

Persónuvernd hjá Ísfélaginu hf.

- Persónuverndarstefna
- Persónuverndaryfirlýsing til starfsmanna
- Reglur vegna tölvukerfa og vinnslu persónuupplýsinga
- Persónuverndaryfirlýsing til umsækjenda um störf (íslenska og enska)

Persónuverndarstefna Ísfélagsins hf.

MARKMIÐ

Ísfélaginu er umhugað um persónuvernd og öryggi persónuupplýsinga sem félagið býr yfir hverju sinni. Ísfélagið vinnur með þær persónuupplýsingar sem félaginu eru veittar sem ábyrgðaraðili.

SKRÁNING OG VINNSLA

Ísfélagið skráir einungis þær upplýsingar um starfsfólk og aðra einstaklinga sem félaginu er skylt að varðveita í samræmi við lög og reglur, kjarasamninga, ráðningarsamninga, samþykki hins skráða eða vegna annarra lögmætra hagsmuna ábyrgðaraðila.

Ísfélagið notast ekki við sjálfvirka ákvarðanatöku, t.d. gerð persónusniðs, í tengslum við vinnslu persónuupplýsinga.

Ísfélagið takmarkar vinnslu persónuupplýsinga við nauðsynlega vinnslu þeirra til að efna samning sem hinn skráði er aðili að eða til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður. Einnig til að uppfylla lagaskyldu sem hvílir á félaginu og vernda brýna hagsmuni hins skráða.

ÖRYGGI, VISTUN OG VARÐVEISLA GAGNA

Ísfélagið leggur áherslu á að tryggja örugga varðveislu persónuupplýsinga með viðeigandi tæknilegum öryggisráðstöfunum.

Ísfélagið nýtir ekki persónuupplýsingar í öðrum tilgangi en þeim sem getið er þegar upplýsingar eru skráðar. Félagið afhendir ekki þriðja aðila persónuupplýsingar nema á grundvelli lagaheimildar, stjórnvaldsfyrirmæla, dómsúrskurðar, skriflegs vinnslusamnings eða samþykkis viðeigandi starfsmanns. Ísfélagið áskilur sér þó rétt til þess að afhenda þriðja aðila ópersónugreinanlegar upplýsingar í lögmætum tilgangi.

Varðveisla gagna sem safnast vegna rafrænnar vöktunar er samkvæmt ákvæðum reglna persónuverndar nr. 837/2006, um rafræna vöktun og meðferð persónuupplýsinga sem verða til við rafræna vöktun. Aðrar persónuupplýsingar eru ekki varðveittar lengur en nauðsynlegt þykir og eytt þegar þær teljast ekki lengur hagnýtar.

Persónuverndaryfirlýsing til starfsmanna

Í tengslum við starf þitt mun Ísfélagið sem ábyrgðaraðili, safna og vinna með persónugreinanlegar upplýsingar þínar í þeim tilgangi sem tilgreindur er hér að neðan. Ísfélagið vinnur persónugreinanlegar upplýsingar um þig í samræmi við gildandi persónuverndarlöggjöf. Yfirlýsing þessi er aðgengileg á innra neti Ísfélagsins og á viðkomandi starfsstöðvum. Vegna þessa viljum við vinsamlegast biðja þig um að fara vel yfir eftirfarandi texta til að skilja hvernig við vinnum með persónuupplýsingar þínar.

HVAÐA GÖGNUM SÖFNUM VIÐ UM ÞIG OG Í HVAÐA TILGANGI

Við söfnum og vinnum eftirfarandi persónuupplýsingar til þess að að unnt sé að ganga frá ráðningarsamningi, frammistöðumati, þjálfun, mönnun og skipulagningu, aðgangi að viðeigandi kerfum, tryggja fylgni við gildandi lög / reglugerðir og innri ferla, uppfylla kröfur varðandi skjölun, meðhöndlun beiðna, kvartana og krafna frá þriðja aðila, meðhöndlun eftirlits og fyrirsurnna frá yfirvöldum, ytri endurskoðendum og lögfræðingum:

Nafn; aldur, fæðingardag, kennitölu, kyn, símanúmer, heimilisfang, dvalarland, fjölskylduaðstæður (t.d hjúskaparstaða og upplýsingar um aðstandendur og nána ættingja) mynd, tölvupóstfang, starfstítil, staðsetning vinnustaðar, deild, auðkennisnúmer starfsmanns, tímaskráningu, upplýsingar um atvinnu og menntun (t.d upplýsingar um fyrri atvinnu, menntun, verkefni o.fl.), launa- og lífeyrisupplýsingar, bankaupplýsingar, uppl. í tengslum við skattgreiðslur og meðlagsgreiðslur, ferðakostnað, frammistöðumat.

Einnig eru líkur á því að við vinnum með eftirfarandi flokka af persónuupplýsingum í tengslum við endurgreiðslu og greiðslu launa: Heilsufarsupplýsingar og aðild að verkalýðsfélagi.

Ísfélagið viðhefur eftirlit með öryggismyndavélum í öryggis- og eignavörslu tilgangi. Myndavélar eru staðsettar utan á húsum félagsins, innanhúss og í skipum. Tilgangur öryggismyndavéla utan á húsi er til að gæta öryggis utan húss og á að hafa fælingarmátt fyrir hugsanleg innbrot eða skemmdarverk á lóðum og húsum. Tilgangur myndavéla innanhúss er að geta fylgst með ákveðnum framleiðslusvæðum í mynd. Tilgangur myndavéla um borð í skipum er í tengslum við veiðar og fiskvinnslu. Upptökur úr myndavélum eru geymdar í mesta lagi 30 daga. Starfsmenn vinnslu, viðhalds auk yfirmanna þeirra og UT deild hafa aðgang að myndum í rauntíma. Sömu starfsmenn hafa aðgang að drifi með myndefni af upptöku. Eyðsla gagna fer fram sjálfkrafa.

FRÁ HVERJUM SÖFNUM VIÐ ÞÍNUM PERSÓNUUPPLÝSINGUM?

Við söfnum persónuupplýsingum frá þér, öðrum starfsmönnum, stjórnendum og opinberum yfirvöldum.

LAGALEGUR GRUNDVÖLLUR FYRIR VINNSLU

Söfnun og vinnsla persónuupplýsinga þinna eru byggðar á 9. gr. laga um persónuvernd og vinnslu persónuupplýsinga. Þeir lögmætu hagsmunir sem Ísfélagið byggir á tengjast frammistöðumati, þjálfun, mönnun, aðgangi að viðeigandi kerfum, fylgni við gildandi lög / reglugerðir og innri ferla, kröfum varðandi skjölun, meðhöndlun beiðna, kvörtunum og kröfum frá þriðja aðila. Um er að ræða aðgerðir sem nauðsynlegar eru fyrir starfsemi okkar og krefjast þess að við söfnum og vinnum með persónuupplýsingar þínar.

DEILING PERSÓNUUPPLÝSINGA ÞINNA

Í tengslum við eitt eða fleiri fyrrgreind atriði, er mögulegt að persónuupplýsingum þínum verði deilt með eftirfarandi viðtakendum: Opinberum yfirvöldum, verkalýðsfélögum, lífeyrissjóðum, faglegum ráðgjöfum (t.d endurskoðendum og lögfræðingum), viðskiptavinum, söluaðilum, og öðrum starfstöðvum Ísfélagsins. Það er mögulegt að gögn þín verði flutt til annarra starfstöðva Ísfélagsins. Eins gætu gögn þín verið flutt til umsjáraðila upplýsingakerfa, þ.m.t. skýjaþjónustu, eða til utanaðkomandi aðila sem vinna með og/eða geyma persónuupplýsingar fyrir Ísfélagið.

HVERSU LENGI GEYMUM VIÐ PERSÓNUUPPLÝSINGAR UM ÞIG?

Við geymum persónuupplýsingarnar svo lengi sem við teljum það nauðsynlegt til að uppfylla þann tilgang sem nefndur er hér að framan, þó ekki lengur en nauðsyn krefur með tilliti til starfssamnings þíns sem og lagalegrar skyldu félagsins.

RÉTTINDI ÞÍN

Með fyrirvara um skilyrði sem nánar er fjallað um í gildandi löggjöf um persónuvernd, þá átt þú rétt á eftirfarandi varðandi persónuupplýsingar þínar:

- Aðgangi, leiðréttingu og eyðingu
- Takmörkun/andmæla vinnslu
- Flutningi persónuupplýsinga þinna

Vinsamlegast athugaðu að þessi réttindi eru ekki algild þar sem þau taka skal mið af ákvæðum laga og lögmætra hagsmuna Ísfélagsins. Þú hefur einnig rétt á að leggja fram kvörtun hjá eftirlitsyfirvaldi sjáir þú ástæðu til þess.

PERSÓNUVERNDARFULLTRÚI

Það er mat Ísfélagsins að ekki sé gerð krafa um að félagið tilgreini sérstakan persónuverndarfulltrúa þar sem meginstarfsemi félagsins lýtur ekki að vinnslu viðkvæmra persónuupplýsinga.

ENDURSKOÐUN PERSÓNUVERNDARYFIRLÝSINGAR

Persónuverndaryfirlýsingin er endurskoðuð reglulega og uppfærð ef tilefni er til. Síðast var hún uppfærð þann 04.09.2019

Reglur vegna tölvukerfa og vinnslu persónuupplýsinga

Hér eru settar fram skýringar og verklagsreglur um aðgangsstjórnun og breytingastjórnun upplýsingakerfa, sem hvort tveggja eru grundvallaratriði í tengslum við upplýsingaöryggi. Einnig er fjallað um afritun, meðferð geymslumiðla, gagnaflutninga og fleiri atriði sem gagnlegt er að hafa í reglunum með tilliti til öryggis upplýsinga og vinnslu þeirra.

AÐGANGSSTJÓRNUN

Vinnulýsingin lýsir ferlinu við aðgangsstýringar að öllum kerfum og tæknumhverfi hjá fyrirtækinu og er ætlað að tryggja samræmt ferli. Vinnulýsingin nær til allra starfsmanna sem hafa aðgang að kerfum fyrirtækisins.

EINKVÆM NOTENDANÖFN

Notendur fá, að því leyti sem það truflar ekki starfsemi rekstrarins, úthlutað einkvæmum notendanöfnum til aðskilnaðar frá öðrum notendum, svo hægt sé að rekja aðgerðir niður á einstaklinga.

AÐGANGSHEIMILDIR – NÝ RÉTTINDI OG BREYTT RÉTTINDI

- UT deild fær beiðni frá yfirmanni þar sem óskað er eftir aðgangi/breyttum heimildum að kerfum.
- Ef samþykki ábyrgðaraðila vantar er óskað eftir því annars er aðgangur ekki veittur né breyttur.

AÐGANGI LOKAÐ

- Beiðni er send frá yfirmanni um að loka eigi öllum aðgangi að kerfum og tölvupósti hjá viðkomandi starfsmanni. Tilgreina skal hvort viðkomandi sé að hætta tímabundið eða fyrir fullt og allt.
- UT deild lokar á allan aðgang þegar beiðni berst í samræmi við lokadagsetningu.

VÍÐTÆK RÉTTINDI

Takmarka á réttindi hvers notanda við þær aðgangsheimildir sem nauðsynlegar eru fyrir viðkomandi svo hann geti sinnt starfsskyldum sínum. Þurfi að auka við aðgangsréttindi starfsmanns þarf yfirmaður viðkomandi starfsmanns að rökstyðja með beiðninni hvers vegna viðkomandi þarf aukin réttindi.

- UT deild fær beiðni frá yfirmanni, þar sem óskað er eftir auknum réttindum starfsmanns.
- Kerfiseigandi/ábyrgðaraðili fer yfir beiðnina og samþykkir ef sýnt er fram á að viðkomandi þurfi umbeðin réttindi vegna starfa sinna og er þá aðgangur veittur af UT deild.

VERKTAKAÐGANGUR

Verktökum er veittur aðgangur í samræmi við eðli þeirrar þjónustu sem þeir veita. Aðgangur skal veittur í samræmi við verktakasamning.

- Ábyrgðaraðili samnings skal senda beiðni á UT deild um stofnun aðgangs þar sem tímarammi aðgangs er tilgreindur.
- Kerfiseigandi/ábyrgðaraðili yfirfer þær heimildir sem óskað er eftir að séu veittar og hversu lengi aðgangurinn skuli vera virkur. Þegar kerfiseigandi/ábyrgðaraðili hefur samþykkt beiðnina er aðgangur veittur.
- Ef verktaki óskar eftir auknum réttindum vegna starfa sinna þá skal óska eftir samþykki kerfiseiganda/ábyrgðaraðila áður en aukin réttindi eru veitt.
- Þegar aðgangur verktaka rennur út skal yfirfara að allur aðgangur hans sé lokaður.

YFIRFERÐ AÐGANGSHEIMILDA

Framkvæma skal reglulegar yfirferðir til þess að staðfesta að aðgangsheimildir notenda séu viðeigandi.

- Kerfisstjóraréttindi í tölvuumhverfi (oftast stýrt með Active Directory) skal rýna á 1 árs fresti
- Aðgangur að öðrum kerfum skal einnig rýna árlega.
- Á 6 mánaða fresti skal sérfræðingur UT deildar rýna aðgang starfsmanna sem hætt hafa störfum og fylgja því eftir að aðgangur sé fjarlægður í þeim tilfellum sem við á.
- Yfirmönnum ber að tilkynna UT deild þegar starfsmenn láta af störfum.

LYKILORÐ

Það er á ábyrgð notanda (starfsmanns) að skipta um lykilorð þegar hann skráir sig inn í kerfin í fyrsta skipti. Starfsmaður ber ábyrgð á aðgangsorði sínu og skal hann tryggja að það komist ekki í hendur annarra. Ef starfsmaður hefur grun um að einhver hafi komist yfir aðgangsorðið skal hann breyta því án tafar.

Ef notandi gleymir lykilorðinu sínu þá skal hann hafa samband við UT deild til þess að fá úthlutað nýju bráðabirgða lykilorði. Sannreyna skal að viðkomandi sé sá sem hann segist vera áður en nýju bráðabirgða lykilorði er úthlutað.

- Skipta þarf um lykilorð á 180 daga fresti.
- Lágmarkslengd eru 8 stafir /tákn.
- Nota skal hástafi, lágstafi og tölustafi/tákn.
- Ekki má endurnýta síðustu 25 lykilorð.
- Misheppnaðar tilraunir til innskráninga eru takmarkaðar við 5 skipti.
- Ekki skal nota lykilorð sem hægt er að tengja auðveldlega við notanda.

SKJÁVÖRN

Nota skal skjávörn með lykilorði sem skal virkja þegar skilið er við starfsstöð. Einnig skulu stillingar vera þannig að eftir 30 mínútur virkjast skjávarinn með lykilorðastillingu sjálfkrafa ef tölvan er ekki í notkun. Í Windows stýrikerfinu gildir til að virkja skjávörnina að velja samtímis „windows merkið og L“ og þá læsist skjárinn. Undantekningar eru á þessu í verksmiðju.

BREYTINGASTJÓRNUN

Tilgangur breytingastjórnunar upplýsingakerfa er að styðja tímanlegar og öruggar breytingar á tölvukerfum í samræmi við þarfir fyrirtækisins. Einnig að lágmarka áhættu sem fylgir breytingum tölvukerfa. Ófullkomin breytingastjórnun UT kerfa getur m.a. leitt til:

- Breytinga á viðskiptaferlum, sem ekki hafa verið samþykktar af stjórnendum.
- Skekkju í reikningshaldi og uppgjöri.
- Að breytingar séu ekki rekjanlegar.
- Að neyðarbreytingar verði erfiðar þar sem ekki er yfirsýn yfir breytingasögu, með tilheyrandi villuhættu.
- Að breytingar séu ekki innleiddar tímanlega.
- Öryggisatvika.
- Að breytingar leiði af sér óviðeigandi aðgangsheimildir.
- Að tölvukerfi verði óvirk, eða ónothæf um tíma.
- Brota á reglum um aðgreiningu starfa.

Eigandi/ábyrgðaraðili skal athuga sérstaklega hvort breyting muni hafa áhrif á vinnslu persónuupplýsinga og hvort viðeigandi lagagrundvöllur sé til staðar. Ef breyting krefst nýs samþykkis skráðs einstaklings, skal sjá til þess að þess sé aflað.

Gerður er vinnslusamningur við alla þriðju aðila sem sjá um uppfærslur, forritun og prófanir.

AÐRIR LIÐIR

AFRITUN

Vinnulýsingin skal tryggja samræmt og rekjanlegt ferli við afritunartöku í öllum kerfum fyrirtækisins sem og að tryggja að endurheimt gagna takist á eðlilegan hátt þegar grípa þarf til að endurheimta gögn. UT deild ber ábyrgð á að kerfi sé afritað.

- Tryggja skal heilleika, áreiðanleika og tiltækileika afrita með því að staðfesta gæði afrita eftir hverja afritatöku
- Mögulegt skal vera að afrita eða endurheimta einstakar skrár eða allt efnið í heild sinni
- Skjalfesta skal afritunarátætlun fyrir allt sem þarf að afrita
- Afrit skal prófa reglulega til að tryggja að upplýsingar á þeim séu nothæfar

RAUNLÆGT ÖRYGGI

- Aðgangur að tölvurými er reynt að takmarka við viðeigandi aðila sem nauðsynlega þurfa aðgang starfa sinna vegna (t.d. UT deild, umsjónarmenn fasteigna, öryggisverði).
- Netþjónar og endabúnaður eru geymdir í öruggu rými eftir því sem kostur er á.

RAFRÆNT EFTIRLIT

Tilgangur rafrænnar vöktunar verður að vera skýr, yfirlýstur og málefnalegur. Þegar eftirlitsmyndavélar eru notaðar skal gæta meðalhófs, t.d. þannig að myndavélar séu ekki fleiri en nauðsynlegt þykir. Einkalífsréttur þeirra sem vöktun sætir skal virða. Vöktun er gerð viðvart með glögglegum merkingum. Einungis þeir sem starfa sinna vegna þurfa aðgang að myndefni skulu hafa hann. Myndefni er eytt innan 30 daga (óheimild er að varðveita efni lengur en í 90 daga).

STARFSUMSÓKNIR OG VEIKINDAVOTTORÐ

Starfsumsóknnum eru eytt á 6 mánaða fresti úr tölvukerfi félagsins. Vottorðum um veikindi er eytt mánaðarlega af launafulltrúum og/eða verkstjórum.

VÉLBÚNAÐUR OG HUGBÚNAÐUR

- Borðtölva, fartölva og annar búnaður í eigu fyrirtækisins á að vera rétt stilltur og ekki er ætlast til þess að starfmenn sæki sér hugbúnað án samþykkis yfirmanns og/eða UT deildar.
- Starfsfólk skal alltaf gæta varúðar og gera nauðsynlegar ráðstafanir til að vernda þann búnað sem viðkomandi hefur undir höndum, s.s. fartölvu, spjaldtölvu og farsíma. Búnaðurinn skal vera örugglega frágenginn þegar hann er ekki í notkun og mikilvægt er að skilja hann aldrei eftir á almannaferi án eftirlits.
- Aðeins skal geyma trúnaðarupplýsingar á tölvubúnaði ef samþykktar öryggislausnir eru uppsettar á vélinni.
- Ekki skal geyma vinnutengd gögn og upplýsingar á búnaði sem ekki eru í eigu fyrirtækisins.
- Tilkynna skal um bilanir eða villur til eiganda/umsjónarmanns eins fljótt og kostur er.

MEÐHÖNDLUN GEYMSLUBÚNAÐAR

- Ef endurnýta á miðla eins og t.d minnislykla skal upplýsingum á þeim eytt þannig að ekki verði hægt að endurheimta upplýsingarnar.
- Ef ekki á að endurnýta miðla skal eyða öllum búnaði sem inniheldur persónulegar upplýsingar.
- Gæta skal þess að búnaður og miðlar sem innihalda persónuupplýsingar séu ekki afhentir þjónustu- eða viðgerðaraðila án viðeigandi öryggisráðstafana, t.d. trúnaðaryfirlýsingar.

VERND UPPLÝSINGA

- Ekki skal vista trúnaðarupplýsingar á tölvum heldur á miðlægum tölvukerfum fyrirtækisins.
- Geyma skal minnislykla og aðra geymslumiðla sem innihalda persónugreinanleg gögn, viðkvæm gögn og trúnaðarupplýsingar á öruggum stað og með lykilorði.
- Gæta skal þess að loka á kerfi eins og Outlook og Skype for Business sem geta birt samskipti eða upplýsingar, þegar kynning eða fundur er í gangi með utanaðkomandi aðilum þar sem sést á skjáinn.
- Starfsmenn skulu aldrei skilja við vinnuaðstöðu sína þannig að viðkvæmar upplýsingar/gögn séu þar óvarin. Gera skal ráðstafanir ef starfsmaður þarf að bregða sér frá í stuttan tíma þannig að upplýsingarnar séu ekki aðgengilegar fyrir aðra en þá sem eiga að hafa aðgang að þeim. Ef starfsmaður þarf að fara í lengri tíma frá vinnuaðstöðu sinni skal hann læsa viðeigandi upplýsingar/gögn inni í skáp eða geymslu.

ÁBYRGÐ

Þagnarskylda: Að fylgja þessum reglum er hluti af vinnu- og trúnaðarskyldum starfsmanns.

Afleiðingar brota: Ef upp koma brot á fylgni við öryggisleiðbeiningar þá verður að meta alvarleika brots í hverju tilviki fyrir sig. Ef brotið telst alvarlegt getur það réttlætt fyrirvaralaus uppsögn.

ORÐSKÝRINGAR

Beiðni: Beiðni er skrifleg ósk um að framkvæma ákveðið skilgreint verk við rekstur upplýsingakerfa. T.d. að stofna notanda, eða útfæra breytingu á virkni kerfis. Beiðni þarf að vera skrifleg og rekjanleg t.d. með notkun beiðnakerfis eða póstkerfis, þar sem beiðnir eru vistaðar og hægt að finna og opna eldri beiðnir.

Kerfiseigandi/ábyrgðaraðili: Yfirmaður deildar eða starfsemi sem stýrir notkun og meðhöndlun viðkomandi upplýsinga, t.d. starfsmannastjóri í tilfelli launa- og mannauðskerfis, fjármálastjóri í tilfelli fjárhagskerfis.

Skráður aðili: Einstaklingur sem viðkomandi persónuupplýsingar eiga við um.

UT deild: Upplýsingatæknideild. Sú deild eða starfsmenn fyrirtækis sem bera ábyrgð á tölvukerfum og búnaði til geymslu og vinnslu upplýsinga. Þegar rekstri og umsjón tölvumála er útvistað er UT deild þjónustuaðilinn.

Persónuverndaryfirlýsing til umsækjenda um störf

Varðandi umsókn þína, mun Ísfélag Vestmannaeyja hf., sem ábyrgðaraðili, safna og vinna með persónugreinanlegar upplýsingar þínar í þeim tilgangi sem tilgreindur er hér að neðan. Vinsamlegast kynntu þér vel eftirfarandi atriði til þess að skilja hvernig við vinnum með persónuupplýsingar þínar.

Hvaða gögnum söfnum við um þig og í hvaða tilgangi?

Við söfnum og vinnum eftirfarandi persónuupplýsingar til þess að meðhöndla umsókn þína og annað tengt ráðningarferlinu og fyrir aðrar stöður innan Ísfélags Vestmannaeyja (ef samþykki hefur verið veitt):

- Nafni; fæðingardegi, netfangi, heimilisfangi, dvalarlandi, símanúmeri, mynd, upplýsingum um fyrri atvinnu og menntun og öðrum upplýsingum sem koma fram í ferilskrá, prófskírteini og öðrum skjölum sem þú hefur útvegað okkur, upplýsingum um meðmælendur, prófniðurstöður og innra mat sem fer fram á þér í tengslum við umsóknina.

Persónusnið: Engin sjálfvirk gagnavinnsla fer fram í tengslum við ráðningarferli hjá Ísfélagi Vestmannaeyja.

Lagalegur grundvöllur fyrir vinnslu: Söfnun og vinnsla persónuupplýsinga þinna er byggð á gildandi persónuverndarlöggjöf.

Frá hverjum söfnum við þínum persónuupplýsingum?: Upplýsingunum er safnað frá þér og eftir atvikum í gegnum umsagnaraðila sem þú bendir okkur á.

Hvert flytjum við gögnin þín?: Við gætum flutt gögnin þín, í tengslum við þau atriði sem nefnd eru hér að ofan, til umsýslu upplýsingakerfa og umsýslu skýlausna sem vinna með eða geyma persónuupplýsingarnar fyrir okkur.

Hversu lengi geymum við persónuupplýsingar um þig?: Við geymum persónuupplýsingarnar svo lengi sem við teljum nauðsynlegt til að uppfylla þann tilgang sem nefndur er hér að ofan, þó ekki lengur en 6 mánuði.

Réttindi þín: Þú nýtur eftirfarandi réttinda samkvæmt lögum um persónuvernd:

- Að hafa aðgang að persónuupplýsingunum.
- Að láta leiðrétta eða eyða persónuupplýsingum.
- Að láta takmarka vinnslu með persónuupplýsingar.
- Að draga til baka samþykki hvenær sem er.
- Að andmæla vinnslu persónuupplýsinga.
- Þú hefur einnig rétt til þess að leggja fram kvörtun hjá eftirlitsfirvaldi sjáir þú ástæðu til þess.

Frekari upplýsingar: Vinsamlegast hafðu samband við okkur í gegnum personuvernd@isfelag.is ef þú hefur einhverjar spurningar varðandi vernd persónuupplýsinga þinna eða ef þú vilt nýta þér lagaleg réttindi þín.

Privacy notice to applicants

In connection with your application, Ísfélag Vestmannaeyja will, as the data controller, collect and process personal data about you for the purposes specified below. Therefore, please read this text carefully in order to understand how we process your personal data.

Which data do we collect about you and for which purposes?

We collect and process the following types of personal data for the purpose of handling your application and related recruitment activities hereto; for other positions within Ísfélag Vestmannaeyja (if you have given consent hereto):

- Your name, date of birth, e-mail address, home address, country of residence, telephone number, photo, employment and education details and other information provided by you in your CV, diploma or any other documents disclosed by you to us, contact details on referees, test results and internal candidate evaluations carried out in connection your application process.

Profiling: No automatic data processing occurs regarding the recruitment process at Ísfélag Vestmannaeyja.

Legal basis of processing: Collection and processing of your personal data is based on the applicable data protection regulation.

From whom do we collect your personal data?: The personal data is collected from you or references given by you to us. We collect and process your data as it is necessary for the performance of a contract, or in order to take steps at your request prior to entering into a contract.

To whom do we transfer your personal data?: We may transfer your personal data to system providers, including cloud service providers who process or store your personal data on our behalf.

How long do we store your data?: We store your personal data for as long as necessary to fulfil the purposes above, however, for no longer than 6 months.

Your rights: Subject to the conditions set out in the applicable data protection legislation, you enjoy the following rights:

- The right to request access to the personal data registered of you
- The right to rectification and erasure the personal data
- The right to restriction of processing
- The right to withdraw your consent at any time
- The right to objection to the processing of your personal data
- You also have the right to lodge a complaint with the competent supervisory authority.

Contact Details: Please contact us at personuvernd@isfelag.is, if you have any questions in regards to the protection of your personal data or if you wish to exercise your legal rights.

Bréf til starfsmanna vegna persónuverndarlöggjafar

Ný persónuverndarlöggjöf sem hefur tekið gildi á Íslandi gerir strangar kröfur til þeirra aðila sem meðhöndla persónuupplýsingar og mögulegar stjórnvaldssektir geta numið háum fjárhæðum. Það er lykilatriði að við vinnum öll saman að því að standa vörð um persónuvernd þeirra einstaklinga sem við meðhöndlum upplýsingar um, hvort sem það eru viðskiptavinir, samstarfsmenn eða aðrir einstaklingar.

Nýju löggin skilgreina persónuupplýsingar sem hvers kyns upplýsingar um 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.

Löggin leggja bann við vinnslu ákveðinna flokka persónuupplýsinga, nema að ákveðnum skilyrðum uppfylltum. Það felur í sér skilgreiningu á því hvað teljast vera viðkvæmar persónuupplýsingar, en það eru upplýsingar er varða kynþátt eða þjóðernislegan uppruna, stjórnmalaskoðanir, trúarbrögð eða heimspekilega sannfæringu, aðild að verkalýðsfélagi og vinnslu erfðafræðilegra upplýsinga, lífkennaupplýsinga í því skyni að persónugera einstakling með einkvæmum hætti, heilsufarsupplýsingar eða upplýsingar er varða kynlíf eða kynhneigð.

Hér eru því nokkur mikilvæg atriði sem hafa þarf í huga:

- Við berum ábyrgð á þeim gögnum sem við öflum í starfi okkar.
- Miklar kröfur eru gerðar um tilkynningar og gagnsæi til þeirra einstaklinga sem vinnslan nær yfir.
- Réttindi einstaklinga skv. löggjöfinni eru ýmis, t.d. að óska eftir aðgengi, leiðréttingu, takmörkun, afriti og eyðingu á persónulegum upplýsingum. Mikilvægt er að allar beiðnir sem berast séu sendar á netfangið personuvernd@isfelag.is. Reynt er að bregðast við beiðni frá skráðum einstaklingum innan 30 daga.
- Brestur á öryggi sem leiðir til óviljandi eða ólögumætrar eyðingar persónuupplýsinga eða þess að þær glattist, verði birtar eða aðgangur verði veittur að þeim í leyfisleysi skal tilkynntur strax til personuvernd@isfelag.is. Þó að þið séuð ekki viss hvort það hafi orðið brestur eða ekki, viljum við að það sé tilkynnt.