Ný reglugerð ESB 2016/679 (Hér eftir kölluð GDPR) um verndun persónuupplýsinga gekk í gildi í maí 2016. Aðildarríkjum ber að innleiða þessa reglugerð í lög 25. maí 2018. Breytingarnar taka einnig gildi á Íslandi á þeim tíma.

Öll fyrirtæki og stofnanir sem vinna með persónuupplýsingar, hvort sem um er að ræða viðskiptavini, eigið starfsfólk notendur eða aðra, verða að fylgja þessari nýju löggjöf.

Brot á lögunum geta haft *alvarlegar efnahagslegar afleiðingar* og hvetur undirritaður því fyrirtæki og stofnanir til að fylgjast vel með þessum nýju lögum og haga undirbúningi sínum með fullnægjandi hætti. Persónuvernd mun eftir sem áður framfylgja lögunum á Íslandi.

Eftirfarandi sektum er hægt að beita skv. lögunum:

Skrifleg viðvörun vegna fyrsta brots, t.d. brot á innbyggðum reglum um friðhelgi, vinnslusamningar ekki til staðar, persónuverndarfulltrúi ekki skipaður, áhrifamat ekki framkvæmt, öryggisrof hefur ekki verið tilkynnt innan tiltekins tíma, svo dæmi sé tekið.

Reglulegar kerfisskoðanir þar sem metið er hvernig fyrirtækið fer eftir GDPR.

Sekt sem nemur 10 000 000 EUR eða 2% af veltu, hvort sem er hærra, ef fyrirtækið vinnur með upplýsingar um einstaklinga yngri en 16. ára án fullnægjandi heimildar forráðamanna(sjá 8.gr.).

Sekt sem nemur 20 000 000 EUR eða 4% af veltu, hvort sem er hærra, ef fyrirtækið brýtur gegn grundvallar atriðum um vinnslu, þar með talið skilyrðum fyrir samþykki.

Hvað er það þá sem þitt fyrirtæki eða stofnun þarf að gera? Á vef persónuverndar er að finna upplýsingar um það.

Þar segir meðal annars:

1. Nýjar skyldur verða lögð á öll fyrirtæki og stofnanir sem vinna með persónuupplýsingar.

Öll fyrirtæki og stofnanir þurfa að skoða löggjöfina og finna út hvað nýju skuldbindingum þau verða að fara eftir.

2. Öll fyrirtæki skulu hafa auðskiljanlega persónuverndarstefnu - auknar kröfur um fræðslu.

Kynning á því hvernig fyrirtækið vinnur með persónuverndar upplýsingar skulu vera á aðgengilegu og auðskiljanlegu formi.

3. Öll fyrirtæki skulu meta áhættu af vinnslu persónuupplýsinga og mögulegar afleiðingar fyrir friðhelgi einstaklinga.

Ef tilteknar vinnsluaðferðir skapa mikla hættu fyrir friðhelgi einstaklinga, verður ábyrgðaraðili að gera grein fyrir þeirri hættu og mögulegum afleiðingum hennar.

4. Persónuvernd skal vera innbyggð í nýjan hugbúnað og upplýsingakerfi.

Nýja löggjöfin krefst þess að nýr hugbúnaður og upplýsingakerfi séu útfærð með sérstaka áherslu á friðhelgi einstaklinga og á þann hátt að hún sé innbyggð í viðkomandi lausn. Gengið verður út frá því að hámarks áhersla á persónuvernd sé sjálfgefin í öllum kerfum.

5. Mörg fyrirtæki og allar opinberar stofnanir þurfa að útnefna sérstakan persónuverndarfulltrúa.

Í öllum tilvikum þar sem opinbert yfirvald eða stofnun fer með persónuupplýsingar eða þar sem fyrirtæki hefur það að sinni meginstarfsemi að vinna með persónuupplýsingar. Hlutverk þessa fulltrúa er að vera sérfræðingur viðkomandi aðila í persónuvernd og tengiliður milli stjórnenda, hinna skráðu og Persónuverndar.

6. Reglurnar gilda einnig um fyrirtæki utan ESB og EES.

Fyrirtæki sem hafa aðsetur utan EES og ESB þurfa einnig að fylgja eftir reglunum ef þau bjóða íbúum í löndum EES eða ESB vörur eða þjónustu.

7. Nýjar skyldur eru lagðar á alla sem vinna upplýsingar fyrir hönd annara.

Þeir sem vinna með persónuupplýsingar fyrir hönd ábyrgðaraðila kallast vinnsluaðilar. Oft er um að ræða **þá sem bjóða upplýsingatækniþjónustu**. Nýju lögin skylda þessa aðila til að setja sér verklagsreglur um vinnslu og meðferð persónuupplýsinga.

8. Öll fyrirtæki eiga að fylgja viðmiðum góðra og gegnra aðila á sínu sviði.

Nýju reglurnar hvetja til þess að starfs- eða faggrein setji sér siða- og hátternisreglur innan hverrar starfsstéttar. Með slíkum reglum verður skýrara hvernig vinna skuli með persónuupplýsingar og vafaatriðum mun fækka. Afla verður staðfestingar Persónuverndar á reglunum.

9. Öll fyrirtæki og stofnanir verða að uppfylla nýjar kröfur um viðbrögð við öryggisbrestum.

Reglur um hvernig bregðast skal við, þegar upp kemur öryggisbrestur, verða strangari. Í stuttu máli sagt á að tilkynna mun fyrr og oftar um öryggisbresti en nú er gert.

10. Brot gegn reglunum geta numið háum sektum.

Ef fyrirtæki eða aðrir sem vinna með persónuupplýsingar brjóta gegn ákvæðum nýju löggjafarinnar geta persónuverndarstofnanir í Evrópu lagt á viðkomandi sekt. Upphæð sektar ræðst af eðli og alvarleika brots.