ML í lögfræði

Vottun og hátternisreglur almennu persónuverndarreglugerðarinnar

Júní, 2020

Nafn nemanda: Bergþóra Friðriksdóttir

Kennitala: 290491-3719

Leiðbeinandi: Alma Tryggvadóttir

Útdráttur

Vottun og hátternisreglur almennu persónuverndarreglugerðarinnar

Í ritgerð þessari verður fjallað um vottun og hátternisreglur sem eru valkvæðar leiðir sem er að finna í fimmta þætti fjórða kafla almennu persónuverndarreglugerðarinnar. Markmið ritgerðarinnar er að skoða hvernig framkvæmd þessara leiða verður háttað og jafnframt að hvaða leiti þær geti nýst mismunandi fyrirtækjum og stofnunum við að uppfylla ábyrgðarskylduna.

Með setningu persónuverndarreglugerðarinnar var lögð ríkari áhersla á að fyrirtæki og stofnanir og aðrir sem bera ábyrgð á vinnslu persónuupplýsinga þurfa að fara eftir ákvæðum persónuverndarlöggjafarinnar en jafnframt að þeir geti sýnt fram á reglufylgnina. Af því leiðir að fyrirtæki og stofnanir þurfa að huga að því hvernig þau takast á við þessa nýju skyldu og hvaða leiðir þeim séu færar til þess. Valkvæðu leiðum persónuverndarreglugerðarinnar er ætlað að geta nýst fyrirtækjunum til þess að sína fram á að vinnsla þeirra uppfylli ákvæði persónuverndarreglugerðarinnar. Leiðirnar eru hins vegar frábrugðnar hvor annarri þrátt fyrir að hafa sama markmið.

Þar sem leiðirnar eru ólíkar þá geta þær höfðað til ólíkra fyrirtækja og stofnana, þar sem þau hafa mismunandi getu til að framfylgja skilyrðum reglugerðarinnar en jafnframt frábrugðin markmið með því að geta sýnt fram á reglufylgnina. Hátternisreglur eru líklegri til að höfða til lítilla og meðalstórra fyrirtækja þar sem þau búa síður yfir nægilegri þekkingu til þess að uppfylla skilyrði vottunar. Þá hentar tvíeðli hátternisreglnanna þessum aðilum vel, þar sem reglurnar nýtast bæði sem leiðbeiningar fyrir fyrirtækin en jafnframt leið til að sýna fram á reglufylgni með persónuverndarlöggjöfinni. Stærri fyrirtæki gætu frekar séð hag sinn í að sækjast eftir vottun, þrátt fyrir að það hafi í för með sér aukinn kostnað, hins vegar þá er ekki hægt að finna sýnilegri leið til að sýna fram á reglufylgni heldur en vottun, því veitir vottun fyrirtækjum ákveðið samkeppnisforskot.

Abstract

Certification and Codes of Conduct under the General Data Protection Regulation (EU) 2016/679

This thesis will cover Certification and Codes of Conduct which are voluntary accountability tools from the fifth section of chapter four of the General Data Protection Regulation, GDPR. The aim of the thesis is to examine how these approaches will be implemented and also to what extent they can benefit different companies and institutions to fulfil the principle of accountability.

When the General Data Protection Regulation came into effect it emphasized that companies and institutions and others responsible for the processing of personal data must comply with the provisions of the regulation, while at the same time being able to demonstrate compliance. As a result, companies and institutions engaged in data processing need to find effective ways how to comply to the regulation. The GDPR voluntary accountability tools are designed help companies and institutions show that their data processing is GDPR compliant. These tools differ in approach though they share the same end result.

The approaches are different and therefore they can appeal to different companies and institutions, as they have different means to fulfil the requirements of the GDPR. Codes of Conduct are more likely to appeal to small and medium-sized companies, since they have less means to meet the certification requirements. The dual nature of the Codes of Conduct is well suited to these parties, as the codes can be used both as guidelines and also as a way to demonstrate compliance with the GDPR. Certification is likely to appeal more to larger companies, even though it entails increased costs. Having a certification is the most visible way of demonstrating compliance and therefore could give those companies a certain competitive advantage.

Lagaskrá

Íslensk lög

Stjórnarskrá lýðveldisins Íslands nr. 33/1944

Lög um Evrópska efnahagssvæðið nr. 2/1993

Stjórnsýslulög nr. 37/1993

Lög um mannréttindasáttmála Evrópu nr. 62/1994

Lög nr. 97/1995 um breytingu á stjórnarskrá lýðveldisins Íslands nr. 33/1944

Lög um Faggildingu o. fl. nr. 24/2006

Lög um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018

Brottfallin lög

Lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000

Evrópuréttur

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 nr.54/2000 EES-viðbætir við Stjtíð EB 114.

Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro small and medium-sized enterprises [2003] OJ L124/36

Consolidated Version of the Treaty of the European Union [2008] OJ C 115/13

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) 46/2018 EES-viðbætir við Stjtíð ESB 6.

Alþjóðlegir sáttmálar

Universal Declaration of Human Rights (10. desember 1948) UNGA Res 17 A(III)

Samningur um vernd einstaklinga varðandi vélræna vinnslu persónuupplýsinga nr. 108 (samþykktur 28. janúar 1981, tók gildi 1. október 1985, undirritaður f.h. Íslands 27. september 1982 og fullgiltur á Íslandi 1. júlí 1991) Stjtíð. C, 5/1991

Lögskýringargögn

Alþt. 1994-1995 A-deild, þskj. 389 - 297. mál.

Alþt. 1999-2000 A-deild, þskj. 399 - 280 mál.

Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál.

Dómaskrá

Hæstiréttur Íslands

Hrd. 27. nóvember 2003 í máli nr. 151/2003

Dómar Evrópudómstólsins

C-518/07 European Commission g. Federal Republic of Germany [2010] ECR I-1885

Úrskurðir og ákvarðanir Persónuverndar

Úrskurður Persónuverndar nr. 2010/906, 17. ágúst 2011

Ákvörðun Persónuverndar nr. 2020010382, 5. mars 2020.

Ákvörðun Persónuverndar nr. 2020010428, 5. mars 2020

1. Inngangur

Við lifum á tímum örra tæknibreytinga og áhrif upplýsingatækninnar á líf einstaklinga og samfélagsins eru gríðarleg. Þróun tækninnar hefur auðveldað daglegt líf okkar til muna en tækninni fylgja einnig ýmsar áskoranir sérstaklega hvað snertir vernd á réttindum og frelsi einstaklinga. Tækniframfarir hafa opnað fyrir þann möguleika að umfangsmikil upplýsingavinnsla hefur átt sér stað um hluti sem enginn gat séð fyrir. Hegðun einstaklinga hefur jafnframt tekið miklum breytingum á síðastliðnum áratugum, fólk gerir nú persónuupplýsingar sínar aðgengilegar í mun meiri mæli en áður fyrr og tæknin gerir það kleift að þessar upplýsingar verða aðgengilegar á alþjóðavísu í gegnum Internetið. Fyrirtækjum og stofnunum er heimilt, með aðstoð tækninnar, að nýta sér þær upplýsingar sem einstaklingar skilja eftir sig á Internetinu án þess að þeir veiti því sérstaka athygli. Má því segja að fyrir einstaklinga sé meginreglan orðin sú, ef þú þarft ekki að greiða fyrir þjónustu á netinu þá ert það þú sem ert söluvaran.[1]

Vernd persónuupplýsinga snertir alla einstaklinga. Í nútímasamfélagi, upplýsingasamfélaginu, má líta svo á að persónuupplýsingar spili jafn stóra rullu og olían gerði á tímum iðnbyltingarinnar. Persónuupplýsingar eru mikilvæg auðlind og ein verðmætasta söluvara sem fyrirtæki geta boðið upp á að skipta einstaklingum upp í flokka og beina „réttum“ upplýsingum að „réttum“ einstaklingum. Persónuupplýsingar eru drifkrafturinn í nútímakerfi. Einkaaðilar og opinberir aðilar þurfa aðgang að persónuupplýsingum til að starfa en vinnslunni geta fylgt vandamál, þar sem hún er svo nátengd grundavallar réttindum einstaklinga. Í meginatriðum má því segja að evrópska persónuverndarlöggjöfin hafi jafnframt haft það markmið að einfalda líf fyrirtækja og stofnanna en ekki aðeins að tryggja réttindi einstaklinga. Í raun er það ávallt réttindi einstaklinganna sem eru í forgrunni enda eiga þeir að njóta verndar löggjafarinnar.[2]

Það eru nýleg dæmi þess að persónuupplýsingar hafi verið nýttar til að hafa áhrif á niðurstöðu kosninga í lýðræðisríkjum og eitt þekktasta er mál Cambridge Analytica. Þar notaði fyrirtækið persónuupplýsingar yfir 50 milljón notenda miðilsins Facebook með því miða

[1] „Persónuupplýsingar Okkar Eru Verðmæt Söluvara“ (*RÚV*, 1. mars 2017) <https://www.ruv.is/frett/personuupplysingar-okkar-eru-verdmaet-soluvara> skoðað 17. mars 2020.
[2] Peter Blume, „Smart Data Protection“ í Peter Wahlgren (ritstj.), *50 years of law and IT: the Swedish Law and Informatics Research Institute: 1968-2018* (Institute for Scandinavian Law 2018) 176–177.

skilaboðum til réttra hópa til að hafa áhrif á þá út frá persónuupplýsingunum sem safnað hafði verið um þá.[3]

Eitt af megin markmiðum nýrra persónuverndarlöggjafar innan Evrópusambandsins[4] var því að tryggja réttindi einstaklinga. 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)[5] tók gildi innan aðildarríkja sambandsins og Evrópska efnahagssvæðisins vorið 2018. Með nýju löggjöfinni fengu því hinir skráðu einstaklingar greiðan aðgang að persónuupplýsingunum sínum, var því upp að vissu marki verið að veita einstaklingum aftur ákvörðunarrétt yfir eigin persónuupplýsingum. Þar sem settar voru skýrari og strangri reglur fyrir vinnslu og skráningu persónuupplýsinga var um leið verið að gera meiri kröfur á fyrirtæki og hið opinbera og í raun hvern þann sem ætlar sér að skrá og vinna persónuupplýsingar. Þeir sem vinna með persónuupplýsingar bera ábyrgð á að farið sé með þær í samræmi við reglur og lög um persónuvernd.

Einn af nýju þáttunum sem voru innleiddir í persónuverndarreglugerðinni var ábyrgðarskyldan, í henni felst að fyrirtæki, stofnanir og aðrir sem bera ábyrgð á vinnslu persónuupplýsinga bera jafnframt ábyrgð á að vinnslan sé í samræmi við ákvæði löggjafarinnar og uppfylli skyldu sína gagnvart henni. Þá er ekki nóg að fylgja ákvæðum persónuverndarreglugerðarinnar heldur þurfa þessir aðilar einnig að geta sýnt fram á reglufylgnina. Það getur reynst dýrkeypt fyrir fyrirtæki og stofnanir að fylgja ekki ákvæðum löggjafarinnar og þar með talið að ábyrgðarskyldan sé ekki uppfyllt. Með persónuverndarreglugerðinni fengu eftirlitsstjórnvöld aukin völd hvað varðar viðurlög vegna brota á ákvæðum löggjafarinnar, þar á meðal miklar sektarheimildir.

Það er því ljóst að vernd persónuupplýsinga er ekki lengur bara rós í hnappagat fyrirtækja og stofnanna sem hafa nægilegt fjármagn og sérfræðiþekkingu til að fylgja reglum um persónuvernd, heldur er þetta nú grundvallar þáttur í starfsemi þeirra og getur reynst dýrkeypt ef ákvæðum reglugerðarinnar er ekki fylgt.

Samhliða því að leggja þessa nýju skyldu á herðar þeirra sem vinna persónuupplýsingar þá voru einnig kynntar til leiks nýjar leiðir, sem og voru skýrðar reglur eldri löggjafar, til þess

[3] Carole Cadwalladr og Emma Graham-Harrison, „Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach“ *The Guardian* (17. mars 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> skoðað 10. mars 2020.
[4] Hér eftir ESB.
[5] Hér eftir pvrg, persónuverndarreglugerðin eða reglugerðin.

að auðvelda fyrirtækjum og stofnunum að fylgja ákvæðum persónuverndarlöggjafarinnar. Bæði er að finna leiðir sem fyrirtækjum og stofnunum ber skylda til að fylgja sem og aðrar sem fyrirtæki og stofnanir hafa fullkomið val um að nýta sér til þess að sýna fram á að þau uppfylli skyldur sínar gagnvart löggjöfinni.

Í þessari ritgerð verður fjallað um ábyrgðarskyldu ábyrgðaraðila og vinnsluaðila, en segja má að hún sé hornsteinn persónuverndarlöggjafarinnar. Hún kveður á um skyldu ábyrgðaraðila og vinnsluaðila til að fylgja ákvæðum persónuverndarreglugerðarinnar en tíundar jafnframt að þessi aðilar geti sýnt fram á fylgni við ákvæði löggjafarinnar. Í ritgerðinni verður lögð sérstök áhersla á að skoða þær tvær leiðir sem fyrirtæki og stofnanir geta nýtt sér til þess að sýna fram á fylgni við ákvæði löggjafarinnar. Það eru annars vegar vottanir, persónuverndarinnsigli og persónuverndarmerki og hins vegar hátternisreglurnar og eftirlit með þeim. Lögð verður áhersla á að skýra hvernig framkvæmdinni á þessum valkvæðu leiðum er háttað en jafnframt fyrirtæki geti nýtt sér þessar leiðir og þá að hvaða leiti þær henta mismunandi fyrirtækjum og stofunum. Ennfremur verður skoðað hlutverk Persónuverndar sem eftirlitsstjórnvalds í tengslum við þessar valkvæðu leiðir til að sýna fram á reglufylgni. Meginmarkmið ritgerðarinnar er því að skýra hvernig framkvæmdinni á valkvæðu leiðum persónuverndarreglugerðarinnar er háttað og að hvaða leiti hvor leið fyrir sig hentar mismunandi fyrirtækjum og stofnunum til að sýna fram á reglufylgni og uppfylla ábyrgðarskylduna sem löggjöfin kveður á um.

Í ritgerðinni verður fyrst stiklað á stóru í sögu verndar persónuupplýsinga, allt frá upphafi mannréttinda og þá með sérstaka áherslu á friðhelgi einkalífs til þeirrar persónuverndarlöggjafar sem er í gildi nú í dag. Þá verður næsti kafli tileinkaður þeim hugtökum sem mikilvægt er að kunna skil á varðandi efni ritgerðarinnar, sem og fjallað verður um meginreglur persónuverndarlöggjafarinnar, þar sem þær eru grundvöllur fyrir alla vinnslu persónuupplýsinga sem og vikið verður að ábyrgðarskyldunni og farið yfir hvað felst í raun og veru í henni. Fjórði kafli ritgerðarinnar verður tileinkaður meginefni ritgerðarinnar, það er hinar valkvæðu leiðir sem fimmti þáttur fjórða kafla persónuverndarreglugerðarinnar kveður á um, það eru þær leiðir sem ábyrgðaraðilar og vinnsluaðila geta nýtt til þess að uppfylla ábyrgðarskylduna sem og að sýna fram á fylgni við ákvæði reglugerðarinnar. Loks í fimmta kafla ritgerðarinnar verður farið yfir helstu niðurstöður.

2. Söguleg þróun verndar persónuupplýsinga

Réttur einstaklinga til einkalífs er náskyldur og tengdur sjálfsákvörðunarréttinum, þ.e. þeim rétti að einstaklingar ráða yfir sér sjálfir og upplýsingunum um sig. Sá sem ræður yfir lífi, líkama sínum og vistarverum er sá sem hefur sjálfsákvörðunarrétt og friðhelgi einkalífs.[6]

2.1. Mannréttindi - Friðhelgi einkalífs og vernd persónuupplýsinga

Upphaf mannréttindaákvæða má rekja til hins klassíska náttúruréttar, en John Locke mælti fyrst fyrir þeim kenningum á 17. öld. Kenningar John Locke fjalla um að innra með manninum er að finna rödd skynseminnar sem segir honum að virða rétt annars til lífs og frelsis, menn ættu að forðast að skaða hvern annan og fremur að leggja sig fram í að hjálpa öðrum. Þessar kenningar kveða á um að hver maður fæðist með ákveðin frelsisréttindi, rétt til lífs, rétt til eigna og rétt til að bjarga sér.[7] Það sem telst til mannréttinda eru ákveðin grundvallarréttindi sem og ákveðin frelsisréttindi einstaklinga, þ.á. rétt einstaklinga til að lifa sínu eigin lífi á sinn hátt, hafa skoðanir og taka ákvarðanir um athafnir sínar án þess að eiga á hættu að sæta utanaðkomandi afskiptum, sérstaklega af hálfu hins opinbera.

Mannréttindavernd á alþjóðavettvangi á ekki langa sögu, það var ekki fyrr en um miðja tuttugustu öldina sem ríki heimsins ákváðu í sameiningu að skuldbinda sig hvort öðru, þrátt fyrir þá miklu áherslu sem hafði verið á árum áður á grunnregluna um að virða skyldi regluna um fullveldi ríkja.[8] Sameinuðu þjóðirnar voru stofnaðar í þeim tilgangi að tryggja heimsfriðinn og friðsamleg samskipti þjóða og í inngangsorðum stofnsáttmála Sameinuðu þjóðanna segir að markmið þeirra sé að bjarga komandi kynslóðum frá hörmungum ófriðar, enda var seinni heimstyrjöldin þá nýafstaðin. Þá var það jafnframt markmið að staðfesta að nýju trú á grundvallarréttindi manna, virðingu þeirra og gildi, jafnrétti kynjanna og allra þjóða óháð stærð þeirra. Í mannréttindayfirlýsingu Sameinuðu þjóðanna frá 1948 er að finna flest þau mannréttindaákvæði sem taka til borgaralegra og stjórnmálalegra réttinda, sem og helstu félagslegu og menningarlegu réttindi. Þá kemur skýrt fram að markmið aðildarríkja sé að efla og virða þessi réttindi. Þrátt fyrir að mannréttindayfirlýsingin hafi ekki verið bindandi þjóðréttarsamningur, þá ruddi hún brautina og lagði grunnin að eftirfarandi samvinnu um alþjóðlega mannréttindasamninga.[9] Í 12. gr. mannréttindayfirlýsingarinnar er að finna ákvæði sem kveður á um friðhelgi einkalífs en þar segir:

6 Sigrún Jóhannesdóttir, *Persónuverndarlög: skýringarrit* (Fons Juris 2015) 21.
7 Kjartan Gunnarsson, „Friðhelgi einkalífs“ (1978) 31 (3) Úlfljótur 171, 173.
8 Alþt. 1994-1995 A-deild, þskj. 389 - 297. mál., kafli IV.
9 sama heimild, kafli IV.

> *„Eigi megi að geðþótta raska einkalífi, fjölskyldulífi, heimili eða bréfskriftum nokkurs einstaklings, né heldur ráðast á æru hans eða mannorð. Ber öllum lagavernd gagnvart slíkum afskiptum eða árásum“*

Þann 4. nóvember 1950 var Mannréttindasáttmála Evrópu (e. European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR))[10] samþykktur í Róm af Evrópuráðinu þar er að finna í 8. gr. ákvæði sem tryggir friðhelgi einkalífs. Voru þá aðildarríki samningsins lagalega skuldbundin til að tryggja friðhelgi einkalífs sem og önnur borgaraleg og stjórnmálaleg réttindi. Þá má finna sambærileg ákvæði sem kveða á um friðhelgi einkalífs í öðrum alþjóðasamningum sem Ísland er aðili að.[11]

Upphaflega var markmiðið með skráningu ákvæða um vernd friðhelgi einkalífs í stjórnarskrá að veita borgurum vernd frá geðþóttaafskiptum stjórnvalda og löggæsluyfirvalda, sérstaklega í tengslum við rannsókn sakamála. Voru því gerðar skýrar kröfur um að lagaheimild þyrfti til húsleitar eða haldlagningu persónulegra skjala. Með aukinni tækniþróun á síðustu áratugum hefur aukist nauðsyn á ákvæðum er vernda friðhelgi einkalífs. Nú eru það ekki aðeins stjórnvöld sem geta nálgast og misnotað persónuupplýsingar einstaklinga, heldur einnig einstaklingar og lögaðilar. Af þeim sökum er ekki aðeins nauðsyn að vernda borgarana fyrir afskiptum stjórnvalda, heldur enn fremur til verndar borgurunum innbyrðis.[12] Hérlendis er í 71. gr. stjskr. kveðið á um rétt einstaklinga til friðhelgi einkalífs, sambærilegt ákvæði er að finna í 8. gr. Mannréttindasáttmála Evrópu sem öðlaðist lagagildi hér á landi þann 30. maí 1994 með lögum um mannréttindasáttmála Evrópu nr. 62/1994.

Í ákvæðum sem kveða á um friðhelgi einkalífs er ekki að finna neina skilgreiningu á hvað felst í hugtakinu sjálfu. Mannréttindadómstóll Evrópu[13] hefur þó skýrt hugtakið í dómaframkvæmd þannig að í einkalífi felilst vernd á andlegu og líkamlegu sjálfræði manns en undir það fellur einnig auðkenni og sjálfsmynd manns og í raun allt það sem einkennir hann sem persónu gagnvart öðrum í samfélaginu og umhverfi sínu.[14] Af þessu er því ráðið að einstaklingar eiga rétt til að ráða nafni sínu, útliti, klæðnaði og fleiru sem tengist sjálfsmynd einstaklings. Þá má segja að aðrir hlutir eins og kynhneigð, kynfrelsi og réttur einstaklinga til

[10] Hér eftir MSE.
[11] Sem dæmi 17. gr. alþjóðasamnings Sameinuðu þjóðanna um borgaraleg og stjórnmálalegréttindi.
[12] Björg Thorarensen, „Friðhelgi einkalífs og fjölskyldu og réttur til að stofna til hjúskapar“ í Davíð Þór Björgvinsson o.fl. (ritstj.), *Mannréttindasáttmáli Evrópu: meginreglur, framkvæmd og áhrif á íslenskan rétt* (Mannréttindastofnun Háskóla Íslands, Lagadeild Háskólans í Reykjavík 2005) 285.
[13] Hér eftir MDE.
[14] Björg Thorarensen (n. 12) 292–293.

að velja hverjum þeir vilja vera í kynferðislegu sambandi við falli undir vernd friðhelgi einkalífs sem og fleiri atriði sem ekki er hægt að telja upp með tæmandi hætti.[15]

Þá er að finna dóma, bæði hérlendis og erlendis, sem staðfesta að undir verndarandlag friðhelgi einkalífs falli persónuupplýsingar. Þetta kemur meðal annars fram í *dómi Hæstaréttar frá 27. nóvember 2003 nr. 151/2003*. Í dómnum var fjallað um kröfu einstaklings á hendur íslenska ríkinu að ógilt yrði synjun landlæknis á beiðni um að heilsufarsupplýsingar úr sjúkraskrá látins föður hans yrðu ekki færðar í gagnagrunn á heilbrigðissviði. Þar sem ekki var hægt að tryggja að upplýsingarnar yrðu ópersónugreinanlegar leit Hæstiréttur svo á að sjúkraskrár hefðu að geyma yfirgripsmiklar upplýsingar um heilsufar manna, læknismeðferðir, lifnaðarhætti og félagslegar aðstæður, þar með talið um atvinnu og fjölskylduhagi. Þar sé að finna nákvæma greiningu á hver sá er sem upplýsingarnar varða. Þá hafa upplýsingar af þessum toga að geyma einhver brýnustu einkamálefni þess einstaklings sem á í hlut, án tillits til þess hvort þær geti talist honum til hnjóðs. Því var það talið ótvírætt að slíkar upplýsingar falla undir ákvæði 71. gr. stjskr. og sú grein veiti sérhverjum manni friðhelgi um einkalíf sitt. Var í niðurstöðu dómsins einnig tekið fram að til að tryggja friðhelgi einstaklingar verði löggjafinn að gæta þess að lög leiði ekki af sér raunhæfa hættu á að persónuupplýsingar komist í hendur annarra einstaklinga eða ríkisvaldsins, sem ekki eiga lögmætt tilkall til slíkra gagna.[16] Sama niðurstaða hefur fengist í málum sem farið hafa fyrir MDE, það er að söfnun og geymsla á upplýsingum um einkahagi og líf einstaklinga geti falið í sér skerðingu á friðhelgi einkalífs og falli undir verndarandlag 8. gr. MSE.

Þá má einnig sjá í athugasemdum við 9. gr. frumvarps, skýringar við 71. gr. stjskr., sem varð að stjórnskipunarlögum nr. 97/1995, en þar er skýrt tekið fram að skráning persónuupplýsinga geti talist vera brot gegn friðhelgi einkalífs, sbr. 71. gr. stjskr. En við mat á því hvort brotið sé gegn verndarandlagi ákvæðisins þá þurfi meðal annars að skoða hversu langt megi ganga í skipulagðri skráningu á lífsháttum einstaklinga og högum og meðferð slíkra upplýsinga. Að auki segir að með setningu skýrrar reglu um friðhelgi einkalífs er gert ráð fyrir að skyldan hvíli á ríkinu að forðast afskipti af einkalífi og persónulegum. En það eitt og sér dugar ekki til að einstaklingar njóti í raun friðhelgi einkalífs, því hættan á að friðhelgin verði brotin stafar ekki aðeins af ríkinu, heldur einnig frá öðrum, bæði einstaklingum og lögaðilum. Verður því krafan um vernd friðhelgi einkalífs ekki aðeins sú að gætt sé að ríkið gangi ekki á

15 sama heimild 288.
16 Hrd. 27. nóvember 2003 í máli nr. 151/2003.

þennan rétt, heldur einnig að sett séu ákvæði í almenna löggjöf til verndar einstaklingum í samskiptum þeirra innbyrðis og við lögaðila.[17]

Í 8. gr. sáttmála Evrópusambandsins um grundvallarréttindi[18] er að finna sjálfstætt ákvæði er kveður á um vernd persónuupplýsinga. Í 1. mgr. 8. gr. er lýst rétti einstaklinga til verndar á eigin persónuupplýsingum. Í 2. mgr. greinarinnar eru taldar upp þær meginreglur sem gilda um vinnslu persónuupplýsinga og rétt einstaklinga til aðgangs að gögnum sem snerta þá sjálfa. Þá er kveðið á um það í 3. mgr. að óháð eftirlitsstjórnvald skuli hafa eftirlit með þessum reglum. Með setningu þessa ákvæðis var vernd persónuupplýsinga skilið frá hefðbundnu ákvæði um vernd friðhelgi einkalífs sem er að finna í 7. gr. sáttmálans. Almennt hefur það verið talið nægja að skrá ákvæði um vernd friðhelgi einkalífs í stjórnarskrár ríkja, en hér gengur Evrópusambandið lengra hvað varðar vernd persónuupplýsinga.

Réttarreglur á sviði persónuverndar byggjast á þeirri forsendu að persónuupplýsingar séu þáttur í friðhelgi einkalífs einstaklinga.[19] Setning reglna um meðferð persónuupplýsinga í löggjöf er einn mikilvægasti þátturinn í að ríki uppfylli þá skyldu sem ákvæði um vernd friðhelgi einkalífs kveða á um. Hérlendis, sem og erlendis, hefur mótast sjálfstætt og umfangsmikið réttarsvið, persónuverndarréttur (e. Data Protection Law) með ítarlegu regluverki sem ríkin hafa sammælst um, enda hindra landamæri ekki flutning persónuupplýsinga. Af þeim sökum er afar mikilvægt að samræmt regluverk gildi milli ríkja sem og eftirlitið með því.[20]

2.2. Evrópureglur um persónuvernd

Evrópusambandið hefur verið í fararbroddi á heimsvísu hvað varðar löggjöf sem veitir persónuupplýsingum vernd, eða allt frá setningu Samnings Evrópuráðsins um vernd einstaklinga við vélræna vinnslu persónuupplýsinga nr. 108 frá 28. janúar 1981. Með honum var brotið blað í sögunni enda fyrsta lagalega bindandi alþjóðasamningurinn sem var samþykktur á réttarsviði persónuverndar.[21] Síðan þá hefur mikið vatn runnið til sjávar og persónuverndarlöggjöf Evrópusambandsins hefur þróast samhliða örum tæknibreytingum.

[17] Alþt. 1994-1995 A-deild, þskj. 389 - 297. mál., athugasemdir við 9. gr.
[18] Sáttmálinn var settur í stofnlög sambandsins með Lissabon-sáttmálanum sem tók gildi 1. desember 2009.
[19] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,,2. Íslenskar réttarreglur um persónuvernd og þróun þeirra.
[20] sama heimild.
[21] „Personal Data Protection | Fact Sheets on the European Union | European Parliament“ <https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection> skoðað 26. febrúar 2020.

2.2.1. Tilskipun Evrópusambandsins 95/46/EB

Evrópuþingið og ráðið setti tilskipun 95/46/EB þann 24. október 1995 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga (e. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)[22]. Við gerð tilskipunarinnar var fyrrnefndur samningur Evrópuráðsins nr. 108 að mestu leyti lagður til grundvallar.[23] Tilskipunin var sett til þess að ná tveim meginmarkmiðum. Annars vegar var lagt upp með vernd persónuupplýsinga og tryggt að með þær væri farið í samræmi við friðhelgi einkalífs. Hins vegar að tryggja frjálst flæði persónuupplýsinga á hinum innri markaði. Fyrir setningu tilskipunarinnar var ósamræmi reglna innan ríkja sambandsins farið að hindra flæði og valda vandræði í efnahagslegu sambandi ríkjanna.[24] Tilskipunin tekur bæði til vinnslu persónuupplýsinga af hálfu einkaaðila sem og opinberra aðila.

Eitt helsta einkenni tilskipunarinnar er að í henni var hugtakið persónuupplýsingar skilgreint mjög rúmt og skyldi ná til allra upplýsinga sem rekjanlegar eru til einstaklinganna sjálfra. Annað einkenni tilskipunarinnar var að meginreglur skyldu ávallt gilda um gæði gagna og vinnslu, almennar reglur um lögmæta vinnslu persónuupplýsinga en sérstakar reglur og önnur skilyrði fyrir vinnslu viðkvæmra persónuupplýsinga. Þá var hinum skráða tryggð ýmis réttindi og að sama skapi skyldu ákveðnar skyldur hvíla á ábyrgðaraðilanum. Ef hann rækir ekki skyldur sínar getur hann bakað sér refsi- og bótaábyrgð. Þá er ábyrgðaraðilanum heimilt að semja við vinnsluaðila til að annast vinnslu persónuupplýsinga sem hann ber ábyrgð á samkvæmt sérstakri heimild.[25]

Þá var með tilskipuninni mælt fyrir um starfsemi sjálfstæðra eftirlitsstofnana í hverju ríki, umræddar stofnanir skyldu hvorki lúta pólitísku boðvaldi, yfirráðum né efnislegri endurskoðun ákvarðana af hálfu annarra stjórnvalda. En ákvarðanir þeirra skyldi bera undir dómstóla. Að auki var að finna ákvæði þar sem sett voru skilyrði fyrir flutningi persónuupplýsinga til þriðju landa, að flutningurinn var óheimill nema ef þær væru fluttar til viðtakanda sem framkvæmdarstjórnin hefur viðurkennt. Jafnframt var kveðið á um starfshóp, hinn svonefnda 29. gr. starfshóp[26], sem sinna skyldi ráðgjafarhlutverki um persónuverndarmálefni. Starfar hann sjálfstætt og vinnur að samræmdri framkvæmd persónuverndarlöggjafar í Evrópu.

[22] Hér eftir tilskipun 95/46/EB.
[23] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 3.3. Tilskipun Evrópusambandsins 95/46/EB.
[24] Sigrún Jóhannesdóttir (n. 6) 30.
[25] sama heimild 31.
[26] 29. gr. starfshópurinn er forveri persónuverndarráðsins.

Loks má nefna að í fimmta kafla tilskipunarinnar, sem bar kaflaheitið „CODES OF CONDUCT“, var að finna 27. gr. sem hvetja átti aðildarríki til að stuðla að setningu starfs- og siðareglna, svo kallaðra hátternisreglna fyrir einstaka atvinnugeira þar sem unnið er með persónuupplýsingar.[27] Var markmið sem stefnt var að með setningu ákvæða um hátternisreglur að stuðla að réttri framkvæmd ákvæða tilskipunarinnar sem og að samræma þær skyldur að sérþörfum hvers atvinnugeira.

Nokkur samtök fyrirtækja innan aðildarríkja ESB nýttu sér þessa leið sem tilskipunin veitti þeim. Meðal þeirra sem settu sér slíkar hátternisreglur eru samtökin Federation of European direct marketing eða FEDMA.[28] Hátternisreglur FEDMA voru þær fyrstu sem voru samþykktar af 29. greinar hópnum, var það gert þann 13. júní 2003, og fengu þær þá almennt gildi innan sambandsins, ferlið tók hins vegar nokkurn tíma þar sem fyrstu drögum að reglunum var skilað inn árið 1998.[29] Það sem tekið var fyrir í hátternisreglunum var meðal annars: Söfnun persónuupplýsinga vegna beinnar markaðssetningar, fjöldapóstsendingar, birting lista, upplýsingar um hvaðan upplýsingarnar eru fengnar og réttur einstaklinga til að mótmæla vinnslunni. Þá var jafnframt að finna í hátternisreglunum sérstök ákvæði varðandi vinnslu persónuupplýsinga barna vegna þátttöku í leikjum þar sem hægt er að hljóta sérstök verðlaun eða sambærilega umbun. Þá var stofnuð sérstök persónuupplýsinganefnd innan FEDMA til þess að hafa eftirlit með hátternisreglunum. Var talið að hátternisreglurnar væru í fullu samræmi við tilskipunina sem og að fjalla um framkvæmd á flóknum vandamálum sem koma upp í tengslum við persónuvernd og beina markaðssetningu. Þannig uppfylltu þær skilyrði 27. gr. tilskipunarinnar.[30]

2.2.2. Persónuverndarreglugerðin 2016/697

Þann 25. janúar 2012 komu fyrstu tillögur að heildar endurskoðun á persónuverndarlöggjöfinni í almennu lagasetningarferli innan ESB. En undirbúningur við þær tillögur kom í kjölfar breytinga á stofnsamþykktum ESB með Lissabonsáttmálanum sem tók gildi 2009. Grundvöllur fyrir breytingunum á persónuverndarlöggjöfinni var lagður með nýjum ákvæðum um

[27] Alþt. 1999-2000 A-deild, þskj. 399 - 280 mál, V.3.9. Starfs- og siðareglur.
[28] FEDMA eru regnhlífasamtök um beina markaðssetningu á hinum Evrópska markaði, meðlimir samtakanna eru landssamtök um beina markaðssetningu innan ríkja Evrópu og þar undir eru um 350 fyrirtæki.
[29] Article 29 Data Protection Working Party, „Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing“ (13. júní 2003) 2 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf>.
[30] sama heimild 6.

persónuvernd í sáttmálanum.[31] Það er annars vegar í 16. gr. þar sem segir að einstaklingar eiga rétt á því vernd friðhelgi einkalífs taki einnig til persónuupplýsinganna þeirra. Mælt var fyrir um að Evrópuþingið og ráðið skuli setja reglur um vernd einstaklinga með hliðsjón af vinnslu persónuupplýsinga af hálfu stofnana á vegum sambandsins og aðilaríkjanna vegna starfsemi sem fellur undir lög sambandsins, sem og reglur um frjálsa miðlun þeirra. Að auki er kveðið á um að óháð yfirvöld skuli hafa eftirlit með því að slíkum reglum sé fylgt. Hins vegar er kveðið á um þetta í 114. gr. sáttmálans um starfshætti ESB að almennar aðgerðir Evrópuþingsins og ráðsins til að vinna að samræmingu á þeim ákvæðum laga og stjórnsýslufyrirmæla aðilaríkjanna sem beinast að stofnunum og starfsemi innri markaðarins.

Rúmum fjórum árum eftir að fyrstu tillögur að heildarendurskoðun persónuverndarlöggjafarinnar komu fram eða þann 27. apríl 2016, samþykkti Evrópuþingið nýja evrópska persónuverndarlöggjöf. Um var að ræða eina umfangsmestu breytingar á persónuverndarlöggjöfinni innan sambandsins í um tvo áratugi.[32]

Þrátt fyrir að ýmis kjarnaatriði úr tilskipun 95/46/EB halda enn gildi sínu[33] var hins vegar nauðsynlegt að gera ákveðnar breytingar á löggjöfinni til þess að sporna við sundurlausri framkvæmd persónuverndar innan sambandsins og þeirri réttaróvissu sem var yfirvofandi innan aðildarríkja. Meðal íbúa þar var algeng sú hugmynd að það væri mikil áhætta fyrir hendi við netnotkun sérstaklega með tilliti til verndar persónuupplýsinga einstaklinga.[34] Staðan var því orðin sú að vernd persónuupplýsinga nutu mismikillar verndar í aðildarríkjunum og var því hindrun í vegi fyrir frjálsu flæði persónuupplýsinga innan og milli ríkja sambandsins. Þessi hindrun á frjálsri för innan sambandsins hafði því áhrif á atvinnustarfsemi, meðal annars að því leyti að það raskaði samkeppni. Jafnframt gátu stjórnvöld ekki sinnt störfum sínum samkvæmt lögum sambandsins og var því nauðsynlegt að gera umræddar breytingar á persónuverndarlöggjöfinni.[35]

Með setningu reglugerðarinnar var markmiðið að gera bót á þessum vanköntum en um leið takast á við breyttan veruleika frá tíma eldri löggjafar. Meðal þeirra breytinga sem kynntar voru til leiks var ný meginregla, öryggisreglan, en hún kveður á um skyldu aðila sem sjá um vinnslu persónuupplýsinga til að tryggja öryggi þeirra í hvívetna. Þá var einnig kynnt til leiks

[31] European Union Agency for Fundamental Rights og Council of Europe, *Handbook on European Data Protection Law: 2018 Edition* (Publications Office of the European Union; ©2018 2018) 28.
[32] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 1. Inngangur.
[33] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 10. liður formála.
[34] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, 4.2. Markmið reglugerðarinnar. .
[35] sama heimild, 4.2. Markmið reglugerðarinnar.

ný skylda fyrir ábyrgðaraðila og vinnsluaðila og nefnist hún ábyrgðarskyldan. Hana á að beita samhliða meginreglunum og var með henni lögð enn meiri áhersla á ábyrgð þeirra sem vinna með persónuupplýsingar að fara að lögunum en jafnframt að þeir aðilar geti sýnt fram á fylgni við ákvæði löggjafarinnar. Aðrar breytingarnar fólu meðal annars í sér að veita einstaklingum betri stjórn yfir persónuupplýsingum sínum og hins vegar að einfalda lagaumhverfið fyrir fyrirtæki og stofnanir sem vinna með persónuupplýsingar.[36] Að sama skapi var stefnt að því að efla hinn stafræna innri markað Evrópu og tryggja öryggi persónuupplýsinga í viðskiptum, sem og veita fyrirtækjum réttaröryggi þar sem þau vinna eftir skýrum og samræmdum reglum. Með því virkar hinn innri markaðurinn eins og honum er ætlað að gera.[37] Var markmiðið að ryðja úr vegi hindrunum á flæði persónuupplýsinga með setningu samræmdrar og öflugrar verndar fyrir alla einstaklinga innan allra ríkja ESB. Ætti vernd réttinda og frelsis einstaklinga í tengslum við persónuupplýsingar þeirra fyrir vikið að vera sú sama innan aðildarríkja. Var þá tryggð einsleit og samræmd beiting á reglunum sem vernda grundvallarréttindi og frelsi einstaklinga í tengslum við vinnslu persónuupplýsingar.[38]

Svo verndin sé skilvirk er mikilvægt að eftirlit sé eins innan aðildarríkjanna en jafnframt er mikilvægt að sömu viðurlög gildi við brotum gegn ákvæðum til verndar persónuupplýsingum í aðildarríkjunum.[39] Voru þar með kynntar til sögunnar stórauknar sektarheimildir til handa eftirlitsstjórnvalda innan aðildarríkjanna. Upphæðirnar eru stigskiptar eftir alvarleika brots og koma til með að verða lagðar á ábyrgðaraðila og vinnsluaðila óháð stærð þeirra. Var það gert í þeim tilgangi að efla og samræma álagningu viðurlaga vegna brota á ákvæðum reglugerðarinnar og skal því hvert eftirlitsstjórnvald hafa heimild til að leggja á stjórnvaldssektir.[40]

Jafnframt eru aðildarríkin hvött til að taka sérstakt tillit til þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja.[41] Þá voru ákvæði eldri laga um hátternisreglur uppfærð og einnig var kynnt til sögunnar nýtt heilstætt vottunarfyrirkomulag. Þau ákvæði sem fjalla um þessar leiðir er að finna í fimmta þætti fjórða kafla reglugerðarinnar, þ.e. 40. gr. – 43. gr. pvrg. En þar er að finna valkvæðar leiðir sem fyrirtæki og stofnanir geta nýtt sér til að sýna fram á að

[36] Frans Timmermans, Andrus Ansip og Věra Jourová, „Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection“ (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_1403> skoðað 27. febrúar 2020.
[37] sama heimild.
[38] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 10. liður formála.
[39] sama heimild, 11. liður formála.
[40] sama heimild, 150. liður formála.
[41] sama heimild, 13. liður formála.

vinnslustarfsemi þeirra sé í samræmi við ákvæði reglugerðarinnar. Þessar valkvæðu leiðir geta spilað lykilhlutverk í reglufylgni ábyrgðaraðila og vinnsluaðila við nýtingu og skráningu persónuupplýsinga, enda geta þessar leiðir hjálpað þessum aðilum að uppfylla ábyrgðarskylduna. Tekið er sérstaklega fram í ákvæðum reglugerðarinnar sem fjalla um hátternisreglurnar og vottunina að það eigi að taka sérstakt tillit til lítilla og meðalstórra fyrirtækja við framkvæmd þeirra. Fjallað verður sérstaklega um þessar leiðir í síðari köflum ritgerðarinnar.

Reglugerðinni var því ætlað að skapa réttarvissu og gagnsæi gagnvart fyrirtækjum, með því að tryggja öllum einstaklingum í aðildarríkjum ESB sömu lagalega bindandi réttindi og skyldur. Sama ábyrgð lögð á herðar ábyrgðaraðilum og vinnsluaðilum sem tryggir sambærilegt eftirlit með vinnslu persónuupplýsinga og sambærileg viðurlög í öllum aðildarríkjum, sem og skilvirkt samstarf milli eftirlitsstjórnvalda aðildarríkjanna.[42]

2.3. Eldri lög um persónuvernd nr. 77/2000

Þann 1. janúar 2001 tóku svo gildi lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000. Með þeim voru ákvæði tilskipunar 95/46/EB leidd í lög og uppfyllti löggjafinn þá skyldu Íslands samkvæmt EES-samningnum með innleiðingu afleiddrar löggjafar ESB í landsrétt.[43] Þar sem um var að ræða innleiðingu á tilskipun þá var hún tekin inn í landsrétt í samræmi við b. lið 7. gr. EES-samningsins og við þær aðstæður hafa stjórnvöld ríkjanna val um form og aðferð við innleiðinguna.

Ekki var innleitt sérstakt ákvæði um hátternisreglur í löggjöfina þrátt fyrir að slíkt ákvæði væri að finna í 27. gr. tilskipunarinnar. En líkt og áður var komið inn á þá var það ekki skylda fyrir ríkin að setja sérstakt ákvæði um setningu hátternisreglna heldur aðeins hvatt til þess af hálfu Evrópusambandsins. Var hins vegar farið þá leið við lagasetninguna að í 5. tl. 3. mgr. 37. gr. laganna yrði kveðið á um að það væri hlutverk Persónuverndar að aðstoða einstaka hópa og starfstéttir við gerð slíkra starfs- og siðareglna um persónuvernd.[44] Í gildistíð laga nr. 77/2000 eru engin dæmi um að hópar eða starfstéttir hafi sett sér hátternisreglur eða starfs- og siðareglur um persónuvernd eins og þær eru nefndar í lögunum.

Þá var ekki að finna ákvæði um vottunarfyrirkomulag enda er það nýtt ákvæði sem kom inn í löggjöfina með setningu persónuverndarreglugerðarinnar.

[42] sama heimild, 13. liður formála.
[43] EES-samningurinn hefur verið lögfestur hér landi og tók hann gildi þann 1. janúar 1994 með setningu laga um Evrópska efnahagssvæðið nr. 2/1993.
[44] Alþt. 1999-2000 A-deild, þskj. 399 - 280 mál, V.3.9. Starfs- og siðareglur.

2.4. Núgildandi persónuverndarlög

Þann 27. nóvember 2017 skipaði dómsmálaráðherra starfshóp sem falið var að semja frumvarp til innleiðingar á persónuverndarreglugerðinni eins og hún yrði aðlöguð að EES-samningnum. Setning nýrra laga sem myndu innleiða hina nýju persónuverndarreglugerð var alger forsenda fyrir þátttöku Íslands í samevrópsku regluverki um persónuvernd og vinnslu persónuupplýsinga.[45] Það var svo þann 6. júlí 2018 sem sameiginlega EES-nefndin tilkynnti að persónuverndarreglugerðin hefði verið tekin upp í EES-samninginn.[46]

Við innleiðingu reglugerðarinnar var farið þá leið að samhliða yrðu sett ný heildarlög sem gæfu heildstæða mynd af þeim reglum sem eru í gildi á réttarsviðinu þó að þá yrði óhjákvæmilega nokkur endurtekning á helstu kjarnaákvæðum reglugerðarinnar, þar sem skyldan samkvæmt a. lið 7. gr. EES-samningsins kveður á um að ríkjum ber að taka upp texta reglugerða sem slíka inn í landslög. Almennt er ekki heimilt að umorða eða breyta textanum við innleiðinguna.[47] Með þeirri aðferð var meðal annars hægt að setja inn í frumvarpið helstu athugasemdir við hvert ákvæði, sem átti þá einnig við um meginákvæði reglugerðarinnar, þar sem farið var yfir hvort um nýja reglu sé að ræða eða önnur mikilvæg atriði sem er að finna í lögskýringargögnum við reglugerðina.[48]

Markmið lagasetningarinnar var meðal annars 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 markað Evrópska efnahagssvæðisins.[49] Þá varð það hins vegar einnig til að lögfesta ákvæði reglugerðar Evrópusambandsins um persónuvernd eins og hún var tekin upp í EES-samninginn. Jafnframt að setja sérreglur til fyllingar við ákvæði reglugerðarinnar þar sem heimilt er að gera slíkt.[50]

Frumvarpið varð svo að lögum um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018[51] tóku þau gildi þann 15. júlí 2018. Þannig var því náð báðum þeim áföngum að lögfesta reglugerðina í heild sinni en einnig að setja ný heilstæð lög um vernd persónuupplýsinga þar sem fram koma helstu meginreglur á einum stað sem og þau sérákvæði

[45] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 7. Meginefni frumvarpsins og efnistök.
[46] „General Data Protection Regulation incorporated into the EEA Agreement | European Free Trade Association“ <https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291> skoðað 15. september 2019.
[47] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 7. Meginefni frumvarpsins og efnistök.
[48] Hér má nefna formálsorð reglugerðarinnar sem og álit og leiðbeiningar frá Evrópska persónuverndarráðinu.
[49] Hér eftir EES.
[50] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 5.1. Almennt.
[51] Hér eftir pvl.

sem gilda aðeins fyrir Ísland. Þá eru allar reglur um efnið og skýringar á meginefni þeirra aðgengilegar á einum stað og reglugerðin birt sem fylgiskjal með lögunum. Þetta er mikilvægt þar sem hin nýja persónuverndarlöggjöf hefur ekki aðeins áhrif á eitt sértækt svið, heldur hefur hún viðtæk áhrif fyrir samfélagið allt. Aðildarríkjum er heimilt að fella inn í landslög þætti úr reglugerðinni sem nauðsyn telst til að gera ákvæðin sem skýrust fyrir þá sem þau taka til.[52]

Með lögunum var því einnig verið að setja sérreglur til fyllingar og viðbótar við ákvæði reglugerðarinnar, þar sem ríki hafa ákveðið svigrúm til setja samkvæmt heimild í ákvæðum reglugerðarinnar. Persónuverndarreglugerðin hefur þá sérstöðu, umfram aðrar ESB-reglugerðir, að hún veitir aðildarríkjum hennar talsvert svigrúm til að setja sérreglur um ákveðin atriði, útfæra sum ákvæði hennar eða víkja frá þeim og í sumum tilvikum er skylda að festa sum ákvæðin í landslög.[53] Almennt hefur framkvæmdin við innleiðingu reglugerða frá ESB verið sú að þær ber að innleiða sem slíka, en það þýðir að texti þeirra er tekinn beint upp og hafa ríki ekki val á því hvernig þau innleiða gerðina, sbr. a. lið 7. gr. EES-samningsins.

Hvergi í persónuverndarlögunum nr. 90/2018 er að finna ákvæði sem kveða á um valkvæðar leiðir sem fimmti þáttur fjórða kafla persónuverndarreglugerðarinnar fjallar um. Af því leiðir að ákvæði reglugerðarinnar um hátternisreglurnar og eftirlit með þeim sem og vottunarferlið gildi hérlendis eins og þau koma fram í reglugerðinni. Hins vegar er kveðið á um hlutverk Persónuverndar, sem eftirlitsstjórnvalds, varðandi þessar valkvæðu leiðir, sbr. 9., 10. og 11. tl. 4. mgr. 39. gr. pvl. Persónuvernd ber samkvæmt þeim ákvæðum að hvetja til setningu hátternisreglna og gefa út álit vegna þeirra, sem og samþykkja viðmið um vottun og láta framkvæma reglubundna endurskoðun á vottunum sem og að birta drög að viðmiðum um faggildingu aðila sem hafa eftirlit með hátternisreglunum. Nánar verður vikið að hátternisreglum og vottun síðar í ritgerðinni.

Að lokum er mikilvægt að taka fram að samkvæmt 5. gr. laga nr. 90/2018 gengur texti reglugerðarinnar framar heldur en lögin ef þau stangast á. Verður því í þessar ritgerð almennt vísað til ákvæða reglugerðarinnar fremur en laga nr. 90/2018, er það gert til einföldunar þar sem að ekki öll ákvæði reglugerðarinnar voru tekin upp í lögin, nema þegar um er að ræða sérstaka ákvæði sem voru sérstaklega útfærð í lögunum, þá verður vísað til þeirra. Þetta á meðal annars við þegar sérstaklega er útfært hlutverk Persónuverndar sem eftirlitsstjórnvalds.

[52] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 8. liður formála.
[53] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, 5.1. Almennt.

3. Helstu hugtök og meginreglur

Í eftirfarandi kafla verður farið yfir hugtök og skilgreiningar sem skipta máli fyrir umfjöllunarefni ritgerðarinnar sem og meginreglurnar persónuverndarlöggjafarinnar. Skilningur þessa efnis er grundvallaratriði fyrir umfjöllun síðari hluta ritgerðarinnar, það er þegar kafað verður ofan í þær valkvæðu leiðir, samkvæmt fimmta þætti fjórða kafla reglugerðarinnar, og hvernig þær nýtast til að sýna fram á reglufylgni. Þá er mikilvægt að skilningur á helstu hugtökum sé til staðar sem og þýðingu meginreglnanna og hvernig þessir mismunandi þættir spila saman í framkvæmd laganna.

3.1. Helstu hugtök

Helstu hugtök varðandi efni persónuverndarreglugerðarinnar eru sett fram í 26 töluliðum 4. gr. pvrg., þó er þar ekki að finna skilgreiningar á öllum hugtökum sem snerta viðfangsefni þessarar ritgerðar og verða að auki reifuð önnur hugtök og skilgreint það sem telst mikilvægt.

Í 1. tl. 1. mgr. 4. gr. pvrg. kemur fram skilgreiningin á hvað felist í og hvað sé átt við þegar talað er um *persónuupplýsingar*. En það eru hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling[54]. Persónugreinanlegur einstaklingur er oft einnig getið sem hinn skráði einstaklingur eða hinir skráðu einstaklingar. Einstaklingur telst svo persónugreinanlegur ef unnt er að persónugreina hann beint eða óbeint hvort sem það sé með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, andlegu, lífeðlisfræðilegu, erfðafræðilegu, efnalegu, menningarlegu eða félagslegu tilliti. Er því alveg skýrt að hugtakið persónuupplýsingar á aðeins við um einstaklinga en nær hvorki til stofnanna né fyrirtækja eða lögpersóna. Kjarni hugtaksins lýtur því að því hvort upplýsingarnar séu rekjanlegar, beint eða óbeint, til einstaklings.[55] Við mat á því hvort upplýsingar séu persónugreinanlegar þá þarf að taka mið af öllum þeim aðferðum sem eðlilegt er að hugsa að ábyrgðaraðili eða annar beiti til að bera kennsl á viðkomandi einstakling. Því er mikilvægt að tekið sé mið af helstu tækninýjungum hvað snertir auðkenni eins og staðsetningargögn, netauðkenni og aðra þættir.[56] Þá nær hugtakið einnig til þeirra upplýsinga sem færðar hafa verið undir gerviauðkenni þar sem möguleiki er að rekja þær aftur til einstaklings með notkun tækni eða viðbótarupplýsinga, slík gögn skulu

[54] Hér eftir hinn skráði einstaklingur eða hinir skráðu einstaklingar
[55] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, um 3. gr.
[56] sama heimild, um 3. gr.

teljast til upplýsingar um persónugreinanlegan einstakling.[57] Hugtakið persónuupplýsingar skal túlkað frekar rúmt heldur en þröngt.[58] Í 9. gr. pvrg. er fjallað um vinnslu viðkvæmara persónuupplýsinga og hún háð sérstökum skilyrðum. Má segja að slík vinnsla sé óheimil nema eitt þeirra skilyrða sem talin eru upp í 2. – 4. mgr. 9. gr. séu uppfyllt. Til *viðkvæmra persónuupplýsinga* teljast kynþáttur eða þjóðernislegur uppruni, stjórnmálaskoðanir, trúarbrögð eða heimspekilegar sannfæringar og upplýsingar um þátttöku í stéttarfélagi. Þá eru þar einnig taldar upp erfðafræðilegar upplýsingar, lífkennaupplýsingar í því skyni að persónugreina einstakling, heilsufarsupplýsingar eða upplýsingar um kynlíf eða kynhneigð einstaklinga, sbr. 1. mgr. 9. gr. pvrg.

Fjallað er um *vinnslu* í 2. tl. 1. mgr. 4. gr. pvrg. Í vinnslu fellst aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar og þá skiptir ekki máli hvort vinnslan er sjálfvirk eða ekki. Þar undir heyrir á meðal annars söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlum með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtening eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging.

Hversu umfangsmikil vinnsla er og tegund persónuupplýsinganna er breytilegt milli fyrirtækja og mismunandi geira, en almennt innan sama geira er tilgangur vinnslunnar sá sami. Því geta samtök fyrirtækja nýtt hátternisreglur til þess að afmarka þær upplýsingar sem nauðsynlegar eru fyrir vinnsluna innan þess atvinnugeira. Slíkt væri jafnframt til hagsbóta fyrir hina skráðu einstaklinga, þar sem hægt væri að tryggja meðalhóf og tryggja upplýsingarétt sem stuðlar að betri vernd fyrir réttindi einstaklinga. Þá væri hægt að nýta vottunarfyrirkomulagið í tengslum við vinnslu viðkvæmra persónuupplýsingar, þar sem hægt væri að nýta sérstök innsigli eða merki til að sýna fram á að vinnsla sé í samræmi við ákvæði reglugerðarinnar. Sem dæmi gætu fyrirtæki eða stofnanir þar sem vinnsla heilsufarsupplýsinga fer fram nýtt sér vottun, þar gæfu persónuverndarmerki eða innsigli til kynna að vinnslan uppfylli skilyrði reglugerðarinnar fyrir viðkvæmar persónuupplýsingar.[59]

[57] 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 nr.54/2000 EES-viðbætir við Stjtíð EB 114., 26. liður formála.
[58] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, um 3. gr.
[59] European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (3. júní 2019) 21 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf> skoðað 22. janúar 2020.

Ábyrgðaraðili er sá sem ákvarðar einn eða í samvinnu við aðra tilgang og aðferðir við vinnslu persónuupplýsinga. Þetta getur verið einstaklingur, fyrirtæki, lögaðili, opinber stofnun eða hvaða annar aðili sbr. 7. tl. 4. gr. pvrg. Það er því ábyrgðaraðili sem ber ábyrgð á vinnslunni. Þá hefur í framkvæmd verið álitið sem svo að það sé lögaðilinn sem sé ábyrgðaraðili frekar en starfsmaður þess lögaðila sem ákveður um vinnsluna. Þetta kom meðal annars fram í *úrlausn Persónuverndar nr. 2010/906.* Kom þar fram að þrátt fyrir að skólahjúkrunarfræðingur hefði safnað heilsufarsupplýsingum um börn þá var Heilsugæsla höfuðborgarsvæðisins ábyrgðaraðilinn en ekki skólahjúkrunarfræðingurinn sem starfsmaður heilsugæslunnar.[60] Þá er það í höndum ábyrgðaraðilans að gæta þess að vinnslan eigi sér lagastoð og uppfylli skilyrði meginreglna um vinnslu. Jafnframt ber ábyrgðaraðili ábyrgð á því að innleidd sé viðeigandi persónuverndarstefna, til þess að gætt sé að gagnsæi vinnslunar. Af ákvæðum reglugerðarinnar er ljóst að ábyrgð ábyrgðaraðilans er mikil það er hann sem þarf að gæta þess að áður en vinnsla hefst sé gripið til viðeigandi tæknilegra og skipulagslegra ráðstafanna.

Í reglugerðinni er einnig að finna heimild til þess að fleiri en einn ábyrgðaraðili ákveði tilgang vinnslunnar og hvaða aðferðir skuli nýta við hana, sbr. 26. gr. pvrg. Þeir þurfa þó að skipta með sér verkum, hvaða ábyrgð hvor þeirra beri á vinnslunni og að uppfyllt séu skilyrði reglugerðarinnar. Skal þetta gert með samkomulagi sem sé aðgengilegt hinum skráðu einstaklingum. Ábyrgðaraðilum eru jafnframt veittar ákveðnar valkvæðar leiðir til þess að tryggja að vinnslan uppfylli skyldur löggjafarinnar, þær leiðir eru hátternisreglur og vottun, óháð því hvort þeir séu einir ábyrgðaraðilar að vinnslunni eða í sameiningu.

Ef algent er innan ákveðinna atvinnugeira að fleiri en einn sé ábyrgðaraðili, þá er hægt að nýta hátternisreglur til þess að skýra út hvernig best sé að takast á við slíkar aðstæður. Þetta getur sérstaklega átt við um upplýsingatæknigreirann en þar eru oftar en ekki fleiri en einn aðili sem smíða hugbúnað. Þar geta hátternisreglur verið til hagsbóta fyrir fyrirtæki og leiðbeint þeim hvernig skal uppfylla skilyrði laganna.

Í 8. tl. 1. mgr. 4. gr. pvrg segir að *vinnsluaðili* sé hver sá einstaklingur, lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila. Vinnsluaðila er aðeins heimilt að sjá um vinnslu persónuupplýsinga og ber þeim skylda til að starfa í samræmi við fyrirmæli ábyrgðaraðila. Þá ber ábyrgðaraðila og vinnsluaðila að gera með sér vinnslusamning samkvæmt. 4. mgr. 28. gr. pvrg. en það er ný regla sem kom inn með reglugerðinni. Jafnframt er aðeins heimilt fyrir ábyrgðaraðila að gera samning við annan aðila til að sjá um vinnslu persónuupplýsinga þegar hann hefur fengið nægilega tryggingu fyrir því

[60] Úrskurður Persónuverndar nr. 2010/906, 17. ágúst 2011.

að vinnsluaðili geri viðeigandi tæknilegar ráðstafanir til að vinnslan uppfylli kröfur reglugerðarinnar og að réttindi skráðra einstaklinga séu nægilega tryggð, sbr. 28. gr. pvrg. Vinnsluaðili getur meðal annars verið aðili sem þróar upplýsingakerfið eða gerir við og viðheldur hugbúnaði sem varðveitir persónuupplýsingar og hefur aðgang að þeim.[61]

Í reglugerðinni er fjallað um *örfyrirtæki, lítil og meðalstór fyrirtæki* (hér eftir lítil og meðalstór fyrirtæki). Í persónuverndarreglugerðinni er ekki að finna skilgreiningu á því hvað telst vera lítil og meðalstór fyrirtæki, því er nauðsynlegt að skilgreina hugtakið. Í formálsorðum reglugerðarinnar segir að við skýringu á hugtökunum örfyrirtæki, lítil og meðalastór fyrirtæki skal byggja á 2. gr. viðaukans við tilmæli framkvæmdastjórnarinnar nr. 2003/361/EB.[62] Markmiðið með skilgreiningu tilmælanna er að stuðla að samræmdri og árangursríkri beitingu, þar sem tryggðar eru þær undanþágur og sá stuðningur sem í boði er fyrir lítil og meðalstór fyrirtæki sé aðeins veittur þeim sem sannarlega falla undir skilgreininguna og þurfa á að halda.[63] Eins og fyrr segir þá er að finna skilgreininguna á hugtökunum í 2. gr. tilmælanna, þar eru viðmið notuð við skilgreininguna, annars vegar um fjölda starfsfólks og hins vegar fjárhagsleg viðmið. Í flokknum *örfyrirtæki* teljast fyrirtæki sem hafa færri en 10 starfsmenn og ársvelta þeirra og/eða efnahagsreikningur er undir 2 milljónum evra. Í næsta flokki eru *lítil fyrirtæki* sem eru skilgreind sem þau fyrirtæki sem hafa færri en 50 starfsmenn og ársvelta og/eða efnahagsreikningur undir 10 milljónum evra. Loks þá eru í flokknum *meðalstór fyrirtæki* sem hafa færri en 250 starfsmenn og ársvelta þeirra fer ekki yfir 50 milljónum evra og/eða efnahagsreikningurinn fer ekki yfir 43 milljónum evra.

Eftirlitsyfirvald eða *eftirlitsstjórnvald* er sjálfstætt opinbert yfirvald sem aðildarríki kemur á fót samkvæmt 51. gr. pvrg., sbr. 22. tl. 4. gr. pvrg. Í þýðingu á reglugerðinni hefur verið notað hugtakið eftirlitsyfirvald, en það er þýðing af enska hugtakinu „supervisory authority“, í íslensku lagamáli hefur löngum verið notast við orðið eftirlitsstjórnvald í stað þess að vísa til orðsins eftirlitsyfirvald sem vart fyrir finnst í íslenskum lögum.[64] Í þessari ritgerð verður orðið eftirlitsstjórnvald notað um stofnunina Persónuvernd hér á landi og sambærilegar stofnanir aðildarríkja EES enda vísar það beint til hugtaksins stjórnvald sem hefur lögformlega merkingu samkvæmt stjórnsýslulögum nr. 37/1993.

61 Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, Um 3. gr. 7. Vinnsluaðili.
62 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 13. liður formála.
63 European Union, *User Guide to the SME Definition.* (Publications Office of the European Union 2017) 4 <http://op.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1> skoðað 17. maí 2020.
64 Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,7. Meginefni frumvarpsins og efnistök.

Persónuvernd fer með eftirlit með framkvæmd laga um persónuvernd sem eftirlitsstjórnvald og gætir því að farið sé að lögum og reglum um vinnslu persónuupplýsinga og ef mistök eiga sér stað þá skuli bætt sé úr annmörkum og mistökum. Þá úrskurðar Persónuvernd í ágreiningsmálum um vinnslu persónuupplýsinga. Persónuvernd er sjálfstæð stofnun sem hefur sérstaka stjórn og af því leiðir að hún tekur ekki við fyrirmælum frá stjórnvöldum eða öðrum aðilum, né verður ákvörðunum hennar skotið til annarra stjórnvalda, sbr. 52. gr. pvrg., enda er sjálfstæðið talið vera einn grunnþátturinn í því að tryggja vernd einstaklinga vegna vinnslu persónuupplýsinga.[65]

Í persónuverndarreglugerðinni er ekki að finna neina skilgreiningu á hugtakinu *vottun*, en kveðið er á um vottun í 42. gr. og 43. gr. pvrg. En almennt er vottun skilgreind sem yfirlýsing eða staðfesting á samræmingu við staðlað form eða aðferð. Alþjóðlegu staðlasamtökin (e. International Organization for Standardization, hér eftir ISO) skilgreina vottun sem „Skrifleg ákvörðun útgefin af óháðri stofnun í formi skírteinis, um að viðkomandi vara, þjónusta eða kerfi uppfylli fyrirfram ákveðnar kröfur.“[66] Vottun er einnig skilgreind sem samræmismat framkvæmt af þriðja aðila.[67]

Hugtökin *vottunarfyrirkomulag, persónuverndarinnsigli og persónuverndarmerki* eru ekki skilgreind í persónuverndarreglugerðinni, en í fimmta þætti fjórða hluta reglugerðarinnar er mikið fjallað um þessi hugtök. Oftar en ekki er vitnað í öll þessi þrjú hugtök saman í persónuverndarreglugerðinni, enda tengjast þau öll þeim ákvæðum sem kveða á um vottun 42. gr. og 43. gr. pvrg. Vottun er önnur þeirra valkvæðu leiða sem fjallað verður um í síðari köflum ritgerðarinnar og fyrirtæki geta nýtt til þess að sýna fram á fylgni við ákvæði reglugerðarinnar. Líkt og áður hefur komið inn á þá má skilgreina að vottun sé staðfesting á samræmingu við fyrirfram ákveðna aðferð við vinnslu persónuupplýsinga. *Innsigli* eða *merki* eru almennt notuð til þess að skrá að staðfest sé samræmi við vottunarferli. Geta þetta verið almennar merkingar eða vörumerki sem gefa til kynna að vottun hafi verið framkvæmd og metið sem svo að vara, þjónusta eða kerfi sé í samræmi við fyrirfram skráða staðla og tilgreind skilyrði séu uppfyllt.[68] Vottunarfyrirkomulagi reglugerðarinnar er ætlað að veita vottun vegna persónuverndar ásamt persónuverndarinnsiglum og persónuverndarmerkjum til að sýna fram á að vinnsla

65 C-518/07 European Commission g. Federal Republic of Germany [2010] ECR I-1885.
66 Þýðing höfundar á: „the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.“
67 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (n. 59) 8.
68 sama heimild.

ábyrgðaraðila og vinnsluaðila sé í samræmi við ákvæði reglugerðarinnar, sbr. 1. mgr. 42. gr. pvrg.

Viðmið vottunar eru þau viðmið sem vinnslustarfsemi eða vinnsluaðgerð fyrirtækja og stofnanna eru metin frá til þess að þær geti hlotið vottun, en í því felst að það er að vinnslustarfsemin hafi verið metin og staðfest.[69]

Hlutur sem vottun snýr að (e. Target of Evaluation). Það er í raun skilgreint sem það fyrirbæri sem vottunin snýr að. Í skilningi ákvæða persónuverndarreglugerðarinnar um vottun á þetta við um þær vinnsluaðgerðir eða hlutar vinnslunnar sem metnar eru við vottun,[70] sem dæmi þá getur tegund persónuupplýsinga verið hluturinn sem vottunin snýr að, eða tæknilegar lausnir sem nýttar eru í vinnslu ábyrgðaraðila eða vinnsluaðila.[71]

Kveðið er á um *hátternisreglur* í fimmta þætti fjórða kafla persónuverndarreglugerðarinnar, en þar er átt við reglur sem samtök, sem fram koma fyrir hönd ákveðinna atvinnugreina eða atvinnugeira, setja sér til að uppfylla skyldur fyrirtækjanna innan geirans gagnvart persónuverndarlöggjöfinni. Hátternisreglur eru valkvæð leið til að sýna fram á reglufylgni samkvæmt persónuverndarlöggjöfinni.[72] Hátternisreglur eiga að endurspegla þarfir þess atvinnugeira og þeirra fyrirtækja sem tilheyra honum. Markmið reglnanna ætti vera að styrkja fyrirtæki á hagkvæman hátt til að laga starfsemi þess geira að persónuverndarlöggjöfinni.

Eigendur hátternisreglna (e. code owners) eru ekki skilgreindir sérstaklega í persónuverndarlöggjöfinni. Þegar samtök fyrirtækja eða aðrir aðilar semja hátternisreglur þá er talað um þá sem eigendur hátternisreglna. Í 2. mgr. 40. gr. er samtökum og öðrum aðilum, sem og fulltrúum flokka ábyrgðaraðila eða vinnsluaðila heimilt að semja hátternisreglur. Sérstaklega er kveðið á um að hvetja skuli slík samtök til þess að setja sér hátternisreglur innan marka persónuverndarlöggjafarinnar, til að einfalda beitingu hennar. Þeir aðilar geti við

69 Information Commissioner's Office, „UK additional accreditation requirements for certification bodies (A.43(1)(b))" 2 <https://ico.org.uk/media/for-organisations/documents/2617241/uk-additional-accreditation-requiremenets-202002.pdf> skoðað 25. maí 2020.
70 sama heimild.
71 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0" (n. 59) 17.
72 European Data Protection Board, „Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 version 2.0" (4. júní 2019) 7 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf> skoðað 3. mars 2020.

setningu reglnanna haft hliðsjón af sérstökum eiginleiknum þeirrar vinnslu sem fer fram innan þeirra atvinnugeira og í samræmi við þarfir meðlima samtakanna.[73]

Evrópska persónuverndarráðið hefur gefið út leiðbeiningar um framkvæmd á hinum valkvæðu leiðum. Hins vegar, eins og komið verður nánar að í síðari köflum, er framkvæmd á þeim reglum sem tengjast þessum hugtökum ekki alltaf skýr en vikið verður að henni sérstaklega í 4. kafla ritgerðarinnar og þá er gott að hafa skilgreint hugtökin svo auðveldara sé að ná utan um efni þeirra kafla.

3.2. Meginreglur um vinnslu persónuupplýsinga

Auk þess að þekkja helstu hugtökin er jafnframt mikilvægt að gera sér grein fyrir túlkun og beitingu meginreglna löggjafarinnar. Þær grundvallarreglurnar sem gilda um alla vinnslu persónuupplýsinga er að finna í 5. gr. pvrg. Ef ekki er hagað vinnslu í samræmi við meginreglurnar þá er ekki hægt að halda því fram að vinnslan sé lögmæt þó hún samrýmist einhverri af þeim heimildum sem finna má í a. til f. lið 1. mgr. 6. gr. pvrg, sbr. 1. - 6. tl. 1. mgr. 9. gr. pvl.[74] Sem dæmi þá getur vinnsla ekki byggt á samþykki nema hún sé einnig sanngjörn.[75] Hér verður stiklað á stóru hvað felst í meginreglunum og nefnd dæmi um hvernig má nýta hátternisreglur til að gæta þess að þeim sé fylgt í framkvæmd. Ekki verða nefnd dæmi varðandi vottunina enda er með henni fremur verið að staðfesta að vinnsla, þess aðila sem hlýtur vottun, sé í samræmi við ákvæði meginreglnanna.

3.2.1. Sanngirnisreglan

Í meginreglunni um sanngirni felst fyrst og fremst að ávallt skal gæta þess að haga vinnslu með lögmætum, sanngjörum og gagnsæjum hætti gagnvart hinum skráða, sbr. a. lið 5. gr. pvrg. Af þessu leiðir að einstaklingum á að vera ljóst hvenær söfnun, skoðun eða vinnsla er á persónuupplýsingum þeirra og þá að hvaða marki og hvort eða hvernig þær verða unnar.[76] Með sanngirni er því átt við að vinnslan sé svo skiljanleg fyrir hinn skráða og þá einnig að ekki sé

[73] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 98. liður formála.
[74] Páll Hreinsson, „Ritröð Lagastofnunar Háskóla Íslands“ í Viðar Már Matthíasson (ritstj.), *Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála* (Lagastofnun Háskóla Íslands 2007) 25.
[75] Article 29 Data Protection Working Party, „Opinion 15/2011 on the definition of consent“ (13. júlí 2011) 34 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> skoðað 12. febrúar 2020.
[76] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 39. liður formála.

reynt að fara með vinnsluna leynt eða hún hulin hinum skráða.[77] Vinnsla persónuupplýsinga telst lögmæt þá verður hún að fara fram með samþykki þess skráða eða vinnslan að byggja á örðum lögmætum grundvelli samkvæmt lögunum og reglugerðinni, eða öðrum grundvallarreglum um persónuvernd og friðhelgi einkalífs.[78] Vinnslan telst ólögmæt ef tilgangur hennar samrýmist ekki almennum sjónarmiðum um persónuvernd. Meginreglan um gagnsæi krefst því þess að hvers kyns upplýsingar sem tengjast vinnslu persónuupplýsinga séu aðgengilegar og auðskiljanlegar, settar fram á skýru og einföldu máli. Reglan um gagnsæi tekur því sérstaklega til þeirra atriða að hinum skráða á að vera ljóst hver sé í raun ábyrgðaraðilinn og hver sé tilgangurinn með vinnslunni.[79]

Til þess að sýna fram á fylgni við sanngirnisregluna getur ábyrgðaraðila að setja sér persónuverndarstefnu vegna vinnslunnar sem sé aðgengileg hinum skráðu einstaklingum hvort sem það sé á heimasíðu, í skilmálum eða senda slíka tilkynningu til þeirra. Í persónuverndarstefnunni væri komið inn á atriði eins og lagalegan grundvöll vinnslunnar. Það getur hins vegar verið vandasamt verkefni fyrir lítil fyrirtæki að setja sér heildstæða persónuverndarstefnu og koma henni til áleiðis til hinna skráðu einstaklinga. Þar sem þau búa almennt ekki yfir þekkingu á persónuverndarlöggjöfinni. Það sem gæti orðið til þess að fleiri ábyrgðaraðilar myndu uppfylla skylduna væri með því að setja leiðbeiningar um hvernig hægt sé að setja slíka stefnu í hátternisreglum innan atvinnugeirans. Þetta getur átt sérstaklega vel við ef um einsleita vinnslu er að ræða innan geirans, þá væri hægt að setja upp format fyrir persónuverndarstefnu sem aðila að hátternisreglunum geta útfært fyrir sína vinnslustarfsemi. Með slíkri framkvæmd væru ábyrgðaraðilar burt séð frá stærð sinni og getu nokkuð öryggir um að uppfyllt sé krafa sanngirnisreglunnar.

3.2.2. Tilgangsreglan

Meginreglan um tilgang vinnslu er ein af grundvallarreglunum á sviði persónuverndarréttarins. Reglan er nátengd sanngirnisreglunni, því ef tilgangurinn er skýr og einstaklingar gera sér grein fyrir hverju má búast, þá má leiða líkur að því að það muni auka gagnsæi og tryggja en fremur lögmæti vinnslunnar. Það sem felst í reglunni er að öll vinnsla persónuupplýsinga verður að vera gerð í fyrirfram ákveðnum og vel skilgreindum tilgangi, en aðeins má nýta

[77] Sigrún Jóhannesdóttir (n. 6) 214.
[78] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 40. liður formála.
[79] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, um 8. gr.

persónuupplýsingarnar ef það rúmast innan upphaflegs tilgagns vinnslunnar.[80] Tilgangsregluna er að finna í b. lið 1. mgr. 5. gr. pvrg. og í henni felst að persónuupplýsingar eru fengnar í skýrt tilgreindum, lögmætum og málefnalegum tilgangi og þær séu ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Ef vinnsla fer ekki fram í samræmi við þessa reglu, óháð því hvort hinn skráði hafi samþykkt vinnsluna, þá er vinnslan ólögmæt. Ábyrgðaraðilanum ber að ákveða tilgang vinnslunnar fyrirfram og má ekki varðveita persónuupplýsingar með það fyrir sjónum að hann gæti notað þær síðar meir.[81]

Hægt væri að nýta hátternisreglurnar til þess að sýna fram á fylgni við þessa reglu sérstaklega innan atvinnugeira þar sem tilgangur vinnslunnar er skýr. Ef sett væri sett ákvæði í hátternisreglurnar þar sem kæmi fram hver tilgangur vinnslunnar væri þá þyrftu meðlimir aðeins að fylgja þeim reglum og þar með sýna fylgni við tilgangsregluna.

3.2.3. Meðalhófsreglan

Samkvæmt meginreglunni sem er að finna í c. lið 1. mgr. 5. gr. á ávallt að gæta þess að haga vinnslunni með þeim hætti að það sé í réttu hlutfalli við það lögmæta markmið sem stefnt er að. Miðar reglan því að því að lágmarka gögn en í því felst að persónuupplýsingar ættu að vera nægilegar, viðeigandi og takmarkaðar við það sem nauðsynlegt er til að ná tilgangi vinnslunnar.[82] Reglan er því matskennd, en það þýðir að leggja þarf mat á það í hverju tilfelli fyrir sig hvort umrædd vinnsla sé nauðsynleg til að ná settu marki og að gætt sé að því að ekki fari fram söfnun, miðlun eða skrásetning ónauðsynlegra persónuupplýsingar. Sem dæmi þá er vinnuveitanda heimilt að halda skrá um forföll starfsmanna sinna en honum er ekki heimilt að skrá ítarlegri upplýsingar en honum er nauðsynlegt í þeim tilgangi til að uppfylla skyldur sínar.[83]

Vert er að nefna að reglan tekur ekki aðeins til vinnslu persónuupplýsinga heldur einnig til aðgangsstýringu að þeim, hversu ítarlegar upplýsingarnar eigi að vera og hversu lengi skuli varðveita þær.[84] Því mætti setja skilyrði fyrir vottun að fyrirtæki eða stofnun hafi virka aðgangsstýringu að persónuupplýsingum og þar með væri hægt að sýna fram á fylgni með reglunni.

[80] European Union Agency for Fundamental Rights og Council of Europe (n. 31) 122.
[81] Páll Hreinsson (n. 74) 26.
[82] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, um 8. gr.
[83] Peter Blume og Jens Kristiansen, *Databeskyttelse på arbejdsmarkedet* (Jurist- og Økonomforbundets Forlag 2002) 87.
[84] Sigrún Jóhannesdóttir (n. 6) 227.

Með hátternisreglum gætu fyrirtæki komið sér saman um hversu lengi þörf sé á að varðveita persónuupplýsingar eftir að einstaklingur hættir í viðskiptum. Þá væri hægt að sinna virku eftirliti með slíkri reglu. Jafnframt væri hægt að setja í hátternisreglur hvaða persónuupplýsingar eru nauðsynlegar fyrir vinnsluna og að óheimilt væri að safna öðrum en þeim sem þær kveða á um.

3.2.4. Áreiðanleikareglan

Ávallt verður að gæta þess að við vinnslu persónuupplýsinga þarf að gæta að þær séu áreiðanlegar og uppfærðar, séu réttar á þeim tímapunkti sem lögmæt vinnsla miðast við og endurspegli á hlutlægan hátt þann veruleika sem verið er að lýsa.[85] Áreiðanleikareglan kveður á um skyldu til að afmá eða leiðrétta persónuupplýsingar sem eru ekki réttar eða teljast ófullkomnar miðað við þann tilgang sem ætlað er að ná með vinnslunni. Markmið reglunnar miðar að því að tryggja gæði persónuupplýsinganna sem unnið er með og koma í veg fyrir að ófagmannleg eða óvönduð vinnsla valdi hinum skráða tjóni eða óhagræði.[86] Ábyrgðaraðila vinnslunnar ber því skylda til að grípa til ráðstafana til að tryggja að óáreiðanlegum persónuupplýsingum verði eytt eða þær leiðréttar.[87]

Til þess að þessari reglu sé fylgt eftir væri hægt að setja ákvæði í hátternisreglur þar sem fram kæmi þessi skylda. Þetta getur sérstaklega átt við þegar vinnsla persónuupplýsinga hefur bein áhrif á einstaklinginn, meðal annars vinnsla af hálfu fjármálafyrirtækja, þá gætu óáreiðanlegar upplýsingar haft áhrif og gæti eftirlit með hátternisreglunum spilað stór hlutverk. Möguleg útfærsla væri að skjalfesta í hátternisreglum hversu oft fyrirtækjum ber að yfirfara og uppfæra persónuupplýsingar til að tryggja áreiðanleika þeirra.

3.2.5. Persónugreiningarreglan

Í e. lið 1. mgr. 5. gr. er kveðið á um persónugreiningarregluna og samkvæmt henni ber að gæta þess að upplýsingar séu ekki á persónugreinanlegu formi lengur en þörf krefur. Samkvæmt reglunni er því mælt fyrir um að upplýsingar skuli varðveita á því formi þar sem ekki er unnt að bera kenns á skráða einstaklinga lengur en nauðsynlegt er miðað við tilgang vinnslunnar. Reglan snýr því að eiginleika vinnslunnar, að gætt sé að vinnslan sé ekki óendanleg, heldur aðeins að því marki sem nægir til að uppfylla tilganginn og af þeim sökum er reglan nátengd

[85] Páll Hreinsson (n. 74) 29.
[86] Sigrún Jóhannesdóttir (n. 6) 234.
[87] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 39. liður formála.

tilgangsreglunni. Við mat á því hvenær ber að eyða persónugreinanlegum gögnum er viðmiðið þegar hinn skráði getur orðið fyrir tjóni vegna vinnslu og/eða varðveislu persónuupplýsinga, enda vega hagsmunir ábyrgðaraðila af vinnslunni ekki þyngra en hins skráða.[88] Ef það er ómögulegt að eyða upplýsingunum í heild sinni, meðal annars ef aðrar sérreglur kveða á um varðveislu þeirra, þá gæti nægt að gera upplýsingarnar ópersónugreinanlegar. Markmiðið er að koma í veg fyrir að persónuupplýsingar safnist upp hjá ábyrgðaraðilum en í því fælist aukin áhætta fyrir friðhelgi einkalífs hins skráða.[89]

Í hátternisreglur mætti setja ákvæði í reglurnar þar sem kveðið er á um skyldu til að nýta dulkóðun eða gerviauðkenni, til þess að tryggja réttindi og frelsi hins skráða sem best.

3.2.6. Öryggisreglan

Með persónuverndarreglugerðinni kom ný meginregla inn í löggjöfina, það er öryggisreglan. Með setningu reglunnar sýnir löggjafinn að aukin áhersla er lögð á öryggi persónuupplýsinga. Vinnsla persónuupplýsinga á að vera framkvæmd með þeim hætti að viðeigandi öryggi sé til staðar, sbr. f. lið 1. mgr. 5. gr., jafnframt að um upplýsingarnar gildi trúnaður, sem felst meðal annars í því að takmarka aðgang og koma í veg fyrir óheimilan aðgang að upplýsinginum og jafnframt þeim búnaði sem notaður er við vinnsluna.[90] Meginreglan um öryggi persónuupplýsinga kveður því á um að gripið sé til nægilegra tæknilegra ráðstafanna til að vernda upplýsingarnar fyrir utanaðkomandi aðgangi að þeim, sem gæti orðið til þess að upplýsingum yrði breytt, stolið eða þeim eytt.[91]

Loks er vert að benda á að öryggisreglan endurspeglast í fjölda ákvæða reglugerðarinnar. Til þess að uppfylla ákvæði reglunnar er hægt að nýta hátternisreglurnar og vottun, það segir meðal annars í 3. mgr. 32. gr. pvrg. að nýta megi þessar leiðir til þess að sýna fram á að gripið hafi verið til nauðsynlegra ráðstafana til að tryggja viðunandi öryggi. Þetta væri meðal annars gert með því að setja ákvæði í hátternisreglurnar um að gripið verði til tæknilegra ráðstafana sem tryggja öryggi persónuupplýsingana, þar á meðal að gera skilyrði fyrir því að fyrirtæki nýti gerviauðkenni eða dulkóðun. Sem og að setja ákvæði um að fyrirtækjum ber að halda vinnsluskrá óháð stærð. Jafnframt gætu samtök fyrirtækja sem starfa í þeim atvinnugeirum þar sem mikil áhætta er fyrir réttindi og frelsi einstaklinga að setja í

88 Peter Blume, *Databeskyttelsesret* (4. udgave, Jurist- og Økonomforbundets forlag 2013) 85–86.
89 Páll Hreinsson (n. 74) 31.
90 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 39. liður formála.
91 European Union Agency for Fundamental Rights og Council of Europe (n. 31) 131.

hátternisreglur skilyrði um framkvæmd á mati á áhrifum á persónuvernd samkvæmt 35. gr. pvrg., þetta gæti meðal annars átt við fyrirtæki þar sem vinnsla viðkvæmra upplýsinga á sér stað, eins og heilsufarsupplýsingar.

3.3. Reglan um ábyrgðarskyldu

Reglan um ábyrgðarskylduna tók gildi við setningu persónuverndarreglugerðarinnar, er því um að ræða nýja reglu sem er að finna í 2. mgr. 5. gr. pvrg. Markmiðið með ábyrgðarskyldunni er að tryggja að kröfur löggjafarinnar um vernd persónuupplýsinga eigi að skila sér í framkvæmdinni. Ábyrgðarreglunni er ætlað að hafa þau áhrif að bæði ábyrgðaraðilar og vinnsluaðilar uppfylli skyldur sínar gagnvart löggjöfinni, það er að þeir fylgi þeim skyldum sem ákvæði löggjafarinnar kveða á um en jafnframt að þeir geti sýnt fram á fylgnina. Megin ábyrgðin hvílir þó á ábyrgðaraðilanum þar sem það er hann sem ber ábyrgð á vinnslunni. Markmið ábyrgðarskyldunnar er því bæði að styrkja stöðu ábyrgðaraðilans sem og þá ábyrgð sem á honum hvílir.[92] Má því segja að tvær skyldur felist í ábyrgðarskyldunni en það er að fyrirtæki og stofnanir, sem bera ábyrgð á vinnslu persónuupplýsinga, þurfa að fylgja meginreglum persónuverndarlöggjafarinnar en jafnframt þurfa þessir sömu aðilar að geta sýnt fram á það reglufylgnina.

Reglan um ábyrgðarskylduna er því ekki bein meginregla heldur mætti frekar líta á hana sem reglu sem eigi að beita samhliða meginreglunum sem taldar eru upp í a. – f. lið 1. mgr. 5. gr. pvrg.[93] Ábyrgðarskyldan er því drifkrafturinn að árangursríkri innleiðingu annarra meginreglna.[94] Þá birtist hún einnig í fjölda ákvæða, sem dæmi þá má segja að í reglunni um innbyggða og sjálfgefna persónuvernd samkvæmt 25. gr. pvrg. endurspeglist þær ríku kröfur sem gerðar eru til ábyrgðaraðila. Við ákvörðunartöku skal ábyrgðaraðili gera viðeigandi tæknilegar ráðstafanir, sem hannaðar eru til að framfylgja með skilvirkum hætti meginreglunum um persónuvernd. Þá ber honum einnig að grípa til viðeigandi ráðstafana til að tryggja að sjálfgefið sé að aðeins þær persónuupplýsingar séu unnar sem nauðsynlegt er til að uppfylla tilgang vinnslunnar.[95]

Í stuttu máli mætti segja að reglan endurspegli áhersluna sem finna má í löggjöfinni að ábyrgðaraðilar beri ríka skyldu til þess að vinnslan sé í samræmi við ákvæði reglugerðarinnar

92 Article 29 Data Protection Working Party, „Opinion 3/2010 on the principle of accountability“ 3 <https://www.dataprotection.ro/servlet/ViewDocument?id=654> skoðað 23. febrúar 2020.
93 sama heimild 10.
94 sama heimild 4.
95 Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, um 24. gr. 1-2. mgr.

og að gripið sé til þeirra tæknilegra og skipulagslegra ráðstafanna til að tryggja fylgnina[96] sem og að reglulega sé sýnt sé fram á árangur þeirra ráðstafana sem gripið hefur verið til.[97] Gagnsæi er jafnframt ómissandi þáttur í ábyrgðarskyldunni sem og fræðsla af hálfu ábyrgðaraðila. Enda skilar slíkt sér almennt í auknu trausti til ábyrgðaraðilans ef almenningur og hinir skráðir einstaklingar gera sér grein fyrir umfangi vinnslunnar, tilgangi hennar og hvaða ráðstafana gripið hefur verið til.

Í reglugerðinni eru settar fram mismunandi leiðir sem geta aðstoðað ábyrgðaraðila og vinnsluaðila til að sýna fram á að gripið hafi verið til viðeigandi tæknilegra og skipulagslegra ráðstafana og að ábyrgðarskyldan sé uppfyllt. Sumum þessara leiða ber aðilum skylda til að fylgja en aðrar eru valfrjálsar. Ómögulegt væri að tilgreina í löggjöfinni tæmandi lista af leiðum sem ábyrgðaraðilum eða vinnsluaðilum, í tilteknum atvinnugreinum eða þar sem tiltekin vinnslustarfsemi fer fram, ber að fylgja til þess að uppfylla ábyrgðarskylduna. Enda er vinnsla persónuupplýsinga frá einum aðila til annars er ólík og þarfir hvers og eins. Það er því hlutverk ábyrgðaraðilans að skilgreina hverjar eru hans þarfir.[98] Við mat á því hvaða ráðstafana ábyrgðaraðili eða vinnsluaðili skuli grípa til verður að taka mið af eðli, umfangi, samhengi og tilgangi vinnslunnar sem og þeirri áhættu sem vinnslan hefur í för með sér fyrir réttindi og frelsi einstaklinga.[99]

Má segja að hornstein ábyrgðarskyldu ábyrgðaraðilans sé að finna í 2. mgr. 5. gr. pvrg. en hins vegar er jafnframt að finna skýrt ákvæði um hvað felst í skyldu hans í 24. gr. pvrg., en það segir í 1. mgr:

> „*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*."

Af ákvæðinu er ljóst að það er alltaf matsatriði til hvaða ráðstafana ábyrgðaraðila ber að grípa til svo að ábyrgðarskyldan sé uppfyllt. Meðal þeirra leiða sem hægt er að grípa til, en þó ekki tæmandi taldar, eru meðal annars í fyrsta lagi að komið sé á verklag um vinnsluna áður en hún hefst. Í öðru lagi að hægt sé skrásetja persónuverndarstefnu, sem aðgengileg er

[96] sama heimild, um 8. gr.
[97] Article 29 Data Protection Working Party, „Opinion 3/2010 on the principle of accountability" (n. 92) 11.
[98] sama heimild 13.
[99] Persónuvernd, „Ábyrgðarskyldan" (*Persónuvernd. Þínar upplýsingar, þitt einkalíf.*) <https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/allar-spurningar-og-svor/abyrgdarskyldan> skoðað 23. mars 2020.

almenningi, um verndun persónuupplýsinga sem gildir við núverandi vinnslu sem og ef hefja á nýja vinnslu persónuupplýsinga. Í þriðja lagi geta ábyrgðaraðilar nýtt sér þá leið sem lögin kveða á um, og undir vissum kringumstæðum er skylda að fylgja, að tilnefna persónuverndarfulltrúa, sbr. 37. gr. pvrg. Í fjórða lagi er að veita starfsmönnum fræðslu, sérstaklega þeim sem koma að vinnslunni og setja upp aðgangsstýringar að persónuupplýsingum. Í fimmta lagi þá þarf að setja upp ferli um hvernig brugðist sé við öryggisbresti og hvernig skuli tilkynna um þegar brestur hefur átt sér stað. Í sjötta lagi er innleiðing á eftirliti með vinnslunni. Slíkt væri hægt að framkvæma með þátttöku í samþykktum hátternisreglum, sbr. 40. gr. pvrg., innan þess atvinnugeira sem ábyrgðaraðili eða vinnsluaðili er þátttakandi í. Jafnframt væri hægt að sækjast eftir vottun, sbr. 42. gr. pvrg., þar sem framkvæmt er eftirlit og tryggt að viðeigandi ráðstafanir séu ekki aðeins til staðar á pappír heldur einnig sé það virkt í framkvæmd vinnslunnar.[100]

Loks er vert að nefna að í 3. mgr. 24. gr. pvrg. er komið inn á nýtingu valkvæðra leiða persónuverndarreglugerðarinnar til þess að sýna fram á reglufylgnina. En í ákvæðinu segir: „*Sé samþykktum hátternisreglum 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*.“ Í næsta kafla ritgerðarinnar verða þessar valkvæðu leiðir skoðaðar með þeim augum að reyna komast að því hvernig ábyrgðaraðilar geta nýtt sér þær til þess að sýna fram á ábyrgðarskylduna.

[100] Article 29 Data Protection Working Party, „Opinion 3/2010 on the principle of accountability“ (n. 92) 11–12.

4. Valkvæðar leiðir til að sýna fram á reglufylgni

Í fimmta þætti fjórða kafla persónuverndarreglugerðarinnar er að finna leiðir sem ábyrgðaraðilum og vinnsluaðilum er heimilt að nýta sér til að sýna fram á reglufylgnina, en mikilvægt er að taka fram að þeim er aldrei skylt að gera slíkt.

Þessar valkvæðu leiðir eru annars vegar hátternisreglur og eftirlit með þeim og hins vegar vottun eða vottunarfyrirkomulag, persónuverndarinnsigli og persónuverndarmerki fyrir fyrirtæki og stofnanir í tengslum við vinnslu persónuupplýsinga. Báðum þessum leiðum, það er beitingu vottunar eða setningu samþykktra hátternisreglna, er ætlað að einfalda líf ábyrgðaraðila sem og vinnsluaðila með því að auka réttaröryggi þeirra gagnvart persónuverndarlöggjöfinni.[101] Þessum leiðum er einnig ætlað að auðvelda fyrirtækjum og stofnunum að uppfylla skyldur sínar gagnvart löggjöfinni, t.d. með því að veita þessum aðilum einfalda leið til þess að tryggja réttindi og frelsi hinna skráðu einstaklinga. Í 77. lið formála að persónuverndarreglugerðinni er lögð áhersla á þetta og segir þar að:

> *„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 hátternisreglur, viðurkennda vottun, viðmiðunarreglur frá persónuverndarráðinu eða ábendingar frá persónuverndarfulltrúa.“***[102]

Jafnframt er lögð áhersla á nýtingu þessara leiða í til að sýna fram á reglufylgni í 81. lið formála að persónuverndarreglugerðarinnar, sérstaklega hvað varðar ábyrgðarskyldu ábyrgðaraðilans, skv. 24. gr. pvrg., gagnvart vinnsluaðilanum en þar er tekið fram að:

> *„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 leita til 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 hátternisreglum eða samþykktu***

[101] Maximilian Grafenstein, „Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the „State of the Art“ of Data Protection-by-Design“ (Social Science Research Network 18. febrúar 2019) SSRN Scholarly Paper ID 3336990 14 <https://papers.ssrn.com/abstract=3336990> skoðað 28. apríl 2020.
[102] Áherslubreytingar höfundar.

vottunarfyrirkomulagi má nota það til að sýna fram á að ábyrgðaraðili uppfylli skuldbindingar sínar. *"*[103]

Því er ljóst að báðum þessum leiðum er ætlað að veita aukið réttaröryggi fyrir þá aðila sem koma að vinnslunni hvort sem um ræðir tiltekna vinnslu einstakra ábyrgðaraðila eða vinnsluaðila eða vinnslu innan ákveðinna geira atvinnulífsins eða opinberra stofnana.[104]

Í persónuverndarlöggjöfinni er lögð rík áhersla á ábyrgðarskylduna og þar af leiðandi verða fyrirtæki og stofnanir að geta sýnt fram á fylgni við ákvæði löggjafarinnar. Báðar valkvæðu leiðirnar, hátternisreglur og vottun, geta auðveldað líf ábyrgðaraðila og vinnsluaðila við að uppfylla skuldbindingar sínar gagnvart löggjöfinni.[105]

4.1. Vottanir, persónuverndarinnsigli og persónuverndarmerki

Með gildistöku 42. gr. og 43. gr. pvrg., var kynnt til sögunnar nýmæli í sögu evrópskra laga, en í ákvæðunum er að finna reglur um vottun, persónuverndarinnsiglin persónuverndarmerki og vottunaraðila.[106] Með setningu ákvæðanna var í fyrsta sinn að finna heilstætt vottunarfyrirkomulag fyrir mismunandi vinnslu, hvort sem um ræðir mjög einfalda eða gríðarlega flókna vinnslu, sem framkvæmd er bæði af hálfu hins opinbera sem og einkaaðila.[107] Í ákvæðunum eru lögð áhersla á að stjórnvöld innan ESB sem og EES skuli hvetja til setningar á vottunarfyrirkomulagi innan EES og jafnvel utan þess.[108]

Með því að fyrirtæki nýti sér vottun er gætt að gagnsæi fyrir neytendur, en jafnframt eykur það samræmi á þeim vörum eða þeirri þjónustu sem veitt er. Vottun er því tækifæri fyrir ábyrgðaraðila og vinnsluaðila til sýna fram á reglufylgni með persónuverndarlöggjöfinni af eigin frumkvæði.[109] Vottunarfyrirkomulaginu er ætlað að bæta gagnsæi og fylgni með reglugerðinni, þar sem það gerir einstaklingum kleift að meta fljótt persónuverndarstig viðkomandi vöru og þjónustu.[110] Slíkt gæti haft í för með sér samkeppnislegt forskot og mögulegan fjárhagslegan ávinning sem og bætta ímynd fyrirtækjanna út á við, því neytendur

[103] Áherslubreytingar höfundar.
[104] European Union Agency for Fundamental Rights og Council of Europe (n. 31) 181.
[105] Information Commissioner's Office, „ICO Codes of Conduct and Certification Schemes Open for Business" (2. mars 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-codes-of-conduct-and-certification-schemes-open-for-business/> skoðað 29. apríl 2020.
[106] Eric Lachaud, „Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful" (2016) 32 (6) Computer Law & Security Review 814, 814–815.
[107] sama heimild 826.
[108] sama heimild 817.
[109] sama heimild.
[110] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 100. liður formála.

sem og aðrir velja þá aðila sem sýnilegt er að hagi vinnslunni í samræmi við ákvæði persónuverndarlöggjafarinnar.

Með vottun er verið að fá einhvern annan en eftirlitsstjórnvöld til þess að staðfesta að vinnsla ábyrgðaraðila eða vinnsluaðila sé í raun í samræmi við ákvæði reglugerðarinnar, nema ef um er að ræða vottun gefna út af eftirlitsstjórnvaldi. Má því segja að þetta breyti hefðbundinni framkvæmd við framfylgd löggjafarinnar, með því að kynna til leiks nýtt og valfrjálst kerfi sem einkageiranum hefur verið falið að leysa úr.

4.1.1. Inntak vottunarinnar

Reglugerðin gefur aðeins rammann fyrir framkvæmd vottunarinnar en Evrópska persónuverndarráðið hefur gefið út leiðbeiningar um vottun samkvæmt 42. og 43. gr. pvrg.[111] sem og leiðbeiningar um faggildingu vottunaraðila samkvæmt 43. gr. pvrg.[112] Vottunin þarf að vera þannig úr garði gerð að hún sé skýr og skiljanlegt við beitingu hennar, svo að almenningur geti áttað sig á hvað sé í raun verið að votta.[113] Grundvöllur vottunarinnar ætti að vera sóttur í meginreglur persónuverndarlöggjafarinnar sem og aðrar grundvallarreglur um persónuvernd. Þar sem að markmið með vottun er ávallt að sýna fram á að vinnsla af hálfu ábyrgðaraðila eða vinnsluaðila sé í samræmi við ákvæði reglugerðarinnar.

Við framkvæmd mats á vinnslustarfsemi vegna vottunar þá verður að líta til eftirfarandi þriggja meginþátta. Það eru fyrst og fremst persónuupplýsingarnar sem vinnslan snýr að, hvers eðlis þær eru og hvert er efnislegt umfang vinnslunnar. Í annan stað eru það hvaða tæknilausnir er verið að nýta við vinnsluna, hvernig eru tæknilegir innviðir (hér er bæði átt við vélbúnað og hugbúnað). Loks þá verður að leggja mat á ferlið og verklagsreglurnar sem tengjast vinnslunni.[114] Allir þessir þrír kjarnaþættir hafa áhrif á uppbyggingu fyrir viðmið vottunar. Það fer svo alltaf eftir hvaða vinnsluaðferð er verið að votta, hversu mikið vægi hver og einn þessara þriggja þátta hefur.[115]

111 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (n. 59).
112 European Data Protection Board, „Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version Adopted after Public Consultation“ (*European Data Protection Board - European Data Protection Board*, 14. desember 2018) <https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_en> skoðað 29. mars 2020.
113 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (n. 59) 15.
114 sama heimild 15–16.
115 sama heimild 16.

Evrópska persónuverndarráðið telur að vottun, samkvæmt ákvæðum reglugerðarinnar, geti tekið bæði til einstakra vinnsluaðgerða eða mengi tengdra vinnsluaðgerða. Í þessu gæti falist að mengi vinnsluaðgerða sé svo tengt að það er ómögulegt að taka eina vinnsluaðgerðina út. Sem dæmi um slíkt væri úrvinnsla fyrirspurna vegna launagreiðslna sem hluti af vinnslu við útborgun launa hver mánaðarmót.[116]

4.1.2. Vottunarfyrirkomulagið

Eins og áður hefur komið inn á þá er að finna ákvæði um vottunarfyrirkomulagið í 42. gr. og 43. gr. reglugerðarinnar. Þó er veitt ákveðið svigrúm við innleiðingu og framkvæmd á ákvæðunum. Eftirlitsstjórnvöldum ríkjanna er gefin svigrúm til þess að meta hvaða útfærsla ákvæðanna henti best fyrir þeirra heimamarkað.[117] Þetta á sérstaklega við um útfærslu á 43. gr. pvrg. sem fjallar um vottunaraðilana og hvaða kröfur þeir þurfa að uppfylla til að þeir hljóti faggildingu. Hérlendis var farið þá leið að faggildingarsvið Hugverkastofu[118] annist hana fyrir hönd íslenskra stjórnvalda[119] að fenginni umsögn Persónuverndar, sbr. 37. gr. pvl.

Í 1. mgr. 42. gr. pvrg. segir að aðildarríkin eigi að hvetja til þess að komið verði á fót vottunarfyrirkomulagi vegna persónuverndar sem og persónuverndarinnsiglum og persónuverndarmerkjum. Enda megi nýta vottunina sem verkfæri til að sýna fram á að vinnsla ábyrgðaraðila og vinnsluaðila sé í samræmi við persónuverndarlöggjöfina. Þá er lögð áhersla á að tekið skal tillit til sérstakra þarfa örfyrirtækja, lítilla og meðalstórra fyrirtækja. Af orðalagi ákvæðisins má ætla að vottunin taki ekki til persónuverndarfulltrúa eða tæknilausna, þar sem skýrt er tekið fram að vinnslan sé vottuð en ekki tæknin notuð er við vinnsluna. Hins vegar þá getur tæknilausn verið partur af vottun á vinnslustarfsemi.

Þá má nýta vottun til þess að miðla persónuupplýsingum til þriðju landa eða alþjóðastofnanna, það er þeirra aðila sem falla utan gildissviðs reglugerðarinnar samkvæmt 3. gr. pvrg. og þeir skuldbinda sig með bindandi og framfylgjanlegum hætti, til að beita viðeigandi verndarráðstöfunum, meðal annars að því er varðar réttindi skráðra einstaklinga sbr. 2. mgr. 42. gr. pvrg. Þetta á þó aðeins við ef um er að ræða vottun sem hefur hlotið almenna vottun Evrópska persónuverndarmerkisins, sbr. 5. mgr. 42. gr. pvrg. Mögulega er hér um að ræða

116 sama heimild.
117 sama heimild 6.
118 Faggildingarstofa skal vera tilgreind 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 o.fl., nr. 24/2006, er það Faggildingarsvið Hugverkastofu sem annast faggildingu fyrir hönd íslenskra stjórnvalda.
119 Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, um 37. gr.

skilvirka leið sem fyrirtæki myndu vilja tileinka sér það sem hægt væri að einfalda verklag fyrir fyrirtæki og stofnanir sem miðla persónuupplýsingum út fyrir samningssvæði EES.

Eins og fyrr segir þá er nýting vottunar algjörlega valfrjáls leið fyrir ábyrgðaraðila og eða vinnsluaðila. Hins vegar er um að ræða verkfæri sem geta nýst þessum aðilum til að auka sýnileika sem og trúverðugleika þeirra, þar sem einstaklingar hafa einhverja staðfestu á að vinnsla þessara aðila sé í samræmi við ákvæði reglugerðarinnar.[120] Þrátt fyrir að ábyrgðaraðilar og vinnsluaðilar ákveði að nýta sér vottun og það sé tæki til að sýna fram á reglufylgnina og þar með uppfylla ábyrgðarskylduna, þá þýðir það ekki að þeir þurfi ekki að fylgja öðrum ákvæðum reglugerðarinnar. Jafnframt þá á vottun ábyrgðaraðila eða vinnsluaðila ekki að hafa áhrif á verkefni eða valdheimildir eftirlitsstjórnvalda, sbr. 4. mgr. 42. gr. pvrg.

Vottunaraðilar eða eftirlitsyfirvöld geta aðeins gefið út vottun á grundvelli þeirra viðmiða sem eftirlitsyfirvaldið hefur samþykkt eða Evrópska persónuverndarráðið. Ef persónuverndarráðið hefur samþykkt viðmiðanirnar getur það leitt til almennrar vottunar, Evrópska persónuverndarmerkisins, sbr. 5. mgr. 43. gr. pvrg. En líkt og fyrr hefur komið fram getur verið grundvöllur alþjóðlegs gagnaflutnings.

Svo hægt sé að veita vottun þarf sá ábyrgðaraðili eða vinnsluaðili sem óskar eftir vottun að láta vottunaraðilanum, eða eftirlitsstjórnvaldinu ef svo stendur, í té allar nauðsynlegar upplýsingar sem og þann aðgang að vinnslustarfsemi sinni sem er nauðsynlegt til að meta hvort uppfyllt séu skilyrði fyrir vottun, sbr. 6. mgr. 42. gr. pvrg.

Loks þegar vottun hefur verið gefin út þá má hún lengst gilda í þrjú ár, en vottunina má endurnýja aftur að því skyldu að skilyrði vottunar eða viðmið séu enn uppfyllt. Ef viðmið vottunar eru ekki uppfyllt þá skulu vottunaraðilar eða eftirlitsstjórnvöld afturkalla hana, sbr. 7. mgr. 42. gr. pvrg. Með þessu er verið að gefa eftirlitsstjórnvöldum auka hlutverk í tengslum við veitingu vottunar. Eftirlitsstjórnvöld sjálf geta ávallt lagt mat á hvort skilyrði vottununar séu fyrir hendi, þetta á ekki aðeins við þegar komið er að lokum útgáfutíma vottunar.[121] Ef skilyrðin eru ekki uppfyllt þá hefur eftirlitsstjórnvaldið heimild til að afturkalla vottunina.

[120] European Union Agency for Fundamental Rights og Council of Europe (n. 31) 183.
[121] Lachaud, „The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument“ (n. 111) 251.

4.1.3. Faggilding vottunaraðila

Í 43. gr. pvrg. er athyglinni beint að skilyrðum og ferlinu við faggildingu á vottunaraðilum sem hafa það hlutverk að votta að samræmi sé á vinnslu persónuupplýsinganna við þau viðurkenndu eða samþykktu viðmið sem vottunina veitir.[122]

Í 1. mgr. 43. gr. er kveðið á um að aðildarríki skuli tryggja að vottunaraðilar séu faggiltir af eftirlitsstjórnvaldinu sjálfu, sbr. a. lið 1. mgr., eða Faggildingarstofu ríkisins, sbr. b. lið 1. mgr., eða af báðum aðilum. Eins og fyrr segir er það faggildingarsvið Hugverkastofu sem annast faggildingu fyrir hönd íslenskra stjórnvalda, þó eftir að Persónuvernd veiti umsögn sína.[123]

Þau skilyrði sem vottunaraðilum ber að uppfylla til þess að geta hlotið faggildingu eru því næst talin upp í a. til e. lið 2. mgr. 43. gr. pvrg. Þar er gerð sú krafa að vottunaraðili geti með fullnægjandi hætti, að mati eftirlitsstjórnvaldsins, sýnt fram á sjálfstæði sitt og sérþekkingu á viðfangsefni vottunarinnar, sbr. a. lið 2. mgr. Að vottunaraðilinn sé skuldbundinn til að virða viðmiðin[124] samkvæmt 5. mgr. 42. gr., sbr. b. lið 2. mgr., að hann komi á verklagi hvað varðar útgáfu, endurskoðun og afturköllun á vottuninni, sbr. c. lið 2. mgr. Þá verður vottunaraðilinn að setja ferli til að annast meðferð kvartana um brot gegn ákvæðum vottunarinnar, einnig verklagi til að meta hvernig ábyrgðaraðili eða vinnsluaðili framkvæmir eða hefur framkvæmt vottunina þar sem gæta þarf sérstaklega að því að slíkt verklag sé gagnsætt fyrir skráða einstaklinga og almenning, sbr. d. lið 2. mgr. Þá þarf vottunaraðili loks að geta sýnt fram á með fullnægjandi hætti, að mati eftirlitsstjórnvaldsins, að verkefni þeirra og skyldustörf leiði ekki til hagsmunaárreksturs, sbr. e. lið 2. mgr. 43. gr. pvrg.

Faggilding vottunaraðila getur aðeins farið fram á grundvelli skilyrða sem hafa verið samþykktar af Evrópska persónuverndarráðinu. En það er verkefni eftirlitsstjórnvaldsins að leggja fyrir ráðið drög að samþykktum skilyrðum sem persónuverndarráðið gefur út álit vegna þess. Þá má faggildingarstofa ekki sjá um veitingu faggildingar nema það sé einnig gætt að þeim kröfum sem fram koma í reglugerð (EB) nr. 765/2008 og Evrópustaðli EN-ISO/IEC 17065/2012 sem lýsa aðferðum og verklagsreglum vottunaraðila, sbr. 3. mgr. 43. gr. Í 4. mgr. er kveðið á um að faggiltir vottunaraðilar skulu sjá um og bera ábyrgð á réttu mati, sem leiðir til vottunar eða afturköllun vottunar, með fyrirvara um ábyrgð ábyrgðaraðila eða vinnsluaðila

122 Eric Lachaud, „ISO/IEC 27701: Threats and Opportunities for GDPR Certification“ (Social Science Research Network 15. janúar 2020) SSRN Scholarly Paper ID 3521250 3 <https://papers.ssrn.com/abstract=3521250> skoðað 29. apríl 2020.
123 Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál, Um 37. gr.
124 Með viðmiðum er átt við þau viðmið sem eftirlitsstjórnvaldið eða persónuverndarráðið samþykkir að gefa megi vottun út vegna.

að farið sé eftir ákvæðum löggjafarinnar. Vottunaraðilar skulu að hámarki hafa faggildingu í fimm ár og hana má endurnýja aftur með sömu skilyrðum uppfylltum. Það er einnig hlutverk vottunaraðilanna að rökstyðja ákvörðun sína við eftirlitsstjórnvöld hvort sem veita á ábyrgðaraðilum eða vinnsluaðilum vottun eða afturkalla hana, sbr. 5. mgr. 43. gr. pvrg.

Þá er vert að taka fram að eftirlitsstjórnvald hefur heimild til að sekta vottunaraðila ef hann sinnir ekki skyldum sínum samkvæmt 42. og 43. gr. pvrg., sbr. b. lið 4. mgr. 83. gr. pvrg. Sú sekt getur numið allt að fjárhæð 10 milljónum evra eða allt að 2% af árlegri heildarveltu.

4.1.3.1. Skilyrði faggildingar vottunaraðila

Eins og komið var inn á í fyrri umfjöllun þá ber persónuvernd samkvæmt 3. mgr. 43. gr. að skilgreina hverjar séu þær kröfur eða þau skilyrði sem vottunaraðili þarf að uppfylla til þess að hljóta faggildingu. Þá ber Persónuvernd jafnframt að leggja þá ákvörðun sína fyrir Evrópska persónuverndarráðið samkvæmt c. lið 1. mgr. 64. gr. pvrg., slíkt hefur ekki verið framkvæmt af hálfu Persónuverndar og þar með hefur ekki verið gefið út álit af hálfu Evrópska persónuverndarráðsins.

Evrópska persónuverndarráðið hefur gefið út leiðbeiningar skilyrði fyrir faggildingu vottunaraðila samkvæmt 43. gr. pvrg.[125] Í kjölfarið hafa eftirlitsyfirvöld ríkjanna sent ráðinu drög að skilyrðum fyrir faggildingu vottunaraðila. Fyrstu eftirlitsstofnanir aðildarríkjanna til að leggja fram drög um slík skilyrði voru breska persónuverndarstofnunin (e. Information Commissioner‘s Office)[126] og persónuverndarstofnunin í Lúxemborg. Á 17. fundi Evrópska persónuverndarráðsins þann 31. janúar 2020 samþykkti ráðið tvö álit í kjölfar þess, eru þau fyrstu álit ráðsins á skilyrðum fyrir faggildingu vottunaraðila. Markmið með álitunum var ætlað að tryggja samræmingu og rétta beitingu þessara skilyrða innan Evrópska efnahagssvæðisins.[127] Síðan þá hafa fleiri eftirlitsyfirvöld sent drög til Evrópska persónuverndarráðsins, þar á meðal eftirlitsstjórnvöld Írlands, Þýskalands og Tékklands og þann 25. maí 2020, gaf ráðið út álit þess efnis.

Til þess að gera sér betur grein fyrir hvað felst í þessum skiluðum er áhugavert er að skoða leiðbeiningar ICO. Með því er hægt að átta sig á hvernig framkvæmdinni þar verður háttað, enda geti það gefið einhverja mynd af því hver framkvæmdin verður hérlendis. Má telja

125 European Data Protection Board, „Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version Adopted after Public Consultation“ (n. 113).
126 Hér eftir ICO
127 Persónuvernd, „17. fundur Evrópska persónuverndarráðsins í Brussel 28.-29. janúar 2020“ (*Persónuvernd. Þínar upplýsingar, þitt einkalíf.*) <https://www.personuvernd.is/personuvernd/frettir/17.-fundur-evropska-personuverndarradsins-i-brussel-28.-29.-januar-2020> skoðað 22. maí 2020.

að hún verið sambærileg þeirri í Bretlandi, sérstaklega í ljósi þess að stuðla á að samræmdri beitingu ákvæða löggjafarinnar eins og farið var yfir fyrr í kaflanum.

Í Bretlandi hefur verið ákveðið að fara þá leið að breska faggildingarstofnunin (e. UK Accreditation Service)[128] mun sinna hlutverki við að veita vottunaraðilum faggildingu, sbr. b. lið. 1. mgr. 43. gr. pvrg., sem er sama leið og farin verið hér á Íslandi, sbr. 37. gr. pvl. Þar sem að ICO mun ekki sjá um faggildinguna þá þurfa skilyrði staðalsins ISO 17065/2012[129] að vera uppfyllt, sbr. sem og þau skilyrði sem gefin hafa verið út af ICO. Skilyrðum ISO 17065 staðalsins skal vera beitt samhliða skilyrðum persónuverndarreglugerðarinnar og bresku persónuverndarlaganna (e. UK Data Protection Act 2018) og gæta verður að því að skilyrði staðalsins slaki ekki á þeim kröfum sem gerðar eru í reglugerðinni eða lögunum. Þá má aðeins gefa út vottun í tengslum við vinnslu persónuupplýsinga af hálfu ábyrgðaraðila eða vinnsluaðila.[130]

Þau atriði sem sérstaklega er fjallað um í leiðbeiningum ICO eru lagalegar skyldur vottunaraðila til þess að hljóta faggildingu frá bresku faggildingarstofunni. Meðal skilyrðana er að vottunaraðili staðfesti að hann sé ekki undir rannsókn ICO eða að gripið hafi verið til lagalegra ráðstafana vegna vinnslu af hans hálfu sem myndi hafa áhrif á faggildingu hans. Breska faggildingastofan mun óska eftir að ICO staðfesti slíkt.[131] Það að vottunaraðili sé ekki viðfangsefni rannsóknar ICO er dæmi um sérstök skilyrði sem ICO setti til viðbótar við þau skilyrði sem er að finna í leiðbeiningum Evrópska persónuverndarráðsins og því gæti Persónuvernd sett sambærilegt skilyrði fyrir faggildingu vottunaraðila hérlendis.

Vottunaraðili verður að sýna fram á hann hafi tryggt viðeigandi ráðstafanir, eins og tryggingar eða varasjóð, til að standa undir skuldum sínum vegna starfa sinna, hvar sem þau fara fram.[132] Starfsmenn vottunaraðilans að uppfylla skilyrði 1. mgr. 43. gr. pvrg. og að hafa þekkingu á tæknilegum atriðum sem varðar vottun vinnslunnar og þekkingu á lögfræði þá sérstaklega varðandi persónuverndarlöggjöfinni. Vottunaraðilinn verður að geta sýnt fram á þessa þekkingu starfsmanna sinna.

Skilyrði er sett fyrir því í leiðbeiningum ICO að vottunaraðili geri samning um framkvæmd vottunarinnar við þá aðila sem sækjast eftir vottun og í honum sé fjallað um viss

128 Hér eftir UKAS
129 Hér eftir ISO 17065
130 Information Commissioner's Office, „UK additional accreditation requirements for certification bodies (A.43(1)(b))" (n. 69) 1.
131 sama heimild 3.
132 sama heimild 4.

atriði. Sem dæmi að í honum séu tiltekin bindandi matsaðferðir með tilliti til markmiða vottunarinnar.[133]

Þrátt fyrir að í þessari umfjöllun sé aðeins stiklað á stóru þá má sjá að um ítarlegar leiðbeiningar er að ræða sem skýra hlutverk faggildingaraðilans sem og hlutverk vottunaraðilans og hvaða skilyrðum hann þarf að huga að þegar óskað er eftir faggildingu. Þó er ljóst að þær byggja að stórum hluta á ákvæðum persónuverndarreglugerðarinnar um vottun. Þó er einnig að finna í þeim sérstök skilyrði sem ICO hefur sett, eins og að vottunaraðili sé ekki viðfangsefni rannsóknar stofnunarinnar. Geta má að ekki hefur reynt á vottunarfyrirkomulagið í Bretlandi[134] enn sem komið er en leiðbeiningarnar voru gefnar út þann 28. febrúar 2020.[135]

4.1.4. Viðmið vottunar

Þeir þættir sem markmið vottunar ætti að tryggja við framkvæmd vinnslunnar eru kölluð viðmið vottunar. Viðmið vottunar eru burðarás vottunarferlisins. Kveðið er á um í 5. mgr. 42. gr. pvrg. að heimilt sé að gefa út vottun sem byggir á grundvelli viðmiðana sem sem eftirlitsstjórnvaldið samþykkir eða Evrópska persónuverndarráðið. Meðal þeirra þátta sem ábyrgðaraðila ber skylda til að fylgja samkvæmt ákvæðum persónuverndarreglugerðarinnar og má nýta sem viðmið vottunar eru meðal annars lögmæti vinnslu skv. 6. gr. pvrg, meginreglurnar persónuverndarlöggjafarinnar sem eru að finna í 5. gr. pvrg., réttindi hinna skráðu einstaklinga sbr. 12. – 23. gr. pvrg., skyldur um innbyggða og sjálfgefna samkvæmt 25. gr. pvrg., þegar við á hvort framkvæmt hafi verið mat á áhrifum á persónuvernd skv. 35. gr. pvrg. og hvaða tæknilegu og skipulagslegu ráðstafana hafi verið gripið til til að tryggja öryggi vinnslunnar sbr. 32. gr. pvrg. Hversu miklu leyti þessi sjónarmið endurspeglast í viðmiðum vottunar getur verið breytilegt eftir umfangi vottunarinnar sem og tegund vinnslustarfsemi.[136]

Til þess að hægt sé að meta samræmi vinnslu við viðmið vottunar, verður að setja upp raunveruleg dæmi. Til dæmis þá fer samræmi við notkun tæknilegra innviða sem nýtast við vinnsluaðgerðir, hvaða tegunda persónuupplýsinga vinnslan nær til og til hvers tæknilegar lausnir voru hannaðar að leysa úr. Því þarf að líta til þess hvert er skipulag fyrirtækisins, þá

133 sama heimild 5–6.
134 Information Commissioner's Office, „Register of Certification Scheme Criteria" (26. febrúar 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/certification-schemes-detailed-guidance/register-of-certification-scheme-criteria/> skoðað 25. maí 2020.
135 Information Commissioner's Office, „ICO Codes of Conduct and Certification Schemes Open for Business" (n. 105).
136 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0" (n. 59) 15.

sérstaklega til atriða eins og flokkun persónuupplýsinga og magns þeirra, hvaða tæknilegu innviðir eru notaðir við vinnsluna, hvers eðlis vinnslan sé og umfang hennar. Þá þarf loks þarf einnig að meta hver er áhættan fyrir hina skráðu. Ennfremur skal hafa í huga að tæknilausnir geta verið mismunandi þó þær þjóni sömu vinnslu. Þess vegna verður að hafa í huga þegar skilgreina skal umfang vottunaraðferðar og ennfremur þegar vottunarviðmiðin eru samin að þau séu ekki of þröng til að útiloka ekki aðrar tæknilausnir, sem sinna sömu vinnslu en hafa aðra hönnun eða uppbyggingu.[137]

Það sem vekur því upp spurningar við skoðun á 5. mgr. 42. gr. pvrg., en þar er kveðið á um að vottun má gefa út á grundvelli viðmiða sem eftirlitsstjórnvald hefur samþykkt, sbr. f. lið 3. mgr. 58. gr. pvrg. eða persónuverndarráðsins samkvæmt 63. gr. pvrg. Túlka má 5. mgr. 42. gr. pvrg. á þá leið að þegar gefa á út vottun þarf annað hvort samþykki eftirlitsstjórnvaldsins eða Evrópska persónuverndarráðsins á viðmiðunum. Hins vegar ef maður skoðar c. lið 1. mgr. 64. gr. pvrg. þá kemur þar fram að eftirlitsstjórnvald skal bera drög að samþykki fyrir vottunarviðmiðin undir Evrópska persónuverndarráðið áður en þau eru samþykkt. Þetta kemur jafnframt fram í leiðbeiningum persónuverndarráðsins nr. 1/2018 að eftirlitsstjórnvöldum ber áður en þau samþykkja viðmið vottunar að leggja drög að ákvörðun sinni fyrir Evrópska persónuverndarráðið.[138]

Hins vegar þá hafa eftirlitsstjórnvöldin heimild til þess að samþykkja vottunarviðmið sbr. f. lið 3. mgr. 58. gr. pvrg. Af þessu leiðir að eftirlitsstjórnvöld verða því, þegar um er að ræða ný vottunarviðmið, skal að leggja drög að samþykki sínu fyrir ráðið, það er ef vottunin tekur til stærra svæðis en aðeins aðildarríkisins. Má því ætla að eftirlitsstjórnvöld hafa heimild til að samþykkja vottunarviðmið fyrir vottun sem hefur aðeins gildi innan þess aðildarríkis.[139] Vert er þó að benda á að ICO hefur gefið út í sínum leiðbeining að til þess að geta samþykkt viðmið vottunar muni það fyrst óska eftir áliti Evrópska persónuverndarráðsins til þess að gæta samræmis innan sambandins. Af þessu álykta að ICO telur sig ávallt þurfa leggja samþykki sitt fyrir ráðið til þess að gæta að samræmi innan sambandsins.[140]

Það að eftirlitsstjórnvöldum ríkja hafi vald til þess að meta sjálf vottunar viðmiðin má telja nokkuð úr takt við meginmarkmið reglugerðarinnar um samræmda beitingu ákvæða reglugerðarinnar. Þar sem að eftirlitsstjórnvöld geta upp á sitt einsdæmi samþykkt viðmið

137 sama heimild 16.
138 sama heimild 23 Viðauki 1.
139 sama heimild 12.
140 Information Commissioner's Office, „How Do We Develop a Certification Scheme?" (27. febrúar 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/> skoðað 3. júní 2020.

vottunar án þess að líta til þess hvernig beiting er á ákvæðum varðandi vottunina innan sambandsins geti það leitt til þess að ójafnvægi myndast á hinum innri markaði.

Er því ekki hægt að telja annað en að framkvæmdin varðandi samþykkt viðmið vottunar, sbr. 5. mgr. 42. gr. pvrg., sé óskýr hvað varðar samþykki, sérstaklega á meðan ekki hefur enn neitt vottunarviðmið verið samþykkt. Líklega mun ákvæðið þó skýrast frekar þegar það kemur til framkvæmdar.

4.1.5. Markmið vottunar

Hægt er að skilgreina markmið vottunarinnar annaðhvort almennt eða í tengslum við tiltekna vinnslu eða tegund vinnslu eða vinnslustarfsemi og þar með sé skýrt að ákveðin partur vinnslunnar falli innan gildissviðs vottunarinnar. Til dæmis að örugg geymsla gagna falli undir vottun á tæknilausn sem snýr að starfrænni vistun gagnanna. Því getur áreiðanlegt mat á samræmi aðeins verið framkvæmt ef tilgangi vottunarinnar, þ.e. til hvaða hluta hún taki, hefur verið lýst nákvæmlega. Lýsa verður skýrt hvaða vinnslustarfsemi vottunin tekur til og þar með hvaða persónuupplýsingar, ferlar, tæknilegir innviðir hafa verið metnir og hverjir ekki. Af þessu leiðir að þeir hlutar vinnslu sem vottunaraðferð nær ekki til hljóta ekki vottun. Í öllum tilvikum er vottun mjög þýðingarmikil hvað varðar þau skilaboð sem hún sendir, þar á meðal hvaða kröfur hafa verið gerðar til hvaða hluta og að þær séu uppfylltar, svo það hafi ekki villandi áhrif á viðskiptavini, neytendur, hina skráðu einstaklinga og almenning.[141] Vottun má ekki og á ekki skapa falskt öryggi. Dæmi um skýrt markmið vottunar merki eða innsigli um örugga innskráningu (e. secure log-in) á vefsíðu á Internetinu, þar sem að innsigli eða merki gefur það skýrt til kynna sú aðferð sem nýtt er til tryggja öryggi persónuupplýsinganna við innskráninguna hafi hlotið vottun.[142]

4.1.6. Lagaleg staða vottunar

Út frá lagalegu sjónarhorni hefur vottun þá merkingu að um sé að ræða ákveðið vörumerki sem verndar réttindi þriðja aðila sem hefur fengið heimild til að nýta vörumerkið.[143] Vottun getur líka verið stjórnunarkerfi þar sem samspil ákveðinna kjarnþátta til þess að komast að ákveðinni niðurstöðu, ef sú niðurstaða fæst má gefa út vottun fyrir annaðhvort ferlið eða útkomu þess.[144]

141 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (n. 59) 17.
142 sama heimild.
143 Lachaud, „Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful“ (n. 106) 816.
144 Lachaud, „The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument“ (n. 111) 34.

Almennt hefur vottun hvorki skýrt lagalegt gildi né skýra lagalega stöðu innan Evrópulöggjafarinnar. Annars vegar þá hefur Evrópska landfræðilega merkingin (e. The European Geographical Indication) stöðu félagamerkis, sem er sérstök merking sem er notuð til að bera kennsl á vöru þar sem gæði, orðspor eða önnur slík einkenni tengjast landfræðilegum uppruna hennar.[145] Hins vegar þá hefur CE merkið hvorki stöðu félagsmerkis né vottunarmerkis. CE merkið veitir framleiðendum fullan aðgang að markaði Evrópu ef þeir hafa slíka merkingu en að sama skapi þá bera þeir fulla ábyrgð á vörunum þrátt fyrir að þær séu vottaðar, sbr. f. lið 1. mgr. 8. gr. tilskipunar Evrópuþingsins og Ráðsins nr. 2001/95/EB um öryggi vöru. Jafnframt er mikið misræmi á lagalegri stöðu vottunar meðal aðildarríkja Evrópusambandsins, sum aðildarríki hafa set ákvæði í þeirra landslög sem kveða á um gildi vottunar, önnur líta á vottun sem félagsmerki og enn önnur kveða ekkert á um lagalegt gildi vottunar innan sinnar löggjafar.[146]

Vottun hefur ávallt lagalegt gildi fyrir aðila vottuninnar því gerður verður samningur um skyldur þeirra. Vottunarsamningurinn sem gerður er á milli vottunaraðilans og ábyrgðaraðila eða vinnsluaðila er lagalega bindandi fyrir báða aðila samningsins.[147] Má segja að þær kröfur sem vottunarsamningurinn felur ábyrgðaraðilum og vinnsluaðilum annars vegar og vottunaraðilanum hins vegar séu sjálfstæðar og óháðar skyldum þeirra gagnvart persónuverndarlöggjöfinni. Þrátt fyrir að búast megi við ákveðinni skörun á milli skyldnanna, sem dæmi þá væri skyldan til að halda vinnsluskrá líklegur partur af flestum vottunum.[148] Af þessu leiðir að aðilar samningsins geta alltaf byggt á honum ef annar aðili fer ekki eftir ákvæðum samningsins.

Vandfundin er sú leið sem er sýnilegri en vottun fyrir ábyrgðaraðila og vinnsluaðila til að sýna fram á reglufylgni fyrir ábyrgðaraðila eða vinnsluaðila. Enda má nýta vottunina sem leið til að sýna fram á að fyrirtæki og stofnanir uppfylli skyldur sínar og geta einföldu merki eða innsigli sýnt fram á að skyldur þeirra samkvæmt ákvæðum reglugerðarinnar séu uppfylltar. Sem dæmi þá getur vottun til sýnt fram á að kröfur um innbyggða og sjálfgefna persónuvernd séu uppfylltar, en það er ekki hægt með hátternisreglum, sbr. 3. mgr. 25. gr. pvrg.

145 „Geographical indications - Trade - European Commission“ <https://ec.europa.eu/trade/policy/accessing-markets/intellectual-property/geographical-indications/index_en.htm> skoðað 1. maí 2020.
146 Lachaud, „The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument“ (n. 111) 252.
147 Irene Kamara o.fl., „Data Protection Certification Mechanisms : Study on Articles 42 and 43 of the Regulation (EU) 2016/679“ (Publications Office of the European Union 6. maí 2019) 183–184 <https://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en> skoðað 5. maí 2020.
148 Irene Kamara, „4 GDPR-certification myths dispelled“ <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> skoðað 16. maí 2020.

Þrátt fyrir að ábyrgðaraðili eða vinnsluaðili hafi sýnt fram á reglufylgni með því að hljóta vottun fyrir vinnsluaðgerðir, þó honum hafi ekki borið skylda til að gera slíkt, þá kemur vottunin sem slík ekki í veg fyrir að eftirlitsstjórnvaldið sinni hlutverki sínu,[149] sem er meðal annars álagning stjórnsýslusekta. En staðfest vottun ábyrgðaraðila eða vinnsluaðila getur haft áhrif á hvort leggja skal á stjórnsýslusekt og þá hve há hún skuli vera samkvæmt j. lið 2. mgr. 83. gr. pvrg. Það fer eftir eðli brotsins hvort nauðsynlegt sé að leggja á stjórnvaldssekt og þá hversu háa sekt heimilt sé að leggja á, getur það komið til lækkunar slíkrar sektar ef vottun er til staðar.[150] Þá getur eftirlitsstjórnvald sektað ábyrgðaraðila og vinnsluaðila sem hlotið hafa vottun en fylgja ekki ákvæðum 42. og 43. pvrg. sbr. a. lið 4. mgr. 83. gr. pvrg. Það að fá vottun og því verklagi sem vottunin tók til sé svo ekki fylgt er ósanngjörn hegðun gagnvart neytendum þar sem vottunin sem slík getur gefið óraunhæfa mynd af stöðunni og veitt falskt öryggi.[151] Þetta er mikilvægt þar sem að sýnileikinn er hvergi meiri fyrir hina skráðu einstaklinga og almenning eins og með vottun, þar sem viðkomandi ábyrgðaraðili hefur fengið merki þess efnis um að hann hagi vinnslu sinni í samræmi við ákvæði löggjafarinnar og að annar óháður aðili hafi staðfest slíkt. Merkingar vegna vottunar geta sjálfkrafa aukið traust almennings og af þeim sökum ætti sá aðili sem hefur fengið slíka vottun en hagar ekki vinnslunni í samræmi við það verklag að hljóta þyngri sektar en ef um aðila sem ekki hefur hlotið vottun.

Þá getur þetta skekkt samkeppni milli einkaaðila sem hafa áhuga á að koma af stað vottunarkerfi og vilja hagnast á því en að sama skapi þá geti eftirlitsstjórnvöld ríkjanna einnig komið upp sambærilegu vottunarkerfi þar sem ekki er tekin þóknun fyrir.[152] Af þessu leiðir að lítill hvati geti verið fyrir einkageirann að hefja þá vegferð að reyna gerast vottunaraðilar, þar sem þeir gættu á hvaða tímapunkti sem er endaði í samkeppni við eftirlitsstjórnvald ríkisins.

Þá verður að telja að framkvæmdin fyrir eftirlitsyfirvöld varðandi samþykki viðmiða vottunar séu nokkuð óljós. Þar sem að samþykkt vottunarviðmið eru grundvöllur vottunar og virðist vera sem svo að setja eigi í gang tvöfallt kerfi, þar sem annars vegar eru viðmið vottunar samþykkt fyrir heimamarkað aðildarríkjanna af eftirlitsstjórnvöldum þar í landi og hins vegar þar sem vottunar viðmiðin eru samþykkt af Evrópska persónuverndarráðinu, þegar

149 Article 29 Data Protection Working Party, „Guidelines on the application and setting of administrative fines (wp253).“ 15 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> skoðað 21. apríl 2020.
150 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 148. liður formála.
151 Lachaud, „Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful“ (n. 106) 820.
152 Lachaud, „ISO/IEC 27701“ (n. 123) 14.

eftirlitsstjórnvald leggur fyrir það drög að ákvörðun sinni, þegar vottun á að gilda almennt á hinum innri markaði.

Má því telja að farið gæti sem svo að ef komið er af stað vottunarkerfi af hálfu einkaaðila innan aðildarríkis að sambærileg vottun gefin út hlotið almenna vottun Evrópska persónuverndarmerkisins að sú vottun sem hefur ekki hlotið samþykki persónuverndarráðsins verði ekki samkeppnishæf lengur. Mögulega væri sú vottun sem gefin er út innan aðildarríkis ekki í samræmi við þá Evrópsku.

Þó má líta svo á að þetta tvöfalda kerfi geti haft þau áhrif að kostnaður við að sækja sér vottun yrði verið breytilegur eftir því til hvaða svæðis hún tekur og þar af leiðandi haft þau áhrif að lítil og meðalstór fyrirtæki hafi möguleika á að sækja sér svæðisbundna vottun. Sem dæmi væri vottun sem gefin er út af vottunaraðila á Íslandi og væri aðeins samþykkt af Persónuvernd, en stærri fyrirtæki sem hafa meira fjárhagslegt bolmagn myndu sækja í þá vottun sem næði yfir stærra svæði, svo sem þá vottun hefði fengið samþykki persónuverndarráðsins og almenna vottun Evrópska persónuverndarmerkisins.

4.1.7. Vottun samkvæmt 42. og 43. gr. pvrg. eða ISO/IEC 27701:2019 staðallinn

Þrátt fyrir að fjögur ár séu síðan að persónuverndarreglugerðin var kynnt til leiks og þar með þessi nýju ákvæði um vottun, þá hefur ekki enn verið staðfest eða gefin út nein vottun af Evrópska persónuverndarráðinu.[153] Persónuverndarráðið hefur þó gefið út leiðbeiningar um hvaða skilyrði og viðmið eigi við um vottunaraðferðir samkvæmt ákvæðum 42. gr. og 43 gr. pvrg.[154]

Alþjóðlegu staðlasamtökin (e. International Organization for Standardization)[155] eru sjálfstæð alþjóðleg samtök sem vottunaraðila 164 ríkja eiga aðild að.[156] Í ágúst 2019 ISO/IEC 27701:2019 staðalinn[157] en ISO staðlarnir og sú vottun sem þeir færa eru verndaðir af höfundarétti og í eigu samtakanna, en ekki opinberir og aðgengilegir eins og vottunarkerfi 42. gr. og 43. gr. pvrg. kveða á um.[158] Staðall ISO 27701 hefur verið hannaður sem viðbót við staðalinn ISO/IEC 27001:2013[159] sem er staðall sem er upplýsingaöryggisstaðall fyrir stjórnun

153 European Data Protection Board, „Register of Certification Mechanisms, Seals and Marks“ (*European Data Protection Board - European Data Protection Board*) <https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en> skoðað 3. maí 2020.
154 European Data Protection Board, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (n. 59) 6.
155 Hér eftir ISO.
156 „ISO - About Us“ (*ISO*) <https://www.iso.org/about-us.html> skoðað 3. maí 2020.
157 Hér eftir ISO 27701
158 Lachaud, „ISO/IEC 27701“ (n. 123) 5.
159 Hér eftir ISO 27001

persónuverndar. ISO staðlarnir eru þekkir meðal fyrirtækja bæði á evrópska markaðnum sem og þeim Asíska og hafa verið gefnar út 32.000 vottanir frá árinu 2005, samkvæmt ársskýrslu ISO fyrir árið 2018.[160] Staðalinn ISO 27701 hefur að geyma viðbótarkröfur og leiðbeiningar sem eiga við um vernd persónuupplýsinga.[161] Staðallinn ISO 27701 er meðal annars fáanlegur hjá Staðlaráði Íslands.

4.1.7.1. ISO 27701 staðalinn ógn eða tækifæri fyrir persónuvernd

Fyrst er mikilvægt að taka fram að ISO 27701 staðallinn hefur ekki verið viðurkenndur sem samrýmanlegur við ákvæði 42. gr. og 43. pvrg. Það sem aðskilur ISO 27701 frá ákvæðum persónuverndarreglugerðarinnar er að staðallinn tryggir öryggi upplýsinganna á meðan reglugerðinni er ætlað að tryggja fleira en aðeins öryggi þeirra, þar á meðal áreiðanleika, lögmæti vinnslunnar, samræmi við meginreglur og skyldur ábyrgðaraðila. ISO staðallinn hefur áhættumiðaða nálgun, sem þýðir að hann miðar að því að greina hættur og takast á við upplýsingaöryggisáhættur vegna vinnslu persónuupplýsinganna. Reglugerðin treystir stundum á áhættumiðaða nálgun til að takast á við víðtækari áhættu gagnvart réttindum og frelsi skráðra einstaklinga.[162] ISO 27701 staðallinn veitir vottun fyrir þá aðila sem vinna með persónuupplýsinga og nýta tæknilausnir við vinnsluna en persónuverndarlöggjöfin miðar ekki aðeins við vernd persónuupplýsinga með stafrænni vinnslu heldur nær hún til allrar vinnslu, þar með talið handvinnslu, t.d. eins og geymslu persónuupplýsinga í skjalaskápum og fleira.[163]

Meðan ISO 27701 hefur ekki verið viðurkenndur sem samrýmanlegur ákvæðum 42. og 43. gr. pvrg. gæti mögulega staðið ákveðin ógn af staðlinum sérstaklega með tilliti til þeirra samkeppni sem hann getur haft í för með sér fyrir ákvæði reglugerðarinnar um vottun. Af því gæti leitt ákveðin lagaleg óvissa sérstaklega þar sem ekki enn hefur verið gefin út vottun sem stenst skilyrði ákvæða reglugerðarinnar. Þar sem ISO staðlarnir eru þekktir á mörkuðum vottunar, en slíkt getur veitt þeim fyrirtækjum sama hafa slíka vottun ákveðið forskot í samkeppni, þar sem neytendur þekkja merkið, það er ISO vottunina. Af þeim sökum gætu þessi tvö kerfi hrundið af stað ákveðinni samkeppni milli þessara tveggja leiða.

Mikilvægt er að taka fram að vottun frá ISO hefur í för með sér mikinn kostnað fyrir fyrirtæki, þar sem, eins og fyrr segir, ISO vottunin er í eigu einkaaðila og varin af höfundarrétti.

160 Sjá skýrslu ISO fyrir 2018 ISO, „Annual Report 2018“ (*ISO*) <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/publication/10/03/PUB100385.html> skoðað 3. maí 2020.
161 Lachaud, „ISO/IEC 27701“ (n. 123) 5.
162 sama heimild 22.
163 sama heimild 6.

En slíkt gengur gegn því sem lagt er upp með í 1. mgr. 42. gr. pvrg. að taka skal sérstaklega tillit til þarfa lítilla og meðalstórra fyrirtækja. Lítil og meðalstór fyrirtæki hafa almennt ekki fjárhagslegt bolmagn til þess að sækja sér ISO vottun.[164] Þar sem reglugerðin miðar að því að einkaaðilar eigi að sinna því verkefni að verða vottunaraðilar, þá er þó fremur ólíklegt að vottun samkvæmt ákvæðum reglugerðarinnar myndi hafa í för með sér kostnað fyrir þá ábyrgðaraðila og vinnsluaðila sem sækjast eftir slíkri vottun, nema ef það væri framkvæmt af hálfu eftirlitsstjórnvalds. Jafnframt þá samrýmis ISO 27701 staðallinn ekki þeirri kröfu sem reglugerðin gerir um að vottunin skuli vera samþykkt af eftirlitsstjórnvaldi, allavega ekki sem stendur þar sem ekkert eftirlitsstjórnvald aðildarríkja ESB hefur samþykkt staðalinn sem samrýmanlegan reglugerðinni.

Þrátt fyrir að staðallinn sé ekki fullkomlega samrýmanlegur við ákvæði reglugerðarinnar þá veitir hann engu að síður þeim ábyrgðaraðilum og vinnsluaðilum ákveðin tækifæri því hann tekur á hlutum sem skipta fyrirtæki miklu máli, öryggi gagnanna.[165] ISO 27701 staðalinn gæti einnig verið nytsamlegt leiðbeiningartæki fyrir ábyrgðaraðila og vinnsluaðila í því að samræma vinnsluna að þeim ákvæðum reglugerðarinnar sem staðallinn tekur til, þó hann sé ekki full samrýmanlegur reglugerðinni og ekki samþykktur af eftirlitsstjórnvöldum. Slíkt gæti því einnig minnkað líkurnar á sektum, þar sem leiða má líkur að því að minnsta kosti að vinnslan sé að hluta til í samræmi við ákvæði reglugerðarinnar.[166]

Þá getur þetta að sama skapi aukið traust neytenda á þeim aðilum sem sækja sér vottunina, þar sem þeir þekkja ISO staðlana. Jafnframt gæti upptaka ISO staðalsins haft þau áhrif á að vernd persónuupplýsinga breiðist út á heimsvísu og hafi mögulega sömu áhrif CE merkið hafði á öryggi, heilsu og umhverfi.[167] Þar sem framleiðendur sem vildu komast inn á Evrópumarkað fóru að framleiða eftir staðlinum, þrátt fyrir að framleiðslan færir fram í örðum hlutum heimsins.[168]

Má einnig leiða líkur að því að fyrirtæki sem hafi nægilegt fjármagn til þess að innleiða ISO 27701 muni gera það þrátt fyrir að hann hafi ekki nú þegar verið samþykktur sem samrýmanlegur ákvæðum 42. og 43. gr. pvrg. enda útilokar hann ekki það að fyrirtæki og stofnanir geri einnig sótt sér vottun samkvæmt ákvæðum reglugerðarinnar. Eins og staðan er núna þá má ekki nýta ISO 27701 til þess að sýna fram á að vinnsla ábyrgðaraðila eða vinnsluaðila uppfylli ákvæði reglugerðarinnar, sbr. 1. mgr. 42. gr. pvrg. Honum er ætlað að

164 sama heimild 16.
165 sama heimild 22.
166 sama heimild 19.
167 sama heimild 23.
168 sama heimild 19.

auðvelda ábyrgðaraðilum og vinnsluaðil að tryggja öryggi persónuupplýsinganna, líkt og önnur ákvæði reglugerðarinnar kveða á um.

Af framsögðu má alveg leiða líkur að því að eftirlitsstjórnvöld munu samþykkja ISO 27701 sem samrýmanlegan ákvæðum reglugerðarinnar. Sérstaklega þar sem að mörg fyrirtæki líta hýru auga til ISO 27701 með vernd persónuupplýsinga í huga og þar með honum séu uppfylltar, alla vega að hluta til, þær skyldur sem persónuverndarreglugerðin leggur á fyrirtækin. Sérstaklega má ætla að þetta eigi við um stærri fyrirtæki sem hafa nægt fjárhagslegt bolmagn og eru þau því tilbúin að fjárfesta í staðlinum, enda hefur meirihluti stórfyrirtækja hafa nú þegar innleitt ISO 27001 staðalinn.[169]

4.1.8. Vottun - raunhæf leið fyrir fyrirtæki og stofnanir?

Eins og áður segir er vottun leið fyrir fyrirtæki og stofnanir til að sýna fram á samræmi á vinnsluaðferðum þeirra við ákvæði persónuverndarreglugerðina. Með því að sækjast eftir vottun á vinnsluaðferðir eru fyrirtæki að nýta sér vottun til að sýna fram á aukið gagnsæi fyrir hina skráðu einstaklinga sem og aðra viðskiptavini sína.[170] Með því að fyrirtæki tileinki sér vottun þá gæti í því falist fjárhagslegur ávinningur fyrir þá aðila, því við ákvörðum um álagningu stjórnvaldssekta muni eftirlitsstjórnvöld líta til þess hvort aðili hafi undirgengist vottun á vinnslustarfsemi sinni sbr. j. lið 2. mgr. 83. gr. pvrg.

Hins vegar þá hafa fæst fyrirtæki nægilega reynslu eða þekkingu af því að nýta sér vottun í tengslum við vinnslu persónuupplýsinga. Ennfremur þá gæti það reynst erfitt verkefni fyrir almenn fyrirtæki að reyna ná samræmi við ákvæði reglugerðarinnar í heild sinni með vottun, þar sem að slíkt ferli kallar bæði á mikla sérfræðiþekkingu, fjármagn og tíma. Af þeim sökum gæti reynst þessum fyrirtækjum dýrkeypt að hoppa á þann vagn að treysta einungis á vottunarfyrirkomulag 42. og 43. gr. pvrg. til að sýna fram á fylgni með löggjöfinni en ættu frekar að reyna vera meðvitaðir að hugsanlegur ávinningur vottunnar kæmi með tíð og tíma, þar sem að ólíklegt megi telja að upptaka vottunar verði einfalt verkefni, sérstaklega meðan ekki hefur komið nægileg reynsla á kerfið.[171] Þrátt fyrir að vottunarfyrirkomulag persónuverndarreglugerðarinnar hafi ekki öðlast neina reynslu eins og er, þá er að finna fjölda

169 IT Governance, „Why Are so Many Organisations Getting Certified to ISO 27001?“ (*IT Governance Blog En*, 18. apríl 2018) <https://www.itgovernance.eu/blog/en/why-are-so-many-organisations-getting-certified-to-iso-27001> skoðað 6. janúar 2020.
170 Tim Hickman, „Guidelines on the Certification Mechanisms under the GDPR“ <https://www.whitecase.com/publications/alert/guidelines-certification-mechanisms-under-gdpr> skoðað 19. apríl 2020.
171 sama heimild.

allan af stöðlum og öðrum vottunum sem hægt sé að nýta til þess að að tryggja að vinnsla aðila sé í samræmi ákvæði löggjafarinnar að hluta til og slíkt er fyrirtækjum til bóta.

Enda má segja að ekki sé að finna einfaldari eða sýnilegri leið fyrir fyrirtæki til að sýna fram á reglufylgni fyrir hinum skráðu einstaklingum, viðskiptavinum og neytendum. Þar sem að ef fyrirtæki hafa hlotið vottun og bera með sér innsigli eða merki þess efnis að það geti haft veruleg áhrif á ákvarðanatöku neytenda eða viðskiptavina við kaup á vöru og þjónustu. Að því leyti getur vottun veitt fyrirtækjum gríðarlegt samkeppnislegt forskot á aðra aðila sem bjóða sömu vöru og þjónustu á sama markaði.[172]

4.2. Hátternisreglur

Hátternisreglurnar samkvæmt ákvæðum 40. gr. og 41. gr. pvrg, eru hugsaðar sem leið fyrir fyrirtæki og stofnanir, hvort sem um er að ræða ábyrgðaraðila eða vinnsluaðila, til að sýna fram á reglufylgni við ákvæði reglugerðarinnar.

Hátternisreglur eru ekki nýtt hugtak í evrópskri persónuverndarlöggjöf þar sem í tilskipun 95/46/EB, forvera persónuverndarreglugerðarinnar, var að finna ákvæði þar sem kveðið var á um að aðildarríkin og framkvæmdastjórn ESB skyldu hvetja til setningu hátternisreglna. Þeim var ætlað að stuðla að réttri framkvæmd ákvæða tilskipunarinnar sem aðildarríkin höfðu innleitt í sína löggjöf, með hliðsjón af sérlögum ríkjanna sem giltu um ákveðna geira, sbr. 1. mgr. 27. gr. tilskipunar 95/46/EB. Nokkur ríki sambandsins tileinkuðu sér þessa valkvæðu leið sem tilskipunin bauð upp á, þeirra á meðal má nefna Bretland og Holland.[173] Samtök eins og FEDMA sem fjallað var um í öðrum kafla ritgerðarinnar, hafa haft gildandi hátternisreglur samkvæmt 27. gr. tilskipunar 95/46/EB allt frá því þær voru samþykktar af 29. gr. starfshópnum árið 2003. FEDMA hefur nú þegar hafið vinnu við endurnýjun hátternisreglna svo þær uppfylli skilyrði persónuverndarreglugerðarinnar.[174]

Hins vegar þá má segja að hlutverk þeirra og vægi hafi verið stóraukið frá því sem áður var. Hátternisreglum persónuverndarreglugerðarinnar er ætlað kynna til leiks hagnýta og hagkvæma leið til að ná betri og samrýmdari vernd fyrir frelsi og réttindi einstaklinga.[175] Þá nýtast þær jafnframt sem leið til að sýna fram á reglufylgni samkvæmt löggjöfinni, sérstaklega þar sem þær geta tengt saman skyldur fyrirtækja og stofnana samkvæmt persónuverndarlöggjöfinni við aðrar lagaskyldur sem þeim ber að uppfylla, hvort sem það er

172 Grafenstein (n. 101) 19.
173 Alþt. 1999-2000 A-deild, þskj. 399 - 280 mál, V.3.9. Starfs- og siðareglur.
174 FEDMA, „Self Regulation – Fedma“ <https://www.fedma.org/work-areas/self-regulation/> skoðað 25. maí 2020.
175 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 5.

innan eins aðildarríkis eða fleiri, það er ef vinnsla persónuupplýsinganna nær út fyrir landamæri ríkisins. Enn fremur þá veita hátternisreglurnar sérstökum atvinnugreinum tækifæri til að meta vinnsluna heildstætt innan geirans og þar með samþykkja sérsniðnar og hagnýtar reglur um vernd persónuupplýsinga, sem bæði mætir þörfum atvinnugeirans og kröfum persónuverndarlöggjafarinnar.[176]

4.2.1. Eðli hátternisreglna

Hátternisreglum mætti lýsa sem sérstökum reglum sem ná til tiltekinna hópa ábyrgðaraðila eða vinnsluaðila. Með því að fylgja slíkum reglum þá eru þeir aðilar einnig að sýna fram á reglufylgni með löggjöfinni. Reglurnar geta verið gagnleg leið til að uppfylla ábyrgðarskylduna, þar sem þeim er ætlað að gefa nákvæma lýsingu á hvað sé heppilegasta leiðin við vinnsluna, en jafnframt þá leið sem sé lögfræðilega og siðfræðilega best fyrir geirann.[177]

Samtök fyrirtækja eða stofnanir sem koma fram fyrir ákveðinn atvinnugeira, hafa val um að setja sér hátternisreglur sem hjálpa þeim fyrirtækjum og stofnunum innan þess geira að uppfylla skyldur sínar gagnvart persónuverndarlöggjöfinni. Það mætti því skýra hátternisreglur sem nokkurskonar leiðbeiningar hvað varðar vernd persónuupplýsinga fyrir fyrirtæki og stofnanir sem ætlað er að samræma vinnslu þeirra með tilliti til þess rekstrarumhverfis sem fyrirtækin eða stofnanirnar starfa í. Með setningu hátternisreglna er sérstaklega búið að meta hvaða meginreglur sem og aðrar skyldur persónuverndarreglugerðarinnar eiga við um starfsemi þessara fyrirtækja og stofnana en jafnframt eru aðrar lagalegar skuldbindingar þeirra hafðar til hliðsjónar. Þá geta fyrirtækin og stofnanirnar betur uppfyllt skyldur sínar gagnvart persónuverndarlöggjöfinni og einnig skyldur sínar gagnvart öðrum landslögum.[178]

Til einföldunar má segja að hlutverk hátternisreglna út frá sjónarhóli fyrirtækja og stofnanna sé þríþætt. Fyrst og fremst, færa þær fulltrúum samtaka fyrirtækja tækifæri til að hanna persónuverndarreglur sem eru sérsniðnar að þeirra atvinnugeira. Í öðru lagi, þá geta hátternisreglunar hjálpað að brúa bilið milli ósamræmanlegra ákvæða landslaga og persónuverndarlöggjafarinnar. Í þriðja lagi, þá eru hátternisreglurnar leið sem ábyrgðaraðilar og vinnsluaðilar geta nýtt til að sýna fram á reglufylgni með löggjöfinni.[179]

176 sama heimild.
177 sama heimild 7.
178 Eric Lachaud, „Adhering to GDPR Codes of Conduct: A Possible Option for SMEs to GDPR Certification“ (Social Science Research Network 5. júní 2019) SSRN Scholarly Paper ID 3399509 1 <https://papers.ssrn.com/abstract=3399509> skoðað 10. maí 2020.
179 sama heimild.

Það er ekki til ein rétt leið við setningu hátternisreglna, heldur verður að útbúa þær með þann atvinnugeira í huga sem þeim er ætlað að sinna svo þær nýtist. Af þessu leiðir að hátternisreglurnar eiga ekki að vera upptalning af þeim skyldum og reglum sem aðilum ber að fylgja samkvæmt persónuverndarlöggjöfinni, því þá eru þær fullkomlega óþarfar, enda ber aðilum í hvívetna að fylgja ákvæðum persónuverndarlöggjafarinnar hvort sem þeir ákveða að setja sér hátternisreglur eður ei. Reglurnar eiga því að taka mið af þörfum þess atvinnugeira sem þær taka til, svo þær nýtist sem sú leið sem persónuverndarreglugerðin ætlar þeim.[180] Þrátt fyrir að hátternisreglur séu sett fram sem leið fyrir samtök fyrirtækja innan ákveðinna atvinnugeira, þá er ekki útilokað að tveir mismunandi atvinnugeirar samnýti hátternisreglur, ef vinnsla þessara tveggja atvinnugeira er sambærileg. En til að slíkt sé heimilt þá verður að vera sérstakur eftirlitsaðili fyrir hvern geira og vera algjörlega skýrt hvert hlutverk hvers eftirlitsaðila er og að það taki til aðeins þessa atvinnugeira, þó þeir starfi eftir sömu hátternisreglunum.[181]

Með setningu hátternisreglna er hægt að taka tillit til mismunandi ábyrgðaraðila og vinnsluaðila og sérstaklega til þarfa lítilla og meðalstórra fyrirtækja.[182] Þar sem sérstaklega er tekið fram í 1. mgr. 40. gr. að líta megi á þetta sem tækifæri til að taka mið af þörfum lítilla og meðalstórra fyrirtækja, þar sem setning hátternisreglna er hagstæð leið fyrir þá aðila sem hafa ekki mikið fjárhagslegt bolmagn til þess að ráðast í kostnaðarsamar aðgerðir til að uppfylla skyldur sínar gagnvart löggjöfinni.[183] Samþykktar hátternisreglur hafa möguleika á að virka sem verkfæri fyrir fyrirtæki og stofnanir sem sýnir fram á að ábyrgðarskyldu bæði ábyrgðaraðila og vinnsluaðila sé uppfyllt.[184] Eftirlitsyfirvöld líta einnig til þess meðal annars við álagningu sekta hvort fyrirtæki fylgi samþykktum hátternisreglum[185] og líta má á fylgni með hátternisreglum getur sem mildandi þátt varðandi viðurlög eftirlitsstjórnvalds, en jafnframt getur það leitt til þyngri viðurlaga.[186]

180 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 5.
181 sama heimild.
182 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 98. liður formála.
183 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 8.
184 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 77. liður formála.
185 Article 29 Data Protection Working Party, „Guidelines on the application and setting of administrative fines (wp253).“ (n. 150) 15.
186 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., 148. liður formála.

Inntak hátternisreglna getur verið mismunandi, því er heimilt fyrir samtök fyrirtækja að setja upp mjög þröngar hátternisreglur sem ná til tiltekinna aðferða við vinnslu eða setja mjög víðtækar reglur sem taka til allra vinnslu sem fer fram innan atvinnugeirans. Það fer því aðeins eftir því hvernig hátternisreglurnar eru samsettar hvernig skuli túlka þær eða ef um er að ræða mjög þröngar hátternisreglur, þá er möguleiki á að þær reglur teljist ekki sýna fram á reglufylgni með öllum ákvæðum persónuverndarlöggjafarinnar.[187] Ef um er að ræða mjög þröngar hátternisreglur er mikilvægt að það sé skýrt svo ekki skapist hætta á fölsku öryggi og almenningur geri sér grein fyrir því sem og aðrir ábyrgðaraðilar og vinnsluaðilar sem hyggjast nýta sér hátternisreglurnar.[188]

4.2.2. Eigendur hátternisreglna

Eins og áður hefur komið fram þá geta samtök fyrirtækja innan ákveðins atvinnugeira eða aðrir aðilar sem eru fulltrúar tiltekinna ábyrgðaraðila eða vinnsluaðila, sbr. 2. mgr. 40. gr. pvrg., sett sér hátternisreglur. Af þessu leiðir að fyrirtæki geta ekki sjálf upp á sitt einsdæmi sett sér hátternisreglur sem uppfylla skilyrði 40. og 41. gr. pvrg., heldur þá er þetta aðeins leið fyrir samtök eða hóp aðila.

Samtök sem vilja setja hátternisreglur fyrir sinn atvinnugeira geta sýnt fram á að þau komi fram fyrir hóp ábyrgðaraðila eða vinnsluaðila, hafi nægilega þekkingu og reynslu innan atvinnugeirans og að þau skilji þarfir hans. Þetta geta verið allt frá svæðisbundnum eða landsbundnum samtökum til alþjóðlegra samtaka. Dæmi um alþjóðasamtök er FEDMA, sem fjallað var um í örðum kafla ritgerðarinnar, FEDMA eru alþjóðleg regnhlífasamtök sem koma fram fyrir bæði svæðisbundin og landsbundin samtök fyrirtækja sem starfa við beina markaðssetningu. Þá er Samtök fjármálafyrirtækja dæmi um landssamtök.

4.2.3. Drög að hátternisreglum

Eins og fram kemur í 5. mgr. 40. gr. pvrg. þá þarf að leggja fyrir eftirlitsstjórnvaldið drög að hátternisreglum. Til þess að eftirlitsstjórnvaldið geti lagt mat á hvort drögin uppfylli skilyrði til að verða samþykkt verða að fylgja þeim upplýsingar um umfang reglnanna. Meðal þessara upplýsinga, eru hverjir séu meðlimir hátternisreglnanna, vinnsluaðferðir, hverjir eru hinir skráðu einstaklingar, tegund upplýsinga sem vinnslan nær til, lögsaga og fleira sem getur skipt máli við matið.[189] Þá þarf einnig að fylgja með hnitmiðuð yfirlýsing þar sem fram koma atriði

[187] Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 3.
[188] European Data Protection Board, „Guidelines 1/2019“ (n. 72) 9.
[189] sama heimild 11, sjá neðanmálsgrein 30.

sem snerta á tilgangi hátternisreglnanna, umfang þeirra og hvernig setning þeirra mun auðvelda árangursríka beitingu persónuverndarlöggjafarinnar.[190]

Drög hátternisreglnanna verða að vera lögð fram af samtökum eða fulltrúum flokka ábyrgðaaðila eða vinnsluaðila. Sá sem leggur drögin fram er eigandi hátternisreglnanna, sbr. 2. mgr. 40. gr. pvrg. Eigandi hátternisreglnanna verður að geta sýnt fram á við eftirlitsstjórnvaldið að samtökin hafi getu til að skilja þarfir meðlima sinna og geti með góðu móti skilgreint vinnsluna sem fer fram innan atvinnugeirans sem hátternisreglunum er ætlað að ná til.[191] Við gerð hátternisreglna þarf að gæta að því að eftirlitsaðilanum sé kleift að sinna eftirliti með þeim.

Í 5. mrg. 40. gr. er fjallað um þegar að samtök hafa samið hátternisreglur, eða hafa í huga að breyta settum hátternisreglum eða rýmka þær, ber þeim skylda að leggja drög að reglunum eða breytingum á þeim til eftirlitsstjórnvaldsins. Það er svo hlutverk eftirlitsstjórnvaldsins að samþykkja drögin ef það telur þau uppfylla skilyrði löggjafarinnar og tryggja viðeigandi verndarráðstafanir. Ef samtökin eða aðrir aðilar eru bundnir við eitt landssvæði og drögin að hátternisreglum hafa verið samþykkt í samræmi við 5. mgr. þá ber eftirlitsstjórnvaldinu að skrá reglurnar sérstaklega og birta þær, sbr. 6. mgr. 40. gr. pvrg.

Eigandi hátternisreglnanna verður að geta greint frá hvert sé markmið, umfang og hvernig þær muni einfalda beitingu ákvæða persónuverndarreglugerðarinnar. Þá nægir ekki að þær gagnist aðildarfélögum heldur einnig hinum skráðu einstaklingum.[192] Einnig verður að koma fram hvort hátternisreglurnar séu landsbundnar eða nái út fyrir landamæri og að fram komi greinar góð lýsing á vinnslunni og hvort reglurnar nái til mismunandi flokka ábyrgðaraðila eða vinnsluaðila.[193] Ef hátternisreglurnar eiga aðeins að vera bundnar við geira innan eins aðildarríkis þá er það eftirlitsstjórnvaldið í því ríki sem metur þær. Þær skulu verða gefnar út á móðurmáli aðildarríkisins, sem dæmi þá væri það Persónuvernd hér á Íslandi sem metur hátternisreglur og gefur samþykki fyrir þeim, ef þær tryggja fullnægjandi verndarráðstafanir, sem eiga að gilda hérlendis samkvæmt 9. tl. 4. mgr. 39. gr. pvl. sbr. m lið 1. mgr. 57. gr. pvrg. Ef sömu reglur eiga að ná út fyrir landssteinanna þá þarf einnig að gefa þær út á ensku.[194] Enn fremur ber Persónuvernd áður en það gefur út ákvörðun um gildi hátternisreglnanna að senda drög að ákvörðun sinni til Evrópska persónuverndarráðsins, sbr. b. lið 1. mgr. 64. gr. pvrg, og fá álit þess efnis.

190 sama heimild.
191 sama heimild 11–12.
192 Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 4.
193 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 12.
194 sama heimild 13.

Mikilvægt er að hátternisreglurnar hafi aukið vægi eða eitthvað meira fram að færa en aðeins það sem kveðið er á um í reglugerðinni.[195] Því ef hátternisreglurnar telja aðeins upp ákvæði reglugerðarinnar þá eru þær gagnslausar. Persónuverndarráðið leggur til að sérreglur sem gilda um atvinnugeirann séu fléttaðar inn í hátternisreglurnar, en jafnframt sé orðalagið í hátternisreglunum aðlagað að atvinnugeiranum. Það verði lagt upp með að reglurnar séu skrifaðar með því orðalagi sem þekkist innan atvinnugeirans í stað þess lögfræðilega orðlags sem er að finna í löggjöfinni.[196] Er það meðal annars gert til að auðvelda skilning meðlima á efni hátternisreglnanna og þar með eru þeir líklegri til að tileinka sér þær.

Ekkert hefur verið gefið út í tengslum við hátternisreglunar sem beinlínis mælir gegn því að innihald reglnanna nái yfir meira efni en aðeins það sem snýr að vinnsluaðferðum, af þessu mætti leiða að innihald reglnanna getur kveðið á um hvaða efni sem er svo lengi sem það stuðlar að réttri beitingu ákvæða reglugerðarinnar.[197]

Hátternisreglurnar verða að hafa viðeigandi verndarráðstafanir vegna þeirra áhættu sem vinnsla getur haft á frelsi og réttindi hinna skráðu einstaklinga. Eigandi hátternisreglnanna verður að staðfesta að þær séu samrýmanlegar landslögum og geta sýnt fram á að hagsmunaraðilum hafi verið boðin þátttaka við að semja drög að reglunum, þar á meðal hinir skráðu einstaklingar þegar kostur er á slíku samráði.[198]

4.2.3.1. Hátternisreglur í fleiru en einu aðildarríki

Ef hátternisreglurnar gilda um vinnslustarfsemi í fleiri en einu aðildarríki, þá ber eftirlitsstjórnvaldinu, áður en það samþykkir drög, breytingu eða rýmkun hátternisreglna að leggja þau fyrir Evrópska persónuverndarráðið, sbr. b. lið 1. mgr. 64. gr. pvrg., í samræmi við málsmeðferð 63. gr. pvrg. Persónuverndarráðið gefur svo álit sitt á hvort reglurnar samrýmist ákvæðum löggjafarinnar og tryggi viðeigandi verndarráðstafanir, sbr. 7. mgr. 40. gr. pvrg. Eftirlitsstjórnvaldinu ber að taka ýtrasta tillit til álits persónuverndarráðsins og skal það senda formanni persónuverndarráðsins tilkynningu þar sem tekið sé fram hvort það muni standa við drögin eða gera breytingu á þeim. Ef breyta á drögunum þá þurfa þau að fylgja með í tilkynningunni, sbr. 7. mgr. 64. gr. pvrg. Ef eftirlitsstjórnvaldið hyggst hins vegar ekki breyta ákvörðun sinni til samræmis við álit persónuverndarráðsins, hvort sem það er í heild sinni eða

195 sama heimild 14.
196 Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 4.
197 sama heimild 15.
198 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 16.

að hluta til þá fer málsmeðferð þess deilumáls samkvæmt c. lið 1. mgr. 65. gr. pvrg., sbr. 8. mgr. 64. gr. pvrg.

Ef álit persónuverndarráðsins er að drögin að hátternisreglunum séu samrýmanlegar ákvæðum löggjafarinnar, þá ber því að leggja álit sitt fyrir framkvæmdarstjórnina, sbr. 8. mgr. 40. gr. pvrg. Framkvæmdastjórnin hefur þá vald til að ákveða hvort hátternisreglurnar hafi almennt gildi innan sambandsins og skal slíkt gert með framkvæmdargerð, sbr. 9. mgr. 40. gr. pvrg. Þá er það einnig hlutverk framkvæmdastjórnarinnar að kynna þær hátternisreglur sem hafa hlotið almennt gildi samkvæmt 9. mrg., sbr. 10. mgr. 40. gr. pvrg. Loks er kveðið á um það í 11. mgr. að það fellur í hlut persónuverndarráðsins að safna saman öllum samþykktum hátternisreglum, hvort sem það eru breytingar eða rýmkanir á reglunum, í skrá og gera þær aðgengilegar almenningi með viðeigandi hætti. Evrópska persónuverndarráðið hefur gefið það út að aðeins hátternisreglur sem hafa fengið slíka almenna viðurkenningu geti gilt fyrir skipulagðan flutning persónuupplýsinga utan samningssvæðisins EES,[199] sbr. e. lið 2. mgr. 46. gr. pvrg.

4.2.4. Samþykktar hátternisreglur

Það fer allt eftir innihaldi hátternisreglnanna, hversu viðtækar eða þröngar þær eru, hvert hlutverk meðlima samtakana sem hafa sett sér hátternisreglur varðandi fylgni með hátternisreglunum og persónuverndarlöggjafarinnar. Samt sem áður þá hefur eftirlitsstjórnvaldið víðtækt hlutverk sérstaklega varðandi gæslu á því að reglurnar þjóni tilgangi sínum.[200] Eftirlitsstjórnvaldið þarf því að fylgjast grannt með stöðu mála varðandi framkvæmd hátternisreglanna og vinna samhliða eftirlitsaðilanum við að leysa úr málum sem koma upp við framkvæmd reglnanna. Eftirlitsaðilinn verður að þó að hafa frumkvæði í viðræðum við eftirlityfirvaldið vegna samræmingar hátternisreglana við persónuverndarlöggjöfina á málum sem uppkoma í tengslum við framkvæmd á reglunum.[201]

Það er svo alltaf eftirlitsstjórnvaldið sem samþykkir eða hafnar breytingum á hátternisreglunum og faggildingu á eftirlitsaðilanum, sbr. 5. mgr. 41. gr. pvrg. Ekki þarf samþykki eftirlitsstjórnvalda við öllum breytingum á hátternisreglunum, eigendum reglnanna er heimilt að gera almennar og minniháttar uppfærslur á þeim, sem dæmi að uppfæra nafn samtakanna sem á reglurnar og svo framvegis, en þær breytingar sem snerta efnislegt innihald

[199] sama heimild 10.
[200] sama heimild 25.
[201] sama heimild.

reglnanna, eins og ef bæta á auka ákvæði við reglurnar, þurfa samþykki hjá eftirlitsstjórnvaldinu, sbr. 5. mgr. 40. gr. pvrg.

4.2.5. Hátternisreglur opinberra aðila

Það segir skýrt í 6. mgr. 41. gr. pvrg. að sú grein eigi ekki við um vinnslu af hálfu opinberra yfirvalda eða stofnanna. Í meginatriðum þá hefur þetta ákvæði þá þýðingu að hið opinbera þarf ekki að hafa faggildan eftirlitsaðila til að sinna eftirliti með sínum hátternisreglum. Með þessu er verið að færa ákvörðunarvaldið yfir til ríkjanna sjálfra, að þau taki ákvörðun hvort skylda eigi opinberar stofnanir þurfi að fá sérstakan faggildan eftirlitsaðila með hátternisreglunum.
Þó að eftirlitsaðili að hátternisreglum opinberra aðila þurfi ekki að hljóta faggildingu, sbr. 6. mgr. 41. gr., þá á slíkt ekki að útþynna kröfuna um skilvirka framkvæmd og eftirlit með hátternisreglunum, þar sem hægt er að ná því með að aðlaga núgildandi endurskoðunarkröfur um að það taki einnig til eftirlits með hátternisreglum.[202]

Við setningu persónuverndarlaga nr. 90/2018 voru ekki sett nein sérstök ákvæði um þær valkvæðu leiðir sem fyrirtæki geta nýtt sér samkvæmt fimmta þætti, fjórða kafla reglugerðarinnar. En í frumvarpinu með lögunum segir að Persónuvernd skuli gefa út leiðbeiningar fyrir framkvæmd hátternisreglnanna,[203] en slíkar leiðbeiningar hafa ekki verið gefnar út. Af þeim sökum þá má ætla að hérlendis gildi það að opinberir aðilar sem hafa sett sér slíkar hátternisreglur þurfi eftirlitsaðili þeirra reglna ekki að hljóta sérstaka faggildingu Persónuverndar að svo stöddu. Hins vegar verður að ætla að Persónuvernd muni taka á þessu máli þegar á þetta mun reyna. Enda gildi nálægðarreglan um þessi ákvæði, það er að ríkin sjálf ráði framkvæmdinni heima fyrir.

4.2.6. Eftirlit með hátternisreglunum

Eftirlit með hátternisreglum skal vera í höndum þriðja aðila sem hefur viðeigandi sérþekkingu á viðfangsefni reglnanna og hefur hlotið faggildingu samkvæmt 1. mgr. 41. gr. pvrg. Jafnframt verður eftirlitsaðilinn að hafa viðeigandi aðstöðu til þess að standast þær kröfur og þá ábyrgð sem fylgir hlutverki hans.[204]

Almennt má telja að eigendur hátternisreglna hafi úr að velja tveim megin leiðum varðandi eftirlit með hátternisreglunum, það er annars vegar ytra eftirlit og hins vegar innra eftirlit. Dæmi um innra eftirlit gæti verið af hálfu sérfræðinefndar eða af sjálfstæðri og óháðri

[202] sama heimild 26.
[203] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, um 23. gr. 5. mgr.
[204] European Data Protection Board, „Guidelines 1/2019“ (n. 72) 13.

deild sem starfar hjá þeim samtökum sem eiga hátternisreglurnar, það er jafnframt þeirra að huga að áhættustýringu svo hægt sé að tryggja sjálfstæði aðilanna.[205] Það getur því verið nauðsynlegt þegar um innra eftirlit er að ræða að grípa til þeirra ráðstafana að skipta um aðila sem sitja í nefndinni. Það ættu sömu reglur að gilda um þessa starfsmenn eins og um persónuverndarfulltrúann, það á ekki að sækja fyrirmæli um störf sín frá öðrum og ætti að vera verndað fyrir viðurlögum eða inngripi er þeir sinna eftirlitshlutverki sínu.[206] Svo hægt sé að tryggja sjálfstæði eftirlitsaðilans gæti þurft að leita til aðila utan samtakana og þar með setja upp ytra eftirlit, til að sýna fram á að það séu í gildi nægilegar verndarráðstafanir til að koma í veg fyrir hagsmunaárekstra. Ef um er að ræða ytra eftirlit með reglunum þá verður sá aðili að geta sýnt fram á að viðeigandi fyrirkomulag sé við lýði sem myndi greina og dregið úr áhættu á hagsmunaárekstrum með fullnægjandi hætti. Ef hætta er á óhlutdrægni þarf eftirlitsaðili að sýna fram á hvernig hann kemur í veg fyrir, eða lágmarkar, slíka áhættu og verndar hlutleysi eftirlitsaðilans.[207]

Ef um er að ræða innra eftirlit og eftirlitsaðili er meðlimur í samtökunum sem reglurnar taka til þá getur hann sýnt fram á sjálfstæði sitt með því að tryggja að hann sé ekki fjárhagslega háður neinum aðila samtakanna. Það er því ákveðin leið fyrir eftirlitsaðilann að sýna fram á sjálfstæði sitt ef hann getur sýnt fram á fjárhagslegt sjálfstæði gagnvart meðlimum samtakana. Eftirlitsaðilinn verður einnig að geta sýnt fram á sjálfstæði sitt við ákvörðun á viðurlögum við brotum á reglunum. Í meginatriðum þá þarf eftirlitsaðilinn, hvort sem um er að ræða innra eða ytra eftirlit að bregðast sjálfstætt við hegðun meðlima reglnanna.

Þá er vert að taka fram að eftirlitsstjórnvald hefur heimild til að sekta eftirlitsaðila að hátternisreglunum ef hann sinnir ekki skyldum sínum samkvæmt 4. mgr. 41. gr. pvrg., sbr. c. lið 4. mgr. 83. gr. pvrg. Sú sekt getur numið allt að 10 milljónum evra eða allt að 2% af árlegri heildarveltu, hvort heldur er hærra.

Loks getur eftirlitsstjórnvald afturkallað faggildingu eftirlitsaðilans, sbr. 5. mgr. 41. gr. pvrg. Af þeim sökum er mikilvægt að eigandi hátternisregla hafi skýrt verklag um hvað skal gera ef svo er í pottinn búið. Afleiðingar þess að afturkalla faggildingu eftirlitsaðilans getur leitt til tímabundinnar eða varanlegrar stöðvunar þar sem skilyrðum um eftirlit með hátternisreglunum er ekki lengur uppfyllt. Slíkt getur haft slæm áhrif á orðspor hátternisreglnanna og rýrt traust hinna skráðu einstaklinga til samtakana og meðlima þeirra.[208]

[205] Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 6.
[206] European Data Protection Board, „Guidelines 1/2019“ (n. 72) 22.
[207] sama heimild.
[208] sama heimild 26.

4.2.6.1. Skilyrði fyrir faggildingu eftirlitsaðila

Í 2. mgr. 41. gr. pvrg. er að finna hver séu hin helstu skilyrði sem eftirlitsaðili þarf að uppfylla svo hann hljóti faggildingu samkvæmt löggjöfinni. Evrópska persónuverndarráðið hefur tekið saman leiðbeiningar um hátternisreglurnar og í þeim er fjallað um þau skilyrði sem eftirlitsaðili verður að uppfylla. Sá sem hyggst verða eftirlitsaðili með hátternisreglunum og sækja sér faggildingu þess efnis verður að uppfylla fjölda skilyrða til að fullnægja kröfum eftirlitstjórnvaldsins og hljóta faggildingu þess. Það er hins vegar hlutverk eigenda hátternisreglnanna að sýna fram á getu þess aðila til að sinna eftirliti og að sá hinn sami uppfylli skilyrðin sem talin eru upp í fyrrnefndri 2. mgr. 41. gr. pvrg.[209]

Fyrsta skilyrðið sem eftirlitsaðili verður að uppfylla til þess að hljóta faggildingu er að hann geti sýnt fram á *sjálfstæði* sitt gagnvart eigendum hátternisreglnanna, sem og meðlimum hátternisreglnanna og atvinnugeiranum sem slíkum. [210]

Annað skilyrði sem eftirlitsaðilinn verður að sýna fram á að hann geti framkvæmt verkefni sín og skyldur án þess að það leiði til *hagsmunaárekstra*, sbr. d. lið 2. mgr. 41. gr. pvrg. Af þeim sökum þurfa eigendur hátternisreglnanna að sýna fram á að eftirlitsaðilinn muni víkja frá þeim verkefnum sem setja þá í stöðu að þeir geta ekki sinnt því hlutverki. Af sama skapi þá verður eftirlitsaðilinn að gæta þess að láta ekki undan þrýstingi, hvort sem það á við um utanaðkomandi eða innanbúðar þrýsting, jafnframt skal aðilinn ekki leita eftir áliti einstaklinga, stofnanna eða samtaka. Ef um er að ræða innra eftirlit, þá er mikilvægt að vernda aðilann fyrir íhlutun eða viðurlögum frá eigendum hátternisreglnanna, eða öðrum tengdum aðilum eða örðum meðlimum samtakanna sem reglurnar taka til.[211]

Í þriðja lagi þarf eigandi hátternisreglnanna þarf að geta sýnt fram á að eftirlitsaðilinn hafi nægilega *sérfræðiþekkingu* til þess að sinna eftirlitinu. Því verða upplýsingar um þekkingu og reynslu aðilans hvað varðar persónuverndarlöggjöfina sem og um vinnslu við starfsemi hjá viðkomandi atvinnugrein eða atvinnustarfsemi. Ennfremur þá nýtist ítarlegur skilningur á þeim vandamálum varðandi persónuvernd og sérfræðiþekking á sértækri vinnslustarfsemi sem reglurnar taka til. Starfsfólk eftirlitsaðilans þarf að hafa nægilega reynslu og þjálfun til að framkvæma eftirlitið, hvort sem það felst í endurskoðun, almennu eftirliti eða gæðaeftirliti.[212]

Fjórða skilyrðið er að eftirlitsaðilinn skal hafa í gildi *verklagsreglur og ferla* til þess að geta með fullnægjandi hætti metið hæfi ábyrgðaraðila og vinnsluaðila sem vilja gerast meðlimir

209 sama heimild 21.
210 sama heimild 21–22.
211 sama heimild 23.
212 sama heimild.

eða þátttakendur að hátternisreglunum, sbr. b. lið 2. mgr. 41. gr. pvrg. Eftirlitsaðili verður að meta út frá verklagsreglunum hvort ábyrgðaraðilar og vinnsluaðilar geti uppfyllt skilyrði hátternisreglnanna. Jafnframt verður eftirlitsaðilinn að geta haft virkt eftirlit með fylgni meðlima að reglunum, hvort sem það er að ræða handahófskennt eftirlit, árlegt eftirlit, regluleg skýrslugerð eða almenn eftirfylgni með notkun spurningarlista. Virkt verklag og ferlar eru mikilvæg tæki sem beita má til að koma í veg fyrir aðstæður þar sem fylgst er með hluta meðlima meðan aðrir fá ekki eins virkt eftirlit.[213]

Í fimmta lagi er gert það að skilyrði að eftirlitsaðilinn hafi virka ferla og verklagsreglur til að takast á við *kvartanir, frávik eða brot á hátternisreglunum* og afar mikilvægt er að gæta gagnsæis við ferlið og að almenningur fái slíkar upplýsingar. Af þeim sökum þarf almenningur að geta með einföldum hætti nálgast kvartanir sem borist hafa eftirlitsaðilanum og fengið að vita hver niðurstaða þeirra mála var, sbr. c. lið 2. mgr. 41. gr. pvrg.[214] Þá verður eftirlitsaðili að hafa heimild til a setja á viðurlög við brotum á hátternisreglunum. Ef meðlimur fer á svig við ákvæði hátternisreglnanna þá verður eftirlitsaðilinn að bregðast skjótt við. Krefjast verður viðeigandi úrbóta og markmið með slíkum aðgerðum af hálfu eftirlitsaðilans ætti alltaf miða að því að koma í veg fyrir endurtekið brot í framtíðinni. Úrræði gætu verið allt frá að gefa út viðvörun, tilkynna til stjórnar viðkomandi meðlims um brot, formleg krafa um tilteknar úrbætur fyrir ákveðin tíma, að meina viðkomandi meðlim um þátttöku ábyrgðaraðilum eða vinnsluaðilum þátttöku, hvort sem það sé tímabundið þar til úrbætur eru gerðar eða til frambúðar. Eftirlitsaðili gæti gripið til þess ráðs að birta þær aðgerðir sem það hefur þurft að grípa til vegna brota á hátternisreglunum, þetta getur sérstaklega átt við þegar um alvarlegri brot er að ræða að þá sé sá aðili nafngreindur.[215]Ef eftirlitsaðili stendur utan við samtökin sem eru eigendur hátternisreglnanna þá ætti verklagið að vera þannig að samtökin fái upplýsingar um hvaða viðurlög gripið var til gegn hvaða meðlim.[216]

Loks er sjötta skilyrðið að eftirlitsaðilinn hafi verklag um hvernig hátta eigi *skilvirkum samskiptum um framkvæmd eftirlitsins til eftirlitsstjórnvaldið*. Þetta tekur einnig til um hvernig samskiptum skal háttað þegar um brot á reglunum er að ræða og hver viðurlögin við þeim voru, jafnframt um hvernig öðru eftirliti er háttað. Sem dæmi að send sé árlega skýrsla til eftirlityfirvaldsins um störf eftirlitsaðilans yfir árið, sbr. 1. mgr. 41. gr. pvrg. Að auki verður að tryggja að eftirlitsstjórnvaldið sé ekki að hindra við að sinna hlutverki sínu, samkvæmt

213 sama heimild neðanmálsgrein 77.
214 sama heimild 24.
215 sama heimild.
216 sama heimild neðanmálsgrein 78.

löggjöfinni. Hátternisreglur þar sem heimild er fyrir meðlimi til að einhliða samþykkja nýjan eftirlitsaðila eða afturkalla umboð slíks án nokkurra tilkomu eftirlitsstjórnvaldsins, væri andstætt 5. mgr. 41. gr. pvrg.[217]

4.2.6.2. Eftirlit með hátternisreglum – sérstaða Íslands

Þegar skilyrði fyrir eftirliti hafa verið skoðuð vakna upp spurningar varðandi framkvæmd þess hérlendis. Ísland býr við ákveðna sérstöðu sökum þess hversu fámenn við erum. Má velta því upp hvort erfiðlega muni ganga fyrir samtök hérna á Íslandi að finna eftirlitsaðila sem geti uppfyllt öll þau skilyrði sem sett eru fyrir faggildingunni. Nándin er svo mikil að þegar skipt er um forstjóra í Kauphöllinni að þá er það jafnvel bróðir þess sem lætur af störfum sem tekur við keflinu.[218]

Þá má einnig velta því upp varðandi fjármögnun eftirlitsins að samtök í helstu atvinnugeirunum hérlendis eru brotabrot af þeim fjölda sem er í sambærilegum samtökum erlendis. Þannig voru t.d. 17 skráðir meðlimir í Samtökunum leikjaframleiðenda á Íslandi árið 2019[219] en í samtökum leikjaframleiðanda (UK Interactive Entertainment) í Bretlandi eru yfir 450 meðlimir.[220]

SMEunited eða UEAPME, sem eru samtök örfyrirtækja, lítilla og meðalstórra fyrirtækja í Evrópu[221] gerði athugasemdir við framkvæmd eftirlits að hátternisreglum. Athugasemdir þeirra snéru aðallega að því að mörg samtök fyrirtækja hafa hvorki fjárhagslegt bolmagn, né nægan mannaforða til þess að setja upp eftirlit við hátternisreglum samkvæmt 41. gr. pvrg. Lögðu þau til að hægt væri að samnýta eftirlitsaðila til þess að takast á við þetta vandamál.[222] Í slíkri lausn gæti þó falist stærra vandamál vegna þeirra sem myndu aðeins fljóta með án þess að uppfylla skilyrði reglnanna, þar sem eftirlitinu gæti orðið ábóta vant sérstaklega ef ekki erum að ræða sambærilega vinnslustarfsemi.

217 sama heimild 25.
218 mbl.is, „Bróðirinn tekur við forstjórastóli Kauphallarinnar“ <https://www.mbl.is/vidskipti/frettir/2019/10/15/brodirinn_tekur_vid_forstjorastolnum/> skoðað 28. maí 2020.
219 Northstack, „State of the Icelandic Game Industry 2019“ (nóvember 2019) 4 <https://www.si.is/media/_eplica-uppsetning/IGI-report-2019-Web-v2.pdf> skoðað 4. júní 2020.
220 UK Interactive Entertainment, „Our members | Ukie“ <https://ukie.org.uk/our-members> skoðað 6. janúar 2020.
221 SMEunited, „About SMEunited“ <https://smeunited.eu/about-us> skoðað 29. maí 2020.
222 SMEunited, „SMEunited Comments on Codes of Conduct and Monitoring Bodies Under Regulation 2016/679“ 2 <https://smeunited.eu/admin/storage/smeunited/190402-smeunited-comments-on-codes-of-conduct-and-monitoring-bodies-under-regulation.pdf> skoðað 1. júní 2020.

4.2.7. Hátternisreglur – leið til að uppfylla ábyrgðarskylduna

Í a. til k. lið 2. mgr. 40. gr. eru talin upp þau atriði sem hátternisreglur geta tekið til og ætlað er að kveða nánar um beitingu ákvæða reglugerðarinnar innan atvinnugeirans. Það sem hátternisreglurnar geta kveðið á um eru sanngirni og gagnsæi vinnslu og lögmæta hagsmuni ábyrgðaraðila fyrir vinnslunni, sbr. a. lið 1. mgr. 5. gr. pvrg. og sbr. 6. gr. pvrg., söfnun persónuupplýsinga meðal annars úr frá hvaða persónuupplýsingar eru nauðsynlegar fyrir vinnsluna, sbr. c. lið 1. mgr. 5. gr. pvrg., og notkun gerviauðkenna við vinnslu persónuupplýsinganna.

Enn fremur væri hægt að tilgreina í hátternisreglunum upplýsingar sem veittar verða almenningi og hinum skráðu einstaklingum, t.d. hvernig hinir skráðu einstaklingar geti leitað réttar síns. Atriði sem varðar vinnslu persónuupplýsinga barna og hvaða upplýsingar þeim eru veittar og hvernig tekið sé tillit til þeirra sérstaklega út frá þeirri vernd sem þau eiga rétt á og hvernig skuli afla samþykkis forsjáraðila. Hvaða tæknilegu og skipulagslegu ráðstafanir gripið hefur verið til vegna vinnslunnar, sbr. 24. gr. pvrg., jafnframt hvernig skal tryggja öryggi vinnslunnar samkvæmt 32. gr. pvrg. Hvernig og hvenær skal tilkynna um öryggisbresti til eftirlitsstjórnvalda og hinna skráðu einstaklinga og enn fremur hvernig skal leysa deilumál milli ábyrgðaraðila og skráðra einstaklinga.

Í 3. mgr. 40. gr. pvrg. er kynnt leið þar sem nýta má hátternisreglur til að tryggja verndarráðstafanir fyrir flutning gagna til þriðja ríkis. Af þessu leiðir að hátternisreglurnar má einnig nýta til að tryggja viðeigandi verndarráðstafanir gildi um vinnsluna ef hún fer fram af hálfu ábyrgðaraðila eða vinnsluaðila sem eru staðsettir utan gildissvæðis persónuverndarreglugerðarinnar, sbr. 3. gr. pvrg. Þetta gæti átt við ef ábyrgðaraðili er aðili að samþykktum hátternisreglum en vinnsluaðili er staðsettur í þriðja ríki, þá megi senda gögn til þess vinnsluaðila ef hann hefur skuldbundið sig að fylgja ákvæðum hátternisreglnanna. Sem dæmi um slíkt væri meðal annars að tryggja hagsmuni og réttindi einstaklinga að upplýsingum. Þetta á þó aðeins við um hátternisreglur sem hafa hlotið almennt gildi skv. 9. mgr. 40. gr. pvrg.

4.2.8. Lagaleg staða hátternisreglna

Ef við lítum á hátternisreglur samkvæmt persónuverndarreglugerðinni út frá lagalegu sjónarhorni þá má halda því fram að þær hafi sömu réttaráhrif og vottun. Þátttaka í samþykktum hátternisreglum er leið sem færir ábyrgðaraðilum og vinnsluaðilum tækifæri á að sýna fram á reglufylgni.

Þrátt fyrir það þá má ekki líta svo á að ef fyrirtæki eða stofnun gerist meðlimur að samþykktum hátternisreglum að fyrirtækið eða stofnunin geti ekki brotið gegn ákvæðum persónuverndarlöggjafarinnar. Því við gerð hátternisreglnanna er það eigandi hátternisreglnanna sem þarf að sýna fram á að inntak reglnanna samrýmist reglugerðinni og að tryggðar séu nægilegar og viðeigandi verndarráðstafanir. Þá eru það í raun aldrei ábyrgðaraðilarnir sjálfir eða vinnsluaðilarnir sem þurfa að sýna fram á fylgnina við hátternisreglurnar við eftirlitsstjórnvaldið. Það þarf aðeins að sýna fram á fylgnina við hátternisreglunar varðandi eftirlit þeirra og þá fyrir eftirlitsaðilanum. Má því lýsa hátternisreglunum á þann veg að þetta sé nokkurskonar blönduð leið til að sýna fram á eigin eftirlit með löggjöfinni (e. hybrid form of self-regulation), þar sem eftirlitsstjórnvald samþykkir ramman og innan þess ramma fer eigin eftirlit fram. Einnig má líta á hátternisreglurnar sem lögákveðið samkomulag um eigið eftirlit, þar sem að eftirlitið fer fram innan ramma löggjafarinnar.[223] Þar sem það er eftirlitsaðilinn sem átti að sýna fram á við eftirlitsstjórnvaldið að samræmi sé á milli hátternisreglnanna og ákvæðum persónuverndarlöggjafarinnar en í raun eru það ekki ábyrgðaraðilarnir eða vinnsluaðilarnir sjálfir, þeir þurfa hins vegar að gæta að fylgni við ákvæði hátternisreglnanna þegar framkvæmt er eftirlit með þeim. Enda getur þátttaka í hátternisreglum þar sem ábyrgðaraðili eða vinnsluaðili fylgir ekki ákvæðum reglnanna haft í för með sér afleiðingar.

Þrátt fyrir að um valkvæða leið sé að ræða fyrir ábyrgðaraðila og vinnsluaðila þá ber þeim að fylgja þeim ef þeir hafa sótt um aðild annars eiga þeir á hættu meðal annars tímabundna eða algjöra útilokun til frambúðar frá þátttöku að hátternisreglunum. Eftirlitsaðila reglnanna ber að tilkynna brot til eftirlitstjórnvalds, sbr. 4. mgr. 41. gr. pvrg. Þá hafa þau úrræði sem eftirlitsaðili að hátternisreglunum grípur til ekki áhrif á hvaða viðurlög eftirlitsstjórnvaldið beitir, enda koma hátternisreglur ekki í veg fyrir að eftirlitsstjórnvaldið sinni hlutverki sínu, sem felst meðal annars í álagningu stjórnvaldssekta.[224]

Fylgni ábyrgðaraðila og vinnsluaðila að hátternisreglum getur samt haft áhrif á hvort eftirlitsstjórnvald ákveður að leggja stjórnvaldsekt við broti og hver fjárhæðin skal vera, sbr. j. lið. 2. mgr. 83. gr. pvrg. Fylgni við hátternisreglur getur komið til lækkunar slíkra sekta eða hækkunar.[225] Sem dæmi þá gæti það komið til hækkunar slíkra sekta ef ábyrgðaraðili hegðar sér ekki í samræmi ákvæði hátternisreglnanna, enda gæti verið litið svo á að aðili hafi nýtt sér

[223] Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 5.
[224] Alþt. 2017-2018 A-deild, þskj. 1029 - 622 mál,, um 23. gr. 5. mgr.
[225] 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) 46/2018 EES-viðbætir við Stjtíð ESB 6., um 23. gr. 5. mgr.

hátternisreglur til þess að villa fyrir um vinnsluaðferðir sínar og þar með veiti það falskt öryggi fyrir hina skráðu einstaklinga.[226]

4.2.9. Hátternisreglur - raunhæf leið fyrir fyrirtæki og stofnanir?

Telja má að með fylgni við hátternisreglur geti falist tækifæri fyrir fyrirtæki og stofnanir þar sem þar sé möguleiki á að gagna inn í tilbúið kerfi sem sniðið er að þeim og þeirra vinnslu. Þar með tryggja að vinnslustarfsemi þeirra sé í samræmi og uppfylli kröfur persónuverndarlöggjafarinnar. Þó fer það eftir eðli samtaka sem semja hátternisreglurnar hvort um sé að ræða fullbúið kerfi, en hátternisreglurnar geta þó verið tækifæri til þess að útbúa slíkt kerfi fyrir meðlimi þeirra. Hátternisreglurnar geta því nýst þessum aðilum sem leiðbeiningar um hvernig sé best að haga vinnslu persónuupplýsinga til þess að tryggja skyldur þeirra gagnvart persónuverndarlöggjöfinni. Þar sem sérstaklega er tekið fram í 77. lið formálsorða reglugerðarinnar að með hátternisreglum megi veita ábyrgðaraðilum sem og vinnsluaðilum leiðbeiningar um hvernig sýna skuli fram á fylgni við reglur, þá segir enn fremur í 81. lið formálsorðanna að ef vinnsluaðili fylgir samþykktum hátternisreglum megi sýna fram á að ábyrgðaraðili uppfyllir skuldbindingar sínar. Þó ber að nefna að ekki er hægt að nýta hátternisreglur til að sýna fram á að skyldum innbyggðrar og sjálfgefinnar persónuverndar samkvæmt 25. gr. séu uppfyllt, sbr. 3. mgr. 25. gr. pvrg.

Þá geta hátternisreglur einnig verið tæki fyrir samtök fyrirtækja til að skapa og ákveða bestu venjur og starfshætti við vinnslustarfsemi geirans. Þar af leiðandi séu hátternisreglurnar mikilvæg auðlind fyrir fyrirtæki sem hægt er að treysta á til þess að takast á við áskoranir í vinnslunni og tryggja mun meira öryggi fyrir persónuupplýsingarnar í samræmi við persónuverndarlöggjöfina. Jafnframt geta hátternisreglur aukið sjálfstraust fyrirtækjanna og réttaröryggi þeirra, þar sem í þeim sé að finna lausnir á þekktum vandamálum í tengslum við vinnslu persónuupplýsinga. Reglurnar hvetja til þróunar á sameiginlegri og samrýmdri aðferð við vinnslu persónuupplýsinga innan tiltekins geira.[227]

Enn fremur geta hátternisreglur verið tækifæri til að öðlast traust almennings á vinnslustarfsemi atvinnugeirans. Þar sem í reglunum getur verið tekið á atriðum sem talið er að valdi vandamálum og áhyggjur almennings koma í ljós eftir almennar umræður í samfélaginu og þar með litið á atriðið sem vandamál innan geirans sjálfs. Með því að fjalla um

[226] Article 29 Data Protection Working Party, „Guidelines on the application and setting of administrative fines (wp253).“ (n. 150) 15.
[227] European Data Protection Board, „Guidelines 1/2019“ (n. 72) 9.

og takast á við slík mál í hátternisreglum er verið að auka gagnsæi fyrir almenning og eyða tortryggni þeirra vegna vinnslu persónuupplýsinganna einstaklinganna sjálfra.[228]

Fylgni með hátternisreglum táknar að ábyrgðaraðili eða vinnsluaðili hafa sjálfir lýst yfir vilja til þess að fara eftir efni hátternisreglnanna án þess að eftirlitsstjórnvald fái haldbærar sannanir fyrir því. Það er eftirlitsaðilinn metur hvort vinnsla af þeirra hálfu sé í samræmi við ákvæði hátternisreglnanna. Af þessu leiðir að fylgni við hátternisreglurnar geti haft sömu réttaráhrif og vottun en þó án þess að aðili tryggi að vinnslan af hans hálfu sé í samræmi við ákvæði reglugerðarinnar.[229] Þó má ætla að þessi staða vari aðeins stutt þar sem að eftirlitsaðili skal sinna eftirliti á því hvort meðlimir hagi vinnslustarfsemi sinni í samræmi við hátternisreglurnar. Hins vegar þá fer það allt eftir því hvernig eftirlitinu er háttað, þá hversu reglulegt það skuli vera.

Þá er jafnframt vert að nefna að hátternisreglunar geta verið góð leið fyrir fyrirtæki til að flytja gögn löglega yfir landamæri og út fyrir gildissvæði reglugerðarinnar, ef hátternisreglurnar hafa hlotið almennt gildi skv. 9. mgr. 40. gr. pvrg., sbr. 3. mgr. 40. gr. pvrg. Ef nægileg jákvæð reynsla færst, gætu hátternisreglurnar orðið grundvöllur fyrir alþjóðlegum gagnaflutningi.[230] Mætti telja að í þessu felist auka hvatning fyrir samtök fyrirtækja og stofnanna til að setja sér hátternisreglur, sérstaklega innan geira þar sem vinnsla upplýsingar er þvert á landamæri. Enda væri þá óþarfi að jafnframt yrði gripið til annarra ráðstafanna við slíkan gagnaflutning.

Eins og áður hefur komið fram þá geta fyrirtæki ekki upp á sitt einsdæmi sett sér hátternisreglur, heldur verða samtök fyrirtækja og stofnana innan geirans eða hópur ábyrgðaraðila eða vinnsluaðila að gera slíkt. Þarf að leiðandi er þetta aðeins raunhæf leið fyrir þau fyrirtæki sem eru meðlimir í samtökum sem hafa áhuga á að hefja þá vegferð að semja slíkar hátternisreglur. Það getur verið hægara sagt en gert, enda felur það í sér mikla vinnu þar sem kortleggja þarf í raun þær lagaskyldur sem aðilum ber að fylgja og sníða hátternisreglunar út frá þeim. Þar sem hátternisreglurnar eiga ekki aðeins að taka upp ákvæði persónuverndarreglugerðarinnar, heldur verða þær að samræma skyldur fyrirtækjanna samkvæmt reglugerðinni að öðrum lagaskyldum. Ef samtökin eru í fyrirsvari fyrir einsleitan geira, þar sem vinnslustarfsemi er að mestu leyti sú sama, getur þetta verið hagkvæm leið og einfaldað líf meðlima samtakana til muna, sérstaklega með tilliti til skyldna samkvæmt

[228] sama heimild 10.
[229] Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 14.
[230] Rita Heimes, „Top 10 operational impacts of the GDPR: Part 9 - Codes of conduct and certifications“ <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/> skoðað 5. maí 2020.

persónuverndarlöggjöfinni. Þá gæti einnig sú staða verið uppi að innan ákveðina atvinnugeira sé svo mikil samkeppni á markaðnummilli fyrirtækja og stofnana að það sé í raun enginn vilji fyrir slíku samstarfi, þrátt fyrir að allir hluteigandi aðilar geti notið góðs af því.

Annað atriði sem þó gæti valdið erfiðleikum fyrir samtök fyrirtækja snýr að framkvæmd eftirlits með hátternisreglunum. Sérstaklega hvað varðar minni samtök sem hafa ekki nægilegt fjárhagslegt bolmagn til þess að halda úti starfsfólki til að sinna eftirliti með hátternisreglunum, þar sem gæta verður að því að ekki verði hagsmunaárekstrar. Þá getur einnig verið kostnaðarsamt að fá utanaðkomandi aðila til þess að sinna þessu eftirliti.

Þá má einnig nefna að hátternisreglur veita fyrirtækjum og stofnunum almennt ekki sama samkeppnislega forskot og vottun getur haft í för með sér, þar sem allur atvinnugeirinn sem njóti góðs af setningu hátternisreglna, frekar en einstök fyrirtæki. Sérstaklega þar sem fyrirtæki fá ekki innsigli eða merki þess efnis að þeir séu meðlimir að hátternisreglum líkt og um vottun væri að ræða. Þar af leiðandi er vottun mun sýnilegri leið fyrir viðskiptavini, neytendur og almenning til þess að sýna fram á fylgni við ákvæði löggjafarinnar.

4.2.9.1. Hátternisreglur - tækifæri lítilla og meðalstórra fyrirtækja

Hátternisreglurnar gætu því verið skilvirk lausn fyrir lítil og meðalstór fyrirtæki, þar sem þau hafa oftast nær takmarkaðar bjargir og þekkingu til að takast á við kröfur persónuverndarlöggjafarinnar. Má telja að fylgni við hátternisreglur hafi sama réttaröryggi og fengist með vottun, en vottuninni fylgi almennt mun meiri kostnaður, bæði hvar varðar kostnað við vottun, en einnig oft á tíðum falinn kostnað eins og kaup á sérfræðiráðgjöf vegna vinnu við vottunina.[231]

Tvíþætt eðli hátternisreglna kemur sér einnig vel fyrir minni aðila á markaði, þar sem samtímis eru reglurnar leiðarljós fyrir þá og kröfur sem þeim ber að fylgja, þar af leiðandi geta hátternisreglur verið leiðbeiningar um hvernig aðila á að hegða sér. Þar sem þessir aðilar hafa almennt hvorki nægileg fjárráð til að kaupa sér sérfræðiráðgjöf, né mannafla til að kynna sér þær skyldur sem hvíla á herðum þess vegna persónuverndarlöggjafarinnar.[232]

Það sem getur valdið erfiðleikum fyrir lítil og meðalstór fyrirtæki er ef þau eru meðlimir í minni samtökum hafa ekki mannafla né fjármagn til að sinna eftirliti. Því mætti telja að stærstu tækifærin fyrir lítil og meðalstór fyrirtæki væru ef þau tengdust sterkum samtökum þar sem vinnsla persónuupplýsinga sé fremur einhæf og einsleit milli allra meðlima samtakanna. Þá

231 Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 14.
232 European Data Protection Board, „Guidelines 1/2019“ (n. 72) 23.

mætti einnig telja að smærri aðilar njóti góðs af því ef stærri fyrirtæki eru innan samtakana sem hafa getu til þess að vinna mestu vinnuna við gerð hátternisreglnanna.

4.3. Hlutverk og verkefni Persónuverndar

Eins og áður hefur verið fjallað um þá gegnir Persónuvernd hlutverki eftirlitsstjórnvalds hér á Íslandi, og sem slíkt þá spilar Persónuvernd stóra rullu bæði við vottunarfyrirkomulagið og samþykki hátternisreglnanna. Líkt og fram hefur komið í fyrri umfjöllun þá þurfa eftirlitsstjórnvöld að samþykkja viðmið vottunar sem og vottunaraðila áður en hann hlýtur faggildingu sem og samþykkja drög að hátternisreglum, birta hátternisreglurnar, samþykkja eftirlitsaðila að hátternisreglunum.

4.3.1. Hlutverk Persónuverndar í tenglum við vottun og hátternisreglur

Hlutverk Persónuverndar felst meðal annars í að samþykkja viðmið vottunar, sbr. 5. mgr. 42. gr. pvrg., en ekki er hægt að gefa út vottun, samkvæmt 42. gr. og 43. gr. pvrg., hérlendis án samþykkis Persónuverndar. Í reglugerðinni er kveðið á um sérstök skilyrði fyrir vottunarviðmiðin, að þau eigi að votta að vinnsla persónuupplýsinga sé í samræmi við ákvæði löggjafarinnar. Þá tekur vottunarfyrirkomulag 42. gr. og 43. gr. pvrg. ekki til einstaklinga eða stjórnkerfa, sbr. 1. mgr. 42. gr. pvrg., Þrátt fyrir að búið sé að ákvarða umfang vottunar á þann hátt sem gert er í greininni þá er samt ekki gert blátt bann við að vottunarfyrirkomulagi verði komið upp fyrir þau atriði sem falla utan gildissviðs 42. gr. og 43. gr. pvrg. Sem dæmi má nefna að persónuverndarstofnanir Spánar og Frakklands hafa komið í gagnið vottunarkerfi vegna vottunar fyrir persónuverndarfulltrúa.[233] Hins vegar má ætla að slík vottun muni aldrei vera talin falla innan gildissviðs 42. og 43. gr. pvrg. þar sem Þetta er meðal þeirra atriða sem Persónuvernd verður að hafa í huga þegar samþykkja skal vottunina að hún falli innan gildissviðs ákvæðanna.

Það er í raun ekkert sem kemur beint í veg fyrir að vottunin taki til fleiri atriða heldur en þeirra sem snerta ákvæði persónuverndarreglugerðarinnar. Þegar vottunin byggir einnig á einhverju öðru en reglugerðinni, þá verður að tryggja hæfni Persónuverndar eða annarra eftirlitsstjórnvalda til að meta vottunina. Jafnvel þó að Persónuvernd hafi strangt til tekið ekki hæfni til að endurskoða viðmið sem byggjast á tæknilegum stöðlum, þá ber Persónuvernd að gera það, ef markmið vottunarinnar er að sýna fram á samræmi við persónuverndarlöggjöfina, sbr. 42. gr. og 43. gr. pvrg. Þannig mætti líta á tæknilausn í slíkri vottun sem tæki til að hjálpa

[233] Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 12.

við að ná markmiðinu, að sýna fram á reglufylgni, og af þeim sökum fellur það undir valdssvið Persónuverndar að meta slíkt. Þess verður þó að gæta að þrátt fyrir að samkvæmt 5. mgr. 42. gr. pvrg. sé heimild fyrir Persónuvernd að samþykkja vottunarviðmið þá má slíkt samþykktarferli ekki verða til þess að fjarlægjast markmið ákvæðanna. Með vottuninni sé verið að tryggja að samræmi við persónuverndarlöggjöfina.[234] Einsleit og samræmd matsaðferð er lykilatriði til þess að bæta lagalega vissu þegar verið er að samþykkja vottunarviðmið.[235]

Eins og komið var inná hér áður þá hafa nú þegar nokkur eftirlitsstjórnvöld óskað eftir áliti Evrópska persónuverndarráðsins vegna skilyrða fyrir faggildingu vottunaraðila. Af því leiðir að ríkin eru farin að huga að því hvernig best sé að haga framkvæmdinni varðandi vottunina. Má því ætla að varðandi framkvæmd vottunar hérlendis að þá sé boltinn hjá Persónuvernd, sem skuli fara huga að setningu slíkra skilyrða og leggja drög þess fyrir Evrópska persónuverndarráðið til þess að hægt sé að koma framkvæmdinni af stað hérlendis.

Hlutverk Persónuverndar varðandi hátternisreglurnar er fyrst og fremst að gefa út álit sitt hvort reglurnar samrýmist ákvæðum reglugerðarinnar og þá samþykkja drögin að hátternisreglunum ef í þeim séu tryggðar nægilegar og viðeigandi verndarráðstafanir, sbr. 5. mgr. 40. gr. pvrg. Þá ber Persónuvernd jafnframt að birta hátternisreglurnar, það er ef þær eiga aðeins að ná til ábyrgðaraðila eða vinnsluaðila sem eru staðsettir innan Íslands, sbr. 6. mgr. 40. gr. pvrg. Ef hátternisreglurnar samrýmast ekki ákvæðum reglugerðarinnar eða hafa ekki viðeigandi verndarráðstafanir, þá ber Persónuvernd að hafna þeim og rökstyðja afstöðu sína. Eiganda hátternisreglnanna er heimilt að uppfæra hátternisreglunar svo þær uppfylli skilyrðin og senda þær aftur til Persónuverndar til skoðunar.[236]

Ef um er að ræða vinnslustarfsemi ábyrgðaraðila eða vinnsluaðila sem eru staðsettir í fleiri en einu ríki ber Persónuvernd, sem lögbært eftirlitsstjórnvald samkvæmt 55. gr. pvrg., að óska eftir áliti Evrópska persónuverndarráðsins á drögunum áður en það samþykkir þau, sbr. 7. mgr. 40. gr. pvrg., sbr. b. lið 1. mgr. 64. gr. pvrg. Ef álit Evrópska persónuverndarráðið staðfestir að hátternisreglunar uppfylli skilyrð til að hafa gildi yfir landamæri þá ber að leggja þær fyrir framkvæmdastjórn Evrópusambandsins til þess að meta hvort þær hafi almennt gildi innan Sambandsins, sbr. 9. mgr. 40. gr. pvrg.

Af framangreindu er því ljóst að ferlið allt frá drögum að hátternisreglum til samþykkis er unnið undir handleiðslu Persónuverndar. Hins vegar þegar kemur að eftirliti með samþykktum hátternisreglum þá hefur það verið útvistað til einkaaðila, þó til þess aðila sem

234 Kamara o.fl. (n. 148) 76.
235 sama heimild 75.
236 Lachaud, „Adhering to GDPR Codes of Conduct“ (n. 179) 5.

hlotið hefur faggildingu frá Persónuvernd, sbr. 1. mgr. 41. gr. pvrg. Eins og farið hefur verið yfir í reglugerðinni þá þarf samhliða því samtök leggi fram drög að hátternisreglum, einnig að óska eftir faggildingu fyrir þann aðila sem mun sinna eftirliti með hátternisreglunum, nema ef eftirlitsaðili hafi nú þegar hlotið faggildingu Persónuverndar.

Ekki voru settar sérstakar reglur um faggildingu eftirlitsaðila að hátternisreglum eins og var gert varðandi vottunaraðila. Það virðist aðeins vera í höndum Persónuverndar að sjá um faggildingu á eftirlitsaðila með hátternisreglunum að uppfylltum skilyrðum sem talin eru upp í 2. mgr. 41. gr. pvrg. En jafnframt ber Persónuvernd að leggja fyrir Evrópska persónuverndarráðið drög að skilyrðum fyrir faggildingu eftirlitsaðila, sbr. 3. mgr. 41. gr. pvrg., sbr. c. lið 1. mgr. 64. gr. pvrg., en það er gert til þess að tryggja samrýmda beitingu reglnanna innan sambandsins.

Þegar persónuvernd hefur sent drög að samþykki til Evrópska persónuverndarráðsins þá Persónuvernd ber að taka ýtrasta tillits til álits persónuverndarráðsins. Jafnframt skal Persónuvernd innan tveggja vikna frá því að álitið berst, senda formanni persónuverndarráðsins tilkynningu hvort það muni standa við drög sín eða gera breytingar á þeim, ef gera á breytingar skal senda persónuverndarráðinu hin breyttu drög, sbr. 7. mgr. 64. gr. pvrg. Þetta á við hvort sem um er að ræða vottunarviðmiðin, skilyrði fyrir faggildingu vottunaraðila, skilyrði fyrir faggildingu eftirlitsaðila að samþykktum hátternisreglum eða samþykktar hátternisreglna sem ná til ábyrgðaraðila eða vinnsluaðila í fleiri en einu ríki. Ef eftirlitsstjórnvaldið ákveður að fara ekki eftir áliti ráðsins, hvort sem það sé í heild eða hluta, og færir rök fyrir afstöðu sinni ber að leita lausn deilunnar samkvæmt c. lið 1. mgr. 65. gr. pvrg., sbr. 8. mgr. 64. gr. pvrg.

Fjöldi eftirlitsstjórnvalda ríkja sambandsins hafa lagt slík drög fyrir Evrópska persónuverndarráðið. Fyrstir til að leggja slík drög fyrir ráðið var Austurríki en auk þeirra hafa, Frakkar, Spánverjar, Belgar, Írar og Bretar skilað inn drögum og persónuverndarráðið hefur nú þegar gefið út álit sitt.

4.3.1.1. Sektarheimildir

Eins og vikið var að í fyrri umfjöllun þá kynnti persónuverndarreglugerðin til sögunnar stórauknar sektarheimildir eftirlitsstjórnvalda. Það fellur því í hlut Persónuverndar að leggja á stjórnvaldssektir vegna brota á ákvæðum löggjafarinnar. Upphæðir sekta eru stigskiptar eftir alvarleika brots og leggjast þær á ábyrgðaraðila og vinnsluaðila óháð stærð þeirra. Skilyrði fyrir álagningu sekta er að finna í 83. gr. pvrg.

Brotum gegn ákvæðum reglugerðarinnar hefur verið skipt upp í þrjá flokka í 4., 5. og 6. mgr. 83. gr. pvrg. Brotum samkvæmt 4. mgr. geta leitt til sekta allt að fjárhæð 10 milljónir evra eða, ef um er að ræða fyrirtæki, allt að 2% af árlegri heildarveltu fyrirtækisins á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra. Undir þetta ákvæði falla ýmis brot gegn skyldum ábyrgðaraðila og vinnsluaðila. Sektir vegna brota á grundvallarreglum um vinnslu, þar á meðal skilyrði fyrir samþykki, réttindi skráðra einstaklinga og miðlun upplýsinga til viðtakanda í þriðja landi eða alþjóðastofnunar varðar allt að 20 milljónir evra eða, ef um fyrirtæki er að ræða, allt að 4% af árlegri heildarveltu á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra, sbr. 5. mgr. Loks er kveðið á um í 6. mgr. ef um er að ræða brot gegn fyrirmælum eftirlitsstjórnvalds, en þau brot falla undir sama sektarþrep og 5. mgr. kveður á um.

Þessum sektarákvæðum er ætlað að hafa varnaðaráhrif af þeim sökum jafnvel frekari hvatning fyrir fyrirtæki og stofnanir til að fylgja ákvæðum persónuverndarreglugerðarinnar uppfylla ábyrgðarskyldu sína gagnvart persónuverndarlöggjöfinni.

Það var í byrjun mars 2020 þegar fyrstu sektarákvarðanir Persónuverndar litu dagsins ljós. Annar úrskurðurinn varðandi Fjölbrautaskólann í Breiðholti[237] en hinn úrskurðurinn varðaði SÁÁ.[238]

4.3.1.2. Framsal á eftirlitshlutverki

Það er því ljóst af öllum framagreindu að eftirlitsstjórnvöld spila stórt hlutverk við samþykki hátternisregla sem og vottunar. Hins vegar þá er farið þá leið í löggjöfinni að fela eftirlitshlutverk með hátternisreglunum og vottuninni yfir til einkaaðila. Vert er þó að nefna að hvorki vottun né hátternisreglur koma í veg fyrir að eftirlitsstjórnvald sinni hlutverki sínu.

Samt sem áður mætti því rök fyrir því að þessum ákvæðum persónuverndarlöggjafarinnar er ætlað að einfalda líf og störf eftirlitsstjórnvalda aðildarríkja. Þar sem að um valkvæðar leiðir er að ræða og aðilar geta sjálfir tryggt eftirlit með þeim, sem gæti haft hvetjandi áhrif á fyrirtæki og stofnanir þar sem jafnframt geta þessar leiðir einfaldað þessum aðilum lífið í tengslum við framfylgningu ákvæða persónuverndarlöggjafarinnar. Þessar leiðir geta því verið öllum aðilum málsins til hagsbóta, það er bæði þeim fyrirtækjum og stofnunum sem nýta sér aðra hvora valkvæðu leiðina. Enda hefur álag á eftirlitsstjórnvöldum aukist til muna eftir gildistöku persónuverndarreglugerðarinnar og almennt eru eftirlitsstjórnvöld frekar að berjast við manneklu en að um offramboð sé á mannafla til þess að

[237] Ákvörðun Persónuverndar nr. 2020010382, 5. mars 2020.
[238] Ákvörðun Persónuverndar nr. 2020010428, 5. mars 2020.

sinna verkefnum þeirra. Sem dæmi þá hefur málafjöldi Persónuverndar fjórfaldast frá því sem það var árið 2002 til ársins 2018.[239]

Af þeim sökum mætti ætla að Persónuvernd, og önnur eftirlitsstjórnvöld, hvetji fyrirtæki og stofnanir til þess að nýta sér þessar leiðir, þó það hafi í för með sér tímabundið aukið álag á eftirlitsstjórnvaldið. Því til lengri tíma er litið gæti nýting á þessum valkvæðu leiðum létt á því álagi sem hvílir á eftirlitsstjórnvöldunum.

[239] Persónuvernd, „Ársskýrsla Persónuverndar 2018“ 11 <https://www.personuvernd.is/media/arsskyrslur/Arsskyrsla-Personuverndar-2018.pdf> skoðað 6. júní 2020.

5. Niðurstöður og lokaorð

Í ritgerðinni var lagt upp með að skýra tvo þætti. Annars vegar að skýra hvernig framkvæmd vottunarfyrirkomulagsins og hátternisreglnanna samkvæmt persónuverndarreglugerðinni sé háttað. Hins vegar var að skoða að hvaða leiti hvor þessara valkvæðu leiða, vottunin og hátternisreglurnar, henti mismunandi fyrirtækjum og stofnunum til þess að sýna fram á reglufylgni og uppfylla ábyrgðarskyldu reglugerðarinnar.

Við skoðun á framkvæmd vottunarinnar samkvæmt 42. og 43. gr. reglugerðarinnar þá er ljóst að nokkri hnökrar virðast vera á framkvæmdinni. Má þar nefna að í fyrsta lagi þá er orðalag 1. mgr. 42. gr. pvrg. fremur þröng, en það útilokar að vottunarfyrirkomulagið geti náð til einstaklinga og stjórnkerfa, þar sem tekið er fram að vottun sé ætlað að sýna fram á að vinnslan uppfylli ákvæði reglugerðarinnar. Af því leiðir að þau vottunarfyrirkomulög sem eru í gildi nú þegar geta átt erfitt með að aðlaga sig að skilyrðum ákvæðisins, eða eins og fjallað var um varðandi ISO 27701 staðalinn.

Eins og vikið var að þá geta einkaaðilar, sem hlotið hafa faggildingu sem vottunaraðilar, gefið út vottun, en jafnframt þá hafa eftirlitsstjórnvöldin sjálf alltaf slíka heimild. Það eitt og sér verður að teljast fremur óheppilegt, þar sem ætla má að slíkt hafi ekki hvetjandi áhrif á einkageirann til að leysa slíkt verkefni. Sérstaklega í ljósi þess að á hvaða tímapunkti sem er gæti faggiltur vottunaraðili lent í samkeppni við eftirlitsstjórnvald vegna veitingu vottunar. Við slíkar aðstæður má telja að fyrirtæki og stofnanir myndu fremur sækjast eftir vottun eftirlitsstjórnvaldsins, heldur en einkaaðila, meðal annars vegna þess að eftirlitstjórnvaldið sem leggur á sektir.

Loks má nefna skyldur eftirlitsstjórnvalda varðandi viðmið vottunar eru fremur óskýr, en ekki er gerð krafa um að eftirlitsstjórnvöld óski eftir áliti persónuverndarráðsins ef vottunin sem slík muni aðeins hafa gildi innan aðildarríkisins sjálfs. Þetta gæti verið varasamt verklag þar sem milli ríkja gæti myndast mismunandi framkvæmd, sem veldur því að erfiðara verður að ná sátt um samrýmt kerfi. Þó má nefna að ICO tekur fram í sínum leiðbeiningum að ætlunin sé að leggja fyrir ráðið drög að samþykktum viðmiðum á vottun einmitt til þess að gætt sé að samræmdri framkvæmd. En eins og staðan er núna þá hefur engin vottun verið gefin út samkvæmt 42. og 43. gr. pvrg. og því eru enn margar spurningar ósvaraðar hvernig framkvæmdinni verður raunverulega hagað og hvernig túlka eigi ákvæðin.

Miðað við vottunina þá er nú þegar komin nokkur reynsla á hátternisreglunar, enda byggja ákvæði persónuverndarreglugerðarinnar á ákvæði sem var að finna í eldri löggjöf. Þar er ekki sama óvissa um framkvæmdina og með vottunina. Þó gæti eftirlit með

hátternisreglunum verið þungt í vöfum og þá sérstaklega hérlendis með tilliti til smæðar landsins þar sem samtök eru oft fáliðuð. Af þeim sökum gæti verið flókið fyrir samtök, sem eigendur hátternisreglna, að tryggja að eftirlitsaðili uppfylli þau skilyrði til þess að geta sinnt eftirliti.

Vikið verður nú að hvaða leiti vottun og hátternisreglur geti hentað mismunandi fyrirtækjum og stofnunum. Þegar lítur að vottuninni þá er þar um að ræða kostnaðarsamari leið sem fyrirtækin að eigin frumkvæði sækjast eftir, ólíkt því sem á við um hátternisreglurnar. Í vottun, þegar til langs tíma litið, getur hlotist ávinningur sem og samkeppnisforskot þar sem hinir skráðu einstaklingar, neytendur, viðskiptavinir og almenningur geta með einföldum hætti lagt mat á hversu örugg vinnsla persónuupplýsinga er innan fyrirtækisins. Af því sögði má draga þá ályktun að vottun henti fyrirtækjum sem hafa til þess fjárhagslegt bolmagn. Hins vegar þá hefur ekki enn verið samþykkt vottun sem byggir á 42. og 43. gr. pvrg., og þar af leiðandi er engin reynsla komin á kerfið, þrátt fyrir það þá er að finna ýmsa aðra staðla og vottanir sem gefnar hafa verið út í tengslum við persónuvernd og mikið af fyrirtækjum nýta sér nú þegar. Í ritgerðinni er tekið dæmi um ISO 27701 staðalinn sem fyrirtæki geta nýtt sér sem tæki til þess að tryggja öryggi við vinnslu persónuupplýsinga þrátt fyrir að hann hafi ekki verið samþykktur sem samrýmanlegur 42. og 43. gr. pvrg., getur hann hjálpað fyrirtækjum að uppfylla skyldur sínar gagnvart persónuverndarreglugerðinni. Loks má ekki útiloka að ISO 27701 staðalinn muni mögulega vera álitin samrýmanlegur ákvæðunum um vottun þegar fram líða stundir.

Hátternisreglur eru annars eðlis heldur en vottunin, þar sem að fyrirtæki geta ekki ein og sér stokkið af stað og sett sér hátternisreglur, það verður að vera innan ákveðins atvinnugeira, þar sem annað hvort samtök koma fram fyrir fyrirtæki og stofnanir sem tilheyra geiranum eða annar aðili. Það sem skiptir þó mestu við gerð hátternisreglna er að sá sem kemur fram, hvort sem um er að ræða samtök eða annan aðila, að hann tali fyrir hönd þeirra sem reglurnar skulu ná til. Þá þurfa hátternisreglurnar að vera settar að í þeim sé að finna eitthvað fleira en aðeins það sem fram kemur í persónuverndarreglugerðinni. Því þarf að kortleggja það regluverk sem fyrirtækin starfa í og sú vinna getur verið tímafrek og kostnaðarsöm. Þá geta hátternisreglurnar bæði nýst til þess að sýna fram á reglufylgnina, bæði við eftirlitsstjórnvöld sem og almenning en jafnframt geta þær verið mikilvægar leiðbeiningar fyrir fyrirtæki í samtökunum um hvernig best sé að hafa vinnslustarfsemi sinni. Má því líta svo á að að fyrir lítil og meðalstór fyrirtæki sem hafa ekki fjárhagslega getu til þess að kaupa sér sérfræðiþekkingu geta hátternisreglur verið skilvirk lausn til að tryggja að vinnsla sé í samræmi við ákvæði persónuverndarlöggjafarinnar slíkt leiðir mögulega til minni hættu á sekt. Því þurfa

samtök fyrirtækja að vera fjárhagslega stöðug og samstíga við setningu hátternisreglna fyrir sinn atvinnugeira, þar gerð þeirra kostar bæði tíma og vinnu.

Til þess að svara rannsóknarspurningunni þá verður að telja að framkvæmd vottunarinnar sé enn sem komið er fremur óljós og þegar reyna mun á reglurnar þá mun túlkun ákvæða skýrast. Framkvæmd hátternisreglnanna er skýrari þar sem reynsla er komin á þá framkvæmd og nú þegar hafa samtök gefið það út að hafin sé vinna við að uppfæra eldri hátternisreglur en slíkt gefur til kynna ánægju þeirra með þessa valkvæðu leið.

Þá er nokkuð ljóst að þessar valkvæðu leiðir henti mismunandi hópum eða tegundum fyrirtækja og stofnana. Þau fyrirtæki sem hafa nægilegt fjármagn og sérþekkingu innanborðs myndu fá mun meira út úr því að sækjast eftir vottun, þar sem það gefur þeim sérstöðu á markaði og þar með mögulegt samkeppnislegt forskot. Á hinum endanum séu lítil og meðalstór fyrirtæki sem almennt hafa ekki nægilegt fjármagn né mannafla til þess að kortleggja hvað þeim ber að gera til þess að uppfylla skyldur sínar gagnvart persónuverndarlöggjöfinni. Fyrir þessi fyrirtæki væri hagstæðast að ganga inn í kerfi eins og það sem hátternisreglurnar geta boðið upp á, því þær eru í eðli sínu tvíþættar það er að hanna kerfi fyrir fyritæki innan geirans til þess að þau uppfylli skyldur sínar gagnvart löggjöfinni sem og að í þeim felst leiðsögn.

Í lokin má nefna að eftirlitsyfirvöld njóti jafnframt góðs af því að fyrirtæki og stofnanir nýti sér þessar valkvæðu leiðir, þar líta má á eftirlitið með hinum valkvæðu leiðum sem mögulegt framsal á eftirlitshlutverkinu. Þó svo að þessar leiðir hafi ekki áhrif á valdheimildir stjórnvaldsins, má ætla að til langs tíma litið geti þessar leiðir létt á álagi.

Heimildaskrá

Article 29 Data Protection Working Party, „Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing“ (13. júní 2003) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf>

——, „Opinion 15/2011 on the definition of consent“ (13. júlí 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> skoðað 12. febrúar 2020

——, „Guidelines on the application and setting of administrative fines (wp253).“ <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> skoðað 21. apríl 2020

——, „Opinion 3/2010 on the principle of accountability“ <https://www.dataprotection.ro/servlet/ViewDocument?id=654> skoðað 23. febrúar 2020

Björg Thorarensen, „Friðhelgi einkalífs og fjölskyldu og réttur til að stofna til hjúskapar“ í Davíð Þór Björgvinsson o.fl. (ritstj.), Mannréttindasáttmáli Evrópu: meginreglur, framkvæmd og áhrif á íslenskan rétt (Mannréttindastofnun Háskóla Íslands, Lagadeild Háskólans í Reykjavík 2005)

Blume P, Databeskyttelsesret (4. udgave, Jurist- og Økonomforbundets forlag 2013)

——, „Smart Data Protection“ í Peter Wahlgren (ritstj.), 50 years of law and IT: the Swedish Law and Informatics Research Institute: 1968-2018 (Institute for Scandinavian Law 2018)

Blume P og Kristiansen J, Databeskyttelse på arbejdsmarkedet (Jurist- og Økonomforbundets Forlag 2002)

Cadwalladr C og Graham-Harrison E, „Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach“ The Guardian (17. mars 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> skoðað 10. mars 2020

European Data Protection Board, „Guidelines 4/2018 on the Accreditation of Certification Bodies under Article 43 of the General Data Protection Regulation (2016/679) - Version

Adopted after Public Consultation“ (European Data Protection Board - European Data Protection Board, 14. desember 2018) <https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_en> skoðað 29. mars 2020

——, „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - Version 3.0“ (3. júní 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf> skoðað 22. janúar 2020

——, „Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 version 2.0“ (4. júní 2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf> skoðað 3. mars 2020

——, „Register of Certification Mechanisms, Seals and Marks“ (European Data Protection Board - European Data Protection Board) <https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en> skoðað 3. maí 2020

European Union, User Guide to the SME Definition. (Publications Office of the European Union 2017) <http://op.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1> skoðað 17. maí 2020

European Union Agency for Fundamental Rights og Council of Europe, Handbook on European Data Protection Law: 2018 Edition (Publications Office of the European Union; ©2018 2018)

FEDMA, „Self Regulation – Fedma“ <https://www.fedma.org/work-areas/self-regulation/> skoðað 25. maí 2020

„General Data Protection Regulation incorporated into the EEA Agreement | European Free Trade Association“ <https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291> skoðað 15. september 2019

„Geographical indications - Trade - European Commission“ <https://ec.europa.eu/trade/policy/accessing-markets/intellectual-property/geographical-indications/index_en.htm> skoðað 1. maí 2020

Grafenstein M, „Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the „State of the Art“ of Data Protection-by-Design“ (Social Science Research Network 18. febrúar 2019) SSRN Scholarly Paper ID 3336990 <https://papers.ssrn.com/abstract=3336990> skoðað 28. apríl 2020

Information Commissioner’s Office, „Register of Certification Scheme Criteria“ (26. febrúar 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/certification-schemes-detailed-guidance/register-of-certification-scheme-criteria/> skoðað 25. maí 2020

——, „How Do We Develop a Certification Scheme?“ (27. febrúar 2020) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/> skoðað 3. júní 2020

——, „ICO Codes of Conduct and Certification Schemes Open for Business“ (2. mars 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-codes-of-conduct-and-certification-schemes-open-for-business/> skoðað 29. apríl 2020

——, „UK additional accreditation requirements for certification bodies (A.43(1)(b))“ <https://ico.org.uk/media/for-organisations/documents/2617241/uk-additional-accreditation-requiremenets-202002.pdf> skoðað 25. maí 2020

ISO, „Annual Report 2018“ (ISO) <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/publication/10/03/PUB100385.html> skoðað 3. maí 2020

„ISO - About Us“ (ISO) <https://www.iso.org/about-us.html> skoðað 3. maí 2020

IT Governance, „Why Are so Many Organisations Getting Certified to ISO 27001?“ (IT Governance Blog En, 18. apríl 2018) <https://www.itgovernance.eu/blog/en/why-are-so-many-organisations-getting-certified-to-iso-27001> skoðað 6. janúar 2020

Kamara I, „4 GDPR-certification myths dispelled“ <https://iapp.org/news/a/four-gdpr-certification-myths-dispelled/> skoðað 16. maí 2020

——, „Data Protection Certification Mechanisms : Study on Articles 42 and 43 of the Regulation (EU) 2016/679“ (Publications Office of the European Union 6. maí 2019) <https://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en> skoðað 5. maí 2020

Kjartan Gunnarsson, „Friðhelgi einkalífs“ (1978) 31 (3) Úlfljótur 171

Lachaud E, „Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful“ (2016) 32 (6) Computer Law & Security Review 814

——, „The General Data Protection Regulation and the Rise of Certification as a Regulatory Instrument“ (2018) 34 (2) Computer Law & Security Review 244

——, „Adhering to GDPR Codes of Conduct: A Possible Option for SMEs to GDPR Certification“ (Social Science Research Network 5. júní 2019) SSRN Scholarly Paper ID 3399509 <https://papers.ssrn.com/abstract=3399509> skoðað 10. maí 2020

——, „ISO/IEC 27701: Threats and Opportunities for GDPR Certification“ (Social Science Research Network 15. janúar 2020) SSRN Scholarly Paper ID 3521250 <https://papers.ssrn.com/abstract=3521250> skoðað 29. apríl 2020

mbl.is, „Bróðirinn tekur við forstjórastóli Kauphallarinnar“ <https://www.mbl.is/vidskipti/frettir/2019/10/15/brodirinn_tekur_vid_forstjorastolnum/> skoðað 28. maí 2020

Northstack, „State of the Icelandic Game Industry 2019“ (nóvember 2019) <https://www.si.is/media/_eplica-uppsetning/IGI-report-2019-Web-v2.pdf> skoðað 4. júní 2020

Páll Hreinsson, „Ritröð Lagastofnunar Háskóla Íslands“ í Viðar Már Matthíasson (ritstj.), Rafræn vinnsla persónuupplýsinga við meðferð stjórnsýslumála (Lagastofnun Háskóla Íslands 2007)

„Personal Data Protection | Fact Sheets on the European Union | European Parliament“ <https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection> skoðað 26. febrúar 2020

„Persónuupplýsingar Okkar Eru Verðmæt Söluvara“ (RÚV, 1. mars 2017) <https://www.ruv.is/frett/personuupplysingar-okkar-eru-verdmaet-soluvara> skoðað 17. mars 2020

Persónuvernd, „17. fundur Evrópska persónuverndarráðsins í Brussel 28.-29. janúar 2020“ (Persónuvernd. Þínar upplýsingar, þitt einkalíf.) <https://www.personuvernd.is/personuvernd/frettir/17.-fundur-evropska-personuverndarradsins-i-brussel-28.-29.-januar-2020> skoðað 22. maí 2020

——, „Ábyrgðarskyldan“ (Persónuvernd. Þínar upplýsingar, þitt einkalíf.) <https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/allar-spurningar-og-svor/abyrgdarskyldan> skoðað 23. mars 2020

——, „Ársskýrsla Persónuverndar 2018“ <https://www.personuvernd.is/media/arsskyrslur/Arsskyrsla-Personuverndar-2018.pdf> skoðað 6. júní 2020

Rita Heimes, „Top 10 operational impacts of the GDPR: Part 9 - Codes of conduct and certifications“ <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/> skoðað 5. maí 2020

Sigrún Jóhannesdóttir, Persónuverndarlög: skýringarrit (Fons Juris 2015)

SMEunited, „About SMEunited“ <https://smeunited.eu/about-us> skoðað 29. maí 2020

——, „SMEunited Comments on Codes of Conduct and Monitoring Bodies Under Regulation 2016/679“ <https://smeunited.eu/admin/storage/smeunited/190402-smeunited-comments-on-codes-of-conduct-and-monitoring-bodies-under-regulation.pdf> skoðað 1. júní 2020

Tim Hickman, „Guidelines on the Certification Mechanisms under the GDPR“ <https://www.whitecase.com/publications/alert/guidelines-certification-mechanisms-under-gdpr> skoðað 19. apríl 2020

Timmermans F, Ansip A og Jourová V, „Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection“ (European Commission - European Commission)

<https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_1403> skoðað 27. febrúar 2020

UK Interactive Entertainment, „Our members | Ukie“ <https://ukie.org.uk/our-members> skoðað 6. janúar 2020