

Innri persónuverndarstefna Hveragerðisbæjar

Samþykkt: 13.09.2018

Tók gildi: 13.09.2018

Endurskoðun: 1. 12.2019

1. Almenn

Í starfsemi Hvergerðisbæjar (hér eftir „Hveragerði“ eða „sveitarfélagið“) er nauðsynlegt að safna og vinna með persónuupplýsingar um einstaklinga. Með persónuupplýsingum er átt við allar upplýsingar sem hægt er að rekja til tiltekins einstaklings, svo sem upplýsingar um nafn, kennitölu, heimilisfang, netfang, símanúmer, fjárhag, heilsufar, IP tölu og fleira.

Þær persónuupplýsingar sem sveitarfélagið hefur undir höndum geta verið um starfsmenn þess, íbúa, viðsemjendur og aðra þriðju aðila sem nauðsynlegt er að eiga samskipti við.

Með þessari persónuverndarstefnu er kveðið á um hvernig Hveragerði skuli safna, geyma og að öðru leyti meðhöndla persónuupplýsingar í samræmi við lög um persónuvernd og vinnslu persónuupplýsinga nr. 90/2018 (hér eftir persónuverndarlög).

Þessari persónuverndarstefnu er einkum ætlað að tryggja:

- að Hveragerði vinni persónuupplýsingar í samræmi við persónuverndarlög og fylgi viðurkenndum starfsreglum til að tryggja öryggi þeirra;
- að sveitarfélagið standi vörð um þau réttindi sem einstaklingar njóta samkvæmt persónuverndarlögum;
- að gagnsæi ríki um hvernig Hveragerði meðhöndlar persónuupplýsingar;
- að sveitarfélagið komi í veg fyrir öryggisbrot.

2. Persónuverndarlög

Í persónuverndarlögum er kveðið á um hvernig sveitarfélagi sé heimilt að safna, geyma og meðhöndla persónuupplýsingar að öðru leyti. Þær reglur gilda óháð því á hvaða formi upplýsingar eru geymdar, svo sem hvort það er á rafrænu formi eða pappírformi.

Óheimilt er að safna persónuupplýsingum nema heimild standi til þess samkvæmt persónuverndarlögum. Þá verður slík söfnun einnig að fara fram með sanngjörnum hætti. Auk

Þess má einungis geyma persónuupplýsingar á öruggum stað og óheimilt er að veita óviðkomandi aðila aðgang að þeim.

Hveragerði mun grípa til allra nauðsynlegra ráðstafana til að tryggja að ávallt sé heimild í persónuverndarlögum til þess að vinna persónuupplýsingar. Auk þess mun sveitarfélagið grípa til nauðsynlegra ráðstafana til að tryggja að ávallt sé farið eftir þeim sex meginreglum sem löggjöfin kveður á um. Þær meginreglur sem átt er við eru í stuttu máli eftirfarandi:

- 1) að persónuupplýsingar séu unnar með sanngjörnum hætti;
- 2) að þeim sé einungis safnað í skýrum tilgangi;
- 3) að ekki sé safnað meiri upplýsingum en nauðsynlegt er;
- 4) að þær séu nákvæmar og uppfærðar þegar þörf krefur;
- 5) að þær séu ekki geymdar lengur en þörf er á;
- 6) að gætt sé að öryggi persónuupplýsinga með viðeigandi varúðarráðstöfunum.

3. Áhættur og ábyrgðir

Lágmarka verður þá áhættu sem felst í því að meðhöndla persónuupplýsingar og koma þarf í veg fyrir eftirfarandi atriði:

- að brotið verði gegn þeirri trúnaðarskyldu sem hvílir á sveitarfélaginu, til dæmis að persónuupplýsingum verði ekki miðlað til óviðkomandi aðila;
- að einstaklingar hafi ekki val um hvort unnið verði með persónuupplýsingar um þá;
- að orðspor Hveragerðis verði fyrir skaða, en í því samhengi má gjarnan hafa í huga þær afleiðingar sem sveitarfélagið yrði fyrir ef brotið er gegn persónuverndarlögum;
- að þeir einstaklingar sem upplýsingarnar eru um verði ekki fyrir tjóni. Hér má hafa í huga þær afleiðingar sem þeir kynnu að verða fyrir ef viðkvæmar persónuupplýsingar um þá kæmust í hendur óviðkomandi aðila.

Allir stjórnendur og starfsmenn Hveragerðis bera einhverja ábyrgð á því hvernig persónuupplýsingar eru meðhöndlaðar. Ríkari skyldur hvíla þó á þeim aðilum sem nefndir eru hér að neðan. Þeir aðilar og efni þeirra skyldna sem á þeim hvíla eru eftirfarandi:

- Sveitarstjórn ber ábyrgð á því að sveitarfélagið framfylgi persónuverndarlögum.
- Persónuverndarfulltrúi ber ábyrgð á:

- að stjórn sveitarfélagsins fái reglulega fræðslu um þær skyldur sem á því hvíla samkvæmt persónuverndarlögum;
- að fara reglulega yfir ferla og stefnur sem tengjast meðferð persónuupplýsinga;
- að veita fræðslu og þjálfna starfsmenn sem meðhöndla persónuupplýsingar;
- að taka á móti og svara spurningum frá þeim einstaklingum sem upplýsingarnar varða;
- að taka á móti beiðnum frá skráðum einstaklingum, svo sem vegna réttar þeirra til aðgangs að gögnum, til að mótmæla vinnslu eða til að gleymast;
- að yfirfara og samþykka alla samninga við utanaðkomandi þriðju aðila sem ætlað er að vinna persónuupplýsingar fyrir hönd sveitarfélagsins;
- að annast samskipti við Persónuvernd.
- Kerfisstjóri ber ábyrgð á:
 - að tryggja að öll kerfi, þjónusta og búnaður fullnægi þeim öryggiskröfum sem gerðar eru samkvæmt persónuverndarlögum;
 - að framkvæma reglulega úttektir sem eiga að tryggja að hugbúnaður virki með öruggum hætti;
 - að meta þá þjónustu sem sveitarfélagið hyggst nýta sér frá utanaðkomandi þriðja aðila, til dæmis þar sem til stendur að geyma gögn.

4. Almennar verklagsreglur um meðferð persónuupplýsinga

Eftirfarandi verklagsreglur um meðferð persónuupplýsinga gilda hjá Hveragerði:

- Einungis þeir starfsmenn sem þurfa þess starfs sín vegna skulu hafa aðgang að persónuupplýsingum.
- Starfsmönnum er óheimilt að deila persónuupplýsingum sín á milli óformlega.
- Starfsmenn skulu reglulega fá fræðslu um þær skyldur sem á þeim hvíla samkvæmt persónuverndarlögum.
- Starfsmenn skulu ávallt gæta fyllsta öryggis þegar þeir meðhöndla persónuupplýsingar.
- Öll lykilorð skulu vera illrekjanleg og þeim má aldrei deila með öðrum.
- Starfsmenn skulu aldrei deila persónuupplýsingum með óviðkomandi aðilum og gildir þar einu hvort um sé að ræða annan starfsmann sveitarfélagsins eða utanaðkomandi aðila.

- Endurskoða skal persónuupplýsingar reglulega og ganga úr skugga um að þær séu réttar.
- Eyða skal persónuupplýsingum með fullnægjandi hætti eða gera þær ópersónugreinanlegar ef ekki er þörf fyrir þær lengur.
- Starfsmenn skulu ráðfæra sig við persónuverndarfulltrúa ef þeir eru í vafa um hvernig skuli meðhöndla persónuupplýsingar.

5. Geymsla á persónuupplýsingum

5.1. Geymsla persónuupplýsinga á pappír

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

- Persónuupplýsingar sem geymdar eru á pappír skulu vera í læstum skjalaskáp eða í læstri skjalageymslu.
- Starfsmönnum ber að tryggja að pappírsgögn, þar sem persónuupplýsingar má finna, séu ekki skilin eftir þar sem óviðkomandi aðilar geta séð þær, til dæmis í prentara.
- Pappírsgögnum skal eytt með fullnægjandi hætti þegar þeirra er ekki lengur þörf.

5.2. Geymsla á persónuupplýsingum með rafrænum hætti

Persónuupplýsingar sem geymdar eru með rafrænum hætti skulu njóta verndar gegn óleyfilegum aðgangi og þess skal gætt að þeim verði ekki eytt fyrir mistök.

- Persónuupplýsingar skulu verndaðar með illrekjanlegum lykilorðum. Lykilorðum skal jafnframt breyta reglulega og starfsmenn skulu aldrei deila þeim sín á milli.
- Ákveðin form sem innihalda persónuupplýsingar, til dæmis geisladiskur eða USB lykill, skulu geymd á læstum stað þegar ekki er verið að nota þau.
- Persónuupplýsingar skal einungis geyma á öruggum drifum og netþjónum. Einungis skal notast við tölvuskýjaþjónustu sem uppfyllir öll þau skilyrði sem persónuverndarlög kveða á um.
- Netþjónar sem innihalda persónuupplýsingar skulu staðsettir á öruggum stað og fjarri almennu skrifstofurými.
- Taka skal afrit af gögnum með reglubundnum hætti og jafnframt skal kanna reglulega hvort afritun tekst.
- Aldrei skal vista persónuupplýsingar beint á fartölvur eða símtæki, svo sem snjallsíma.

- Vernda skal alla netþjóna og tölvur sem innihalda persónuupplýsingar með viðeigandi öryggisbúnaði og eldveggjum.

6. Notkun á persónuupplýsingum

Þegar starfsmaður meðhöndlar persónuupplýsingar er áhættan fyrir sveitarfélagið og þann einstakling sem upplýsingarnar varða hvað mest, til dæmis að persónuupplýsingar glatist eða að þær verði teknar ófrjálsri hendi. Við notkun á persónuupplýsingum skulu starfsmenn ávallt hafa eftirfarandi reglur í huga:

- Þegar unnið er með persónuupplýsingar skulu starfsmenn ávallt gæta þess að tölvuskjáiir séu læstir þegar farið er frá borðum.
- Persónuupplýsingum skal ekki deilt óformlega á milli starfsmanna.
- Persónuupplýsingar skulu ekki sendar með tölvupósti nema fyllsta öryggis sé gætt.
- Persónuupplýsingar skal dulkóða áður en þær eru sendar með rafrænum hætti.
- Persónuupplýsingar skal aldrei senda út fyrir Evrópska efnahagssvæðið nema fyrir því sé sérstök lagaheimild.
- Starfsmenn skulu ekki vista afrit af persónuupplýsingum á eigin tölvu.

7. Nákvæmni persónuupplýsinga

Persónuverndarlög gera kröfu um að gripið sé til viðeigandi öryggisráðstafana sem eiga tryggja að persónuupplýsingar séu réttar. Hversu mikilla ráðstafna þarf að grípa til veltur á því hve mikil áhrif ónákvæmar upplýsingar hafa á hinn skráða.

Allir starfsmenn Hveragerðis skulu grípa til hæfilegra og skynsamlegra ráðstafana til að tryggja að persónuupplýsingar séu nákvæmar og réttar. Eftirfarandi verklagsreglur skal hafa í huga:

- Persónuupplýsingar skal geyma á eins fáum stöðum og mögulegt er.
- Starfsmenn skulu ekki halda til haga upplýsingum sem ekki er þörf fyrir á eigin stað.
- Sveitarfélagið skal auðvelda einstaklingum að fá ónákvæmar persónuupplýsingar leiðréttar.
- Persónuupplýsingar skulu uppfærðar um leið og í ljós kemur að þær séu ekki réttar. Sem dæmis skal fjarlægja gamalt símanúmer starfsmanns úr gagnagrunnum um leið og það uppgötvast.

8. Aðgangur einstaklinga

Allir einstaklingar sem Hveragerði á upplýsingar um eiga rétt á eftirfarandi:

- Að vera upplýstir um það hvernig sveitarfélagið mætir skyldum sínum samkvæmt persónuverndarlögum.
- Að fá vitneskju um hvaða upplýsingar það eru sem sveitarfélagið á um þá.
- Að vera upplýstir um af hverju sveitarfélagið hefur þær undir höndum.
- Að krefja sveitarfélagið um aðgang að sínum persónuupplýsingum.

Þegar beiðni um aðgang berst mun Hveragerði grípa til allra nauðsynlegra ráðstafana til að tryggja að um sé að ræða réttan aðila. Beiðni skal vera einstaklingum að kostnaðarlausu og mun sveitarfélagið veita framangreindar upplýsingar innan þeirra tímamarka sem persónuverndarlög kveða á um.

9. Upplýsingar til einstaklinga

Markmið Hveragerðis er að einstaklingar séu meðvitaðir um að sveitarfélagið vinni persónuupplýsingar um þá og að þeir skilji:

- af hverju sveitarfélagið safnar persónuupplýsingum;
- hvernig sveitarfélagið notar persónuupplýsingar;
- hvernig þeir geti leitað réttar síns.

Hveragerði hefur birt persónuverndarstefnu til að upplýsa einstaklinga um framangreind atriði. Hægt að er að nálgast skjalið á heimasíðu sveitarfélagsins www.hveragerdi.is. Jafnframt hefur sveitarfélagið sent tilkynningu með sambærilegum upplýsingum til starfsmanna. Allir starfsmenn ættu að hafa fengið skjalið til yfirlesturs.

Hveragerði 13. september 2018


Aldis Hafsteinsdóttir

Bæjarstjóri

