Persónuverndarstefna Securitas hf.

1. Inngangur

Persónuverndarstefna þessi („**persónuverndarstefnan**“) skýrir hvernig Securitas („**fyrirtækið**“ eða „**við**“) meðhöndlar og að öðru leyti vinnur persónuupplýsingar starfsmanna sinna, viðskiptavina, verktaka og annarra einstaklinga, eins og við á hverju sinni, hvort heldur sem er í hlutverki ábyrgðaraðila eða vinnsluaðila.

Persónuverndarstefnan gildir um allar persónuupplýsingar sem við vinnum, óháð því á hvaða miðli upplýsingarnar eru geymdar og óháð því hvort þær tengjast fyrrum eða núverandi starfsmönnum, verktökum, viðskiptavinum, umbjóðendum, byrgjum, hluthöfum, notendum vefsíðu eða öðrum skráðum einstaklingum.

2. Skilgreiningar

Nafn fyrirtækis: Securitas hf., Skeifunni 8, 108 Reykjavík; sími: 580 700; netfang: securitas@securitas.is; veffang: www.securitas.is.

Starfsmenn fyrirtækisins: Allir starfsmenn, stjórnendur, verktakar, ráðgjafar og aðrir, sem vinna í þágu og/eða koma fram fyrir hönd fyrirtækisins.

Ábyrgðaraðili: Aðili, sem ákveður tilgang og aðferðir við vinnslu persónuupplýsinga.

Vinnsluaðili: Aðili, sem vinnur persónuupplýsingar á vegum ábyrgðaraðila.

Persónuupplýsingar: Sérhverjar persónugreinanlegar upplýsingar um skráðan einstakling eða upplýsingar sem hægt er að nota til að persónugreina hann, beint eða óbeint, af upplýsingunum einum og sér eða með frekari gögnum, sem eru í vörslu fyrirtækisins eða sem fyrirtækið getur auðveldlega nálgast. Viðkvæmar persónuupplýsingar teljast einnig til persónuupplýsinga, ásamt persónuupplýsingum þar sem beitt hefur verið gerviauðkenni. Hins vegar teljast nafnlausar upplýsingar ekki til persónuupplýsinga eða þegar tilvísun til einstaklingsins hefur verið endanlega fjarlægð úr skrám. Persónuupplýsingar geta verið staðreyndir (t.d. nafn, tölvupóstur, staðsetningargögn eða fæðingardagur) eða skoðun á aðgerðum eða hegðun hins skráða. Dæmi um persónuupplýsingar eru nafn einstaklings, kennitala, heimilisfang, netauðkenni, starfskjör, viðskiptahegðun, einn eða fleiri þættir sem einkenna einstakling í líkamlegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti og aðrar sambærilegar upplýsingar, sem teljast til persónuupplýsinga samkvæmt persónuverndarlögum.

Viðkvæmar persónuupplýsingar: Upplýsingar um kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir, heimspekilega sannfæringu (þ.m.t. trúarbrögð) eða aðild að stéttarfélagi, líkamlegt eða andlegt heilbrigði, kynlíf og kynhneigð, erfðafræðilegar upplýsingar og lífkennaupplýsingar, ásamt persónuupplýsingum er varða sakfellingu í refsimálum og refsiverð brot.

Skráður einstaklingur (eða „hinn skráði“): Tilgreindur eða persónugreinanlegur einstaklingur, sem persónuupplýsingarnar varða. Hinn skráði einstaklingur getur verið ríkisborgari eða með heimilisfesti í hvaða landi sem er og kann að eiga tiltekin réttindi er varða persónuupplýsingar sínar.

Samþykki: Óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða um að hann samþykki, með yfirlýsingu eða ótvíræðri staðfestingu, vinnslu persónuupplýsinga um sig.

Afdráttarlaust samþykki: Samþykki sem krefst skýrrar og sértækrar viljayfirlýsingar (þ.e.a.s. ekki aðeins staðfestingar).

Sjálfvirk einstaklingsmiðuð ákvarðanataka (SEÁ): Þegar ákvörðun er tekin eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerð persónusniðs, sem hefur réttaráhrif að því er skráðan einstakling varðar eða snertir hann á sambærilegan hátt að verulegu leyti.

Vinnsla: Sérhver athöfn þar sem persónuupplýsingar eru notaðar, þ.m.t. söfnun, skráning eða varðveisla upplýsinganna, ásamt sérhverri aðgerð eða röð aðgerða þar sem unnið er með upplýsingarnar, þ.m.t. flokkun, breyting, heimt, notkun, miðlun, eyðing eða eyðilegging, sem og miðlun upplýsinganna til þriðja aðila.

Sjálfvirk gagnavinnsla: Sérhver sjálfvirk vinnsla persónuupplýsinga til að meta ákveðna þætti er varða hagi einstaklings, einkum að greina eða spá fyrir um þætti er varða frammistöðu hans í starfi, fjárhagsstöðu, heilsu, smekk, áhugamál, áreiðanleika, hegðun, staðsetningu eða hreyfanleika. Gerð persónusniðs er dæmi um sjálfvirka gagnavinnslu.

Gerviauðkenni og notkun gerviauðkenna: Þegar unnið er með persónuupplýsingar á þann hátt að ekki er lengur hægt að rekja þær til tiltekins skráðs einstaklings án viðbótarupplýsinga, að því tilskildu að slíkum viðbótarupplýsingum sé haldið aðgreindum og að beitt sé tæknilegum og skipulagslegum ráðstöfunum til að tryggja að persónuupplýsingarnar sé ekki hægt að rekja til persónugreinds eða persónugreinanlegs einstaklings.

Öryggisbrot við vinnslu persónuupplýsinga: Sérhver aðgerð eða aðgerðarleysi sem leggur í hættu öryggi, trúnað, heilleika eða aðgengi að persónuupplýsingum eða verklegum, tæknilegum, reglubundnum eða skipulagslegum öryggisráðstöfunum sem fyrirtækið eða þjónustuaðilar þess hafa komið upp til að vernda persónuupplýsingarnar. Brot, sem leiðir til þess að persónuupplýsingar glatist, breytist, verði birtar eða aðgangur veittur af þeim í leyfisleysi, telst vera öryggisbrot við vinnslu persónuupplýsinga.

Mat á áhrifum á persónuvernd: Mat, sem er ætlað að auðkenna og draga úr áhættuþáttum við vinnslu persónuupplýsinga. Mat á áhrifum á persónuvernd getur verið framkvæmt sem hluti af innbyggðri persónuvernd og skal mat á áhrifum á persónuvernd vera framkvæmt á öllum meiri háttar kerfum eða á öllum meiri háttar breytingum fyrirtækisins á vinnslu persónuupplýsinga.

Innbyggð persónuvernd: Þegar viðeigandi tæknilegar og skipulagslegar ráðstafanir hafa verið gerðar til að standast kröfur persónuverndarlaga um innbyggða persónuvernd.

Persónuverndarlög: Lög um persónuvernd og vinnslu persónuupplýsinga sem í gildi eru á hverjum tíma, ásamt öðrum réttarheimildum, sem byggjast á þeim.

Persónuverndarfulltrúi: Fulltrúi, sem við höfum skipað á grundvelli persónuverndarlaga. Ef persónuverndarfulltrúi hefur ekki verið skipaður, er hér átt við þann starfsmann eða það teymi sem ber ábyrgð á persónuverndarmálum hjá okkur.

EES: Ríki evrópska efnahagsvæðisins, þ.e. 28 ríki Evrópusambandsins, Ísland, Liechtenstein og Noregur.

3. Gildissvið

Vönduð og lögmæt vinnsla persónuupplýsinga er órjúfanlegur hluti af starfsemi okkar.

Allir starfsmenn fyrirtækisins eru þátttakendur í persónuverndarstefnu okkar og höfum við innleitt viðeigandi verkferla, aðferðir, þjálfun, öryggisþætti og aðra þætti með það að markmiði að tryggja fylgni við persónuverndarstefnuna.

4. Meginreglur um vinnslu persónuupplýsinga

Við fylgjum meginreglum um vinnslu persónuupplýsinga í samræmi við persónuverndarlög, en þar segir að persónuupplýsingar skuli vera:

a) Unnar með lögmætum, sanngjörnum og gagnsæjum hætti („lögmæti, sanngirni og gagnsæi“).

b) Fengnar í skýrt tilgreindum, lögmætum og málefnalegum tilgangi („takmörkun vegna tilgangs“).

c) Nægilegar, viðeigandi og takmarkast við það sem nauðsynlegt er miðað við tilganginn með vinnslunni („lágmörkun gagna“).

d) Áreiðanlegar og ef nauðsyn krefur, uppfærðar („áreiðanleiki“).

e) Varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf er á miðað við tilgang vinnslunnar („geymslutakmörkun“).

f) Unnar með þeim hætti að viðeigandi öryggi persónuupplýsinganna sé tryggt, þ.m.t. vernd gegn óleyfilegri eða ólögmætri vinnslu og gegn glötun, eyðileggingu eða tjóni fyrir slysni, með viðeigandi tæknilegum og skipulagslegum ráðstöfunum („heilleiki og trúnaður“).

g) Eingöngu miðlað til annara landa ef fullnægjandi verndarráðstafanir eru til staðar („takmörkun á miðlun“).

h) Gerðar aðgengilegar hinum skráða einstaklingi og honum gert kleift að beita rétti sínum hvað persónuupplýsingar hans varðar („réttindi hins skráða“).

Við erum ábyrg fyrir því að farið sé eftir meginreglunum hér að ofan og þurfum að geta sýnt fram á það („ábyrgðarskylda“).

5. Lögmæti, sanngirni og gagnsæi

5.1 Lögmæti og sanngirni

Persónuupplýsingar skulu vera unnar með lögmætum, sanngjörnum og gagnsæjum hætti gagnvart skráðum einstaklingi.

Okkur er aðeins heimilt að afla, vinna og deila persónuupplýsingum á sanngjarnan og lögmætan hátt og aðeins í sérstaklega tilgreindum tilgangi. Persónuverndarlög takmarka hvernig persónuupplýsingar skulu meðhöndlaðar. Þessar takmarkanir koma ekki í veg fyrir vinnslu persónuupplýsinga, heldur sjá þær til þess að við vinnum persónuupplýsingar á sanngjarnan hátt, án þess að vinnslan hafi neikvæð áhrif á hinn skráða einstakling.

Persónuverndarlög heimila aðeins vinnslu, ef a.m.k. eitt af eftirfarandi skilyrðum er uppfyllt:

a) Skráður einstaklingur hefur gefið samþykki sitt fyrir vinnslunni;

b) vinnslan er nauðsynleg vegna framkvæmdar samnings, sem skráður einstaklingur á aðild að;

c) vinnslan er nauðsynleg til að uppfylla lagaskyldu, sem hvílir á fyrirtækinu;

d) vinnslan er nauðsynleg til að vernda brýna hagsmuni hins skráða einstaklings eða

e) vinnslan er nauðsynleg vegna lögmætra hagsmuna okkar og hagsmunir eða grundvallarréttindi og frelsi hins skráða, sem krefjast verndar persónuupplýsinga, vega ekki þyngra.

Þá skilgreinum við og skjalfestum grundvöll fyrir vinnslu hvers vinnsluþáttar persónuupplýsinga í starfsemi okkar.

5.2 Samþykki

Sem ábyrgðaraðili er okkur aðeins heimilt að vinna persónuupplýsingar á grundvelli skýrra heimilda persónuverndarlaga, þ.m.t. á grundvelli samþykkis.

Skráður einstaklingur er talinn samþykkja vinnslu persónuupplýsinga, ef hann gefur til kynna með skýrum hætti, með viljayfirlýsingu eða annarri athöfn, að hann samþykki vinnsluna.

Samþykki þarfnast skýrrar athafnar. Þar af leiðandi fela þögn, reitir sem þegar er búið að haka við eða aðgerðaleysi því ekki í sér samþykki. Ef hinn skráði gefur samþykki sitt með skriflegri yfirlýsingu, sem einnig varðar önnur málefni, skal beiðnin um samþykki sett fram á þann hátt að hún sé auðgreinanleg frá hinum málefnunum, á skiljanlegu og aðgengilegu formi og skýru og einföldu máli.

Skráður einstaklingur á rétt á að draga samþykki sitt til baka hvenær sem er og skal fyrirtækið verða við slíkri beiðni svo fljótt sem auðið er.

Samþykki gæti þurft að vera endurnýjað ef við hyggjumst vinna persónuupplýsingar í nýjum og ósamrýmanlegum tilgangi, sem ekki var tilgreindur þegar hinn skráði einstaklingur gaf samþykki sitt í upphafi. Að því gefnu að við getum ekki stuðst við aðra heimild til vinnslu, er afdráttarlaust samþykki almennt notað sem grundvöllur vinnslu viðkvæmra persónuupplýsinga, sjálfvirkrar einstaklingsmiðaðrar ákvörðunartöku og miðlunar persónuupplýsinga yfir landamæri.

Yfirleitt styðjumst við aðrar heimildir við vinnslu flestra tegunda viðkvæmra persónuupplýsinga (og þurfum þar af leiðandi ekki afdráttarlaust samþykki). Þegar afdráttarlauss samþykkis er krafist, munum við tryggja að samþykkið sé að fullu í samræmi við ákvæði persónuverndarlaga.

Okkur ber ávallt að afla sönnunar á því að samþykkis hafi verið aflað og halda skrár um öll veitt samþykki, svo að við getum sýnt fram á að kröfum persónuverndalaga sé gætt, hvað samþykki varðar.

5.3 Gagnsæi (tilkynningar til hins skráða)

Persónuverndarlög krefjast þess að ábyrgðaraðili útskýri fyrir hinum skráða einstaklingi með ítarlegum hætti hvaðan persónuupplýsingum er safnað, m.a. hvort persónuupplýsingum hafi verið aflað frá hinum skráða einstaklingi eða frá þriðja aðila. Við munum koma slíkum útskýringum til skila með viðeigandi hætti, á aðgengilegu formi og á skýru og einföldu máli svo hinn skráði einstaklingur geti auðveldlega skilið þær.

Þegar við söfnum persónuupplýsingum beint frá hinum skráða einstaklingi, þ.m.t. vegna mannauðs- eða starfsmannamála, látum við hinum skráðum einstaklingi í té allar þær upplýsingar sem persónuverndarlög krefjast, þ.m.t. heiti og samskiptaupplýsingar ábyrgðaraðila og persónuverndarfulltrúa, hvernig og af hverju við vinnum, miðlum, verndum og geymum tilteknar persónuupplýsingar. Er þetta kynnt hinum skráða einstaklingi þegar hann veitir okkur persónuupplýsingarnar við upphaf vinnslu.

Þegar persónuupplýsingum er safnað með óbeinum hætti (t.d. þegar upplýsingar eru fengnar frá þriðja aðila eða þeim er aflað af miðli sem er aðgengilegur almenningi), látum við hinum skráða einstaklingi í té allar þær upplýsingar sem persónuverndarlög krefjast eins fljótt og auðið er eftir að upplýsinganna er aflað. Þá gætum við þess að þriðji aðilinn hafi safnað upplýsingunum í samræmi við persónuverndarlög og á grundvelli, sem samræmist fyrirhugaðri vinnslu okkar á persónuupplýsingunum.

6. Takmörkun vegna tilgangs

Persónuupplýsingar skulu aðeins vera fengnar í skýrt tilgreindum og lögmætum tilgangi. Þær skulu ekki vera unnar frekar á þann hátt að ósamrýmanlegt sé þeim tilgangi.

Okkur er óheimilt að nota persónuupplýsingar í nýjum, ólíkum eða ósamrýmanlegum tilgangi við þann, sem upphaflega var gert ráð fyrir, nema við höfum tilkynnt hinum skráða einstaklingi um hinn nýja tilgang og hann hefur gefið samþykki sitt fyrir slíkri breyttri vinnslu (sé öflun samþykkis nauðsynleg).

7. Lágmörkun persónuupplýsinga

Persónuupplýsingar skulu vera nægilegar, viðeignandi og takmarkast við það sem nauðsynlegt er miðað við tilgang vinnslunnar.

Okkur er aðeins heimilt að afla persónuupplýsinga sem eru nauðsynlegar og ekki safna meiri upplýsingum en þörf er á. Við gætum þess að allar persónuupplýsingar, sem safnað er, séu nægjanlegar og viðeigandi miðað við tilgang vinnslunnar.

Okkur ber að gæta þess að eyða persónuupplýsingum eða gera þær ópersónugreinanlegar þegar ekki er lengur þörf á persónuupplýsingunum vegna tilgangs vinnslunnar.

8. Áreiðanleiki

Persónuupplýsingar skulu vera áreiðanlegar og, ef nauðsyn krefur, uppfærðar. Tryggja skal að persónuupplýsingar, sem eru óáreiðanlegar, verði eytt eða þær leiðréttar án tafar.

Okkur ber að gæta þess að persónuupplýsingar, sem við búum yfir, séu áreiðanlegar, réttar, uppfærðar og viðeigandi miðað við tilgang vinnslunnar.

Við athugum áreiðanleika persónuupplýsinganna þegar þeim er aflað og með reglulegu millibili eftir öflun. Við gerum viðeigandi ráðstafanir til að eyða eða lagfæra óáreiðanlegum eða óuppfærðum persónuupplýsingum.

9. Geymslutakmörkun

Persónuupplýsingar skulu varðveittar á því formi að ekki sé unnt að persónugreina skráða einstaklinga lengur en þörf krefur, miðað við tilganginn með vinnslu upplýsinganna.

Okkur er óheimilt að varðveita persónuupplýsingar á formi þar sem unnt er að persónugreina skráða einstaklinga lengur en þörf er á miðað við upphaflegan tilgang vinnslunnar.

Við fylgjum stefnu um varðveislu gagna, til að stuðla að því að persónuupplýsingum sé eytt eftir hæfilegan tíma miðað við tilgang varðveislunnar, nema lög krefjist þess að slíkar upplýsingar séu varðveittar í lengri tíma.

Við gerum viðeigandi ráðstafanir til að eyða öllum persónuupplýsingum, sem ekki er lengur þörf á í samræmi við viðeigandi lög, verkferla og stefnu fyrirtækisins.

Við gætum þess að hinum skráða einstaklingi sé tilkynnt um hversu lengi upplýsingar eru geymdar og hvernig lengd þess tíma er ákveðin.

10. Heilleiki og trúnaður

10.1 Öryggi persónuupplýsinga

Við tryggjum viðeigandi öryggi persónuupplýsinga, þ.m.t. með vernd gegn óleyfilegri eða ólögmætri vinnslu og gegn glötun, eyðileggingu eða tjóni fyrir slysni, með viðeigandi tæknilegum og skipulagslegum ráðstöfunum.

Við höfum innleitt persónuverndarráðstafanir, sem eru hæfilegar miðað við stærð, eðli og rekstur fyrirtækisins, magn og eðli persónuupplýsinga, sem við eigum eða vinnum fyrir hönd annarra og áhættu (þ.m.t. með notkun dulkóðunar og gerviauðkenna þegar við á). Til að tryggja öryggi vinnslunnar, höfum við til staðar viðeigandi ferla, sem eru prófaðir reglulega.

Við kunnum að miðla persónuupplýsingum til þriðja aðila, sé um að ræða þjónustuaðila sem hefur samþykkt viðeigandi stefnur og ferla, hefur samþykkt að gera viðeigandi verndarráðstafanir og að öðru leyti uppfyllir skilyrði ábyrgs vinnsluaðila.

Við gætum að gagnaöryggi með því að tryggja trúnað, heilleika og aðgengi að persónuupplýsingum með eftirfarandi hætti:

a) Með trúnaði er átt við að aðgengi að persónuupplýsingum er takmarkað við þá aðila, sem þurfa að nota upplýsingarnar og hafa heimild til þess.

b) Með heilleika er átt við að persónuupplýsingarnar eru nákvæmar og eiga við tilgang vinnslunnar.

c) Með aðgengi er átt við að þeim, sem er heimilt að nota persónuupplýsingarnar, sé tryggður aðgangur að persónuupplýsingunum þegar þeir þurfa á þeim að halda í lögmætum tilgangi.

10.2 Tilkynning um öryggisbrot við vinnslu persónuupplýsinga

Persónuverndarlög krefjast þess að ábyrgðaraðili tilkynni sérhvert öryggisbrot við vinnslu persónuupplýsinga til eftirlitsyfirvalda. Í ákveðnum tilvikum skal ábyrgðaraðili jafnframt tilkynna skráðum einstaklingum um öryggisbrot. Þá ber vinnsluaðila að tilkynna ábyrgðaraðila um öryggisbrot, sem verða við vinnslu vinnsluaðila.

Við höfum komið upp ferlum um hvernig skal meðhöndla möguleg öryggisbrot við vinnslu persónuupplýsinga og munum við tilkynna viðeigandi eftirlitsyfirvöldum, skráðum einstaklingum og ábyrgðaraðilum um öryggisbrot eins og lög mæla fyrir um.

11. Takmörkun á miðlun persónuupplýsinga út fyrir EES

Persónuverndarlög takmarka miðlun persónuupplýsinga út fyrir EES til þess að tryggja viðeignandi persónuvernd einstaklinga. Miðlun persónuupplýsinga yfir landamæri er talin eiga sér stað þegar persónuupplýsingar frá einu landi eru fluttar, sendar, skoðaðar eða með öðrum hætti eru gerðar aðgengilegar í öðru landi. Okkur er aðeins heimilt að flytja persónuupplýsingar út fyrir EES með slíkum hætti, ef a.m.k. eitt af eftirfarandi skilyrðum er uppfyllt:

a) Þegar framkvæmdastjórn Evrópusambandsins hefur ákveðið að þriðja landið tryggi fullnægjandi vernd;

b) viðeigandi verndarráðstafanir eru til staðar, svo sem bindandi fyrirtækjareglur, stöðluð ákvæði um persónuvernd, sem eftirlitsyfirvald hefur samþykkt og framkvæmdastjórn Evrópusambandsins viðurkennt, viðurkenndar hátternisreglur eða viðurkennt vottunarkerfi;

c) hinn skráði einstaklingur hefur verið upplýstur um mögulega áhættu slíks flutnings og hefur gefið afdráttarlaust samþykki sitt fyrir flutningnum eða

d) miðlunin er nauðsynleg vegna annara tilvika, sem skapa heimild til miðlunar samkvæmt persónuverndarlögum, þ.m.t. til að efna samning milli fyrirtækisins og hins skráða, vegna almannahagsmuna, til að stofna, hafa uppi eða verja réttarkröfur, til að verja hagsmuni hins skráða, ef hann er ekki sjálfur fær um að gefa samþykki sitt og í afmörkuðum tilvikum vegna lögmætra hagsmuna fyrirtækisins og

e) sú vinnsla sem felst í slíkum flutningi persónuupplýsinga að öðru leyti samræmist ákvæðum persónuverndarlaga.

12. Réttindi hins skráða

Við meðferð fyrirtækisins á persónuupplýsingum ber okkur að gæta að réttindum hins skráða einstaklings. Skráður einstaklingur hefur m.a. rétt á að:

a) Draga samþykki sitt til baka hvenær sem er;

b) fá tilteknar upplýsingar um vinnslu ábyrgðaraðila á persónuupplýsingum sínum;

c) óska eftir aðgangi að þeim persónuupplýsingum, sem við vinnum um hann;

d) andmæla vinnslu persónuupplýsinga til beinnar markaðssetningar;

e) óska eftir að persónuupplýsingum sé eytt, ef þær eru ekki lengur nauðsynlegar í þeim tilgangi sem lá að baki söfnun eða annarri vinnslu þeirra, að óáreiðanlegar persónuupplýsingar verði leiðréttar eða ófullkomnar persónuupplýsingar verði fullgerðar;

f) takmarka vinnslu í ákveðnum tilvikum;

g) andmæla vinnslu, sem hefur verið réttlætt á grundvelli lögmætra hagsmuna eða almannahagsmuna;

h) óska eftir afriti af samningum, þar sem persónuupplýsingum hans er miðlað út fyrir EES;

i) andmæla ákvörðun, sem er tekin eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerð persónusniðs og SEÁ;

j) koma í veg fyrir vinnslu, sem er líkleg til að skaða eða er íþyngjandi fyrir hinn skráða einstakling eða annan aðila;

k) vera gert viðvart um öryggisbrot á vinnslu persónuupplýsinga, sem líklegt er að leiði af sér mikla hættu fyrir réttindi og frelsi hans;

l) beina kvörtun til eftirlitsyfirvalda og

m) í viðeigandi tilvikum, óska eftir að fá persónuupplýsingar er varða hann sjálfan, á skipulegu, algengu, tölvulesanlegu sniði eða að senda þessar upplýsingar til annars ábyrgðaraðila.

Við sannreynum deili á skráðum einstaklingi, sem óskar eftir aðgangi að persónuupplýsingum á grundvelli ofangreindra réttinda.

13. Ábyrgð

13.1 Ráðstafanir

Við höfum til staðar viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að farið sé eftir meginreglum um vinnslu persónuupplýsinga.

Til að standast kröfur persónuverndarlaga, ber fyrirtækinu að hafa til staðar og skjalfesta viðeigandi úrræði og ráðstafanir, þ.m.t. með því að:

a) Skipa hæfan persónuverndarfulltrúa (sé slíkt nauðsynlegt) og framkvæmdastjóra sem er ábyrgur fyrir persónuverndarmálum;

b) styðjast við innbyggða persónuvernd þegar unnið er með persónuupplýsingar og framkvæma mat á áhrifum á persónuvernd þegar vinnsla er líkleg til að hafa í för með sér mikla áhættu fyrir réttindi og frelsi hins skráða einstaklings;

c) innleiða persónuvernd í starfsemi fyrirtækisins, þ.m.t. með persónuverndarstefnu þessari, tengdum stefnum, leiðbeiningum, skilmálum og tilkynningum;

d) reglulega þjálfa starfsmenn fyrirtækisins um persónuverndarlög, persónuverndarstefnu, tengdar stefnur og persónuverndarleiðbeiningar og um önnur persónuverndarmál, t.d. réttindi hins skráða einstaklings, samþykki, heimild til vinnslu, mat á áhrifum um persónuvernd og öryggisbrot við vinnslu persónuupplýsinga og

e) reglulega prófa og endurskoða þær ráðstafanir sem gerðar hafa verið til að stuðla að réttri persónuvernd, til að meta hvort allar kröfur um persónuvernd séu uppfylltar.

13.2 Skjölun

Við skjalfestum með nákvæmum hætti vinnslu persónuupplýsinga, að því marki sem slíkrar skráningar er krafist samkvæmt persónuverndarlögum. Við höldum skrá yfir vinnslustarfsemi okkar, þ.m.t. skrá yfir samþykki hinna skráðu einstaklinga og hvernig samþykkis er aflað. Í skránni kemur m.a. fram heiti og samskiptaupplýsingar ábyrgðaraðila og persónuverndarfulltrúa (ef hann hefur verið skipaður), tilgangur vinnslunnar, lýsing á flokkum skráðra einstaklinga og flokkum persónuupplýsinga, flokkar viðtakenda, sem fengið hafa eða munu fá persónuupplýsingar í hendur, hvar persónuupplýsingarnar eru geymdar, miðlun persónuupplýsinga, fyrirhuguð tímamörk varðandi eyðingu persónuupplýsinga og almenn lýsing á öryggisráðstöfunum. Til að útbúa slíkar skrár er nauðsynlegt að persónuupplýsingar séu skráðar með þeim hætti að fram komi allar þær upplýsingar, sem hér að ofan greinir, ásamt því að flæði persónuupplýsinganna sé skýrt.

13.3 Þjálfun og endurskoðun

Fyrirtækið sér starfsmönnum fyrir fullnægjandi þjálfun þannig að þeim sé kleift að fylgja persónuverndarlögum. Fyrirtækið prófar kerfi og ferla fyrirtækisins til að meta hvort kröfum persónuverndarlaga sé mætt og hvort til staðar séu nægjanlegar varnir og hvort úrræði séu í boði til að gætt sé að notkun og vernd persónuupplýsinga með fullnægjandi hætti.

13.4 Innbyggð persónuvernd og mat á áhrifum á persónuvernd

Fyrirtækinu ber að gera viðeigandi tæknilegar og skipulagslegar ráðstafanir, sem skulu vera gerðar til að framfylgja meginreglum um persónuvernd og fella nauðsynlegar verndarráðstafanir inn í vinnslu persónuupplýsinga með skilvirkum hætti (innbyggð persónuvernd), t.d. með notkun gerviauðkenna.

Fyrirtækið hefur metið með hvaða hætti unnt er að tryggja innbyggða persónuvernd í öllum forritum, kerfum og ferlum, sem eru notuð til að vinna persónuupplýsingar með hliðsjón af:

a) Nýjustu tækni;

b) kostnaði við framkvæmd;

c) eðli, umfangi, samhengi og tilgangi vinnslunnar og

d) mislíklegri og misalvarlegri áhættu af vinnslunni fyrir réttindi og frelsi hins skráða einstaklings.

Fyrirtækið mun einnig framkvæma mat á áhrifum á persónuvernd, sé um að ræða áhættusama vinnslu í skilningi persónuverndarlaga, þ.m.t. við:

a) Beitingu nýrrar tækni eða breyttrar tækni (forrit, kerfi eða ferlar í hvoru tilviki fyrir sig);

b) sjálfvirka gagnavinnslu, þ.m.t. gerð persónusniða og við SEÁ;

c) umfangsmikla vinnslu viðkvæmra persónuupplýsinga eða

d) kerfisbundið og umfangsmikið eftirlit með svæði sem er aðgengilegt almenningi.

Mat á áhrifum á persónuvernd skal fela í sér:

a) Lýsingu á fyrirhuguðum vinnsluaðgerðum og tilganginum með vinnslunni, þ.m.t. eftir atvikum lögmætum hagsmunum ábyrgðaraðilans;

b) mat á því hvort vinnsluaðgerðirnar eru nauðsynlegar og hóflegar miðað við tilganginn með þeim;

c) mat á áhættu fyrir réttindi og frelsi skráðra einstaklinga og

d) ráðstafanir sem fyrirhugað er að grípa til gegn slíkri áhættu og fyrirkomulag við að tryggja vernd persónuupplýsinga og sýna fram á að farið sé að persónuverndarlögum.

13.5 Sjálfvirk vinnsla (þ.m.t. gerð persónusniða) og sjálfvirk einstaklingsmiðuð ákvarðanataka

Almennt er SEÁ óheimil ef hún hefur réttaráhrif að því er varðar hinn skráða einstakling eða snertir hann á sambærilegan hátt að verulegu leyti, nema ákvörðunin:

a) Byggist á afdráttarlausu samþykki hins skráða;

b) er heimiluð í lögum eða

c) er forsenda þess að unnt sé að gera eða framkvæma samning við hinn skráða einstakling.

Sé ákvörðun tekin, sem byggir á sjálfvirkri gagnavinnslu (þ.m.t. gerð persónusniða), ber fyrirtækinu að gera hinum skráða einstaklingi grein fyrir andmælarétti sínum í síðasta lagi þegar fyrst er haft samband við hann. Skal rétturinn vera settur skýrt fram og aðgreindur frá öðrum upplýsingum. Þess að auki skal gera viðeigandi ráðstafanir til að vernda réttindi og frelsi og lögmæta hagsmuni hins skráða.

Fyrirtækinu ber einnig að gera hinum skráða einstaklingi grein fyrir þeirri aðferðafræði, sem er beitt í ákvörðunartökunni eða gerð persónusniðsins, mikilvægi og fyrirhuguðum áhrifum, ásamt því að gefa hinum skráða einstaklingi rétt til íhlutunar, að láta skoðun sína í ljós og vefengja ákvörðunina.

Mat á áhrifum á persónuvernd mun verða gert áður en sjálfvirk gagnavinnsla (þ.m.t. gerð persónusniðs) eða SEÁ hefst.

13.6 Bein markaðssetning

Okkur ber að fylgja tilteknum reglum þegar við styðjumst við beina markaðsetningu.

Þörf er á fyrirfram samþykki hins skráða þegar stuðst er við beina rafræna markaðssetningu, (t.d. með tölvupósti eða smáskilaboðum). Ekki er þörf á samþykki þegar beinni rafrænni markaðsetningu er beint að núverandi viðskiptavini fyrirtækisins og við höfum þegar aflað samskiptaupplýsinga um hinn skráða í viðskiptum við hann og um er að ræða markaðsetningu á sambærilegum vörum eða þjónustu, ásamt því að við höfum gefið einstaklingum tækifæri á að afþakka markaðssetningunna strax í upphafi þegar við öfluðum upplýsinganna og jafnframt í öllum skilaboðum þar á eftir.

Réttur hins skráða til að andmæla vinnslu í þágu beinnar markaðssetningar skal vera kynntur fyrir honum og skal andmælarétturinn settur skýrt fram og aðgreindur frá öðrum upplýsingum.

Ef hinn skráði andmælir vinnslu í þágu beinnar markaðssetningar, skal vinnslu hætt eins fljótt og auðið er. Ef hinn skráði nýtir þennan rétt sinn, skal ekki vinna persónuupplýsingar frekar í slíkum tilgangi. Vinnslu skal hætt að því marki að einungis sé haldið eftir nægjanlegum upplýsingum til að tryggja að óskir einstaklingsins varðandi markaðssetningu séu virtar í framtíðinni.

13.7 Miðlun persónuupplýsinga

Almennt er okkur óheimilt að miðla persónuupplýsingum, nema gerðar hafi verið viðeigandi verndarráðstafanir og fullnægjandi heimild sé til staðar.

Okkur er aðeins heimilt að miðla persónuupplýsingum til starfsmanna, ef viðtakandi upplýsinganna hefur ástæðu til að öðlast upplýsingarnar vegna starf síns og miðlunin er í samræmi við viðeigandi takmarkanir á miðlun persónuupplýsinga.

Okkur er aðeins heimilt að miðla persónuupplýsingum til þriðju aðila, t.d. til þjónustuveitenda í hlutverki vinnsluaðila okkar, ef:

a) Þeir þurfa nauðsynlega á upplýsingunum að halda til að framfylgja þjónustusamningi;

b) miðlun persónuupplýsinga er í samræmi við persónuverndarskilmála eða tilkynningu, sem birt hefur verið hinum skráða einstaklingi og samþykkt af honum þegar þörf er á samþykki;

c) þriðji aðilinn hefur samþykkt að fylgja nauðsynlegum öryggisstöðlum, stefnum og ferlum og hefur gert viðeigandi öryggisráðstafanir;

d) miðlunin er í samræmi við viðeigandi takmarkanir á miðlun persónuupplýsinga yfir landamæri og

e) fyrir liggur undirritaður, skriflegur samningur sem inniheldur viðurkennd samningsákvæði, sem heimila miðlun til þriðja aðila samkvæmt persónuverndarlögum.

14. Breytingar á persónuverndarstefnu þessari

Við áskiljum okkur þann rétt að breyta persónuverndarstefnu þessari hvenær sem er, án fyrirvara.

Ef persónuverndarstefnunni er breytt, munum við gefa út nýja útgáfu, þar sem útgáfudagur og listi yfir gerðar breytingar koma fram.