Innri persónuverndarstefna

Vestmannaeyjabæjar

Efnisyfirlit

Samþykkt: xx.xx.2019

Tók gildi: xx.xx.2019

Endurskoðun: xx.xx.2020

Almennt

Í starfsemi Vestmannaeyjabæjar 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 og aðra þriðju aðila sem nauðsynlegt er að eiga samskipti við.

Með þessari persónuverndarstefnu er kveðið á um hvernig Vestmannaeyjabær 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 Vestmannaeyjabær

- vinni persónuupplýsingar í samræmi við persónuverndarlög og fylgi viðurkenndum starfsreglum til að tryggja öryggi þeirra,
- standi vörð um þau réttindi sem einstaklingar njóta samkvæmt persónuverndarlögum,
- meðhöndli persónuupplýsingar með gagnsæjum hætti og
- lágmarki þá áhættu sem brot á persónuverndarlögum getur haft í för með sér.

Persónuverndarlög

Í persónuverndarlögum er kveðið á um hvernig sveitarfélaginu 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 pappírsformi.

Óheimilt er að safna og vinna með persónuupplýsingar nema heimild standi til þess samkvæmt persónuverndarlögum. Þá verður slík söfnun og vinnsla 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.

Vestmannaeyjabær mun grípa til nauðsynlegra ráðstafana til að tryggja að ávallt sé heimild í persónuverndarlögum til þess að vinna með 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) Persónuupplýsingar séu unnar með sanngjörnum og lögmætum hætti.
2) Persónuupplýsingum sé einungis safnað í skýrum og lögmætum tilgangi.
3) Ekki sé safnað og unnið meira með persónuupplýsingar en nauðsynlegt er.
4) Persónuupplýsingar séu nákvæmar og uppfærðar þegar þörf krefur.
5) Persónuupplýsingar séu ekki geymdar lengur en þörf er á.
6) Gætt sé að öryggi persónuupplýsinga með viðeigandi varúðarráðstöfunum.

Áhættur og ábyrgðir

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

- 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 Vestmannaeyjabæjar verði fyrir skaða, en gjarnan má hafa í huga þær afleiðingar sem sveitarfélagið yrði fyrir ef brotið er gegn persónuverndarlögum og
- 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 persónuupplýsingar þeirra kæmust í hendur óviðkomandi aðila.

Allir stjórnendur og starfsmenn Vestmannaeyjabæjar 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:

- Bæjarstjórn 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 þjálfa 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 samþykkja alla samninga við utanaðkomandi þriðja aðila sem ætlað er að vinna persónuupplýsingar fyrir hönd Vestmannaeyjabæjar,
  - að vega og meta hvort tilkynna þurfi öryggisbrest til viðeigandi aðila og
  - 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 hug- og vélbúnaður virki með öruggum hætti og
  - að meta þá þjónustu sem sveitarfélagið hyggst nýta sér frá utanaðkomandi þriðja aðila, til dæmis þar sem til stendur að geyma gögn.

Almennar verklagsreglur um meðferð persónuupplýsinga

Eftirfarandi verklagsreglur um meðferð persónuupplýsinga gilda hjá Vestmannaeyjabæ:

- 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 og fylgja þeim leiðbeiningum sem hér koma fram.
- Gæta skal þess að öll lykilorð séu illrekjanleg og þeim má aldrei deila með öðrum.
- Starfsmenn skulu aldrei deila persónuupplýsingum með óviðkomandi aðila 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.

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 sem geymdar eru á pappír skulu vera í læstum skjalaskáp eða í læstri skjalageymslu eftir því sem við verður komið.
- 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.

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 skal vernda með illrekjanlegum lykilorðum. Lykilorðum skal jafnframt breyta reglulega og starfsmenn skulu aldrei deila þeim sín á milli.

- Ef persónuupplýsingar eru geymdar á ákveðnu formi, til dæmis á geisladiski eða USB lykli, þá skal geyma þau á læstum stað þegar ekki er verið að nota þau eftir því sem við verður komið.
- Persónuupplýsingar skal einungis geyma á tilgreindum drifum og netþjónum. Einungis skal notast við tölvuskýjaþjónustu sem uppfyllir 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.

Notkun á persónuupplýsingum

Þegar starfsmaður meðhöndlar persónuupplýsingar er áhættan fyrir Vestmannaeyjabæ 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 fylgja eftirfarandi reglum:

- Þegar unnið er með persónuupplýsingar skulu starfsmenn ávallt gæta þess að tölvuskjáir séu læstir þegar farið er frá borðum.
- Starfsmönnum er 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.
- Dulkóða skal persónuupplýsingar áður en þær eru sendar með rafrænum hætti.
- Persónuupplýsingar skal aldrei senda út fyrir Evrópska efnahagssvæðið nema fyrir því sé sérstök lagaheimild.
- Starfsmönnum er óheimilt að meðhöndla persónuupplýsingar utan vinnustaðar nema unnt sé að tryggja fullnægjandi öryggi þeirra.

- Þegar unnið er með persónuupplýsingar í rafrænu kerfi í gegnum fjaraðgang skulu starfsmenn gæta að umhverfi sínu.
- Starfsmenn skulu ekki vista afrit af persónuupplýsingum á eigin tölvu.

Viðbrögð við öryggisbresti

Samkvæmt persónuverndarlögum telst það vera öryggisbrestur þegar óviðkomandi aðili fær aðgang að persónuupplýsingum, þær glatast eða er breytt í leyfisleysi. Eftirfarandi reglur skulu gilda um öryggisbresti og viðbrögð því:

- Halda skal skrá um frávik í upplýsingaöryggi, til dæmis ef starfsfólk fylgir ekki verklagsreglum um geymslu á persónuupplýsingum.
- Tilkynna skal persónuverndarfulltrúa um hvert það frávik sem verður í upplýsingaöryggi, til dæmis ef óviðkomandi aðili kemst yfir persónuupplýsingar.
- Bregðast skal við öryggisbrestum í samræmi við persónuverndarlög, þ.e. með tilkynningu til Persónuverndar og einstaklinga þegar við á. Ef öryggisbrestur á sér stað þarf að tilkynna persónuverndarfulltrúa Vestmannaeyjabæjar þegar í stað um atvikið. Persónuverndarfulltrúi Vestmannaeyjabæjar er Dattaca Labs og er hægt að hafa samband í síma 517 3444 eða með því að senda á netfangið dpo@dattacalabs.com. Það er persónuverndarfulltrúi Vestmannaeyjabæjar sem vegur og metur hvort tilkynna þurfi öryggisbrest til Persónuverndar og einstaklinga.
- Mikilvægt er að starfsmönnum sveitarfélagsins sé kunnugt um það að ef öryggisbrestur á sér stað sem metinn er tilkynningaskyldur til Persónuverndar, þarf tilkynning að eiga sér stað innan 72 klukkustunda frá því að starfsmaður varð hans var. Það undirstrikar mikilvægi þess að Dattaca Labs fái vitneskju þegar í stað um öryggisbrest.
- Öryggisbrest ber að rannsaka og grípa skal til skynsamlegra ráðstafana til að tryggja að sambærileg atvik endurtaki sig ekki.

Nákvæmni persónuupplýsinga

Persónuverndarlög gera kröfu um að gripið sé til viðeigandi ráðstafana sem eiga að tryggja að persónuupplýsingar séu nákvæmar og réttar. Hversu mikilla ráðstafana þarf að grípa til veltur á

því hve mikil áhrif ónákvæmar upplýsingar geta haft á þann einstakling sem upplýsingarnar eru um.

Allir starfsmenn Vestmannaeyjabæjar skulu grípa til hæfilegra og skynsamlegra ráðstafana til að tryggja að persónuupplýsingar séu nákvæmar og réttar. Eftirfarandi verklagsreglum skal fylgja:

- Persónuupplýsingar skal geyma á eins fáum stöðum og mögulegt er.
- Sveitarfélagið skal auðvelda einstaklingum að fá ónákvæmar persónuupplýsingar leiðréttar.
- Persónuupplýsingar skulu uppfærðar um leið og í ljós kemur að þær séu ekki réttar. Sem dæmi skal fjarlægja gamalt netfang starfsmanns úr gagnagrunnum um leið og það uppgötvast.

Aðgangur einstaklinga

Allir einstaklingar sem Vestmannaeyjabær 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 Vestmannaeyjabær grípa til allra nauðsynlegra ráðstafana til að tryggja að um sé að ræða réttan aðila. Beiðni skal vera einstaklingum að kostnaðarlausu og mun Vestmannaeyjabær veita framangreindar upplýsingar innan þeirra tímamarka sem persónuverndarlög kveða á um.

Upplýsingagjöf til einstaklinga

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

- af hverju sveitarfélagið safnar persónuupplýsingum um þá,

- hvernig sveitarfélagið notar upplýsingar um þá og
- hvernig þeir geti leitað réttar síns.

Vestmannaeyjabær hefur sent frá sér persónuverndaryfirlýsingu um hvernig það vinnur með persónuupplýsingar um einstaklinga. Þeir aðilar og aðrir geta nálgast það skjal á heimasíðu sveitarfélagsins vestmannaeyjar.is.

Persónuverndarstefna þessi var samþykkt 15.10.2019 af bæjarráði og staðfest þann 31.10.2019 í bæjarstjórn Vestmannaeyjabæjar.