Skeiða- og Gnúpverjahreppur

Innri persónuverndarstefna

Efnisyfirlit

1. Almennt

Skeiða- og Gnúpverjahreppur (hér eftir einnig nefnt „sveitarfélagið“) þarf vegna lögbundinna verkefna að vinna með persónuupplýsingar einstaklinga. Með persónuupplýsingum er átt við allar upplýsingar sem hægt er að tengja við einstakling, t.d. nafn, kennitölu, heimilisfang, netfang, símanúmer, fjárhagsupplýsingar, IP tölu o.s.frv. Viðkvæmar persónuupplýsingar eru m.a. upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, trúarbrögð eða lífsskoðun, stéttarfélagsaðild, heilsufarsupplýsingar, kynlíf og kynhneigð, erfðafræðilegar- og lífkennaupplýsingar.

Frekari skilgreining á persónuupplýsingum má m.a. finna hér
https://www.personuvernd.is/fyrirtaeki-og-stjornsysla/spurt-og-svarad/allar-spurningar-og-svor/hvad-eru-personuupplysingar-1

Þær persónuupplýsingar sem Skeiða- og Gnúpverjahreppur hefur undir höndum tengjast ýmist íbúum sveitarfélagsins, starfsmönnum þess eða þriðja aðila sem nauðsynlegt er að eiga samskipti við.

Innri persónuverndarstefna Skeiða- og Gnúpverjahrepps kveður á um hvernig vinnslu persónuupplýsinga skuli háttað, með vinnslu persónuupplýsinga er t.d. átt við söfnun, skráningu, flokkun, notkun, skoðun, varðveisla, eyðing og eyðilegging sbr. lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér eftir nefnd „persónuverndarlög“).

Þessari innri persónuverndarstefnu er einkum ætlað að tryggja:

- að Skeiða- og Gnúpverjahreppur vinni persónuupplýsingar í samræmi við persónuverndarlög og fylgi formlegum verkferlum til að tryggja öryggi þessara upplýsinga;
- að vinnsla persónuupplýsinga, þ.m.t. meðhöndlun þeirra sé gagnsæ;
- að réttindi einstaklinga séu í hvívetna virt í samræmi við persónuverndarlög;
- að koma í veg fyrir möguleg öryggisbrot við vinnslu persónuupplýsinga og lágmarka áhættu sem brot á persónuverndarlögum getur haft í för með sér.

Innri persónuverndarstefna skiptist í þrjá megin kafla, persónuverndarlög, ábyrgð og áhættu og almennar verklagsreglur sem aftur skiptast í nokkra undirkafla.

2. Persónuverndarlög

Persónuverndarlög kveða á um með hvaða hætti sveitarfélagi er heimilt að safna, varðveita og vinna persónuupplýsingar. Persónuverndarlög taka til þessara upplýsinga óháð formi eða skráarsniði þeirra, þ.e. hvort upplýsingarnar eru rafrænar eða á pappír.

Óheimilt er að safna persónuupplýsingum nema heimild standi til þess samkvæmt persónuverndarlögum og þeim lögbundnu skyldum sem hvíla á sveitarfélaginu. Söfnun persónuupplýsinga skal fara fram með sanngjörnum hætti og skal varðveita þær á öruggum stað. Óheimilt er að veita óviðkomandi aðgang að þessum upplýsingum.

Horft er sérstaklega til sex meginreglna sem settar eru fram í 8. gr. persónuverndarlaga um heimildir fyrir vinnslu persónuupplýsinga:

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

6. að þær séu unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt.“

3. Ábyrgð og áhætta

Ábyrgðaraðli, Skeiða- og Gnúpverjahreppur, ber ábyrgð á því að vinnsla persónuupplýsinga uppfylli ávallt meginreglur persónuverndarlöggjafarinnar og skal sveitarfélagið staðfesta það með skjölum og verklagsreglum. Sveitarfélagið getur einnig tilgreint til hvaða ráðstafana skuli grípa t.d. vegna skráningu frávika o.s.frv.

Þær meginreglur sem sveitarfélaginu ber að fylgja eru:

1. Sanngirnisregla – lýtur að réttindum einstaklinga. Ábyrgðaraðli þarf að sýna fram á að einstaklingar hafi fengið fullnægjandi fræðslu þegar við á og að einstaklingur hafi aðgang að sínum persónuupplýsingum.
2. Tilgangsregla – lýtur að vinnslu persónuupplýsinga. Öll vinnsla verður að hafa skýran tilgang.
3. Meðalhófsregla – ekki skal vinna meiri persónuupplýsingar en þörf er á. Skrár yfir vinnslustarfsemi og mat á áhrifum persónuverndar (MÁP) geta nýst við mat á því hvort vinnsla sé nægjanleg eða hvort verið er að safna upplýsingum sem ekki er þörf á að afla.
4. Áreiðanleikaregla – persónuupplýsingar skulu vera réttar. Til að sýna fram á að áreiðanleikareglu hafi verið fylgt er nauðsynlegt að geta vísað til skriflegra verkferla t.d. vegna breytinga á upplýsingum í rafrænum kerfum. Þetta er sérstaklega mikilvægt í ljósi þess að sveitarfélagið er afhendingarskylt á Héraðsskjalasafn Árnesinga og því mikilvægt að skrá réttar upplýsingar.
5. Varðveisluregla – í tilfelli sveitarfélagsins er með óheimilt að ónýta skjöl sbr. lög nr. 77/2014 um opinber skjalasöfn. Skjölum, upplýsingum sem innihalda persónuupplýsingar er ekki eytt.
6. Öryggisreglan – lýtur að því að tryggja öryggi persónuupplýsinga. Ábyrgðaraðili þarf að skjalfesta áhættumat hvað varðar öryggi persónuupplýsinga og ákveða með hvaða hætti brugðist verður við þeim frávikum sem geta komið upp. Í þessu felst einnig mat á áhrifum persónuverndar (MÁP) og skjalfesting á verkferlum vegna tilkynninga um öryggisbrest. Sveitarfélagið skal halda skrá yfir alla öryggisbresti og geta sýnt Persónuvernd skrána, sé þess óskað.

Margir stjórnendur og starfsmenn sveitarfélagsins bera ábyrgð á vinnslu persónuupplýsinga. Ríkari skyldur hvíla á þeim aðilum sem nefndir eru hér fyrir neðan. Þeir aðilar og efni þeirra skyldna eru m.a. eftirfarandi:

- Sveitarstjóri, oddviti og stjórnendur hverrar stofnunar bera ábyrgð á því að sú stofnun/rekstrareining sem þeir veita forstöðu framfylgi persónuverndarlögum.
    - Þetta á einnig við um búnað og aðrar ráðstafanir er tengjast aðgengi að þriðju aðila að skjölum eða gögnum sem innihalda persónuupplýsingar.
    - Stjórnendur meta þá þjónustu sem sveitarfélagið og stofnanir hyggjast nýta sér frá utanaðkomandi þriðja aðila, t.d. hýsing gagna sveitarfélagsins og tengingar við gagnagrunna sem nota þarf vegna ýmissa verkefna.

- Þriðji aðli, t.d. þjónustuaðilar vegna reksturs og umsjón tölvukerfa og gagnakerfa sem sveitarfélagið eða stofnanir þess þurfa að hafa aðgang að til að uppfylla lagaskyldu, bera ábyrgð á:
    - að öll kerfi og þjónusta fullnægi þeim öryggiskröfum sem settar eru fram í persónuverndarlögum;
    - að reglulega séu framkvæmdar úttektir sem eiga að tryggja að hugbúnaður og annar búnaður sem sveitarfélagið nýtir sér sem hlut af þeirri þjónustu sem er keypt standist öryggiskröfur.
- Persónuverndarfulltrúi ber ábyrgð á eftirfarandi:
    - að yfirstjórn sveitarfélagsins og stjórnendur fái reglulega fræðslu um þær skyldur sem hvíla á sveitarfélaginu skv. persónuverndarlögum;
    - að farið sé reglulega yfir stefnur og verkferla sem tengjast vinnslu persónuupplýsinga;
    - veita starfsmönnum sem vinna með persónuupplýsingar fræðslu;
    - að taka á móti og svara spurningum starfsmanna og einstaklinga sem upplýsingarnar varða;
    - aðstoða við að svara beiðnum frá skráðum einstaklingum, s.s. vegna aðgangs að skjölum, mótmæla vinnslu eða réttarins til að gleymast;
    - yfirfara og gera athugasemdir vegna samninga er tengjast vinnslu persónuupplýsinga, s.s. samninga við þriðju aðila vegna vinnslu á persónuupplýsingum fyrir sveitarfélagið;
    - annast samskipti við Persónuvernd.

4. Almennar verklagsreglur vegna vinnslu persónuupplýsinga

Eftirfarandi almennar verklagsreglur um vinnslu persónuupplýsinga gilda hjá sveitarfélaginu og öllum stofnunum þess. Þess utan eru til skjalavistunaráætlanir og formlegir verkferlar sem taka skjalavörslu og vinnslu persónuupplýsinga, t.d. hvernig ákveðnar fyrirspurnir og erindi skulu afgreidd m.t.t. persónuverndarlaga.

- Einungis þeir starfsmenn sem þurfa starfs sín vegna skulu hafa aðgang að persónuupplýsingum.
- Starfsmönnum er með öllu óheimilt að deila persónuupplýsingum sína á milli óformlega.
- Starfsmenn skulu reglulega frá fræðslu um þær skyldur sem á þeim hvíla samkvæmt persónuverndarlögum.
- Starfsmenn skulu ávallt gæta fyllsta öryggis við vinnslu persónuupplýsinga og fylgja bæði almennum verklagsreglum sem hér koma fram auk sértækra verklagsreglna sem settar eru um vinnslu og afgreiðslu persónuupplýsinga.
- Öll lykilorð skulu vera illrekjanleg og þeim má ekki deila með öðrum starfsmönnum eða utanaðkomandi aðilum.
- Starfsmenn skulu aldrei deila persónuupplýsingum með óviðkomandi aðilum, gildir einu hvort um er að ræða annan starfsmann sveitarfélagsins eða utanaðkomandi aðila.
- Endurskoða skal persónuupplýsingar reglulega og tryggja að þær séu réttar.

- Persónuupplýsingum má ekki eyða nema það sé gert í samræmi við lög nr. 77/2014 um opinber skjalasöfn.
- Starfsmenn skulu leita til persónuverndarfulltrúa séu þeir í vafa um hvernig vinnslu/meðhöndlun persónuupplýsinga skulu háttað.

4.1 Geymsla á persónuupplýsingum

Geymsla persónuupplýsinga á pappír

Persónuupplýsingar sem geymdar eru á pappír skulu vera á öruggum stað þar sem óviðkomandi aðili getur ekki nálgast þær.

- Persónuupplýsingar geymdar á pappír skal varðveita í læstum hirslum, skjalaskáp(um) eða skjalageymslu.
- Aðgengi að hirslum og geymslum skal stýrt og ljóst hvaða starfsmenn hafa aðgang.
- Starfsmönnum ber að tryggja að skjöl á pappír sem innihalda persónuupplýsingar séu ekki aðgengilegar óviðkomandi aðilum, s.s. í prentara.
- Starfsmenn skulu í einu og öllu virða þær aðgangstakmarkanir sem settar eru að hálfu sveitarfélagsins vegna vinnslu persónuupplýsinga.
- Eyðing á pappírsskjölum sem innihalda persónuupplýsingar má aðeins eyða í samræmi við þau ákvæði sem koma fram í skjalavistunaráætlunum stofnana og í gildandi lög þar um. Ef heimild er til staðar skal skjölunum eytt með fullnægjandi hætti.

Geymsla á persónuupplýsingum með rafrænum hætti

Persónuupplýsingar sem geymdar eru á rafrænu formi, skráarsniði, skal varðveita með sama hætti og pappírsskjöl, þ.e. aðeins þeir starfsmenn sem þurfa starfs síns vegna að hafa aðgang að persónuupplýsingum fá aðgang. Þess skal gætt að þessum persónuupplýsingum sé ekki eytt fyrir mistök eða vangá.

- Persónuupplýsingar skal vernda með illrekjanlegum lykilorðum. Lykilorðum skulu starfsmenn breyta reglulega og óheimilt er með öllu að deila lykilorðum.
- Persónuupplýsingar skal ekki varðveita á lausum geisladiskum, minnislyklum, hörðum diskum o.s.frv. heldur á miðlægum netþjón. Persónuupplýsingar verða ekki varðveittar á geisladiskum, minnislyklum, utan á liggjandi hörðum diskum.
- Persónuupplýsingar skal einungis varðveita á fyrir fram skilgreindum drifum, netþjónum sem eru með öryggisstýringu.
- Skýjalausnir skal aðeins nota ef þær standast þær kröfur sem persónuverndarlög kveða á um.
- Netþjónar sem innihalda persónuupplýsingar skal staðsetja á öruggum stað m.t.t. gagnaöryggis og aðgangi óviðkomandi aðila að tæknirými.
- Afritun af rafrænum skjölum/gögnum skal vera reglubundin og þá skal kanna reglulega hvort afritun hafi tekist til að tryggja áreiðanleika gagnanna.
- Aldrei skal vista persónuupplýsingar beint á fartölvur eða farsíma starfsmanna eða farsíma í eigu sveitarfélagsins.
- Vernda skal alla netþjóna og tölvur sveitarfélagsins og öll önnur tæki með viðeigandi öryggisbúnaði og eldveggjum til að tryggja öryggi og áreiðanleika gagnanna.

4.2 Vinnsla eða notkun persónuupplýsinga

Við vinnslu og notkun á persónuupplýsingum skulu starfsmenn ávallt fylgja eftirfarandi reglum til að tryggja öryggi og lágmarka áhættu við alla vinnslu persónuupplýsinga, s.s. vegna gagnaleka, deilingar, breytinga, þjófnaðar eða eyðingu upplýsinga:

- Þegar unnið er með persónuupplýsingar skulu starfsmenn ávallt gæta þess að læsa tölvum og tölvuskjám þegar þeir fara frá starfsstöð sinni.
- Starfsmönnum er með öllu óheimilt að deila persónuupplýsingum sín á milli með óformlegum hætti.
- Forðast skal að senda persónuupplýsingar með tölvupósti nema unnt sé að tryggja fullnægjandi öryggi þeirra. Meginregla skal vera sú að viðkvæmar persónuupplýsingar séu sendar með sniglapósti.
- Dulkóða skal persónuupplýsingar áður en þær eru sendar með rafrænum hætti, s.s. í tölvupósti.
- Persónuupplýsingar má ekki senda út fyrir Evrópska efnahagssvæðið nema fyrir því liggi sérstök lagaheimild.
- Starfsmönnum er óheimilt að vinna með persónuupplýsingar utan vinnustaðar nema unt sé að tryggja fullnægjandi öryggi upplýsinganna.
- Starfsmönnum er með öllu óheimilt að tafa afrit af persónuupplýsingum óháð skráarsniði þessara upplýsinga, þ.e. á pappír eða á rafrænu skráarsniði til notkunar á eigin tölvu eða öðrum búnaði sem les upplýsingarnar.

4.3 Viðbrögð við öryggisbroti

Samkvæmt persónuverndarlögum er aðgengi óviðkomandi aðila að persónuupplýsingum skilgreint sem öryggisbrot. Þetta á einnig við um breytingar á persónuupplýsingum án viðeigandi heimildar, glötun eða eyðing persónuupplýsinga.

Um öryggisbrot gildir eftirfarandi:

- Halda skal skrá um frávik í upplýsingaöryggi t.d. ef starfsmenn sveitarfélagsins fylgja ekki verklagsreglu um vistun/varðveislu á persónuupplýsingum.
- Tilkynna skal persónuverndarfulltrúa um öll frávik sem verður á upplýsingaöryggi, t.d. ef óviðkomandi aðili kemst með einhverju móti yfir persónuupplýsingar.
- Bregðast skal við öryggisbrotum í samræmi við persónuverndarlög m.a. með tilkynningu til Persónuverndar og þeirra einstaklinga sem við á innan 72 klst. telji starfsmenn og persónuverndarfulltrúi líklegt að öryggisbresturinn leiði til áhættu fyrir réttindi og frelsi einstaklinga.
- Ávallt skal hafa samráð við persónuverndarfulltrúa þegar öryggisbrestur kemur upp og eins ef tilkynna þarf um öryggisbrest til Persónuverndar.
- Öryggisbrot ber að rannsaka og grípa skal til viðeigandi ráðstafana til að tryggja að sambærileg atvik endurtaki sig ekki.

4.4 Réttar persónuupplýsingar
4.5 Aðgangur einstaklinga

Allir einstaklingar sem Skeiða- og Gnúpverjahreppur vinnur persónuupplýsingar um eiga rétt á eftirfarandi:

- Að vera upplýstir um hvernig sveitarfélagið mætir skyldum sínum samkvæmt persónuverndarlögum.
- Að fá vitneskju um hvaða persónuupplýsingar það eru sem sveitarfélagið hefur yfir að ráða.
- Að vera upplýstir um tilgang þessarar söfnunar og í hverju vinnsla þessara persónuupplýsinga er fólgin.
- Að fá aðgang að persónuupplýsingum um þá sjálfa.

4.6 Upplýsingagjöf til einstaklinga

Sveitarfélagið leitast við að upplýsa íbúa og aðra einstaklinga um að sveitarfélagið vinni persónuupplýsingar um þá og að íbúum sé ljóst af hverju sveitarfélagið safnar persónuupplýsingu um þá, hver tilgangur vinnslu þessara upplýsinga er og hvernig einstaklingar geta leitað réttar síns.

Skeiða- og Gnúpverjahreppur hefur sett sér persónuverndarstefnu þar sem fram kemur hvernig vinnsla persónuupplýsinga er háttað. Persónuverndarstefnu Skeiða- og Gnúpverjahrepps er hægt að nálgast á heimasíðu sveitarfélagsins www.skeidgnup.is.

Innri persónuverndarstefna Skeiða- og Gnúpverjahrepps var samþykkt í sveitarstjórn 02.03.2022 og tók gildi samstundis.

16 FRIÐUR OG RÉTTLÆTI

Þessi stefna vinnur samkvæmt heimsmarkmiðum Sameinuðu þjóðanna nr. 16.6 og 16.10 um ábyrgð stofnanna með gagnsæi að leiðarljósi og að grundvallarréttindi séu tryggð í samræmi við landslöggjöf og alþjóðasamninga.