Nóvember 2017

Hvað þýða nýjar persónuverndarreglur fyrir sveitarfélögin?

-Leiðbeiningar-

1. Hvaða þýðingu hafa nýju persónuverndarreglurnar fyrir sveitarfélögin?

Áætlað er að ný reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (hér eftir nefnd „reglugerðin“) komi til framkvæmda á Íslandi 2018 á grundvelli skuldbindinga Íslands skv. EES-samningnum. Þá er stefnt að því að ný persónuverndarlög taki gildi á sama tíma, sem munu úfæra tiltekin ákvæði reglugerðarinnar sem bjóða upp á sveigjanleika fyrir aðildarríki á EES-svæðinu. Drög að frumvarpi til nýrra persónuverndarlaga liggja ekki fyrir á þessari stundu en Persónuvernd hefur, með leyfi Þýðingarmiðstöðvar utanríkisráðuneytisins, birt drög að þýðingu á reglugerðinni á heimasíðu sinni. [1]. Var það gert til að auðvelda aðilum að undirbúa sig undir hinar nýju persónuverndarlöggjafar, en mikil áhersla hefur verið lögð á slíkan undirbúning af hálfu Persónuverndar.

Vegna þessa hefur Samband íslenskra sveitarfélaga tekið saman helstu atriði sem hafa áhrif á rekstur sveitarfélaga og stofnana þeirra (hér eftir nefnd einu nafni “sveitarfélög”) í þeim tilgangi að aðstoða þau við undirbúning nýrra laga. Voru leiðbeiningar þessar upphaflega sendar út og birtar á heimasíðu sambandsins í júlí en hafa nú verið uppfærðar m.v. þær ábendingar sem borist hafa m.a. frá Persónuvernd auk þess sem bætt hefur verið við skýringar og ferli m.a. á grundvelli leiðbeininga sem gefnar eru út af vinnuhópi 29. gr.[2] og vísað er til á nokkrum stöðum, en almenna slóð á síðu hópsins er að finna í fótnótum hér að neðan.

Sambandið tekur fram að þessar leiðbeiningar eru unnar út frá þeim upplýsingum sem nú liggja fyrir um komandi nýja löggjöf. Þar sem ekki liggja fyrir frumvarpsdrög er mögulegt að eitthvað kunni að breytast, þó ekki verði um nein grundvallaratriði að ræða þegar gerðin verður innleidd í íslensk lög. Vísað er í greinar reglugerðarinnar í leiðbeiningum þessum eftir því sem við á sem og leiðbeininga vinnuhóps 29 svo hægt sé að skoða ítarefni og þann lagatexta sem býr að baki.

Ljóst er að ný lög munu leggja ríkari kröfur á herðar sveitarfélaga að því er varðar m.a., hvernig unnið er úr persónuupplýsingum og á hvaða formi þær eru geymdar. Munu nýju lögin veita einstaklingum mun meiri

[1] https://www.personuvernd.is/media/frettir/DROG_thyding_GDPR_2016_679.pdf
[2] www.ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

réttindi en núgildandi lög auk þess sem þau munu innhalda rífleg sektarákvæði sem beita má ef sveitarfélög gerast sek um öryggisbrot á persónuverndarupplýsingum.

Við lestur leiðbeininga, reglugerðar og nýrra laga þegar þau liggja fyrir er mikilvægt að sveitarfélög hafi í huga að þau geta bæði verið ábyrgðaraðilar og vinnsluaðilar í skilningi nýrra laga og er því mikilvægt að þau skoða hlutverk sín og ábyrgð út frá þessum skilgreiningum:

Ábyrgðaraðili: er sá sem ákvarðar, einn eða í samvinnu við aðra, tilgang og aðferðir við vinnslu persónuupplýsinga; ef tilgangur og aðferðir við slíka vinnslu eru ákveðin í lögum. Til dæmis má nefna að sveitarfélag er ábyrgðaraðili að vinnslu upplýsinga um sitt eigið starfsfólk. Eins er það ábyrgðaraðili þegar skráðar eru upplýsingar í velferðarþjónustu um notendur eða nememdur hjá grunn- og leikskólum. Mikil ábyrgð hvílir á ábyrgðaraðila sbr. ábyrgðarregla sem fjallað er um í næsta kafla.

Vinnsluaðili: er sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila. Sveitarfélög og stofnanir þeirra eins og byggðarsamlög gætu talist vera vinnsluaðilar í skilningi laganna ef þau eða stofnanir þeirra taka að sér ákveðna þjónustu sem felur í sér vinnslu persónuupplýsinga, t.d. þjónusta á velferðarsviði þar sem veittar eru upplýsingar um heilsufar.

Hafa verður í huga að þó vinnsluaðili geti líka verið ábyrgur þá er ábyrgðarskyldan að meginstefnu á ábyrgðaraðila og sveitarfélög hafí flestum tilvikum stöðu ábyrgðaraðila í skilningi laganna.

Þumalputtareglan er sú að ef upplýsingar um einstaklinga eru vistaðar og/eða unnar hjá sveitarfélögum í skilningi laganna þá bera þau ábyrgð á þeim.

2. Helstu skilgreiningar og meginreglur um vinnslu persónuupplýsinga

Við lestur þessara leiðbeininga er athygli vakin á eftirfarandi skilgreiningum sem skipta miklu máli við lestur allra gagna:

Vinnsla: aðgerð eða röð aðgerða þar sem persónuupplýsingar eru unnar, hvort sem vinnslan er sjálfvirk eða ekki, s.s. söfnun, skráning, flokkun, kerfisbinding, varðveisla, aðlögun eða breyting, heimt, skoðun, notkun, miðlun með framsendingu, dreifing eða aðrar aðferðir til að gera upplýsingarnar tiltækar, samtenging eða samkeyrsla, aðgangstakmörkun, eyðing eða eyðilegging.

Sambandið bendir á að nánast öll meðhöndlun og vistun gagna falli undir þessa skilgreiningu og er mikilvægt fyrir sveitarfélög að hafa það í huga.

Persónuupplýsingar: eru hvers kyns upplýsingar um persónugreindan eða persónugreinanlegan einstakling; einstaklingur telst persónugreinanlegur ef unnt er að persónugreina hann, beint eða óbeint, svo sem með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, lífeðlisfræðilegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti.

Mikilvægt er að sveitarfélög átti sig á því að hugtakið er afar rúmt eins og skilgreiningin ber með sér.

Viðkvæmar persónuupplýsingar: Samkvæmt 9. gr. reglugerðarinnar er bannað að unnið sé með persónuupplýsingar er varða **kynþátt** eða **þjóðernislegan uppruna**, **stjórnmálaskoðani**r, **trúarbrögð** eða **heimspekilega sannfæringu** eða **aðild að verkalýðsfélagi** og að vinna **erfðafræðilegar upplýsingar**,

lífkennaupplýsingar í því skyni að persónugreina einstakling með einkvæmum hætti, **heilsufarsupplýsingar** eða **upplýsingar er varða kynlíf** einstaklings eða **kynhneigð**, nema að mjög ströng skilyrði séu fyrir hendi eins og ótvírætt samþykki eða vinnslan sé liður í lögmætri starfsemi stofnunar eins og t.d. starfsemi félagsþjónustu og greiningarstöðva þegar um heilsuupplýsingar og greiningar er að ræða.

Þá gildir sérregla um vinnslu persónuupplýsingar er varða sakfellingar í refsimálum og refsiverð brot. sbr. 10. gr.

Mikilvægt er að hafa í huga að þó að viðkvæmar persónuupplýsingar séu eingöngu þær sem listaðar eru í 9. gr. reglugerðar og merktar eru í feitletri hér að framan er gerð mikil krafa til allarar söfnunar upplýsingar og sérstaklega ef upplýsingar eru þess eðlis að ljóst er að gæta beri ítrustu varúðar, t.d. upplýsingar um forsjá barns. Í slíkum tilvikum er mikilvægt að sveitarfélög hugi að því sérstaklega hvort lagaheimild sé til vinnslu upplýsinga og ef ekki hvort nauðsynlegt sé að safna þeim. Ef talið er nauðsynlegt að safna/vinna upplýsingar og ekki er fyrir hendi lagaskylda verður að afla samþykkis.

Samþykki skráðs einstaklings: óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um hann sjálfan.

Er í þessu sambandi rætt um upplýst samþykki sem skal ávallt að vera veitt með skýrri staðfestingu. Hún skal gefin af fúsum og frjálsum vilja og ná til allra aðgerða sem framkvæmdar eru. Þögn, aðgerðaleysi og rafrænt hak, sem gerir fyrirfram ráð fyrir samþykki flokkast ekki sem samþykki

Öryggisbrot við meðferð persónuupplýsinga: er brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi,

Sjá nánar 4. gr. og 9. -10. gr. reglugerðar

Í 5. gr. reglugerðarinnar er fjallað um **sjö meginreglur** um vinnslu persónuupplýsinga sem mikilvægt er að hafa í huga við alla vinnslu sveitarfélaga á persónuupplýsingum hvort sem um er að ræða viðkvæmar upplýsingar eða ekki:

1. Að unnið sé úr upplýsingum á sanngjarnan, lögmætan og gagnsæjan hátt
2. Að upplýsingum sé einungis safnað í skýrum og lögmætum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi (takmörkun vegna tilgangs),
3. Að upplýsingar séu nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilgang (takmörkun gagna)
4. Að upplýsingarnar séu áreiðanlegar og uppfærðar eftir þörfum (áreiðanleiki)
5. Að upplýsingar séu ekki varðveittar á því formi að unnt sé að persónugreina einstaklinga lengur en þörf er á nema lög kveði á um annað (geymslutakmörkun).
6. Að öryggi persónuupplýsinga sé tryggt, þ.m.t. með því að vernda þær gegn óleyfilegri og ólögmætri vinnslu og gegn því að þær glatist eða verði fyrir tjóni, með tæknilegum og skipulagslegum ráðstöfunum (heilleiki og trúnaður)

7. Ábyrgðaraðili er ábyrgur fyrir því að farið sé að meginreglunum og hann þarf að geta sýnt fram á það (ábyrgðarskylda). Það getur hann gert m.a. með því að leggja fram gögn sem staðfesti hvernig hann fer að meginreglum.

Sambandið bendir á að ábyrgðarskyldan er nýmæli og leggur hún afar ríkar skyldur á ábyrgðaraðila. Er mikilvægt að sveitarfélög kynni sér vel þá ábyrgð sem þau bera sem ábyrgðaraðilar. Fjallað er ítarlegar um ábyrgðarskyldu í kafla 4.

Sjá nánar 5. gr. reglugerðarinnar

3. Hvað þurfa sveitarfélögin að gera nú og hvernig eiga þau að skipuleggja undirbúning?

Þrátt fyrir að vinna við innleiðingu á reglugerðinni sé á eftir áætlun hvetur sambandið sveitarfélög til að hefja undirbúning fyrir nýja löggjöf hið fyrsta, ef undirbúningur er ekki nú þegar hafinn, enda leggja hin nýju lög mikla ábyrgð á sveitarfélög. Mikilvægt er því að sveitarfélögin fari ítarlega yfir það hvernig þau eru í stakk búin að takast á við hertar kröfur á þessu sviði.

Sambandið bendir á að áður en farið er af stað í innleiðingu reglugerðarinnar í starfsemi sveitarfélaga er heppilegt verklag að hvert sveitarfélag setji saman teymi sem stýri umræddu verkefni. Reglugerðin gildir þvert á svið og því mikilvægt að hafa fjölbreyttan hóp sem kemur að verkefninu og hefur reynslu af stjórnun á vinnslu persónuupplýsinga. Í slíku teymi gætu t.d. verið lögfræðingur, tæknimanneskja, mannauðsstjóri og fulltrúi yfirstjórnar.

Þá er mikilvægt í upphafi að sveitarfélög/teymi skoði hvað er nú þegar fyrir hendi hjá þeim, eru t.d. til staðar gæðakerfi, öryggisstefnur, hefur verið framkvæmd áhættumat á vinnslu o.s.frv. Er rétt í þessu sambandi að skoða hvort gerðir hafi verið vinnslusamningar við aðila sem þjónusta tölvukerfi og aðrar tæknilegar lausnir. Skoða þarf hvort slíkir samningar uppfylli nýja löggjöf. Sambandið bendir á að vinnslusamningur sem afhentur var sem form í tengslum við Mentor mál væri hér mjög góð byrjun og væri þá hægt að endurskoða hann þegar ný lög taka gildi.

Í fyrri leiðbeiningum var talað um fyrstu skref við innleiðingu og í framhaldinu áætlunargerð. Sambandið telur rétt í ljósi þess hve styttist í gildistöku að einfalda fyrri leiðbeiningar og mælir með að gerð séu drög að vinnu við innleiðingu í þremur skrefum. Leggur sambandið til að sveitarfélög hagi vinnu sinni við undirbúning í samræmi við neðangreinda áætlun:

Fyrstu skref:

1. Sveitarfélög kynni sér efni reglugerðarinnar, m.a. með lestri og dreifingu þessara leiðbeininga og með því að sækja námskeið.
2. Hafin verði sem fyrst skoðun á því hvaða persónuupplýsingum er verið að safna og hvernig unnið er úr þeim. Við kortlagningu á vinnslu verði sérstaklega skoðað:
    a. Hvaða upplýsingum er verið að safna (almennar/viðkvæmar)?
    b. Er lagagrundvöllur fyrir hendi fyrir söfnun? Ef svo er hver er hann?
    c. Hversu lengi er verið að geyma upplýsingar?

    Sambandið bendir á að í mörgum tilvikum fellur geymsla upplýsinga sem sveitarfélög afla undir lagaskyldu eins og t.d. lög um opinber skjalasöfn nr. 77/2014. Ef óvissa er um ákvæði laganna og hvernig haga skuli geymslu er hægt að hafa samband við lögmann þjóðskjalasafns sem er sérfræðingur í persónuverndarmálum.
3. Við kortlagningu sé kannað og tryggt að varsla og vinnsla upplýsinga sé hið minnsta í samræmi við núgildandi lög.

    Persónuvernd hefur bent á að ef svo er þá séu stofnarnir komnar 50% á leið við undirbúning

Sambandið bendir á að við kortlagningu og greiningu á nauðsynlegum úrbótum er mikilvægt að greining eigi sér stað á skyldum samkvæmt nýjum lögum eins og hvort sveitarfélag þurfi að halda skrá yfir vinnslustarfsemi, tilnefning persónuverndarfulltrúa, framkvæmd mats á áhrifum á persónuvernd o.s.frv.

Næstu skref:

4. Greining á nauðsynlegum úrbótum miðað við nýja löggjöf.
    a. Hvernig á að bregðast við upplýsingarétti hins skráða?
    b. Gildir réttur til að gleymast að einhverju leyti eða er geymsla í samræmi við lagaákvæði?
    c. Getur verið að flutningsréttur verði virkur, t.d. ef senda á gögn úr félagsþjónustu á milli stofnanana?
    d. Er persónuvernd innbyggð í tölvubúnað? Hvernig er upplýsingaöryggi háttað. Fá upplýsingar frá þeim sem veita þjónustu. Mögulega þarf að uppfæra stjórnkerfi og upplýsingaöryggisstefnu.
    e. Framkvæma áhættumat á ferlum þar sem við á.
5. Semja þarf verklagsreglur um persónuvernd og persónuverndarstefna sett. Hér kæmi vel til greina að sveitarfélög vinni saman og mögulega með aðkomu sambandsins. Í slíkri persónuverndarstefnu þarf að koma fram að sveitarfélag hafi að leiðarljósi að:
        a. tryggja vinnslu persónuupplýsinga (má nefna meginferla, lagalega vinnslu)
        b. tryggja að fengið sé samþykki hins skráða eða að vinnsla byggi á tilgreindri lagaheimild
        c. haft sé eftirlit með öryggisbrotum og þau tilkynnt
        d. að framkvæmdar séu innri úttektir (persónuverndarfulltrúi ber ábyrgð á þeim)
        e. farið verði í úrbætur, ef þarf, í samræmi við niðurstöður innri úttektar
        f. tryggja leynd, réttleika, tiltækanleika og þol gagna

6. Skipuleggja breytingar á vinnslu m.v. greininguna, þannig að vinnuferlar séu skráðir til að tryggja að farið verði að nýjum lögum. Mikilvægt er að tryggja rekjanleika allra samskipta við einstakling við vinnslu.

Lokaskref:

7. Innleiðing úrbóta

Hér getur verið um að ræða að breytingar á ferlum séu kynntar og nýir samningar gerðir við vinnsluaðila.

Mikilvægt að sveitarfélög forgangsraði til hvaða aðgerða er gripið hvenær og valið sé skynsamlegt í ljósi fjárheimilda og tíma til stefnu.

Ekki er ólíklegt að ferli taki 3-6 mánuði og er mikilvægt að reyna að dreifa álagi við innleiðingu jafnt.

Ef einhverjir liðir í áætlun nást ekki áður en lög taka gildi þá er mikilvægt að vera með áætlun um hvernig skuli lokið við innleiðingu varðandi það sem ekki næst áður en ný lög taka gildi

8. Þjálfun starfsmanna á grundvelli vinnu teymis og innleiðingu úrbóta. Ítarefni um ný lög, kynning á nýjum ferlum, öryggisatriðum o.s.frv.
9. Skipun persónuverndarfulltrúa. Skylda hvílir á öllum opinberum stofnunum þ.m.t. sveitarfélögum að skipa. Um störf hans er nánar fjallað í kafli 9.

Mikilvægt er að teymi þarfagreini hversu mikið starf slíkur sérfræðingur eigi að vinna og að honum séu veittar þær heimildir sem nýju lögin kveða á um. Ef ekki er talin þörf á heilu stöðugildi gætu sveitarfélög eða stofnanir sammælst um að nýta sameiginlega einn persónuverndarfulltrúa. Sambandið bendir auk þess á erindi Harðar Helga Helgasonar lögmanns sem flutt var á málstofu Stofnunar stjórnsýslufræða um farsæla innleiðingu. Þar er m.a. að finna yfirlitsmynd yfir kortlagningu á vinnslu sjá:

http://www.stjornsyslustofnun.hi.is/sites/stjornsyslustofnun.hi.is/files/gudruney/2017-03-03_stjornsyslustofnun-verkfaerakistan.pdf

4. Nýjar skyldur sveitarfélaga - ábyrgðarskylda og upplýsingaskylda

Með nýrri löggjöf takast sveitarfélög á hendur nýjar og mun strangari skuldbindingar en þau gera samkvæmt núgildandi lögum. Hinar nýju skyldur fela m.a.í sér að auknar kröfur eru gerðar til ábyrgðaraðila að geta sýnt fram á reglufylgni auk þess sem ýmis ný réttindi einstaklinga eru kynnt til sögunnar og réttindi sem nú þegar eru til staðar aukin. Fjallað er um ný réttindi einstaklinga í kafla 6 en réttindi þeirra eru nátengd skyldum sveitarfélaga. Þær skyldur sem mest koma við sveitarfélögin eru ábyrgðarskyldan og breytt upplýsingaskylda og verður fjallað um þær í þessum kafla.

Í ábyrgðarskyldu felst að ábyrgðaraðili er ábyrgur fyrir því að farið sé að meginreglum 5. gr. reglugerðarinnar um vinnslu og þarf hann að geta sýnt fram á þetta sbr. 2. mgr. 5. gr. Þarf ábyrgðaraðili því að gera tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að vinnsla fari fram í samræmi við reglugerðina. Þau tæki sem ábyrgðaraðili getur gripið til við að sýna fram á eftirfylgni eru ma. með því að skjalfesta stefnu og verklagsreglur um einstaka skyldur, að vera með samþykktar hátternisreglur, geta sýnt fram á vottun auk skipunar persónuverndarfulltrúa.

Í ábyrgðarskyldu felst jafnframt að hafa verður samvinnu við persónuverndaryfirvöld samkvæmt beiðni.

Sambandið bendir sérstaklega á að þegar sveitarfélög eru ábyrgðaraðilar að vinnslu persónuupplýsinga þá bera þau ábyrgð á því að allir starfsmenn þekki reglurnar og vinni eftir þeim. Verði öryggisbrot vegna meðferðar persónuupplýsinga hjá sveitarfélögum þá getur það leitt til þess að þau verði sektuð s sem skaðabótaskylda getur verið fyrir hendi gagnvart skráðum einstaklingi. Sjá nánar í kafla 13.

Að því er varðar upplýsingarétt þá er sveitarfélögum skylt við vinnslu og söfnun persónuupplýsinga að upplýsa skráða einstaklinga um söfnun og vinnslu í ríkum mæli, en með nýrri löggjöf er upplýsingaskyldan aukin og gerð skýrari.

Ábyrgðaraðili skal gera viðeigandi ráðstafanir til að láta skráðum einstaklingi í té þær upplýsingar í tengslum við vinnslu á gagnorðu, gagnsæju, skiljanlegu og aðgengilegu formi og skýru og einföldu máli, einkum þegar um er að ræða upplýsingar sem beint er sérstaklega til barns.

Ábyrgðaraðili skal auðvelda skráðum einstaklingi að neyta réttar síns, og ekki neita að verða við beiðni hins skráða um að neyta réttar síns nema hann sýni fram á að hann sé ekki í aðstöðu til að staðfesta deili á hinum skráða. Ábyrgðaraðilinn skal veita skráðum einstaklingi upplýsingar um aðgerðir, sem gripið er til vegna beiðni innan mánaðar frá viðtöku beiðninnar.

Verði ábyrgðaraðili ekki við beiðni skráðs einstaklings skal hann tilkynna honum, án tafar og í síðasta lagi innan mánaðar frá viðtöku beiðninnar, um ástæðurnar fyrir því að það var ekki gert og um möguleikann á að leggja fram kvörtun hjá Persónuvernd.

Upplýsingar sem sveitarfélögum ber að veita við öflun persónuupplýsinga hjá skráðum einstaklingi eru eftirfarandi:

1. Heiti og samskiptaupplýsingar sveitarfélags og persónuverndarfulltrúa
2. Tilgangur með fyrirhugaðri vinnslu persónuupplýsinganna og hver lagagrundvöllur hennar er.
3. Hvaða lögmætu hagsmunir það eru sem ábyrgðaraðili gætir,
4. Hvaða persónupplýsingar eru vistaðar og/eða unnið með.
5. Grundvöllur fyrir vinnslu persónuupplýsinga – lagaákvæði eða samþykki. Ef vinnsla byggir á samþykki skal upplýst um rétt til að draga samþykki til baka
6. Hver er viðtakandi persónuupplýsinga sem vistaðar og/eða unnar eru.
7. Hversu lengi persónuupplýsingarnar eru geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða hversu lengi þær eru geymdar.
8. Réttindi einstaklinga til aðgangs að upplýsingum, láta leiðrétta þær, eyða þeim, eða takmarka vinnslu þeirra og til að andmæla vinnslu, auk réttarins til að flytja eigin gögn.
9. Réttur til að leggja fram kvörtun hjá Persónuvernd.
10. Ef upplýsingar eru fengnar frá öðrum en skráðum einstaklingi, hvaðan þær eru fengnar og hvort þær koma frá opinberum aðilum.
11. Hvort það að veita persónuupplýsingar sé krafa samkvæmt lögum eða samkvæmt samningi eða krafa sem er forsenda þess að hægt sé að gera samning og einnig hvort skráðum einstaklingi sé

skylt að láta persónuupplýsingarnar í té og mögulegar afleiðingar þess ef hann veitir ekki upplýsingarnar

12. Ef sveitarfélag hyggst vinna persónuupplýsingarnar frekar í öðrum tilgangi en þeim sem lá að baki söfnun þeirra skal það láta hinum skráða í té upplýsingar um þennan nýja tilgang áður en sú frekari vinnsla hefst, ásamt öðrum viðeigandi viðbótarupplýsingum.

Upplýsingar sem veittar eru einstaklingum skulu vera án endurgjalds.

Sjá nánar 12.-14. gr. reglugerðar

5. Skrár yfir vinnslustarfsemi

Hjá stærri sveitarfélögum, eða þar sem starfsmenn eru **fleiri en 250** ber að halda skrá yfir vinnslustarfsemi sem fram fer á ábyrgð hans. Nálgast má tölur um stöðugildi hjá sveitarfélögum Í árbók sveitarfélaga 2017 en samkvæmt þeim tölum er um að ræða 12 sveitarfélög[3] sem þurfa að halda slíka skrá.

Þessi skylda hvílir ekki á sveitarfélögum eða stofnunum þess ef starfsmenn eru 250 eða færri, nema ef vinnslan, sem þar er innt af hendi, er líkleg til að leiða af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, vinnslan sé ekki tilfallandi eða taki til sérstakra flokka upplýsinga. Að því marki sem sveitarfélög eða stofnanir þeirra vinna reglubundið með upplýsingar, eða vinna með viðkvæmar persónuupplýsingar, s.s. um heilsufar, þá þarf viðkomandi ábyrgðaraðili að útbúa slíka skrá. Við gerð skráarinnar er hjálplegt að hafa fyrst kortlagt þá vinnslu persónuupplýsinga sem fram fer hjá hverjum ábyrgðaraðila, en slík kortlagning getur nýst í undirbúning að gerð skráar yfir vinnslustarfsemi.

Um vinnsluskrár og það sem þar þarf að koma fram er fjallað í 30. gr. reglugerðarinnar, en þar þarf að koma fram:

- Heiti og samskiptaupplýsingar ábyrgðaraðila og persónuverndarfulltrúa
- Tilgangur vinnslunnar
- Lýsing á flokkum skráðra og persónuupplýsinga
- Hverjir munu fá upplýsingarnar, þ.m.t. þriðju aðilar
- Ef við á, flutningur til annarra landa á gögnum
- Fyrirhuguð tímamörk fyrir eyðingu, eða lagaskylda til að geyma
- Lýsing á öryggisráðstöfunum við geymslu og vinnslu gagna

Afar mikilvægt er að þau sveitarfélög sem þurfa að halda slíka skrá fari að huga að hvernig það skuli gert, bæði hvað varðar ferli og hugbúnað. Sambandið bendir á að skynsamlegt er fyrir sveitarfélög að sameinast í undirbúningi við þessa vinnu.

[3] Samkvæmt árbókinni munu eftirfarandi sveitarfélögum verða skylt að halda skrá yfir vinnslustarfsemi: Reykjavíkurborg, Kópavogsbær, Garðabær, Hafnafjarðarbær, Mosfellsbær, Reykjanesbær, Akraneskaupstaður, Ísafjarðarbær, Sveitarfélagið Skagafjörður, Akureyrarbær, Fjarðabyggð, Vestmannaeyjabær,

Hér að neðan er finna dæmi um yfirlit um hvað skuli koma fram í vinnsluskrá, en í slíkri skrá þarf að aðgreina vinnslustarfsemi og fylla út tilvitnaðar upplýsingar við hverja vinnslustarfsemi.

	Controllers (Article 30(1))	Processors (Article 30(2))
Records of What	Processing Activities	Categories of Processing Activities carried out on behalf of a controller
Contact Info	Name and contact details of: - Controller - Where applicable, the joint controller - The controller's representative - The data protection officer (DPO)	Name and contact details of: - The processor or processors - Each controller on behalf of which processor is acting - Where applicable of the controller and processors representatives - DPO (if any)
Purpose of Processing	The purposes of the processing	n/a
Data Subjects	A description of the categories of data subjects	n/a
Personal Data	A description of the categories of personal data	n/a
Recipients	The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations	n/a
Security	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)
Cross-Border Transfers	Where applicable, transfers of personal data to a third country or an international organization Safeguards on the transfer from list in Article 49(1)	Where applicable, transfers of personal data to a third country or an international organization Safeguards on the transfer from list in Article 49(1)
Retention	The envisaged time limits for erasure of the different categories of data	n/a

6. Réttindi einstaklinga sem sveitarfélög verða að fara eftir

Einn megintilgangur nýrrar löggjafar er að veita einstaklingum betri vernd og færa þeim aukinn ákvörðunarrétt yfir persónuupplýsingum sínum í þeim tilgangi að fela þeim stjórn yfir því hver vinnur upplýsingar um þá, hvenær og í hvaða tilgangi. Mikilvægt er að sveitarfélög kynni sér vel réttindi einstaklinga þar sem þau verða að tryggja að skráðir einstaklingar geti notið þessara réttinda. Ef sveitarfélag brýtur gegn reglunum mun Persónuvernd hafa heimild til að sekta það eða kveða á um önnur þvingunarúrræði samkvæmt lögunum. Samkvæmt upplýsingum frá Persónuvernd verður þó aðaláhersla á að sveitarfélög hugi að meðalhófsreglu sbr. 5. gr. reglugerðarinnar og safni ekki upplýsingum sem ekki verða notaðar. Þá er líklegt að eingöngu verði beitt áminningum fyrst um sinn ef sveitarfélög geta sýnt fram á að þau séu sannarlega að huga að innleiðingu reglna og að um óhapp hafi verið að ræða.

Ný löggjöf felur í sér þessi nýju réttindi:

1. Rétturinn til að gleymast

Skráðir einstaklingar eiga rétt á því í vissum tilvikum að persónuupplýsingar um þá séu leiðréttar eða þeim eytt, t.d. ef upplýsingarnar eru ekki lengur nauðsynlegar í þágu þess tilgangs sem þeirra var upphaflega aflað í, ef vinnsla byggist á samþykki og samþykki er dregið til baka og ef persónuupplýsingar hafa verið meðhöndlaðar í andstöðu við ný lög. Þessi réttur er þó háður takmörkunum þegar um er að ræða lagaskyldu til að varðveita upplýsingar t.d. á grundvelli laga um opinber skjalasöfn.

Sjá nánar 17. gr. reglugerðar

2. Réttur til leiðréttingar

Skráður einstaklingur á rétt á að fá áreiðanlegar persónupplýsingar leiðréttar án tafa. Hann á einnig rétt á að láta fullgera ófullkomnar eða óáreiðanlegar persónuupplýsingar.

Sjá nánar 16. gr. reglugerðar

3. Réttur til að flytja eigin gögn (gildir að mjög litlu ef einhverju leiti gagnvart sveitarfélögum)

Skráðir einstaklingar eiga rétt á því að upplýsingar sem þeir láta af hendi, á grundvelli samþykkis eða samnings, til fyrirtækja eða annarra sem veita þjónustu á netinu, verði fluttar að beiðni skráðs einstaklings til annarra aðila á borð við samfélagsmiðla, netþjónustur eða streymiþjónustur. Skráðir einstaklingar eiga einnig rétt á því að fá persónuupplýsingar sínar á hefðbundnu sem og stafrænu formi svo framarlega sem það er tæknilega mögulegt. Þessi skylda mun hins vegar gilda mjög takmarkað um sveitarfélög þar sem þær upplýsingar sem sveitarfélög safna falla sjaldnast undir hreyfanleika skjala samkvæmt reglugerð.

Vinnuhópur 29 um reglugerðina hefur gefið frá sér álit á hreyfanleika gagna (e. Data Portability) og yfirlit með algengum spurningum og svörum um hreyfanleika og er hægt að nálgast það hér:

https://www.personuvernd.is/ny-personuverndarloggjof-2018/leidbeiningar-fra-29.-gr.-vinnuhopi-esb/

Sjá nánar 20. gr. reglugerðar

4. Auknar kröfur til samþykkis fyrir vinnslu

Samþykki skráðra einstaklinga þarf ávallt að vera veitt með skýrri staðfestingu, s.s. með skriflegri yfirlýsingu. Yfirlýsingin þarf hið minnsta að vera ótvíræð, gefin af fúsum og frjálsum vilja og ná til allra aðgerða sem framkvæmdar eru. Þögn, aðgerðaleysi og rafrænt hak, sem gerir fyrirfram ráð fyrir samþykki flokkast ekki sem samþykki. Er mælt með því að útbúin verði samþykkis eyðublöð vegna þessa.

Sjá nánar 8. gr. reglugerðar

5. Réttur til upplýsinga um vinnslu og til aðgangs að eigin persónuupplýsingum

Skráðir einstaklingar eiga rétt á því að sveitarfélögin veiti upplýsingar um vinnslu og meðferð persónuupplýsinga um viðkomandi á hnitmiðuðu, skiljanlegu og aðgengilegu formi og á skýru og einföldu máli. Upplýsingar má veita skriflega eða á annan hátt, m.a. með rafrænum hætti, og skulu þær veittar eigi síðar en mánuði frá því að ósk barst.

Sjá nánar 15. gr. reglugerðar

6. Börnum veitt sérstök vernd

Netþjónustur (t.d. samfélagsmiðlar) verða að afla samþykkis foreldra áður en börn undir 16 ára aldri skrá sig í slíka þjónustu. Heimilt er að kveða á um lægra aldurstakmark í landslögum en þó ekki lægra en 13 ára. Séu upplýsingar ætlaðar börnum eru gerðar þær kröfur að upplýsingar miðist við skilning þeirra og þroska.

Sjá nánar 8. gr. reglugerðar

7. Réttur til að krefjast takmörkunar á vinnslu

Skráður einstaklingur getur í ákveðnum tilvikum krafist þess að sveitarfélag takmarki vinnslu á persónuupplýsingum hans.

Sjá nánar 18. gr. reglugerðar

8. Andmælaréttur

Skráður einstaklingur á rétt á að andmæla vinnslu persónuupplýsinga er varða hann sjálfan í ákveðnum tilvikum. Getur ábyrgðaraðili í slíkum tilvikum ekki unnið persónuupplýsingarnar frekar nema hann geti sýnt fram á mikilvægar lögmætar ástæður fyrir vinnslunni sem ganga framar hagsmunum, réttindum og frelsi hins skráða eða því að stofna, hafa uppi eða verja réttarkröfur.

Sjá nánar 21. gr. reglugerðar

7. Þarf að meta áhættu við vinnslu persónuupplýsinga (DPIA)?

Við mat á ferlum við vinnslu persónuupplýsinga hjá sveitarfélögum verður að meta sérstaklega hvort vinnsluaðferðir skapi mikla hættu fyrir friðhelgi einstaklinga. Á þetta einkum við þar sem notast er við nýja tækni við vinnslu og með hliðsjón af eðli, umfangi, samhengi og tilgangi vinnslunnar (sjá skilgreiningu á vinnslu í kafla 2). Í þeim tilvikum skulu sveitarfélög í samráði við persónuverndarfulltrúa framkvæma mat á áhrifum fyrirhugaðra vinnsluaðgerða á vernd persónuupplýsinga áður en vinnslan hefst. Ef um er að ræða vinnslu á viðkvæmum persónuupplýsingum (sjá skilgreiningu á viðkvæmum persónuupplýsingum í kafla 2) skal alltaf fara fram mat á áhrifum. Vakin er sérstök athygli á því að ef gerðin verður innleidd óbreytt þá þarf að áhættumeta öll launakerfi þar sem stéttarfélagsupplýsingar eru viðkvæmar persónuupplýsingar. Mögulegt er þó að taka á þessu í kjarasamningum þannig að kjarasamningar kveði á um að vinnuveitendur hafi heimild til vinnslu þessara upplýsinga til að sleppa við áhættumat. Sambandið bendir á að sé talið nauðsynlegt að áhættumeta vinnslu þurfi slíkt áhættumat hvorki að vera flókið né vandasamnt.

Við mat á áhrifum er mikilvægt að skoða innra og ytra umhverfi vinnslunnar, skrá meginferla, hver ber ábyrgð á vinnslunni og setja kröfur um að leynd, réttleiki og tiltækileiki séu hluti af vinnslunni. Mikilvægt er að við framkvæmd mats á áhrifum sé stuðst sé við þekktar og áreiðanlegar aðferðir eins og t.d. SIPOC [4] sem greinir ekki bara gögnin heldur líka umhverfið.

Þetta er mikilvægt þar sem sveitarfélag þarf að gera sér grein fyrir þeirri hættu og mögulegum afleiðingum af vinnslunni, einkum vegna mögulegra öryggisbrota og afleiðinga þeirra.

Sveitarfélög skulu einkum láta fara fram mat á áhrifum á persónuvernd, þegar um er að ræða:

a) kerfisbundið og umfangsmikið mat á persónulegum þáttum (profiling). Hér gæti t.d. verið um greiningarvinnu að ræða á grundvelli heilsufarsupplýsinga.

b) umfangsmikla vinnsl viðkvæmra persónuupplýsinga, eða

c) kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi, m.a. með myndavélum.

[4] Suppliers, Inputs, process, outputs and Customer.

Þurfi að framkvæma slíkt mat þarf það að gerast áður en vinnsla hefst. Þarf þá mat á áhrifum að fela í sér að lágmarki:

a) kerfisbundna lýsingu á fyrirhuguðum vinnsluaðgerðum og tilgangi með vinnslunni, þ.m.t., eftir atvikum, lögmætum hagsmunum ábyrgðaraðilans,

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

c) mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga, og

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

Hér þarf að ganga úr skugga um að mat á áhrifum fari ávallt fram við framangreindar aðstæður, þar sem skoðað er sérstaklega hver er ógnin, hversu miklir veikleikar eru og hvaða varnir eru til staðar. Slíkt er hægt að tryggja með gerð verklagsreglna og ferla um mat á áhrifum og hvernig eigi að bera sig að þegar leitað er forálits Persónuverndar. Hér skiptir líka miklu máli aðkoma persónuverndarfulltrúans.

Rétt er að benda á að Fjármálaráðuneytið hefur birt handbók um sjálfsmat í árangri í stjórnun CAF[5] sem hægt er að styðjast við við skoðun og mat á ferlum a.m.k. í stærri sveitarfélögum. Þar kemur fram að aðalmarkmið CAF sé fjórþætt:

1. Kynna opinberri stjórnsýslu grundvallaraðferðir gæðastjórnunar og leiða hana eftir þeirri braut, með notkun og sjálfsmati, frá núverandi „skipuleggja–innleiða“ yfir í röð aðgerða sem leiða að lokum til umbótahringsins „skipuleggja-innleiða-meta-bæta“ (Plan-Do-Check-Act / PDCA),

2. Auðvelda sjálfsmat hjá opinberum stjórnsýslu- og þjónustustofnunum í því skyni að fram fari greining og umbætur,

3. Vera brú milli mismunandi aðgerða sem notaðar eru í gæðastjórnun,

4. Auðvelda samanburð og lærdóm milli opinberra stofnana.

Vinnuhópur 29 um reglugerðina hefur gefið frá sér álit um mat á áhrifum og er hægt að nálgast það hér:

https://www.personuvernd.is/ny-personuverndarloggjof-2018/leidbeiningar-fra-29.-gr.-vinnuhopi-esb/

Sjá nánar 35. gr. reglugerðar

Sambandið bendir á að ef niðurstaða mats á áhrifum gefur til kynna að vinnslan myndi hafa mikla áhættu í för með sér, nema ábyrgðaraðilinn grípi til ráðstafana til að draga úr henni, skal ábyrgðaraðilinn hafa samráð við Persónuvernd áður en vinnsla hefst.

Sjá nánar 36. gr. reglugerðar

[5] Common assessment framework. sjá: www.stjornarradid.is/verkefni/rekstur-og-eignir-rikisins/skipulag-og-stjornun-rikisstofnana/sjalfsmat-a-arangri-i-stjornun-caf/

8. Persónuvernd verður að vera sjálfgefin og innbyggð í nýjan hugbúnað og upplýsingakerfi.

Samkvæmt nýju löggjöfinni skal nýr hugbúnaður og upplýsingakerfi vera útfærð með sérstaka áherslu á friðhelgi einkalífsins, s.s. með lágmörkun gagnasöfnunar og að valið kerfi sé feli í sér sem minnsta áhættu og safni eins litlum persónuupplýsingum og hægt er og að persónuvernd sé innbyggð í viðkomandi lausn. Verður gengið út frá því að hámarks áhersla á persónuvernd sé sjálfgefin og innbyggð í öll kerfi og skipulagslegar ráðstafanir, svo sem ferla eða verklagsreglur þar sem vinnsla er ákveðin. Skal þannig gera viðeigandi ráðstafanir til að tryggja að sjálfgefið sé að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar hverju sinni. Við slíkt er mikilvægt að skoðað sé hver er grundvöllur vinnslunnar, þ.e. byggir hún á lagaheimild eða samþykki og hvaða takmörkunum er hún háð vegna þessa. Þarf að huga að þessu sérstaklega við fræðslu starfsmanna, einkum þá sem vinna við tæknimál.

Heimilt verður að nota samþykkt vottunarfyrirkomulag, sbr. 42. gr. reglugerðar, til að sýna fram á að þessar kröfur séu uppfylltar. Gera má ráð fyrir að slíku vottunarfyrirkomulagi verði komið á af hálfu dómsmálaráðuneytisins og Persónuverndar þannig að sveitarfélög geti samið við aðila með slíkar vottanir og er mælt alveg sérstaklega með því að eingöngu verði samið við aðila sem hafi slíka vottun eða uppfylli ISO staðla eins og t.d. 9001 og 27001.

Á grundvelli þessa verða sveitarfélög að ganga úr skugga um að þegar nýr hugbúnaður eða tækni er tekin í notkun við vinnslu persónuupplýsinga séu þessar kröfur uppfylltar. Ekki eru gerðar sömu kröfur til eldri hugbúnaðar en þó ber að innleiða reglugerð að því leyti sem hægt er. Skýjalausnir þarf jafnframt að skoða sérstaklega og hvort þær bjóði upp á nægjanlega vernd samkvæmt nýjum lögum.

Sjá nánar 25. gr. og 42. gr. reglugerðar

9. Hvenær þarf að skipa persónuverndarfulltrúa og nánar um störf hans

Öll opinber yfirvöld eða stofnanir, þ.m.t. sveitarfélög og stofnanir þess (fyrir utan dómstóla) verða að tilnefna persónuverndarfulltrúa sbr. 37. gr. reglugerðar. Nefna hér viðeigandi grein rg.

Ef ábyrgðaraðili eða vinnsluaðili er opinbert yfirvald eða stofnun er heimilt að tilnefna einn persónuverndarfulltrúa fyrir fleiri en eitt slíkt yfirvald eða stofnun, að teknu tilliti til stjórnskipulags þeirra og stærðar. Í þessu felst að eitt sveitarfélag, ásamt stofnunum þess, getur tilnefnt einn persónuverndarfulltrúa. Þá gætu minni sveitarfélög tilnefnt saman einn persónuverndarfulltrúa. Áður en slíkt er ákveðið þarf þó að fara fram greining á því hversu umfangsmikið starf viðkomandi persónuverndarfulltrúa komi til með að vera. Deili nokkur sveitarfélög eða stofnanir persónuverndarfulltrúa þarf hvert þeirra að gera samning við persónuverndarfulltrúann.

Sambandið bendir á að persónuverndarfulltrúa er jafnframt heimilt að gegna öðrum störfum hjá sveitarfélagi.

Persónuverndarfulltrúi skal tilnefndur á grundvelli faglegrar hæfni sinnar og sérþekkingar á lögum og lagaframkvæmd á sviði persónuverndar og getu til að vinna verkefni sem honum eru falin í 39. gr. reglugerðarinnar. Ríkar kröfur eru gerðar til þess að hann fái mikla þjálfun og miðli þekkingu til annarra

starfmanna. Sveitarfélag skal tryggja að hann hafi ekki skyldustörf á höndum sem leiði til hagsmunaárekstra við starf viðkomandi sem persónuverndarfulltrúi.

Persónuverndarfulltrúi skal koma að öllum málum sem varða meðferð persónuupplýsinga og er hann tengiliður fyrir sveitarfélagið við Persónuvernd og hina skráðu. Það þýðir að öllum spurningum og beiðnum frá hinum skráðu, er varða meðferð og geymslu persónuupplýsinga og hvernig þeir geta nýtt rétt sinn, skal beint til hans.

Sveitarfélög skulu tryggja að persónuverndarfulltrúi hafi starfsskilyrði sem tryggi að hann geti sinnt starfi sínu í samræmi við lögin og að hann komi með viðeigandi hætti og tímanlega að öllum málum sem tengjast vernd persónuupplýsinga.

Persónuverndarfulltrúi skal vera óháður í störfum sínum sem persónuverndarfulltrúi og ekki taka við skipunum yfirmanns varðandi þau störf. Sveitarfélög eiga að tryggja að hann fái engin fyrirmæli varðandi framkvæmd verkefna sinna skv. 39. gr. og skal hann heyra beint undir æðsta stjórnunarstig hjá ábyrgðaraðila eða vinnsluaðila. Enn fremur skal hvorki víkja honum úr starfi né refsa honum fyrir framkvæmd verkefna sinna. Persónuverndarfulltrúi er bundinn trúnaðar- og þagnarskyldu.

Persónuverndarfulltrúi skal a.m.k. sinna eftirfarandi verkefnum:

1. Upplýsa og ráðleggja sveitarfélagi og starfsmönnum þess um skyldur skv. reglugerðinni og persónuverndarlögum.
2. Hafa eftirlit með fylgni við löggjöfina og stefnu sveitarfélagsins, þ.m.t. úthlutun ábyrgðar, vitundarvakningu, þjálfun starfsfólks og úttektir, en telji persónuverndarfulltrúi að úttekt þurfi, þá er ekki heimilt að hafna því.
3. Veita ráðgjöf og aðstoða við mat á áhrifum sbr. 35. gr. reglugerðarinnar og fylgjast með framkvæmd þess.
4. Vinna með og vera tengiliður við Persónuvernd.

Sambandið bendir á að sveitarfélögum er heimilt að útvista verkefnum persónuverndarfulltrúa. Sé það gert er hins vegar mikilvægt að vandað sé valið þar sem ekki er unnt að útvista ábyrgð og ber sveitarfélag því ábyrgð ef persónuverndarfulltrúi sinnir ekki skyldum sínum.

Sjá leiðbeiningar frá vinnuhópi ESB um persónuverndarfulltrúa: https://www.personuvernd.is/ny-personuverndarloggjof-2018/leidbeiningar-fra-29.-gr.-vinnuhopi-esb/

Sjá nánar 37. - 39. gr. reglugerðar.

10. Allir vinnsluaðilar takast á hendur nýjar skyldur

Vinnsluaðilar eru þeir sem vinna með persónuupplýsingar fyrir hönd ábyrgðaraðila, en sveitarfélög geta mögulega verið í báðum hlutverkum, til dæmis í þeim tilvikum þar sem stofnanir sveitarfélaga eins og byggðasamlög taka að sér sérverkefni eins og aksturþjónustu þar sem heilsuupplýsingar eru vistaðar. Vinnsluaðilar eru þó almennt séð fyrirtæki á sviði upplýsingatækniþjónustu, en geta líka verið einstaklingar sem sinna afmörkuðum verkefnum fyrir sveitarfélög, mætti sem dæmi nefna einstaklinga sem vinna

gæðarannsóknir og vinnustaðaskýrslur. Er það nýmæli í reglugerðinni að sjálfstæðar skyldur eru nú lagðar á vinnsluaðila þegar unnið er með persónuupplýsingar fyrir hönd ábyrgðaraðila.

Sambandið bendir á að einungis skal leita til þeirra vinnsluaðila sem veita nægjanlegar tryggingar fyrir því að þeir geri viðeigandi tæknilegar og skipulagslegar ráðstafanir til að vinnsla uppfylli kröfur persónuverndarlaga og að vernd réttinda skráðra einstaklinga sé tryggð. Mikilvægt er að sveitarfélög hafi þetta sérstaklega í huga þegar samið er við aðila hvort sem um er að ræða félag eða einstakling. ***Mikilvægt er að í vinnslusamningi komi fram sú krafa sveitarfélaga að uppfyllt séu skilyrði laga um persónuvernd eins og þau eru á hverjum tíma.***

Vinnsluaðili ber sjálfstæða ábyrgð og getur orðið efnahagslega ábyrgur til jafns við ábyrgðaraðila ef vinnsla brýtur í bága við lögin. Þá getur vinnsluaðili þurft að tilnefna persónuverndarfulltrúa, sbr. 37. gr. reglugerðarinnar. Einnig er lögð sú skylda á vinnsluaðila að tilkynna til ábyrgðaraðilans þegar öryggisbrot verður.

Helstu skyldur vinnsluaðila verða eftirfarandi:

1. Vinna eingöngu með persónuupplýsingar samkvæmt skjalfestum fyrirmælum ábyrgðaraðila, þ.m.t. að því er varðar miðlun persónuupplýsinga til þriðja lands eða alþjóðastofnunar. Þetta er sérstaklega mikilvægt að hafa í huga ef sveitarfélag hyggst taka í notkun tölvuský til að vista gögn en í slíkum tilvikum er mikilvægt er að skoða sérstaklega hvort heimilt sé að flytja upplýsingar úr landi.
2. Tryggja að aðilar sem hafa heimild til vinnslu persónuupplýsinga hafi gengist undir trúnaðarskyldu eða heyri undir viðeigandi lögboðna trúnaðarskyldu.
3. Gæta að upplýsingaöryggi og geri ráðstafanir sbr. 32. gr. reglugerðar.
4. Tilkynna þegar í stað um öryggsbrot við meðferð persónuupplýsinga
5. Virða skilyrði reglugerðarinnar um ráðningu annars vinnsluaðila, sbr. 2. og 4. mgr. 28. gr.
6. Aðstoða ábyrgðaraðila við að uppfylla skyldu sína að svara beiðnum um að skráðir einstaklingar fái neytt réttar síns
7. Aðstoða ábyrgðaraðila við tryggja að skyldur skv. 32.-36. gr. séu uppfylltar.
8. Eyða eða skila öllum persónuupplýsingum til ábyrgðaraðilans eftir að veitingu þjónustunnar lýkur, nema ef lög kveða á um annað.
9. Veitai ábyrgðaraðila aðgang að öllum upplýsingaum, sem nauðsynlegar eru til að sýna fram á að skuldbindingarnar séu uppfylltar, gefa kost á úttektum og leggja sitt af mörkum til þeirra.

Vinnsluaðilum er skylt að upplýsa ef þeir telja að fyrirmæli sveitarfélaga séu andstæð lögum eða persónuverndarstefnu og verður sveitarfélag að skoða slíkt sérstaklega og mögulega í samstarfi við Persónuvernd.

Vinnsluaðila er ekki heimilt að ráða annan vinnsluaðila til að sinna verkefnum sem honum eru falin án heimildar frá ábyrgðaraðila.

Sjá nánar 28.gr. og 32. – 36. gr. reglugerðar

11. Sveitarfélög geta sett sér siða- og hátternisreglur

Lögin gera ráð fyrir því að fyrirtæki og stofnanir geti sett sér siða- eða hátternisreglur innan hverrar starfstéttar, þar sem fjallað verði um góða og viðurkennda starfshætti með tilliti til meðferðar persónuupplýsinga. Tilgangur með slíkum reglum er að skýra betur hvernig vinna eigi eftir lögunum og fækka vafaatriðum. Ákveði einstaka starfstéttir, t.d. skólar eða velferðarþjónustuaðilar, að setja sér slíkar reglur þá þarf að afla staðfestingar á reglunum hjá Persónuvernd.

Sjá nánar 41. – 42. gr. reglugerða

12. Tilkynningar og viðbrögð vegna öryggisbrota

Öryggisbrot við meðferð persónuupplýsinga eru samkvæmt reglugerð brot á öryggi sem leiða til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi. Þau nýmæli er nú að finna í reglugerðinni að skylt verður að tilkynna til Persónuverndar um öryggisbresti *innan 72 klst.* Að sama skapi falla úr gildi reglur um tilkynningarskylda vinnslu sem í gildi eru í dag. Í ljósi þess skamma tímafrests sem gefinn er til að tilkynna um brot er mikilvægt að fyrir hendi séu skýrir verkferlar um tilkynningu öryggisbrota. Ávallt skal tilkynna öryggisbrot til Persónuverndar. Þá getur einnig þurft að tilkynna hinum skráðu sjálfum um að öryggisbrot hafi átt sér stað. Þó geta verið ákveðnar undantekningar á því, s.s. ef ljóst þykir að brot feli ekki í sér hættu á að brjóta gegn réttindum skráðra einstaklinga.

Eins og áður segir skulu alltaf sendar tilkynningar til Persónuverndar og innan 72 tíma. Ef ekki næst að tilkynna innan tímamarka skal tilgreina ástæður þessa.

Í tilkynningu til Persónuverndar skal koma fram:

a) lýsing á eðli öryggisbrots við meðferð persónuupplýsinga, þ.m.t., ef hægt er, þeim flokkum og áætluðum fjölda skráðra einstaklinga sem það varðar og flokkum og áætluðum fjölda skráninga persónuupplýsinga sem um er að ræða,

b) Nafn og samskiptaupplýsingar persónuverndarfulltrúa þar sem hægt er að fá frekari upplýsingar,

c) lýsing á sennilegum afleiðingum öryggisbrots við meðferð persónuupplýsinga,

d) lýsing á þeim ráðstöfunum sem gripið hefur verið til eða fyrirhugað er að gera vegna öryggisbrots við meðferð persónuupplýsinga, þ.m.t. ráðstöfunum til að milda hugsanleg skaðleg áhrif þess

Ef líklegt er að öryggisbrot við meðferð persónuupplýsinga leiði af sér mikla hættu fyrir réttindi og frelsi einstaklinga skal skráðum einstaklingum tilkynnt um eðli öryggisbrots á skýru og einföldu máli og til hvaða ráðstafana hafi verið gripið í þeim tilgangi.

Ekki þarf að tilkynna um brot til skráðra einstaklinga ef:

a) Gripið hefur verið til viðeigandi tæknilegra og skipulagslegrar verndarráðstafana og upplýsingar gerðar ólæsilegar þeim sem ekki hefur aðgangsheimild, s.s. með dulkóðun.
b) Gripið hefur verið til ráðstafana og ólíklegt er að hætta skapist aftur
c) Ef tilkynning hefur í för með sér óhóflega fyrirhöfn, þá má birta almenna tilkynningu eða grípa til sambærilegra ráðstafana.

Sjá nánar 33. – 34. gr. reglugerðar

13. Afleiðingar brota

Samkvæmt reglugerðinni mun Persónuvernd fá heimild til að leggja á stjórnsýslusektir vegna brota á nýjum lögum. Skulu sektir vera í réttu hlutfalli við brot og hafa varnaðaráhrif. Er því afar mikilvægt að sveitarfélög vinni heimavinnu sína á grundvelli nýrra laga og gangi úr skugga um að öll vinnsla persónuupplýsinga sé í samræmi við ákvæði reglugerðarinnar. Í því felst m.a. að ganga úr skugga um að fullnægjandi lagagrundvöllur sé fyrir vinnslunni (6.-9. gr.), farið sé að meginreglum (5. gr.), réttindi hinna skráðu séu tryggð (III. kafli) og að viðkomandi sveitarfélag hafi uppfyllt allar þær skyldur sem á það eru lagðar, s.s. um gerð vinnsluskráa, tilnefningu persónuverndarfulltrúa, gripið til öryggisráðstafana o.s.frv. Þá þarf viðkomandi sveitarfélag að geta sýnt með gögnum fram á reglufylgni, sbr. 2. mgr. 5. gr. reglugerðarinnar. Er þetta ekki síst mikilvægt í ljósi þeirra sektarheimilda sem Persónuvernd mun fá þegar reglugerðin kemur til framkvæmda. Samkvæmt reglugerðinni er heimild til að sekta lögaðila eftirfarandi: fyrir vægari brot, eins og þau eru skilgreind í í 4. mgr. 83. gr. reglugerðarinnar, munu stjórnsýslusektir geta numið allt að 2% af heildarveltu eða 10 milljónir evra á heimsvísu, hvort sem er hærra. Fyrir alvarlegri brot, eins og þau eru skilgreind í 5. mgr. sömu greinar, munu stjórnsýslusektir geta numið allt að 4% af heildarveltu á heimsvísu eða 20 milljónir evra, hvort sem er hærra. Ekki liggur fyrir hvort Persónuvernd muni hafa sömu sektarheimildir gagnvart sveitarfélögum, en það er í höndum löggjafans að ákveða við innleiðingu. Vert er þó að geta þess að ef sveitarfélög hafa gert allt sem í sínu valdi stendur til að innleiða ný lög og öryggisráðstafanir þá er líklegt að eingöngu verði beitt áminningu a.m.k. fyrst um sinn svo framarlega sem brotið var óhapp og í fyrsta sinn, en Persónuvernd hefur lagt ríka áherslu að sveitarfélög hugi að meðalhófsreglu sbr. 5. gr. reglugerðarinnar og safni ekki upplýsingum sem ekki verða notaðar og hefji vinnu við innleiðingu.

Þrátt fyrir óvissu með sektir sem hægt verður að leggja á sveitarfélög er ljóst að um umtalsverðar fjárhæðir verður að ræða. Sambandið bendir sérstaklega á að þar sem um er að ræða stjórnvaldssekt þá þarf Persónuvernd ekki að sýna fram á ásetning eða sanna tjón, heldur einungis að líta til þeirra viðmiða sem nýju lögin kveða á um.

Sjá nánar 83. gr. reglugerðar

Auk stjórnsýslusekta þá geta sveitarfélög líka orðið skaðabótaskyld gagnvart einstaklingum sem hafa orðið fyrir eignatjóni eða óefnislegu tjóni vegna brots á ákvæðum nýrra laga.

Sjá nánar 82. gr. reglugerðar

14. Mögulegir samstarfsfletir hjá sveitarfélögum við innleiðingu

Sambandið bendir á að þar sem þær persónuverndarupplýsingar sem sveitarfélög vinna með og lögbundin þjónusta þeirra er sú sama er mikið tækifæri fyri r sveitarfélög að vinna saman að innleiðingu á nýjum lögum. Við vinnslu þessara leiðbeininga hefur sambandið rekist á eftirfarandi þætti sem sveitarfélög gætu haft hag á að vinna saman við en ekki er um endanlega talningu að ræða:

1. Vinna við vinnsluskrá – hér væri ákjósanlegt að sveitarfélög skiptust á upplýsingum um hvernig þau muni uppfylla lagaskyldu. Á að gera samning við hugbúnaðaraðila um forrit til að vinna í eða útbúa eigin forrit?
2. Öryggisstefna, vinna við áhættumat og öryggismál almennt – sambandið telur afar gagnlegt ef þeir sem hafa öryggis og tölvumál á sinni könnu hjá sveitarfélögum hafi samvinnu og skiptist á upplýsingum.
3. Setning verklagsreglna og persónuverndarstefnu – þessi skjöl geta verið eins í sveitarfélögum.
4. Hvernig á að bregðast við upplýsingabeiðni einstaklinga – útbúa ferla og form.
5. Vinna staðlaðra skjala – hér mætti nefna vinnslusamninga, samþykkiseyðublöð, trúnaðaryfirlýsingar o.s.frv. Sambandið mun jafnframt skoða að vinna einhver slík skjöl fyrir sveitarfélög.
6. Setning siðareglna – telji sveitarfélög heppilegt að setja siðareglur á ákveðnum sviðum þjónustu þá væri samstarf æskilegt. Sambandið minnir á að ef samdar eru siðareglur þá þarf að tilkynna um þær til Persónuverndar.

15. Frekari upplýsingar

Auk síðna sem vísað er til í fótnótum í leiðbeiningum þessum bendir sambandið á:

Á heimasíðu Persónuverndar er að finna hjálplegar upplýsingar og ítarefni, m.a. drög að þýðingu á reglugerðinni, yfirlitsbæklinga og slóðir á leiðbeiningar, þar er t.d. að finna öll álit vinnuhóps 29 o.fl.:

https://www.personuvernd.is/ny-personuverndarloggjof-2018/

http://www.eugdpr.org/ - Heimasíða reglugerðarinnar. Hér má finna finna svör við algengum spurningum, hverjar eru lykilbreytingar ofl.:

Samræmdar leiðbeiningar um einstök efnisatriði reglugerðar ESB nr. 2016/679 (GDPR) 29. gr. hópsins:

www.ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

En þetta eru eftirfarandi leiðbeiningar:

- Flutningsréttur (e. Data portability)
- Persónuverndarfulltrúi (e. Data Protection Officers)
- Samvinna persónuverndarstofnanna og tilnefningu forystueftirlitsyfirvalds (e. Identifying a controller or processor's lead supervisory authority)
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, wp248
- Tilkynningar um öryggisbrot (e. Personal Data Breach Notification) (til umsagnar)
- Sjálfvirk ákvarðanataka og gerð persónusniða (e. Automated individual decision-marking and profiling) (til umsagnar)

Persónuvernd Norðmanna er líka með mjög gott efni á sinni síðu, sjá: www.datatilsynet.no

Persónuvernd í Bretlandi:https://ico.org.uk/

http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/