FYRIRTÆKI OG STOFNANIR

í nýju persónuverndarumhverfi

Ný persónuverndarlöggjöf hefur tekið gildi á Íslandi. Öll fyrirtæki, stofnanir og aðrir sem vinna með persónuupplýsingar, hvort heldur um eigið starfsfólk, viðskiptavini, notendur eða aðra, verða að fylgja hinni nýju löggjöf.

Ég er með lítið/meðalstórt fyrirtæki, til hvers þarf ég að líta hvað varðar nýja persónuverndarlöggjöf?

Öll vinnsla persónuupplýsinga þarf að styðjast við einhverja heimild, svo sem samþykki eða lagaheimild. Ef um viðkvæmar persónuupplýsingar er að ræða í skilningi laganna þarf jafnframt að uppfylla sérstök viðbótarskilyrði. Viðkvæmar persónuupplýsingar samkvæmt lögunum eru til að mynda upplýsingar um heilsufar, stéttarfélagsaðild, kynþátt, þjóðernislegan uppruna, stjórnmálaskoðanir og trúarbrögð.

Þá þarf við meðferð persónuupplýsinga ávallt að gæta að meginreglum laganna um gæði gagna og vinnslu. Þannig skal þess meðal annars gætt að þær séu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi. Auk þess þarf varðveisla þeirra og öryggi að vera í samræmi við tilgang vinnslu, eðli og umfang þeirra upplýsinga sem unnið er með hverju sinni.

Hvað eru persónuupplýsingar?

Persónuupplýsingar eru allar upplýsingar um persónugreindan eða 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 annað sambærilegt.

Er fyrirtækið mitt ábyrgðaraðili eða vinnsluaðili?

Í persónuverndarlögum er greint á milli svokallaðra ábyrgðaraðila og vinnsluaðila. Ábyrgðaraðili er sá sem ákveður tilgang og aðferðir við vinnslu persónuupplýsinga, en vinnsluaðili er sá sem vinnur með persónuupplýsingar á vegum ábyrgðaraðila. Vinnsluaðili getur því til dæmis verið fyrirtæki sem tekur að sér að vinna með persónuupplýsingar fyrir einhvern annan.

Á báðum aðilum hvíla tilteknar skyldur samkvæmt persónuverndarlögum og þegar notast er við vinnsluaðila þarf að liggja fyrir vinnslusamningur sem inniheldur meðal annars fyrirmæli ábyrgðaraðila til vinnsluaðila.

Hvað er vinnsluskrá og þarf ég að halda slíka skrá?

Samkvæmt persónuverndarlögum ber flestum fyrirtækjum og stofnunum að halda vinnsluskrá, þ.e. skrá yfir þá vinnslu persónuupplýsinga sem fer fram og hvernig að henni er staðið. Öll fyrirtæki sem vinna með persónuupplýsingar reglulega, til dæmis í tengslum við launavinnslu, þurfa því að halda vinnsluskrá, óháð starfsmannafjölda. Með því að útbúa vinnsluskrá fæst almennt góð yfirsýn yfir þá vinnslu persónuupplýsinga sem á sér stað á hverjum vinnustað og getur hún því verið heppilegt fyrsta skref í því að laga starfsemina að nýjum persónuverndarlögum.

Hvernig á að upplýsa hinn skráða um fyrirkomulag vinnslu?

Ábyrgðaraðila ber skylda til að fræða þá einstaklinga sem hann vinnur með persónuupplýsingar um. Þá fræðsluskyldu má meðal annars uppfylla með persónuverndarstefnu, þ.e. stefnu um meðhöndlun persónuupplýsinga. Þörf á að útbúa sérstaka persónuverndarstefnu fer eftir atvikum hverju sinni, svo sem efni og umfangi þeirrar vinnslu persónuupplýsinga sem fer fram hjá viðkomandi ábyrgðaraðila. Veita þarf upplýsingar um hvers vegna unnið er með upplýsingarnar, hvaða tegundir upplýsinga eru notaðar, hvort miðla á upplýsingunum til þriðja aðila, hvort flytja á upplýsingarnar úr landi, réttindi hins skráða, hvaðan upplýsingarnar koma, hvernig hafa má samband við ábyrgðaraðila og rétt hins skráða til að kvarta til Persónuverndar, svo að dæmi séu nefnd. Sjónarmiðin að baki þessu eru þau að hvers kyns vinnsla persónuupplýsinga á að vera lögmæt og sanngjörn. Einstaklingum ætti því að vera það ljóst þegar persónuupplýsingum um þá er safnað, þær notaðar, skoðaðar eða unnar á annan hátt og að hvaða marki þær eru eða munu verða unnar. Þá krefst meginregla laganna um gagnsæi þess að hvers kyns upplýsingar og samskipti, sem tengjast vinnslu persónuupplýsinga, séu auðveldlega aðgengileg og á skýru og einföldu máli.

Þarf mitt fyrirtæki eða stofnun að ráða persónuverndarfulltrúa?

Ábyrgðaraðili og vinnsluaðili þurfa að tilnefna persónuverndarfulltrúa í sérhverju tilviki þar sem:

1. vinnsla er í höndum stjórnvalds;

2. meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í vinnsluaðgerðum sem krefjast, sakir eðlis síns, umfangs eða tilgangs, umfangsmikils, reglubundins og kerfisbundins eftirlits með skráðum einstaklingum;

3. meginstarfsemi ábyrgðaraðila eða vinnsluaðila felst í umfangsmikilli vinnslu viðkvæmra persónuupplýsinga eða upplýsinga sem varða sakfellingar í refsimálum og refsiverð brot.

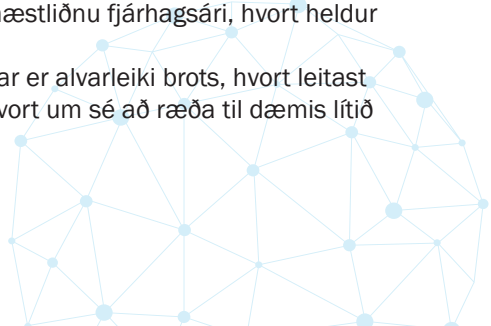
Meta þarf hvort eitthvert framangreindra skilyrða sé fyrir hendi og skoða í hverju tilfelli fyrir sig hvort nauðsynlegt sé að tilnefna persónuverndarfulltrúa.

Mat á áhrifum á persónuvernd

Ef tilteknar vinnsluaðferðir skapa mikla áhættu fyrir réttindi og frelsi einstaklinga verður ábyrgðaraðili að framkvæma mat á áhrifum á persónuvernd. Í slíku mati þarf að gera grein fyrir áhættunni og mögulegum afleiðingum hennar. Ef niðurstaða matsins er sú að áhættan sé mikil og að ábyrgðaraðila sjálfum sé ekki fært að draga úr henni verður að leita fyrirframsamráðs við Persónuvernd vegna vinnslunnar.

Brot gegn lögum um persónuvernd varða sektum

Fyrir vægari brot gegn persónuverndarlögunum geta sektir numið frá 100 þúsund krónum til 1,2 milljarða króna, eða allt að 2% af árlegri heildarveltu fyrirtækis á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra. Fyrir alvarlegri brot geta sektir numið frá 100 þúsund krónum til 2,4 milljarða króna, eða allt að 4% af árlegri heildarveltu fyrirtækis á heimsvísu á næstliðnu fjárhagsári, hvort heldur er hærra.
Meðal þess sem haft getur áhrif á fjárhæð sektar er alvarleiki brots, hvort leitast hafi verið við að draga úr afleiðingum þess og hvort um sé að ræða til dæmis lítið fyrirtæki eða alþjóðlegt stórfyrirtæki.



Hvar á mitt fyrirtæki/stofnun að byrja?

1 Kynnið ykkur nýju reglurnar vandlega

Lög og reglur um persónuvernd má finna á vefsíðu Persónuverndar. Þar er einnig að finna margvíslegar upplýsingar og leiðbeiningar sem uppfærðar eru reglulega.

2 Hafið yfirsýn yfir hvaða persónuupplýsingar unnið er með

Öll fyrirtæki, stofnanir og aðrir sem vinna með persónuupplýsingar verða að hafa yfirsýn yfir upplýsingarnar sem unnið er með, hvaðan þær koma og á hvaða lagalega grundvelli meðhöndlun þeirra er byggð. Verið viss um að hafa slíka yfirsýn. Hér er vinnsluskrá mikilvægt verkfæri. Sniðmát fyrir vinnsluskrá má finna á vefsíðu Persónuverndar.

3 Staðfestið að allir verkferlar uppfylli kröfur laganna

Séu þegar fyrir hendi góðar verklagsreglur um innra eftirlit sem þjóna tilgangi sínum og sem starfsmenn þekkja er auðveldara að fá yfirsýn yfir það sem þarf að laga. Yfirfarið gildandi verklagsreglur um vinnslu persónuupplýsinga.

4 Útbúið og innleiðið persónuverndarstefnu – uppfyllið fræðsluskyldu

Á ábyrgðaraðila hvílir skylda til að fræða hinn skráða um vinnslu persónuupplýsinga um hann. Þá fræðsluskyldu má m.a. uppfylla með persónuverndarstefnu, þ.e. stefnu um meðhöndlun persónuupplýsinga.

5 Hugið að öryggi gagna

Hagið varðveislu og öryggi persónuupplýsinga í samræmi við tilgang vinnslu, eðli og umfang upplýsinganna. Viðkvæmar persónuupplýsingar krefjast meiri verndar en almennar persónuupplýsingar.

6 Fylgið reglum um eyðingu gagna - Rétturinn til að gleymast

Fyrirtæki skulu eyða persónuupplýsingum þegar þeirra er ekki lengur þörf, hvort sem hinn skráði fer fram á það eður ei. Athugið að stjórnvöldum er almennt óheimilt að eyða gögnum.

7 Tilkynnið Persónuvernd um öryggisbresti

Tilkynna þarf Persónuvernd um öryggisbrest innan 72 klukkustunda frá því að ábyrgðaraðili verður hans var. Eins þarf að tilkynna hinum skráða um öryggisbrestinn ef líklegt er að hann leiði af sér mikla áhættu fyrir réttindi og frelsi hins skráða.

8 Athugið hvar persónuupplýsingarnar eru geymdar

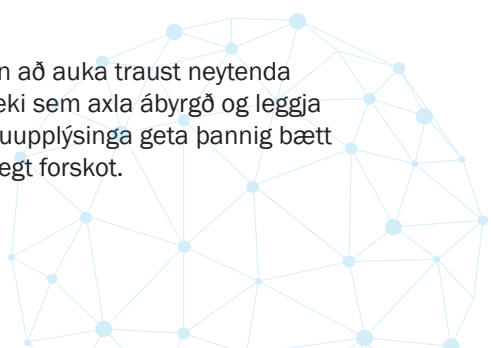
Eru gögn geymd í tölvuskýi? Gangið úr skugga um hvort persónuupplýsingar eru geymdar innan eða utan Evrópska efnahagssvæðisins. Óheimilt er að flytja persónuupplýsingar út fyrir EES-svæðið nema að uppfylltum ákveðnum skilyrðum.

9 Gætið að reglum um innbyggða og sjálfgefna persónuvernd

Er upplýsingakerfið ykkar hannað á þann hátt að það standist kröfur um innbyggða og sjálfgefna persónuvernd? Getur fyrirtækið/stofnunin svarað fyrirspurnum frá almenningi um vinnslu persónuupplýsinga á innan við mánuði?
Nýja löggjöfin krefst þess að hugbúnaður og verkferlar séu útfærðir með sérstaka áherslu á persónuvernd og á þann hátt að hún sé innbyggð í viðkomandi lausn. Hönnun hugbúnaðar þarf því að taka mið af því að öryggi persónuupplýsinganna sé tryggt, meðal annars ef áföll verða í rekstri kerfa. Þá þarf að hanna lausnir með það í huga að einstaklingar geti nýtt sér réttindi sín samkvæmt persónuverndarlögunum, svo sem aðgangsrétt og rétt til að flytja eigin gögn.

10 Nýtið tækifærin!

Rétt meðferð persónuupplýsinga er til þess fallin að auka traust neytenda og annarra í garð fyrirtækja og stofnana. Fyrirtæki sem axla ábyrgð og leggja metnað sinn í að tryggja öryggi og vernd persónuupplýsinga geta þannig bætt samkeppnisstöðu sína og skapað sér viðskiptalegt forskot.



Þessi bæklingur var fjármagnaður af Evrópusambandinu
- The European Union's Rights, Equality and Citizenship Programme
(2014-2020)

Frekari upplýsingar og fróðleik um hinar nýju reglur má nálgast á vefsíðu Persónuverndar,
www.personuvernd.is

Rauðarárstíg 10, 105 Reykjavík
Sími: 510 9600 | postur@personuvernd.is