Febrúar 2018

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 25. maí 2018 á grundvelli skuldbindinga Íslands skv. EES-samningnum. Þá er stefnt að því að ný persónuverndarlöggjöf taki gildi á sama tíma hér á landi, sem mun úfæra tiltekin ákvæði reglugerðarinnar sem bjóða upp á sveigjanleika fyrir aðildarríki á EES-svæðinu. Drög að frumvarpi til nýrra persónuverndarlaga, án greinargerðar og skýringa með ákvæðum frumvarpsins, hafa verið kynnt hagsmunaaðilum. Í frumvarpinu er að finna helstu ákvæði reglugerðarinnar auk þess sem tekin er afstaða til atriða þar sem sveigjanleiki er fyrir hendi. Í frumvarpinu kemur skýrt fram að reglugerðin gildir að öðru leyti fullum fetum á Íslandi. Persónuvernd hefur, með leyfi Þýðingarmiðstöðvar utanríkisráðuneytisins, birt drög að þýðingu á reglugerðinni á heimasíðu sinni[1] og er ekki líklegt að þau drög taki miklum breytingum.

Þegar þessi útgáfa af leiðbeiningum er samin eru þrír mánuðir þar til að stefnt er að gildistöku laganna án þess að fullbúið frumvarp liggi fyrir. Því hefur Samband íslenskra sveitarfélaga tekið saman helstu atriði sem geta haft áhrif á rekstur sveitarfélaga og stofnana þeirra (hér eftir nefnd einu nafni “sveitarfélög”) í þeim tilgangi að aðstoða þau við undirbúning vegna nýrrar lagasetningar enda tíminn til stefnu afar knappur. Er þetta þriðja útgáfa af leiðbeiningunum sem hafa verið uppfærðar eftir því sem efni hafa verið til og hefur þessi útgáfa að geyma ítarlegri skýringar á grundvelli leiðbeininga sem gefnar voru út af vinnuhópi 29. gr.[2]

Ný persónuverndarlöggjöf mun leggja ríkari kröfur á sveitarfélögin að því er varðar m.a. vinnslu persónuupplýsinga, að hve miklu leyti og á hvaða formi þær eru geymdar. Þá munu nýju lögin veita einstaklingum meiri réttindi en gildandi löggjöf auk þess sem þau innhalda sektarákvæði sem beita má ef sveitarfélög gerast sek um öryggisbrot á persónuverndarupplýsingum. Rétt er að geta þess að frumvarpsdrögin gera ekki greinarmun á einkaaðilum og opinberum aðilum. Af því leiðir að Persónuvernd hefur heimild til þess að leggja sektir á sveitarfélög og geta sektarfjárhæðirnar verið allt frá 100 þúsund krónum yfir í 22 milljarða króna í alvarlegustu tilfellum. Að áliti sambandsins er hér um afar íþyngjandi

[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

ákvæði að ræða gagnvart sveitarfélögunum enda leggur reglugerðin það í hendur aðildarríkja að ákveða hvort heimila eigi að leggja sektir á opinbera aðila og að hve miklu leyti.

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, þó mun algengara sé að þau séu í hlutverki ábyrgðaraðila, en mikilvægt er 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. Mikil ábyrgð hvílir á ábyrgðaraðila sbr. ábyrgðarreglu sem fjallað er um í næsta kafla.

Dæmi: *Sveitarfélag er ábyrgðaraðili að vinnslu upplýsinga um sitt eigið starfsfólk. Eins er það ábyrgðaraðili þegar skráðar eru upplýsingar í velferðarþjónustu um notendur eða nemendur í grunn- og leikskólum*.

Á samstarfsvettvangi sveitarfélaga, í gegnum byggðarsamlög og önnur samvinnuverkefni sveitarfélaga geta fleiri en eitt sveitarfélag talist vera ábyrgðaraðilar.

Vinnsluaðili: er sá sem vinnur persónuupplýsingar á vegum ábyrgðaraðila og þarf að fara að fyrirmælum ábyrgðaraðila varðandi vinnslu.

Dæmi: *Sveitarfélög og stofnanir þeirra eins og byggðarsamlög gætu talist vera vinnsluaðilar í skilningi laganna ef þau eða stofnanir þeirra taka að sér ákveðna þjónustu fyrir hönd t.d. annars sveitarfélags sem felur í sér vinnslu persónuupplýsinga. Hér gæti verið um að ræða þjónusta á velferðarsviði þar sem sveitarfélag sem óskar eftir þjónustu sendir upplýsingar áfram til sveitarfélags sem veitir þjónustu.*

Samkvæmt nýju lögunum geta bæði ábyrgðaraðili og vinnsluaðili borið ábyrgð en ábyrgðarskyldan er samt að meginstefnu á ábyrgðaraðila.

Meginreglan 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 fellur undir þessa skilgreiningu. Það að vista gögn í skjalaskáp eða að eyða gögnum telst þannig til vinnslu í skilningi laganna.

Dæmi um algenga vinnslu hjá sveitarfélögum eru: launagreiðslur, færslur í kerfi eins og Mentor og Námsfús, allt sem vistað er í kerfum eins og One, og öll móttaka gagna á öllum sviðum, t.d. í félagsþjónustu eða í tengslum við umsókn um byggingarleyfi.

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. Geta upplýsingar þannig verið persónugreinanlegar með óbeinum hætti, svo sem ef þær vísa til húsvarðar hjá grunnskóla í ákveðnu sveitarfélagi og í því sveitarfélag er einungis einn grunnskóli og húsvörður og þar með ljóst um hvern ræðir.

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 óheimilt að vinna með persónuupplýsingar er varða **kynþátt** eða **þjóðernislegan uppruna**, **stjórnmálaskoðanir**, **trúarbrögð** eða **heimspekilega sannfæringu** eða **aðild að verkalýðsfélagi**. Enn fremur er óheimilt að vinna **erfðafræðilegar upplýsingar** og **lífkennaupplýsingar** í því skyni að persónugreina einstakling með einkvæmum hætti, sem og **heilsufarsupplýsingar** eða **upplýsingar er varða kynlíf** einstaklings eða **kynhneigð**. Afar ströng skilyrði þarf að uppfylla svo vinnsla sé heimil eins og skýr lagaheimild, ótvírætt samþykki eða vinnslan sé liður í lögmætri starfsemi stofnunar eins og t.d. starfsemi félagsþjónustu og greiningarstöðva þegar um heilsufarsupplýsingar og greiningar er að ræða.

Sveitarfélög vinna með mikið af viðkvæmum persónuupplýsingum.

Dæmi um viðkvæmar persónuupplýsingar*: stéttarfélagsupplýsingar um starfsmenn, heilsufarsupplýsingar í félagsþjónustu, leik- og grunnskólum. Vegna þessa er afar mikilvægt að þau geri sér grein fyrir þeim miklu takmörkunum sem eru á vinnslu viðkvæmra persónuupplýsinga. Í ákvörðun persónuverndar nr. 1203/2015 í svokölluðu Mentor máli lagði Persónuvernd bann við því að viðkvæmar persónuupplýsingar væru vistaðar inn í Mentor nema að útbúið yrði sérstakt umhverfi fyrir slíkar upplýsingar sem myndi tryggja öryggi þeirra.*

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 allrar söfnunar upplýsingar og sérstaklega ef upplýsingar eru þess eðlis að ljóst er að gæta beri ítrustu varúðar, t.d. upplýsingar um forsjá barns, fjárhagsupplýsingar o.þ.h.. 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 fyrir vinnslunni en einstaklingi er aldrei skylt að veita slíkt samþykki.

Samþykki skráðs einstaklings: er 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 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. Þetta þýðir þó ekki að samþykki verði að vera skriflegt og verður áfram hægt að óska eftir samþykki í gegnum netið, t.d. til þess að fá að birta myndir af börnum á vefsíðum leik- og grunnskóla, en þá er krafan sú að ósk um samþykki komi fram á skýran hátt þannig að ljóst sé hvað er verið að samþykkja.

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.

Dæmi um öryggisbrot: *ef trúnaðarupplýsingar úr tölvukerfum grunnskóla yrðu aðgengilegar öllum við tæknilega yfirfærslu.*

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. **Lögmætisreglan**: Að unnið sé úr upplýsingum á sanngjarnan, lögmætan og gagnsæjan hátt
2. **Tilgangsreglan:** Að upplýsingum sé einungis safnað í skýrum og lögmætum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi
3. **Meðalhóf/lágmörkun gagna**: Að upplýsingar séu nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilgang (takmörkun gagna)
4. **Áreiðanleikareglan**: Að upplýsingarnar séu áreiðanlegar og uppfærðar eftir þörfum (áreiðanleiki)
5. **Varðveislureglan:** 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. **Öryggisreglan**: 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. **Ábyrgðarreglan:** Ábyrgðaraðili er ábyrgur fyrir því að farið sé að meginreglunum og hann þarf að geta sýnt fram á það. Það getur hann gert m.a. með því að leggja fram gögn sem staðfesti hvernig meginreglunum sé fylgt.

Sambandið bendir á að öryggis- og ábyrgðarreglan eru nýmæli. Leggur ábyrgðarskyldan afar ríkar skyldur á ábyrgðaraðila þar sem hann þarf ekki einungis að fara eftir öllum meginreglum, heldur þarf hann líka að sýna fram á að hann hafi gert það. Fjallað er ítarlegar um ábyrgðarskyldu í kafla 4.

Sjá nánar 5. gr. reglugerðarinnar

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

Sambandið hvetur þau sveitarfélög sem ekki hafa hafið undirbúning að gera það hið fyrsta enda innleiðing nýrra laga umfangsmikið verkefni og mikil ábyrgð lögð á sveitarfélög með lögunum. 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 heppilegt verklag er 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, tæknifulltrúi, skjalavörður (héraðsskjalavörður eða skjalavörður sveitarfélags) mannauðsstjóri og fulltrúi yfirstjórnar.

Þá er mikilvægt í upphafi að sveitarfélög/teymi skoði hvað sé nú þegar fyrir hendi hjá þeim, t.d. hvort til staðar séu gæðakerfi, öryggisstefnur og hvort áhættumat á vinnslu upplýsinga hefur verið framkvæmt. 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 fyrrnefnt Mentor mál er góð fyrirmynd þegar semja á við vinnsluaðila.

Sambandið telur raunhæft við innleiðingu að miða við áætlun sem sett er fram í skjalinu *Persónuvernd skref fyrir skref* sem nálgast má hér:

http://www.samband.is/media/personuvernd/Personuvernd-skref-fyrir-skref.pdf

Sambandið bendir á afar hjálplega fyrirlestra frá Vigdísu Evu Líndal frá Persónuvernd og Herði Helga Helgasyni lögmanni hjá Landslögum af Persónuverndardegi sambandsins 1. des. 2017, sjá:

http://www.samband.is/um-okkur/fundir-og-radstefnur/personuverndardagur og

12 skrefa áætlun um undirbúning fyrir GDPR frá bresku persónuverndarsamtökunum:

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

4. Nýjar skyldur sveitarfélaga - ábyrgðarskylda og upplýsingaskylda

Með nýrri löggjöf takast sveitarfélög á hendur nýjar og mun strangari skuldbindingar en þau gera samkvæmt gildandi lögum. Auknar kröfur eru nú gerðar til ábyrgðaraðila að sýna 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 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. Þarf ábyrgðaraðili að sýna fram á framangreint. Ábyrgðaraðili getur sýnt fram á eftirfylgni t.a.m. með því að skjalfesta stefnu og verklagsreglur um einstaka skyldur, vera með samþykktar hátternisreglur, sýna fram á vottun og skipun persónuverndarfulltrúa. Í tilviki sveitarfélaga getur m.a. verið um að ræða persónuverndar- og upplýsingaöryggisstefnu, ferla sem byggja á vinnsluskrám, reglur um meðferð gagna og notkun tölva og síma. Í ábyrgðarskyldu felst jafnframt samvinna við persónuverndaryfirvöld samkvæmt beiðni. Þessi skylda er hins vegar ný og mun skýrast betur á næstu misserum, þ.e. hvernig best er að framfylgja henni.

Sambandið bendir sérstaklega á að þegar sveitarfélög eru ábyrgðaraðilar að vinnslu persónuupplýsinga þá bera þau ábyrgð á því að allir starfsmenn þekki reglurnar og starfi eftir þeim. Verði öryggisbrot vegna

meðferðar persónuupplýsinga hjá sveitarfélögum þá getur það leitt til þess að þau verði sektuð og að til skaðabótaskyldu geti stofnast 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 ríku 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 ætlaðar eru börnum. Ekki liggja fyrir leiðbeiningar um hversu langt ábyrgðaraðilar þurfa að ganga við að leita að upplýsingum en sennilegt er að miðað verði við góðan og gegnan sérfræðing/sveitarfélag í því sambandi, þ.e. hversu langt myndi sveitarfélag sem er með sín kerfi á hreinu ganga til að sækja þau gögn sem mögulegt er að nálgast.[3] Þetta er hins vegar önnur skylda sem mun skýrast nánar á næstu misserum og ekki ólíklegt að Persónuvernd muni þurfa að skera úr um í einhverjum tilvikum hversu langt þurfi að ganga til að uppfylla skylduna.

Sambandið minnir á að hér þarf eingöngu að afhenda persónugreinanleg gögn þannig að ef gripið er til aðgerða eins og dulkóðunar varðandi til dæmis ákveðin eldri gögn þá eru þau ekki lengur persónugreinanleg.

Sveitarfélögum ber því að auðvelda skráðum einstaklingi að neyta réttar síns, og ekki neita að verða við beiðni nema sýnt sé 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, þ.e. hvernig leit var háttað, 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, t.d. lög um opinber skjalasöfn nr. 77/2014.
3. Hvaða persónupplýsingar eru vistaðar og/eða unnið með.
4. Grundvöllur fyrir vinnslu persónuupplýsinga – lagaákvæði eða samþykki. Ef vinnsla byggir á samþykki skal upplýst um rétt til að draga samþykki til baka.
5. Hver er viðtakandi persónuupplýsinga sem vistaðar/unnar eru, sveitarfélag, eða stofnanir þess eins og grunnskólar.
6. Hversu lengi persónuupplýsingarnar eru geymdar eða, sé það ekki mögulegt, þær viðmiðanir sem notaðar eru til að ákveða hversu lengi þær eru geymdar hér nægir í tilvikum sveitarfélaga að vísa í lög um opinber skjalasöfn.

[3] Sbr. Bonus Pater regla sem stuðst er við einkum í skaðabótarétti.

7. 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.
8. Réttur til að leggja fram kvörtun hjá Persónuvernd.
9. Ef upplýsingar eru fengnar frá öðrum en skráðum einstaklingi, hvaðan þær eru fengnar og hvort þær koma frá opinberum aðilum, t.d. ef kallað er eftir upplýsingum úr þjóðskrá, eða RSK eða öðrum aðilum.
10. 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
11. 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. Þær upplýsingar sem ekki varða einstaklinginn sjálfan, geta verið í stöðluðu formi og nægir þá að vísa til þeirra með skýrum hætti þegar upplýsingabeiðni er afhent.

Sjá nánar 12.-14. gr. reglugerðar

5. Skrár yfir vinnslustarfsemi

Í 5. mgr. 30. gr. reglugerðarinnar er gert ráð fyrir að aðili, þ.m.t. sveitarfélög, þurfi ekki að halda vinnsluskrá ef um er að ræða vinnustað með færri en 250 starfsmenn. Nú er hins vegar gengið út frá því að nánast öll sveitarfélög verði gert skylt að halda vinnsluskrá. Byggir þetta á því að þær takmarkanir sem eru á 250 starfsmanna undanþágunni eru það takmarkandi og verða túlkaðar þannig að í raun er ekki um neina undanþágu að ræða. Persónuvernd hefur sjálf lýst því yfir að skylda til að halda vinnsluskrá hvíli á öllum sveitarfélögum, nema ef vinnslan leiðir ekki af sér áhættu fyrir réttindi og frelsi skráðra einstaklinga og hún er tilfallandi (þ.e. ekki regluleg). Öll sveitarfélög og stofnanir þeirra sem vinna reglubundið með persónuupplýsingar verður því skylt að útbúa slíka skrá.

Um vinnsluskrár og það sem þar þarf að koma fram er fjallað um í 30. gr. reglugerðarinnar. Vakin er athygli á því að í mörgun liðum er talað um upplýsingar „ef við á“ og „ef mögulegt er“ og hefur í samtölum við Persónuvernd komið fram að vinnsluskráin þarf ekki að vera eins ítarleg og greinin gefur til kynna.

Helstu upplýsingar sem þurfa að koma fram í vinnsluskrá eru eftirfarandi:

- Heiti og samskiptaupplýsingar ábyrgðaraðila og persónuverndarfulltrúa
- Tilgangur vinnslunnar (t.d. veiting þjónustu, ráðning starfsmanns)
- Lýsing á flokkum skráðra einstaklinga (t.d. einstaklingur eða starfsmaður) og persónuupplýsinga (t.d. heilsufarsupplýsingar og starfsferilsskrá)
- Hverjir munu fá upplýsingarnar (t.d. starfsmenn sem fara með mál og mannauðsdeild)
- Lýsing á vinnslu/verkferli, oft talað hér um hjarta vinnsluskrárinnar þar sem lýst er því ferli sem fer í gang við vinnslu eins og ráðningu starfsmanns.

- Fyrirhuguð tímamörk fyrir eyðingu, eða lagaskylda til að geyma – Fyrir sveitarfélög mun í flestum tilvikum nægja að vísa í lög um opinber skjalasöfn nr. 77/2014.

Með vinnsluskrá er átt við skrá yfir allar <u>tegundir vinnslu</u> sem unnar eru hjá hverju sveitarfélagi. Ekki er um að ræða málaskrá þar sem hvert mál sem er unnið er skráð, heldur nægir að sveitarfélög eigi skráningu um allar tegundir vinnslu.

Mikilvægt er að áður en sveitarfélög hefjast handa við gerð vinnsluskráa að notkunargildi hennar sé ákveðin. Á hún t.d. að vera kjarni í gæðakerfi? Ef svo er þá er gott að hafa tengingu í gæðakerfi í henni. Á hún á vera stjórntæki fyrir áhættumat? Þá þarf að útbúa hana með þann möguleika. Eða á eingöngu að vera um lýsingu á verkferlum að vera? Ef svo er þá ætti viðmiðið að vera að hafa skrána eins einfalda og hægt er og miða við upplýsingar hér að framan.

Þegar vinna er hafin við greiningu á ferlum fyrir vinnsluskrá þurfa sveitarfélög að skoða hvaða upplýsingar er unnið með og greina hvernig er unnið skuli með þær.

Í samtölum sambandsins við sérfræðinga á þessu sviði hefur verið bent á að skynsamlegt sé að byrja vinnsluskrá á launakerfi og starfsmannamálum hjá sveitarfélögum. Byggir það á því að þar er vinnsla nánast alls staðar eins og felur m.a. í sér eftirtaldar vinnslur:

1. Starfsumsókn
2. Ráðningarferli I
3. Launaákvörðun
4. Aðgangur starfsmanns að upplýsingum og kerfum
5. Útgreiðsla launa
6. Orlofsmál
7. Starfsmannaviðtöl
8. Launaviðtöl
9. Áminning
10. Veikindaleyfi
11. Eineltismál og kynbundið áreiti
12. Starfslok
13. Meðferð upplýsinga eftir starfslok

Í vinnsluskrá fyrir launakerfi og starfsmannamál þarf að búa til skrá með þessum framangreindu tegundum vinnslu og öðrum vinnslum sem mögulega eru fyrir hendi.

Við gerð vinnsluskrár er mikilvægt að unnið sé með þeirri deild eða því sviði sem mun útbúa vinnsluskrá og að gott samráð og flæði upplýsinga eigi sér stað með þeim starfsmönnum sem þar starfa til að þeir geri sér grein fyrir hvaða vinnslur eiga sér stað. Í tilviki launagreiðslna og starfsmannamála yrði því vinnan unnin í samstarfi við starfsmenn þeirra deilda. Er vinnsluskrá síðan útbúin á grundvelli þeirrar vinnu. Sérfræðingar hafa bent á að við þessa greiningu hafi það verið árangursríkast að þessi vinna sé unnin á fundum þar sem unnið er úr fyrir fram útgefnum spurningalistum.

Þegar vinnu við vinnsluskrá hjá einni deild er lokið, er hægt að fara yfir á annað svið hjá sveitarfélögum, t.d. þjónustusvið hvers sveitarfélags, sem síðan skiptist niður í frekari svið eins og: félagsþjónustu, skipulags- og byggingaleyfa og framkvæmda og aðra þjónustu. Er mikilvægt þegar um margskonar þjónustu er að ræða að vinna vinnsluskrá fyrir hvert svið. Að því loknu væri rökrétt að fara yfir á fræðsluvið hvers

sveitarfélags en heppilegast hefur verið talið að enda á UT deild þar sem hún er til staðar, þar sem flestar vinnslur þar eru í raun afgreiðsla á vinnslum frá öðrum deildum.

Bendir sambandið á að hluti sveitarfélaga eru langt komin með slíka vinnu og því afar gagnlegt ef þau sveitarfélög eru reiðubúin að deila reynslu sinni með þeim sem skemmra eru komin, enda vinnsla þeirra oft eins eða a.m.k. sambærileg.

Hér að neðan er finna dæmi um hvernig vinnsluskrá getur litið út. Þetta er þó ekki hið eina sanna form vinnsluskráa enda fer það eftir því í hvaða tilgangi á að nota vinnsluskrá hversu flókin hún er.

Hefur Reykjavíkurborg jafnframt útbúið einfalda gerð af vinnsluskrá sem dæmi um hvernig slík skrá getur litið út og verður hún send á pósthóp um persónuvernd og verður jafnframt hægt að nálgast hana á heimasíðu Sambands íslenskra sveitarfélaga.

	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. Rétt er þó að geta þess að mörg þessara réttinda gilda aðeins að takmörkuðu leyti um sveitarélögin þar sem vinnsla þeirra byggir á lagaheimild í flestum tilvikum. Mikilvægt er þó að átta sig á réttindum þar sem brot getur valdið því að Persónuvernd beiti sektum eða kveður á um önnur þvingunarúrræði samkvæmt lögunum.

Sambandið mælir með því að útbúin séu form varðandi þessi réttindi, t.d. samþykkiseyðublað, ósk um upplýsingar o.fl. og að unnið sé að samræmingu eyðublaðaforma innan lögfræðingahóps um persónuvernd.

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.

Sambandið bendir á að þessi réttur er háður takmörkunum þegar um er að ræða lagaskyldu til að varðveita upplýsingar t.d. á grundvelli laga um opinber skjalasöfn og mun að öllum líkindum ekki gilda um sveitarfélög að nokkru leyti. Sambandið bendir á að ef koma upp álitamál í þessu sambandi þá er rétt að leita til héraðsskjalavarða og persónuverndar um það.

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

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. Sveitarfélög munu hins vegar áfram flytja ákveðin gögn á milli sín við veitingu þjónustu þó sá flutningur falli ekki undir lög um persónuvernd

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. Ekki er nauðsynlegt að um skriflega yfirlýsingu sé að ræða en 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, sem geta þó verið rafræn svo framarlega sem þau uppylla skilyrði að ofan. Væri t.d. stutter texti þar sem fram kæmi að foreldri samþykkti með haki að það veitt leikskóla heimild til að birta myndir af börnum á heimasíðu skóla eða svæði á facebook fullnægjandi, enda skýrt hvað væri verið að samþykkja og ekki krafa um samþykki.

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.

Að því er varðar sveitarfélög þá felst þessi lagaskylda í því að kynna réttindi til barna á skýran og einfaldan hátt.

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, væri það þó **einungis í þeim tilvikum þar sem vinnsla persónuupplýsinga er umfram lagaheimildir.**

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.

Þessi skylda gildir að mjög takmörkuðu leyti um sveitarfélög og getur einstaklingur ekki andmælt vinnslu sem byggir á lagaheimild.

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 vinnsla viðkvæmra persónuupplýsinga, t.d. við heilbrigðisþjónstu, eða

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

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,

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.

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

Hér þarf að ganga úr skugga um að mat á áhrifum fari ávallt fram við framangreindar aðstæður, þar sem skoðað er sérstaklega hver sé 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 áfram á 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

Ef niðurstaða mats á áhrifum gefur til kynna að vinnslan mun hafa í för með sér mikla áhættu, 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

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

Samkvæmt nýju löggjöfinni skal nýr hugbúnaður og nýtt upplýsingakerfi útfært með sérstaka áherslu á friðhelgi einkalífsins. Þannig skuli lágmarka gagnasöfnun og velja kerfi sem felur í sér sem minnsta áhættu og safni eins litlum persónuupplýsingum og hægt er. Þá þurfipersónuvernd að vera 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 ferlar 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 skoðahver er grundvöllur vinnslunnar, þ.e. byggir hún á lagaheimild eða samþykki og hvaða takmörkunum er hún háð

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

vegna þessa. Þarf að huga að þessu sérstaklega við fræðslu til starfsmanna, einkum þá sem starfa að tæknimálum.

Heimilt verður að nota samþykkt vottunarfyrirkomulag, sbr. 42. gr. reglugerðar, til að sýna fram á að þessar kröfur séu uppfylltar. Frumvarpsdrögin gera ráð fyrir slíku vottunarfyrirkomulagi og að því verði komið á í gegnum Einkaleyfastofu. Hagsmunaaðilar hafa þó gert verulegar athugasemdir við kerfið þar sem þeir telja einkaleyfastofu ekki í stakk búna að sinna hlutverki í lögunum. Vottunarkerfi er hins vegar mikilvægt sveitarfélögunum til að semja 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. reglugerðarinnar.

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 viðkomandi persónuverndarfulltrúa.

Sambandið bendir á að persónuverndarfulltrúa er heimilt að gegna öðrum störfum hjá viðkomandi 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 öðlist mikla þjálfun og miðli þekkingu til annarra starfmanna. Sveitarfélag ber þó að 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 lög og að hann komi með viðeigandi hætti og tímanlega að öllum málum sem tengjast vernd persónuupplýsinga.

Persónuverndarfulltrúi skal vera óháður í störfum sínum og ekki taka við skipunum yfirmanns varðandi framkvæmd verkefna sinna skv. 39. gr. Persónuverndarfulltrúi heyrir beint undir æðsta stjórnunarstig hjá ábyrgðaraðila eða vinnsluaðila. Óheimilt er að víkja persónuverndarfulltrúa 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.

Sveitarfélögum er heimilt að útvista verkefnum persónuverndarfulltrúa. Sé það gert er hins vegar mikilvægt að undirstrika að ekki er unnt að útvista ábyrgð og ber sveitarfélag því ábyrgð ef persónuverndarfulltrúi sinnir ekki skyldum sínum.

Sjá leiðbeiningar frá Persónuvernd um persónuverndarfulltrúa:

https://www.personuvernd.is/media/leidbeiningar-personuverndar/Leidbeiningar-um-personuverndarfulltrua_16_2.pdf

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 heilsufarsupplýsingar eru vistaðar. Meginreglan er þó áfram sú að sveitarfélög eru ábyrgðaraðilar við veitingu þjónustu. Vinnsluaðilar eru þó almennt séð fyrirtæki á sviði upplýsingatækniþjónustu, en geta líka verið einstaklingar sem sinna afmörkuðum verkefnum fyrir sveitarfélög. Sem dæmi mætti 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 ábyrgðaraðila þegar öryggisbrot verður.

Helstu skyldur vinnsluaðila verða eftirfarandi:

1. Vinna eingöngu með persónuupplýsingar samkvæmt skjalfestum fyrirmælum ábyrgðaraðila. 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 gera 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 notið 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. Hér er rétt að nefna að hugbúnaðarfélög hafa þó almennt lýst því yfir að ómögulegt sé að tryggja að eyðing eigi sér stað í öllum afritum. Koma mun betur í ljós hvaða kröfur verða hér gerðar og hvað er framkvæmanlegt í þeim efnum á næstu misserum.
9. Veita ábyrgðaraðila aðgang að öllum upplýsingum, 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 leiðbeiningar frá Persónuvernd um vinnsluaðila:

https://www.personuvernd.is/media/leidbeiningar-personuverndar/Leidbeiningar-fyrir-vinnsluadila_16.2.2018.pdf

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.

Dæmi um öryggisbrot: *má nefna ef trúnaðargögn úr grunnskóla eða félagsþjónustu yrðu gerð öllum aðgengileg fyrir mistök eða t.d. við flutning á milli tölvukerfa.*

Líkt og að framan greinir, skal alltaf sendar tilkynningar til Persónuverndar og innan 72 tíma. Ef ekki næst að tilkynna innan tímamarka skal tilgreina ástæður þess.

Í tilkynningu til Persónuverndar skal koma fram:

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

b) nafn og samskiptaupplýsingar persónuverndarfulltrúa,

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 öryggisbrotsins, þ.m.t. ráðstafanirtil 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 annarra sambærilegra ráðstafana.

Sjá leiðbeiningar Persónuverndar vegna öryggisbrota:

https://www.personuvernd.is/media/leidbeiningar-personuverndar/Leidbeiningar-um-oryggisbrot_16.2.2018_3.pdf

Sjá nánar 33. – 34. gr. reglugerðar

13. Afleiðingar brota

Samkvæmt reglugerðinni og drögum að frumvarpi 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, að gripið sé til öryggisráðstafana o.s.frv. Þá þarf viðkomandi sveitarfélag að geta sýnt fram á reglufylgni með gögnum, sbr. 2. mgr. 5. gr. reglugerðarinnar. Er þetta ekki síst mikilvægt í ljósi þeirra sektarheimilda sem Persónuvernd mun fá þegar reglugerðin kemur til framkvæmda og ef frumvarp verður samþykkt í núverandi horfi. En samkvæmt því getur Persónuvernd lagt sektir á sveitarfélög sem nema allt frá 100 þúsund krónum yfir í 22 milljarða króna í alvarlegustu tilfellum, eða um 2% af heildarveltu þegar umvægari brot er að ræða eða 4% fyrir alvarlegari brot eftir því hvor upphæðin er hærri.

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 ný löggjöf kveður á um.

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

Sjá nánar 82.-83. 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 fyrir sveitarfélög að vinna saman að innleiðingu á nýjum lögum. Hefur sambandið skipað tvo vinnuhópa í þessu sambandi: lögfræðingahóp um Persónuvernd og UT hóp um persónuvernd sem hafa þegar hafið vinnu á þessu sviði. Jafnframt hafa héraðsskjalaverðir skipað vinnuhóp sem hægt er að leita til við skjalastefnu o.fl. Telur sambandið að sveitarfélög gætu haft hag af því að vinna saman að eftirfarandi atriðum, þó ekki sé um tæmandi talningu að ræða:

1. Gerð og 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 eigið 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

Á heimasíðu Persónuverndar https://www.personuvernd.is/ny-personuverndarloggjof-2018/

er að finna hjálplegar upplýsingar og ítarefni, m.a. drög að þýðingu á reglugerðinni, yfirlitsbæklinga og slóðir á leiðbeiningar. Einnig er þar að finna öll álit vinnuhóps 29 og hefur Persónuvernd nýlega birt þrennar leiðbeiningar:

Leiðbeiningar um persónuverndarfulltrúa

Leiðbeiningar um öryggisbrot

Leiðbeiningar fyrir vinnsluaðila, sjá:

https://www.personuvernd.is/efst-a-baugi/leidbeiningar-personuverndar-um-personuverndarfulltrua

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

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/