi. Þá er vísað til framangreindrar heimildar aðildarríkja til að mæla fyrir um að slík stofnun, samtök eða félag eigi rétt á að leggja fram kvörtun í því aðildarríki, óháð því hvort hinn skráði hefur veitt umboð til þess hafi það ástæður til að ætla að réttindi skráðs einstaklings hafi verið brotin við vinnslu persónuupplýsinga. Jafnframt er tekið fram að ekki megi heimila stofnuninni, samtökunum eða félaginu að krefjast bóta fyrir hönd skráðs einstaklings án umboðs hans, en það leiðir af almennum reglum laga hér á landi að slíks umboðs er þörf eigi stofnun eða samtök að taka við bótum.

Í 3. mgr. frumvarpsgreinarinnar er undirstrikað að Persónuvernd geti 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 ákvæði laganna, reglna settra á grundvelli þeirra eða einstökum fyrirmælum. Þannig er ekki skilyrði fyrir því að stofnunin hefji rannsókn máls að kvörtun þar um hafi borist, en algengt er í framkvæmd að henni berist ábendingar frá einstaklingum um ágalla á vinnslu persónuupplýsinga sem verða tilefni þess að rannsókn hefst.

Í 4. mgr. eru talin upp önnur helstu verkefni Persónuverndar í 16. töluliðum en sú upptalning er ekki tæmandi og vísar 17. tölul. þannig til þess að stofnunin sinni öðrum störfum sem tengjast vernd persónuupplýsinga. Þessi listi yfir verkefni byggist á 57. gr. reglugerðarinnar um atriði sem skylt er að eftirlitsstjórnvald hafi með höndum. Í þessari upptalningu eru fölginn öll þau verkefni sem Persónuvernd sinnir nú þegar á grundvelli 3. mgr. 37. gr. gildandi laga, þótt orðalag breytist lítillega í sumum atriðum. Helstu nýju lögboðnu verkefni sem felld eru undir stofnunina tengjast ýmsum nýmælum reglugerðarinnar og eru þau talin upp í 7. – 15. tölul. þessa frumvarpsákvæðis. Þá er í 16. tölul. ákvæðisins viðhaldið þeirri skyldu stofnunarinnar að birta árlega skýrslu um starfsemi sína, sbr. 7. tölul. 3. mgr. 37. gr. núgildandi laga, og er ekki stefnt að breytingum í því tilliti. Í ársskýrslunni hefur verið gefið yfirlit yfir helstu verkefni Persónuverndar á undanliðnu ári, upplýsingar um málafjölda og þróun hans, og yfirlit yfir úrskurði, álit og ákvarðanir. Í þessu sambandi ber einnig hafa í huga að Persónuvernd birtir jafnharðan á vefsíðu sinni upplýsingar um starfsemi sína, þar á meðal helstu ákvarðanir, álit og úrskurði í ágreiningsmálum. Þess er þó gætt að afmá persónuauðkenni málsaðila við þá birtingu.

Um 40. gr.

Ákvæði þetta um heimild Persónuverndar til gjaldtöku vegna eftirlits er samhljóða 4. mgr. 37. gr. núgildandi laga. Þannig getur Persónuvernd ákveðið að ábyrgðaraðili skuli greiða þann kostnað sem hlýst af eftirliti. Einnig er lagt til að Persónuvernd geti ákveðið að ábyrgðaraðili greiði kostnað við úttekt á starfsemi hvort heldur í tengslum við undirbúning útgáfu vinnsluleyfis sem sótt hefur verið um eða í öðrum tilvikum. Frumvarpið stefnir því ekki að neinum breytingum frá því sem nú gildir um gjaldtöku en bætir þó við fyrirmælum um að ráðherra setji gjaldskrá um efnið. Yrði slík gjaldskrá sett að fengnum tillögum Persónuverndar og myndi falla í hlut þess ráðherra sem persónuverndarmálefni heyra undir að setja slíka gjaldskrá.

Um 41. gr.

Þessi grein er hin fyrsta í röð þriggja ákvæða frumvarpsins, 41.-43. gr. sem lúta sérstaklega að valdheimildum Persónuverndar í tengslum við eftirlitshlutverk hennar sem lýst var í 39. gr. Þessar þrjár frumvarpsgreinar byggjast á ákvæði 58. gr. reglugerðarinnar en samkvæmt 1.-3. mgr. þeirrar greinar eru valdheimildir eftirlitsstjórnvalds þrjúþættar og eftirfarandi, 1) rannsóknarheimildir 2) valdheimildir til að gera ráðstafanir til úrbóta og 3) leyfisveitinga- og ráðgjafaheimildir.

Þetta frumvarpsákvæði lýtur að fyrsta þættinum um rannsóknarheimildir Persónuverndar við eftirlitsstörf. Það er hliðstætt 1. mgr. 58. gr. reglugerðarinnar en bætir við atriðum sem tengjast framkvæmd á beitingu valdheimilda, s.s. um að leita skuli liðveislu lögreglu ef einhver leitast við að hindra Persónuvernd í eftirlitsstörfum sínum. Í ákvæðinu er að mestu leyti að finna heimildir sem Persónuvernd hefur þegar skv. 38. gr. gildandi laga, s.s. til að krefja ábyrgðaraðila, vinnsluaðila og þá sem starfa á þeirra vegum um allar þær upplýsingar og skriflegar skýringar sem hún þarf til að rækja hlutverk sitt við framkvæmd eftirlits. Þá skal Persónuvernd hafa aðgang að öllum þeim gögnum hjá ábyrgðaraðila og vinnsluaðila sem nauðsynleg eru við framkvæmd laganna. Í 6. tölul. er mælt fyrir um aðgang að húsnæði þar sem vinnsla persónuupplýsinga fer fram eða gögn eru varðveitt, þ.m.t. hvers kyns gagnavinnsлубúnaður. Persónuvernd getur framkvæmt hverja þá prófun eða eftirlitsaðgerð sem hún telur nauðsynlega og krafist nauðsynlegrar aðstoðar starfsfólks á 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 settum samkvæmt þeim er Persónuvernd heimilt að fela lögreglustjóra að stöðva til bráðabirgða starfsemi viðkomandi og innsigla starfsstöð hans þegar í stað. Þá er tekið fram í 4. mgr. ákvæðisins að réttur Persónuverndar til að krefjast upplýsinga eða aðgangs að starfsstöðvum og tækjabúnaði verði ekki takmarkaður með vísan til reglna um þagnarskyldu. Hliðstætt ákvæði er í 2. mgr. 38. gr. gildandi laga, en það styðst við þau rök að ella yrði Persónuvernd illmögulegt að rækja þær eftirlitsskyldur sem á hana eru lagðar skv. þessari grein.

Um skýringar á valdheimildum persónuverndarstofnana er m.a. fjallað í 122. lið formála reglugerðarinnar. Samkvæmt því á eftirlitsstofnun að vera til þess bær á yfirráðasvæði eigin aðildarríkis að beita þessum valdheimildum og vinna þau verkefni sem henni eru falin samkvæmt reglugerðinni. Þá segir að valdheimildirnar verði einkum virkar vegna vinnslu í tengslum við starfsemi starfsstöðvar ábyrgðaraðila eða vinnsluaðila á yfirráðasvæði ríkisins, vinnslu opinberra yfirvalda eða einkaaðila á persónuupplýsingum í þágu almannahagsmuna, vinnslu sem hefur áhrif á skráða einstaklinga á umræddu yfirráðasvæði og vinnslu af hálfu ábyrgðaraðila eða vinnsluaðila, sem hefur ekki staðfestu í Sambandinu, þegar hún beinist að skráðum einstaklingum sem búa á svæðinu. Þá segir að á meðal þess sem falli undir umræddar heimildir ætti að vera meðferð kvartana frá skráðum einstaklingi, framkvæmd rannsókna á beitingu reglugerðarinnar og vitundarefning meðal almennings um ógnir, reglur, verndarráðstafanir og réttindi í tengslum við vinnslu persónuupplýsinga.

Um 42. gr.

Þessi frumvarpsgrein telur upp úrræði sem Persónuvernd hefur við eftirlitsstörf sem felast í því að gefa fyrirmæli um ráðstafanir til úrbóta. Þessi upptalning byggist á samsvarandi ákvæði í 2. mgr. 58. gr. reglugerðarinnar. Um sum þeirra atriða sem hér birtast er þegar fjallað í núgildandi lögum, einkum í 40. gr. þeirra sem fjallar um stöðvun vinnslu persónuupplýsinga og fyrirmæli um að eyða þeim eða gera ráðstafanir sem tryggja lögmæti vinnslu. Fjallað er um slíkar ráðstafanir í 6. og 7. tölul. þessa frumvarpsákvæðis.

Þá er að finna ýmis nýmæli um úrræði Persónuverndar í 1.-5. tölul. ákvæðisins, s.s. að stofnunin geti veitt ábyrgðaraðila viðvörðun um að líklegt sé að fyrirhugaðar vinnsluaðgerðir muni brjóta í bága við ákvæði reglugerðarinnar, svo og að unnt sé að veita ábyrgðaraðila eða vinnsluaðila áminningu hafi slíkar aðgerðir brotið gegn henni. Getur slík áminning komið til álita út frá sjónarmiðum um meðalhóf, þ.e. að veitt sé áminning í stað sektar vegna brota sem ekki teljast stórfelld, eða að í stað þess að ákveðið sé að leggja sekt á aðila sé því vægara úrræði beitt í fyrstu að veita honum kost á að bæta úr ágöllum á vinnslu með áminningu. Í samræmi við þetta er í 148. lið formála reglugerðarinnar bent á að gefa megi út áminningu í stað sektar þegar um er að ræða minni háttar brot eða ef sektin, sem líklegt er að lögð verði á, yrði óhófleg

byrði fyrir einstakling. Þá getur beiting dagsektá einnig komið til skoðunar, áður en ákveðið er að leggja á stjórnslusekt, sbr. einnig 45. gr. frumvarpsins.

Um 43. gr.

Þessi frumvarpsgrein telur upp heimildir sem tengjast leyfisgjöf Persónuverndar þar sem hún á við og heimildir sem tengjast ráðgjafarhlutverki hennar. Greinin byggist á hliðstæðu ákvæði í 3. mgr. 58. gr. reglugerðarinnar. Er hér um nýmæli að ræða frá því sem fram kemur í núgildandi lögum en í ákvæðinu eru útfærð nánar ýmis verkefni stofnunarinnar sem lýst er í 39. gr. frumvarpsins sem tengjast ráðgjöf og leyfisveitingum, en þar er einnig vísað til dreifðra ákvæða í reglugerðinni sem geta verkefna stofnunarinnar af þessum toga.

Um 44. gr.

Í þessari grein er hnykkt á því að stjórnarmenn og starfsmenn Persónuverndar séu bundnir þagnarskyldu. Sú skylda leiðir af almennum reglum hvað varðar starfsmenn stofnunarinnar sbr. 18. gr. laga um réttindi og skyldur starfsmanna ríkisins nr. 70/1997. Rétt þykir að tilgreina sérstaklega að stjórnarmenn séu einnig bundnir þeirri skyldu enda eru þeir ekki í föstu starfi við stofnunina og ekki nauðsynlega ríkisstarfsmenn heldur. Þá er ætlast til að þeir sem vinna verkefni á vegum stofnunarinnar gangist undir sömu skyldu varðandi vitneskju sem þeir fá við framkvæmd slíkra verkefna um það sem leynt á að fara. Ákvæðið er í samræmi við fyrirmæli 2. mgr. 54. gr. reglugerðarinnar um að fulltrúar og starfsmenn eftirlitsstjórnvalds skuli í samræmi við lög aðildarríkis vera bundnir þagnarskyldu, bæði á meðan starfssambandið vari og eftir að því ljúki, með tilliti til trúnaðarupplýsinga sem þeir hafi fengið við skyldustörf sín eða við beitingu valdheimilda sinna. Þá er tekið fram að á meðan starfssambandið vari skuli þagnarskyldan einkum gilda um tilkynningar einstaklinga um brot gegn reglugerðinni.

Í 2. mgr. kemur fram að ákvæði um þagnarskyldu standi 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. Hliðstætt ákvæði gildir þegar samkvæmt 39. gr. núgildandi laga. Ljóst er að reglugerðin mælir fyrir um enn frekari samvinnu á milli eftirlitsstofnana Evrópuríkja en tilskipun ESB, m.a. þegar reynir á samstarf þeirra og gagnkvæma aðstoð innan hins samræmda eftirlitskerfis, skv. VII. kafla reglugerðarinnar. Í tengslum við það getur verið óhjákvæmilegt að skiptast á upplýsingum sem falla undir ákvæði laga um þagnarskyldu og þykir nauðsynlegt að taka af skarið um að þagnarskylduákvæði standi því ekki í vegi að Ísland geti efnt slíkar skuldbindingar sínar samkvæmt reglugerðinni að þessu leyti.

Í 3. mgr. frumvarpsins er mælt fyrir um þegar gerðir eru skilmálar skv. 33. gr. laganna getur Persónuvernd ákveðið að ábyrgðaraðili og vinnsluadili, 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. Getur verið mikilvægt að ganga frá því með ótvíræðum og formlegum hætti að þagnarskylda nái ekki síður til þeirra sem vinna með slíkar upplýsingar, sbr. einnig 3. tölul. 1. mgr. 33. gr. frumvarpsins.

Um 45. gr.

Í þessari frumvarpsgrein er mælt fyrir um heimildir til að leggja á dagsektir til þess að knýja um að farið sé að tilgreindum fyrirmælum Persónuverndar skv. 42. gr. frumvarpsins, þ.e. um að takmarka eða banna vinnslu skv. 6. tölul., leiðréttu eða eyða persónuupplýsingum skv. 7. tölul. eða um tímabundna stöðvun gagnaflæðis til þriðja lands eða alþjóðastofnunar. Greinin er efnislega hliðstæð dagsektákvæði í 41. gr. núgildandi laga. Þar er kveðið á um að sektir geti numið allt að 100.000 kr. fyrir hvern dag sem líður eða byrjar að líða án þess að fyrirmælum Persónuverndar sé fylgt. Í ljósi verðlagsþróunar frá því að löggin voru samþykkt fyrir 18 árum er eðlilegt að hækka þessa fjárhæð og er því lagt til að dagsektir geti numið að hámarki 200.000 kr. fyrir hvern dag. Í lögum þar sem fjallað er um dagsektir er fjárhæð þeirra mjög breytileg og dæmi um mjög háar dagsektir má t.d. finna í 11. gr. laga nr. 87/1998 um opinbert eftirlit á fjármálamarkaði nr. 87/1998, þar sem dagsektir geta numið frá 10.000 kr. til 1 millj. kr. á dag. Hér ber þó að hafa í huga að samkvæmt þeim lögum myndu dagsektir nær alltaf beinast að lögaðilum, þ.e. fyrirtækjum á fjármálamarkaði, en dagsektir samkvæmt persónuverndarlögum geta beinst jafnt að lögaðilum sem einstaklingum og er reyndar dæmi um að Persónuvernd hafi lagt dagsektir á einstakling.

Beiting dagsekta getur verið áhrifaríkt úrræði og í sumum tilvikum getur, með hliðsjón af meðalhófsreglu stjórnsýslunnar, verið eðlilegra að grípa til þess fremur en að stöðva starfsemi. Slíkt hlýtur þó að vera háð mati hverju sinni.

Samkvæmt 2. mgr. falla dagsektir ekki á ef ákvörðun Persónuverndar er skotið til dómstóla fyrir en að gengnum endanlegum dómi. Þannig verður dagsektum ekki beitt fyrir en að liðnum áfrýjunarfresti þegar héraðsdómi er áfrýjað en að öðrum kosti að gengnum dómi Hæstaréttar.

Auk þess sem dagsektir verða bæði lagðar á lögaðila og einstaklinga, eins og fyrir greinir, verða þær lagðar á opinbera aðila rétt eins og einkaaðila samkvæmt gildandi lögum, sem og þessu ákvæði frumvarpsins. Það sama hefur gilt í Noregi á grundvelli hliðstæðs dagsektaákvæðis í núgildandi norskum lögum um persónuvernd. Í löggjöfinni hér á landi má einnig finna sérákvæði um að dagsektir verði lagðar á lögaðila, sbr. 116. gr. sveitarstjórnarlaga nr. 138/2001 sem heimilar að ráðherra leggi dagsektir á sveitarfélög við ákveðnar aðstæður.

Hefur dagsektaákvæði núgildandi laga nr. 77/2000 verið skýrt í ljósi refsiaákvæðisins í 42. gr. þeirra um að gera megi lögaðilum fésekt skv. II. kafla A almennra hegningarlaga. Í 19. gr. b. sem þar stendur segir að sérákvæði laga um refsiaðbyrgð lögaðila gildi, nema annað sé þar tekið fram, um sérhvern ópersónulegan aðila sem getur átt réttindi og borið skyldur að íslenskum rétti, þar með talin hlutafélög, einkahlutafélög, samlagshlutafélög, evrópsk fjárhagsleg hagsmunafélög, sameignarfélög, samvinnufélög, almenn félög, sjálfseignarstofnanir, stjórnvöld, stofnanir og sveitarfélög.

Frumvarpið gerir ráð fyrir því að refsiaðbyrgð lögaðila verði aflögð, en þess í stað komi heimild til að leggja stjórnvaldssektir á lögaðila, hvort heldur einkaaðila eða opinbera aðila, eins og nánar verður rætt í skýringum með næsta frumvarpsákvæði. Það hefur þó engin áhrif á heimildina til að leggja dagsektir á lögaðila og stendur hún, sem fyrir segir, því óbreytt frá gildandi lögum.

Um 46. gr.

Í þessari grein er fólgið veigamikið nýmæli sem reglugerðin kveður á um. Persónuvernd er hér veitt heimild til að leggja stjórnvaldssektir á hvern þann sem brýtur gegn einhverju þeirra ákvæða reglugerðarinnar og laga þessara sem talin eru upp í ákvæðinu. Geta sektir numið háum fjárhæðum, líklega með því hæsta sem um getur í íslenskum lögum. Þess má geta til samanburðar að skv. lögum nr. 161/2002 um fjármálafyrirtæki geta stjórnvaldssektir numið 800 millj. kr. að hámarki á lögaðila. Í þessu tilliti er íslenska ríkinu skylt að innleiða fyrirmæli reglugerðarinnar um sektafjárhæðir. Er þetta í fyrsta skipti sem Evrópureglur kveða á um skyldur ríkja til að leggja stjórnvaldssektir á þá sem brotlegir gerast við persónuverndarlög.

Í gildandi lögum hefur heimild til að leggja á stjórnvaldssektir ekki verið til staðar, ólíkt því sem við á um t.d. norsk lög þar sem slíkar heimildir hefur verið að finna í nokkur ár. Í lögum 77/2000 er hins vegar að finna almennt ákvæði um refsingar í 42. gr. Samkvæmt því ákvæði varðar brot á ákvæðum laganna og reglugerðum settum samkvæmt þeim fésektum eða fangelsi allt að þremur árum nema þyngri refsing liggi við samkvæmt öðrum lögum. Sama refsing liggur við ef ekki er farið að fyrirmælum Persónuverndar. Þá er tilgreint, eins og fyrir var lýst, að þegar brot er framið í starfsemi lögaðila megi gera lögaðilanum fésekt, en þar undir falla auk starfsemi á sviði einkaréttar, stjórnvöld, stofnanir og sveitarfélög.

Könnun á framkvæmd þessa refsiaákvæðis leiðir í ljós að aldrei hefur verið gefin út ákæra fyrir brot á persónuverndarlögum hvorki gegn lögaðila né einstaklingi. Sú leið er farin í frumvarpi þessu að afleggja refsiaðbyrgð lögaðila vegna brota á persónuverndarlögum enda ljóst að stjórnvaldssektir stefna að sama tilgangi. Þær ættu því að veita lögaðilum nauðsynlegt aðhald og varnaðaráhrif enda geta þær numið háum fjárhæðum sem fyrir segir. Myndi áframhaldandi heimild til að leggja fésektir á lögaðila í refsiskyni auk stjórnvaldssektanna litlu bæta við til að auka varnaðaráhrif en væri frekar til þess fallin að valda óvissu enda óljóst um gagnsemi þess að viðhalda tvöföldu viðurlagakerfi. Í þessu sambandi er fylgt fyrirmynd úr norska frumvarpinu til nýrra persónuverndarlaga, þar sem felld eru niður refsiaákvæði núgildandi laga þar í landi gagnvart lögaðilum en aðeins sett ákvæði um stjórnvaldssektir.

Þrátt fyrir að frumvarp þetta geri ekki ráð fyrir refsiaðbyrgð lögaðila sem fyrir segir, er áfram ráðgert að einstaklingar geti sætt refsiaðbyrgð þegar um stórfellt brot er að ræða, en nánar verður vikið að því í umfjöllun um 48. gr. frumvarpsins.

Í 2. og 3. mgr. þessa frumvarpsákvæðis er tilgreint nánar í hvaða tilvikum háttsemi varðar stjórnvaldssektum og fjárhæð sekta. Þessi ákvæði taka mið af 2.-6. mgr. 83. gr.

reglugerðarinnar. Sá greinarmunur er gerður á þeim brotum, sem talin eru upp í annars vegar 2. mgr. og hins vegar 3. mgr. frumvarpsákvæðisins, að brot skv. því síðarnefnda eru álitin alvarlegri en skv. því fyrrnefnda og varða því hærri sektum. Lúta brot skv. 2. mgr., sem rétt er að taka fram í ljósi framangreinds að ekki eru álitin léttvæg þó svo að um ræði lægri sektarfjárhæðir, fyrst og fremst að vanrækslu á skyldum ábyrgðar- og vinnsluaðila, m.a. til að tryggja öryggi vinnslu skv. ákvæðum reglugerðarinnar, til að tilkynna Persónuvernd eða einstaklingi um öryggisbrot og til að láta fara fram mat á áhrifum persónuverndar eða fyrirframsamráð við Persónuvernd þar sem það á við. Eru fjárhæðir sekta við þessum brotum í lægri flokki af tveimur og geta numið allt frá 100 þús. kr. til 1,2 milljarða kr. (10 millj. evra skv. 4. mgr. 83. gr. reglugerðarinnar) eða, ef um er að ræða fyrirtæki, allt að 2% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra.

Þau brot sem talin eru upp í 3. mgr. teljast af alvarlegri toga eins og fyrr greinir, m.a. í ljósi beinna skaðlegra afleiðinga þeirra fyrir grundvallarréttindi skráðra einstaklinga. Þar eru m.a. talin upp brot á grundvallarreglum 5., 6., 7. og 9. gr. reglugerðarinnar, þ.m.t. um samþykki hins skráða, brot á réttindum skráðra einstaklinga skv. III. kafla reglugerðarinnar og brot á reglum um miðlun upplýsinga til viðtakanda í þriðja landi eða alþjóðastofnunar skv. 44.-49. gr. reglugerðarinnar. Þá teljast það brot skv. þessari málsgrein ef neitað er að verða við skyldu til að veita Persónuvernd aðgang að öllum gögnum og húsnæði við rannsókn máls skv. lögunum eða ef ekki er farið að fyrirmælum stofnunarinnar um takmörkun eða bann við vinnslu persónuupplýsinga, leiðréttingu eða eyðingu þeirra, eða stöðvun gagnaflæðis. Getu stjórnvaldssektir við þessum alvarlegri brotum numið frá 100 þús. kr. til 2,4 milljarða kr. (20 millj. evra skv. 6. mgr. 83. gr. reglugerðarinnar) eða, ef um er að ræða fyrirtæki, allt að 4% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra.

Í þessum ákvæðum frumvarpsins eru umreiknaðar í íslenskar krónur þær sektarfjárhæðir sem tilgreindar eru í 4. og 6. mgr. 83. gr. reglugerðarinnar, en þar er mælt fyrir um að stjórnvaldssektir geti numið allt að 10 milljónum evra og 20 milljónum evra. Þykir fara betur á því að vísa til íslensks gjaldmiðils í íslenskum lögum um efnið enda bæði gagnsærra og skýrara fyrir þá sem vinna eftir lögunum.

Í 4. mgr. frumvarpsákvæðisins er því lýst að heimilt sé að leggja stjórnvaldssektir bæði á einstaklinga og lögaðila, þar á meðal stjórnvöld og stofnanir sem falla undir gildissvið stjórnsýslulaga. Hér er því ekki gerður greinarmunur á milli einkaaðila og opinberra aðila, frekar en í gildandi lögum þar sem refsíðabyrgðin nær jafnt til beggja. Samkvæmt 7. mgr. 83. gr. reglugerðarinnar er það valkvætt fyrir aðildarríki hvort þau veita heimildir í landslögum til að leggja stjórnvaldssektir á opinbera aðila. Með hliðsjón af því að stjórnvöld bera refsíðabyrgð skv. lögum nr. 77/2000 á sama hátt og lögaðilar og því að önnur Norðurlönd hafa valið að nýta framangreinda heimild þykir eðlilegt að álagning stjórnvaldssekta taki líka til stjórnvalda. Þá er nauðsynlegt að hafa í huga að í mörgum tilvikum vinna stjórnvöld með umfangsmikið magn persónuupplýsinga, bæði almennra og viðkvæmra. Slíkar upplýsingar geta m.a. lotið að félagslegri stöðu, heilsufari, upplýsingum um refsiverðan verknað og kynhneigð einstaklinga. Þá getur vinnslan einnig tekið til viðkvæmra hópa á borð við börn og fatlað fólk. Að sama skapi er mikilvægt að veita sérstök varnaðaráhrif með því að heimila álagningu stjórnvaldssekta á stjórnvöld og gæta jafnræðis milli opinberra aðila og lögaðila þegar kemur að eftirfylgni við persónuverndarlöggjöfina.

Í 5. mgr. þessa frumvarpsákvæðis er tekið fram að ákvarðanir um stjórnvaldssektir skuli teknar af stjórn Persónuverndar, eins og getið var í skýringum með 38. gr. frumvarpsins, enda er litið svo að um meiriháttar efnislegar og íþyngjandi ákvarðanir sé að ræða, sem eru auk þess á einu stjórnsýslustigi og þurfa í því ljósi að fá sérlega vandaða meðferð.

Þá er tekið fram í 6. mgr. að heimild Persónuverndar til að leggja á stjórnvaldssektir falli 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.

Um 47. gr.

Eins og fram kemur í 46. gr. og skýringum með henni geta stjórnvaldssektir vegna brota á reglugerðinni og lögunum varðað stjórnvaldssektum sem nema afar háum fjárhæðum og eru umtalsvert hærri en það sem tíðkast hefur hér á landi í álagningu slíkra sekta. Ljóst er að verulega mikið þyrfti til að koma svo að 2 milljarða króna sekt yrði lögð á þann sem brýtur

gegn persónuverndarreglunum. Í reglugerðinni er ekki neinn greinarmunur á sektarfjárhæð eftir því hvort einstaklingur eða lögaðili á í hlut, en eðli málsins samkvæmt hljóta svo háar sektarfjárhæðir eingöngu að koma til álíta þegar um er að ræða mjög fjársterk fyrirtæki af stærðargráðu sem tæplega verður fundin hér á landi. Þá er ljóst að rannsókn á broti og sektarákvörðun getur beinst að alþjóðlegum fyrirtækjum. Geti alvarleg brot í starfsemi þeirra valdið umtalsverðu tjóni fyrir þúsundir eða jafnvel milljónir skráðra einstaklinga. Er því ekki útilokað að sektarfjárhæð geti orðið enn hærri þegar haft er í huga að sekt getur numið allt að 4% af árlegri heildarveltu fyrirtækis.

Mikilvægt er að samræmi verði á milli persónuverndarstofnana í Evrópu um hvernig sektarákvörðunum er beitt í ljósi þess að eitt meginmarkmið reglugerðarinnar er að tryggja samræmda og einsleita beitingu ákvæða hennar. Til að ná þessu markmiði þurfa evrópskar persónuverndarstofnanir að hafa samráð um beitingu sektarheimilda. Þess má geta að starfshópur skv. 29. gr. tilskipunar ESB hefur gefið út leiðbeiningar um efnið sem samþykktar voru 3. október 2017, WP 253 (Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679). Þar er meðal annars bent á að framkvæmd við álagningu stjórnvaldssekta innan ríkja á svæðinu er í mótun og er hvatt til þess að persónuverndarstofnanir leitist við að koma á samræmdri beitingu sektarákvarðana með viðvarandi samvinnu um efnið. Þessu megi t.d. ná með gagnkvæmum upplýsingaskiptum á fundum milli þeirra þar sem gerður verði samanburður á framkvæmd stofnana í þessu tilliti. Má ætla að þegar Evrópska persónuverndarráðið tekur til starfa verði gefnar út frekari leiðbeiningar um efnið.

Álagning stjórnvaldssektar verður að vera í réttu hlutfalli við brot í hverju tilviki en jafnframt þurfa að vera til staðar viðmið um hvernig fjárhæð hennar er ákveðin og hvaða atriða skuli líta til. Er það markmið þessa frumvarpsákvæðis að setja slík viðmið fram, en það er samhljóða upptalningu atriða í 2. mgr. 83. gr. reglugerðarinnar. Efni þessara viðmiða er m.a. dregið saman í 148. lið formála reglugerðarinnar. Bent er á að við ákvörðun sekta á að taka tilhlýðilegt tillit til þess hvers eðlis brotið er, hversu alvarlegt það er og hversu lengi það hefur staðið yfir, hvort það var framið af ásetningi, til hvaða aðgerða var gripið til að draga úr tjóni, hversu mikil ábyrgðin var eða hvort um fyrri brot sem skipta máli er að ræða, hvernig eftirlitsstjórnvaldið komst á snoðir um brotið, hvort ráðstöfunum sem settar voru gagnvart ábyrgðaraðila eða vinnsluaðila var fylgt og hvort hátternisreglum var fylgt ásamt öðrum mildandi eða íþyngjandi þáttum. Auk þess er áréttað í 150. lið formálans að eftirlitsstjórnvald skal ákveða sekt í hverju einstöku tilviki með hliðsjón af öllum viðeigandi kringumstæðum í viðkomandi máli, einkum að teknu tilhlýðilegu tilliti til eðlis, alvarleika og lengdar brotsins og afleiðinga þess og ráðstafana sem gerðar hafa verið til að tryggja að skuldbindingar samkvæmt reglugerðinni séu uppfylltar og til að koma í veg fyrir eða draga úr afleiðingum brotsins. Tekið er fram að þegar stjórnsýslusektir eru lagðar á aðila sem ekki eru fyrirtæki ætti að taka tillit til almenns tekjustigs í aðildarríkinu og fjárhagsstöðu aðilans þegar viðeigandi sektarfjárhæð er ákveðin. Einnig er bent á að nota má samræmingarkerfi reglugerðarinnar til að stuðla að samræmdri beitingu stjórnsýslusekta á milli ríkja.

Um 48. gr.

Í greininni er mælt fyrir um refsingar, annars vegar þegar um er að ræða brot á efnisreglum laganna og reglugerðarinnar um vinnslu persónuupplýsinga og hins vegar þegar brotið er gegn þagnarskylduákvæðum.

Í reglugerðinni er ekki lögð skylda á ríki til að gera brot á ákvæðum hennar refsiverð. Í 84. gr. hennar er þó hvatt til að aðildarríkin setji reglur um önnur viðurlög við brotum á reglugerðinni, einkum brotum sem varða ekki stjórnsýslusektum skv. 83. gr. hennar, og geri allar nauðsynlegar ráðstafanir til að sjá til þess að þeim sé komið til framkvæmda. Slík viðurlög skuli vera skilvirk, í réttu hlutfalli við brot og hafa varnaðaráhrif. Til að varpa frekara ljósi á þetta kemur fram í 148. lið formálans að aðildarríkin ættu að geta sett reglur um refsiviðurlög vegna brota á reglugerðinni, þ.m.t. vegna brota á innlendum reglum sem samþykktar eru samkvæmt henni og innan ramma hennar. Bent er á að slík refsiviðurlög geta einnig gert ráð fyrir að viðkomandi sé sviptur þeim ávinningi sem hann hafði af brotum á reglugerðinni. Þá er gerður sá fyrirvari að ákvörðun refsiviðurlaga vegna brota á innlendum reglum og stjórnsýsluviðurlögum megi ekki leiða til brots á meginreglunni um að verða ekki saksóttur eða refsað tvívegis fyrir sama brot (ne bis in idem), eins og Dómstóll ESB hefur túlkað hana.

Sú leið er farin í frumvarpi þessu að afleggja ekki með öllu refsíabyrgð einstaklinga þannig að álagning stjórnslusekta taki við í öllum tilvikum. Hér er m.a. litið til fyrirmyndar í þýsku lögunum frá 30. júní 2017 um innleiðingu reglugerðarinnar sem mælir fyrir um refsíabyrgð í nánar skilgreindum stórfelldum brotum. Það eykur varnaðaráhrif gagnvart einstaklingum, t.d. fyrirsvarsmönnum fyrirtækja þar sem fram fer umfangsmikil vinnsla persónuupplýsinga, að fangelsisrefsing sé lögð við alvarlegustu brotum en hér er miðað við sama refsiramma og í 42. gr. gildandi laga eða fangelsi allt að þremur árum. Jafnframt verður þá unnt skv. förmælum ákvæðisins að gera ávinning af broti upptækan. Það hefur hins vegar ekki sérstaka þýðingu að gera brot lögaðila refsiverð, enda yrðu viðurlög ávallt í formi fjárgreiðslu hvort eð er og við ákvörðun stjórnvaldssektar er hægt að taka tillit til ávinnings lögaðila af brotinu. Skilyrði fyrir því að refsíabyrgð einstaklings skv. 1. mgr. þessa frumvarpsákvæðis verði virk er að brotið sé stórfellt og er því jafnframt lýst hvað felst í því, þ.e. að litið er til ásetnings, umfangs og afleiðinga. Þannig telst brot stórfellt þegar það er framið af ásetningi, 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.

Í 2. mgr. frumvarpsákvæðisins er tekið fram að hafi fyrirsvarsmaður lögaðila, starfsmaður hans eða annar á hans vegum framið brot í starfsemi lögaðilans megi gera honum refsingu, samhliða stjórnvaldssekt sem lögaðilanum er gerð skv. 46. gr. Af þessu er ljóst að refsíabyrgð einstaklings leysir ekki fyrirtæki undan mögulegri álagningu stjórnslusektar vegna sama brots. Hins vegar er ótvírætt að sama einstaklingi verður ekki bæði refsað fyrir brot samkvæmt þessu ákvæði frumvarpsins og látinn sæta stjórnvaldssekt, enda yrði með því farið gegn meginreglunni um að verða ekki saksóttur eða refsað tvívegis fyrir sama brot (ne bis in idem) sem fram kemur í 4. gr. 7. viðauka við mannréttindasáttmála Evrópu. Vakni grunur um alvarlegt brot, t.d. við rannsókn máls, hjá Persónuvernd verður stofnunin að meta hvort það skuli kært til lögreglu eða hvort leggja skuli á stjórnslusekt.

Í 3. mgr. þessa frumvarpsákvæðis er fjallað um refsiviðurlög við broti á þagnarskyldu sem varðar sektum eða fangelsi allt að 3 árum. Í 36. frumvarpsins er mælt fyrir þagnarskyldu persónuverndarfulltrúa en vísað er til frekari skýringa með því ákvæði um skyldur persónuverndarfulltrúa í þeim efnum.

Í 44. gr. er hins vegar mælt fyrir um þagnarskyldu starfsmanna Persónuverndar. Er brot á þagnarskyldu opinberra starfsmanna reyndar einnig refsiverð skv. 136. gr. almennra hegningarlaga nr. 19/1940, en samhengis vegna þykir rétt að safna ákvæðum um brot á þagnarskyldu hér á einn stað. Þá vísar frumvarpsákvæði þetta til þagnarskyldu ábyrgðaraðila og vinnsluaðila sem gangast undir slíka skyldu með sérstakri yfirlýsingu þess efnis í tengslum við gerð skilmála skv. 33. gr. Er þyngri refsing lögð við hafi þessir einstaklingar framið brot til þess að afla sér eða öðrum óréttmæts ávinnings en þá getur fangelsi varðað allt að 3 árum.

Í lokamálsgrein þessa ákvæðis er mælt fyrir um heimildir til upptöku á ávinningi af broti á lögunum og reglugerðinni og hlutum sem notaðir eru til að fremja brot. Um það er vísað til ákvæða VII. kafla A almennra hegningarlaga og þarfnast það ekki frekari skýringar hér.

Um 49. gr.

Eins og fram kom í skýringum við 48. gr. frumvarpsins er lagt til að stórfelld brot einstaklings verði refsiverð, en eins og lýst var í umfjöllun um stjórnvaldssektir verður einnig hægt að leggja slíkar sektir á einstaklinga. Í þessu ákvæði er lagt til að sett verði ákvæði um verklag við rannsókn mála þar sem meint brot einstaklings geta bæði varðað stjórnvaldssektum og refsiviðurlögum og um samskipti milli Persónuverndar og lögreglu og ákærvalds. Eru breytingarnar til þess fallnar að samhæfa hið almenna viðurlagakerfi og viðurlagakerfi Persónuverndar í þeim tilvikum þar sem refsing og stjórnsluviðurlög eru bæði lögbundin sem viðurlög við broti, þannig að ekki komi til þess að málið verði rannsakað á sama tíma bæði hjá Persónuvernd og lögreglu og til að tryggja að einstaklingar fái ekki tvenns konar viðurlög fyrir sömu háttsemi. Er hér m.a. sótt fyrirmynd til ákvæðis í 112. gr. c í lögum um fjármálafyrirtæki nr. 161/2002, eins og þeim var breytt með lögum nr. 55/2007 við endurskoðun á ákvæðum um viðurlög við brotum sem þar getur, svo og til annarrar löggjafar um brot á fjármálamarkaði.

Í 1. mgr. er mælt fyrir um að Persónuvernd meti hvort meint brot einstaklings skuli kært til lögreglu eða hvort hjá stofnuninni fari fram á því rannsókn sem lykti með álagningu stjórnvaldssektar. Við mat sitt á þessu ber Persónuvernd að styðjast við þau viðmið sem fram

koma í 48. gr. og lýst var í skýringum við það ákvæði, þ.e. hvenær brot telst vera stórfellt. Í ákvæðinu er jafnframt kveðið á um að ákvörðun Persónuverndar um að kæra mál til lögreglu teljist ekki til stjórnsýsluákvörðunar og því gildi ákvæði IV.–VII. kafla stjórnsýslulaga ekki um slíkar ákvarðanir stofnunarinnar. Þá er mælt fyrir um að með kærunni til lögreglu skuli fylgja afrit þeirra gagna sem grunur um brot sé studdur við. Ekki er um að ræða skyldu Persónuverndar til að kæra brot, en það veltur sem fyrr segir á mati stofnunarinnar hvort sú leið sé farin. Þá er einnig ljóst að rannsókn lögreglu á meintu broti einstaklings skv. 48. gr. og útgáfa ákæru er ekki háð því að kæra komi frá Persónuvernd. Því gilda almennar reglur um að aðrir geti kært slíkt brot eða mögulega að lögregla hefji rannsókn að eigin frumkvæði, sbr. einnig 52. gr. laga um meðferð sakamála nr. 88/2008. Eðlilegt væri þó að samráð yrði haft við Persónuvernd, m.a. til að fyrirbyggja að rannsókn hefjist á báðum stöðum, en það er einmitt markmið þessa frumvarpsákvæðis að tryggja að samvinna eigi sér stað milli stofnana.

Þetta markmið endurspeglast í 2.–4. mgr. frumvarpsákvæðisins. Samkvæmt 2. mgr. er Persónuvernd þannig heimilt að láta lögreglu og ákærvaldi í té upplýsingar og gögn sem stofnunin hefur aflað og tengjast meintum brotum samkvæmt 48. gr. Þá er tilgreint að Persónuvernd sé heimilt að taka þátt í aðgerðum lögreglu sem varða rannsókn þeirra brota.

Með sama hætti er lögreglu og ákærvaldi heimilt skv. 3. mgr. að láta Persónuvernd í té upplýsingar og gögn sem þau hafa aflað og tengjast þeim brotum sem tilgreind eru í 48. gr. og mögulega einnig brotum sem aðeins varða stjórnsýslusektum skv. 46. gr. Lögreglu er heimilt að taka þátt í aðgerðum Persónuverndar sem varða rannsókn hennar á brotum á lögunum og reglugerðinni. Hér ber einnig að líta til 41. gr. frumvarpsins sem fjallar um valdheimildir Persónuverndar við eftirlitsstörf en í 2. og 3. mgr. þeirrar greinar er fjallað um aðkomu lögreglu, vegna rannsókna Persónuverndar á meintum brotum á reglugerðinni og lögunum.

Í lokamálgrein þessa frumvarpsákvæðis er kveðið á um heimild ákæranda til að senda eða endursenda mál til Persónuverndar til meðferðar og ákvörðunar í þeim tilvikum þar sem ekki eru talin efni til útgáfu ákæru og ætluð refsiverð háttsemi varðar jafnframt stjórnsýsluviðurlögum. Á ákvæðið við hvort sem lögregla eða ákærvald hafa tekið mál upp að eigin frumkvæði eða fengið það sent frá eftirlitsaðilanum

Um 50. gr.

Ákvæði þetta tekur mið af hliðstæðum lagaákvæðum sem hafa verið sett í ýmis sérlög á sviði fjármálamarkaðar í tengslum við rannsókn eftirlitsstjórnvalda á brotum sem leitt geta til stjórnsýsluviðurlaga. Á meðan ekki er í stjórnsýslulögum almennt ákvæði um rétt einstaklings til að fella ekki sök á sjálfan sig við rannsókn á stjórnsýslustigi, þykir æskilegt að inntak réttarins verði fest í persónuverndarlöggjöf, enda geta stjórnsýsluviðurlög, þar á meðal stjórnsýslusektir, talist viðurlög við „refsiverðu broti“ í skilningi 1. mgr. 6. gr. mannréttindasáttmála Evrópu.

Mannréttindadómstóll Evrópu hefur í dómum sínum talið að það sé þáttur í réttlátri málsmeðferð skv. 6. gr. mannréttindasáttmála Evrópu að þeim sem sakaður er um refsiverða háttsemi í skilningi þess ákvæðis sé óskýlt að tjá sig eða láta í té upplýsingar sem leitt geta til sakfellingar hans. Þar sem ákvæði sáttmálans hafa verið lögtekin hér á landi gildir rétturinn til að fella ekki á sig sök hér við meðferð stjórnsýslumála þar sem til greina kemur að leggja á stjórnvaldssekt sem telst vera viðurlög við „refsiverðu broti“ í skilningi 1. mgr. 6. gr. sáttmálans. Til þess að stuðla að því að rétturinn til að fella ekki á sig sök sé virtur í framkvæmd er talið æskilegt að inntak hans verði lögfest með skýrum hætti eins og lagt er til hér.

Um 51. gr.

Í þessari grein er mælt fyrir um bótaskyldu ábyrgðaraðila eða vinnsluaðila vegna tjóns sem verður þegar unnið hefur verið með persónuupplýsingar í andstöðu við ákvæði reglugerðarinnar, laga þessara, reglna settra á grundvelli þeirra eða fyrirmæli Persónuverndar. Er hér byggt 82. gr. reglugerðarinnar um bótarétt og bótaábyrgð, en meðal nýmæla sem hún felur í sér er að ekki aðeins ábyrgðaraðilar heldur einnig vinnsluaðilar geta borið skaðabótaábyrgð vegna brota sem leiða til tjóns, hvort heldur fjárhagslegs eða ófjárhagslegs. Í 146. lið formála reglugerðarinnar er tekið fram að túlka beri hugtakið „tjón“ vítt í ljósi dómaframkvæmdar dómstóls ESB og að skráðir einstaklingar ættu að fá fullar skaðabætur fyrir það tjón sem þeir verða fyrir.

Í 82. gr. reglugerðarinnar er nánar rætt um samspil ábyrgðar á milli ábyrgðaraðila og vinnsluaðila. Þannig er tekið fram í 2. mgr. að ábyrgðaraðili, sem tekur þátt í vinnslu, skuli bera

ábyrgð á því tjóni sem hlýst af vinnslunni. Vinnsluaðili skuli því aðeins bera ábyrgð á tjóni, sem hlýst af vinnslu, hafi hann ekki uppfyllt sérstakar skyldur vinnsluaðila samkvæmt reglugerðinni eða ef hann hefur ekki fylgt lögum fyrirmælum ábyrgðaraðilans eða farið gegn þeim. Þá er tekið fram í 4. mgr. 82. gr. reglugerðarinnar að ef fleiri en einn ábyrgðaraðili eða vinnsluaðili, eða bæði ábyrgðaraðili og vinnsluaðili, koma að sömu vinnslu og þeir bera ábyrgð á tjóni sem af henni hlýst skuli hver ábyrgðaraðili eða vinnsluaðili vera ábyrgur fyrir öllu tjóninu til að tryggja hinum skráða fullar skaðabætur. Af þessu er ljóst að ábyrgðaraðili eða vinnsluaðili sem hefur greitt fullar skaðabætur getur í kjölfarið gert endurkröfu á aðra ábyrgðaraðila eða vinnsluaðila sem tóku þátt í sömu vinnslu, sbr. einnig niðurlagsorð 146. liðar formála reglugerðarinnar.

Segja má að skaðabótaábyrgð ábyrgðaraðila og vinnsluaðila leiði í reynd af almennum skaðabótareglum íslensks réttar, en eigi að síður þykir rétt að orða um hana sérstaka reglu í frumvarpinu í samræmi við fyrrgreint ákvæði reglugerðarinnar.

Þá er ljóst að hvorki ábyrgðaraðila né vinnsluaðila verður gert að bæta tjón sem hann sannar að hvorki verði rakið til mistaka né vanrækslu af hans hálfu, sbr. lokamálslið 1. mgr. þessa frumvarpsákvæðis og 3. mgr. 82. gr. reglugerðarinnar, en af þessu er ljóst að sönnunarbyrði um það hvílir á honum.

Um 52. gr.

Í ákvæði þessu er mælt fyrir um heimild til þess að reglugerðir verði settar um meðferð persónuupplýsinga í tiltekinni starfsemi og hjá einstökum starfsstéttum og stendur ákvæðið óbreytt frá 1. mgr. 45. gr. í núgildandi lögum. Ákvæðið felur í sér heimild til að setja nánari ákvæði um framkvæmd laganna eftir aðstæðum og þörfum á afmörkuðum sviðum. Er hér um heimild ráðherra að ræða en ekki skyldu og veitir ákvæðið svigrúm til að útfæra nánari ákvæði laganna og reglugerðarinnar eftir því sem tilefni gefst til um þessi efni í þeirri öru þróun sem á sér stað á sviði upplýsingatækni og vinnslu persónuupplýsinga.

Um 53. gr.

Í gildistökuákvæði frumvarpsins er lagt til lögin öðlist þegar gildi. Reglugerð ESB kemur til framkvæmda innan ESB 25. maí 2018. Þegar frumvarp þetta er lagt fram hefur gerðin ekki enn verið tekin upp í EES-samninginn en drög að ákvörðun sameiginlegu EES-nefndarinnar þess efnis liggja fyrir á grundvelli samkomulags sem náðst hefur um aðlögun gerðarinnar að EES-samninginum. Eftir er að ganga frá formlegu samþykki sameiginlegu nefndarinnar sem ætla má að liggi fyrir innan nokkurra vikna frá því að frumvarp þetta er lagt fram og þá þarf einnig að fá heimild Alþingis til að staðfesta ákvörðun sameiginlegu EES-nefndarinnar, en tillaga til þingsályktunar þar um hefur verið lögð fyrir Alþingi.

Þessar sérstöku aðstæður leiða þó ekki til þess að ekki sé hægt að samþykkja frumvarpið enda er fellur það innan valdheimilda löggjafans að meta það hvort rétt er að samþykkja frumvarpið en mikilvægt er að það verði að lögum sem næst framangreindu tímamarki sem reglugerðin kemur til framkvæmda innan ESB.

Um ákvæði til bráðabirgða I.

Með ákvæði til bráðabirgða I er lagt til að stjórn Persónuverndar sem situr við gildistöku laganna sitji út skipunartímabil sitt sem stendur til 9. júní 2020, en þá skipi ráðherra nýja stjórn í samræmi við fyrirmæli 38. gr. frumvarpsins. Röksemdir að baki þessu er að ákveðin reynsla þurfi að vera til staðar í stjórn stofnunarinnar þegar lögin taka gildi til að takast á við hin margvíslegu nýju verkefni sem stofnuninni eru falin þar á meðal að móta stefnu um álagningu stjórnvaldssekta. Þá er ljóst að frestur til að undirbúa gildistöku laganna er afar stuttur. Með hliðsjón af því hefur þýðingu að búa yfir reynslu á túlkun og framkvæmd núgildandi laga til að tryggja ákveðna samfellu við framkvæmd nýrra laga.

Um ákvæði til bráðabirgða II.

Með ákvæði til bráðabirgða II er lagt til að reglugerðir svo og reglur, fyrirmæli og leyfi sem Persónuvernd eða ráðherra hafa gefið út á grundvelli laga nr. 77/2000 skuli halda gildi, enda fari þau ekki í bága við lög þessi og reglugerð ESB.

Er hér um að ræða nokkurt safn reglna hvort heldur í reglugerðum gefnum út af ráðherra eða reglum og fyrirmælum Persónuverndar sem sumar hverjar hafa mikla þýðingu á sviði

persónuverndar. Má þar nefna sem dæmi reglugerð nr. 322/2001 um meðferð persónuupplýsinga hjá lögreglu, sbr. einnig ákvæði til bráðabirgða III í frumvarpi þessu og 52. gr. þess), reglur nr. 837/2006 um rafræna vöktun og meðferð persónuupplýsinga sem verða til við rafræna vöktun og reglugerð nr. 246/2001 um söfnun og miðlun upplýsinga um fjárhagsmálefni og lánstraust. Mikilvægt er að ekki skapist tómarúm við gildistöku nýrra persónuverndarlaga og að þessar reglur gildi eftir því sem við getur átt innan ramma reglugerðarinnar og laganna á meðan unnið verður að undirbúningi á endurskoðun þeirra og setningu frekari reglna á sviði persónuverndar. Þá er lagt til að leyfi sem Persónuvernd hefur gefið út í gildistíð núgildandi laga standi áfram enda fari þau ekki í bága við reglur frumvarpsins og reglugerðina.

Um ákvæði til bráðabirgða III.

Hér er lagt til að tiltekin ákvæði laga á grundvelli frumvarpsins gildi um vinnslu persónuupplýsinga sem varða almannaoðryggi, landvarnir, öryggi ríkisins og starfsemi ríkisins á sviði refsivörslu þar til tilskipun (ESB) 2016/680, þar sem er að finna reglur um vinnslu persónuupplýsinga á því sviði, hefur verið innleidd í íslenskan rétt. Ástæðan er sú að vegna 6. mgr. 4. gr. frumvarpsins, sem undanskilur slíka vinnslu gildissviði reglna samkvæmt því, myndi lagaramma um vinnslu persónuupplýsinga hjá meðal annars lögreglu að öðrum kosti skorta. Brýnt er að komið verði í veg fyrir þá aðstöðu. Þá skal tekið fram að upptalningin á þeim ákvæðum sem lagt er til að gildi í umræddu samhengi byggist á efni fyrrnefndrar tilskipunar.