

Mida toob kaasa isikuandmete töötlemise uus reeglistik

Selle aasta kevadel võeti Euroopa Liidus vastu isikuandmete kaitse üldmäärus („General Data Protection Regulation”, GDPR), mis asendab 1995. aastast pärineva andmekaitse direktiivi. GDPR on liikmesriikidele otsekohalduv ning rakendub juba pooleteise aasta pärast ehk 2018. aasta mais.

Andmekaitse reformi eesmärk on internetiajastul anda füüsilistele isikutele suurem kontroll oma isikuandmete üle, luua digitaalse ühisturu jaoks kohandatud reeglistik ning ühtlane andmekaitse tase kogu ELis.

GDPRi mõju on äärmiselt laialt ulatav, kuna uued põhimõtted kehtivad kõikidele ELi ettevõtjatele ja organisatsioonidele, kes töötlevad isikuandmeid. Samuti on üldmäärust kohustatud järgima need ettevõtted, mis pole ELis asutatud, kuid töötlevad ELis olevate andmesubjektide isikuandmeid seoses kaupade ja teenuste pakkumisega ELis.

Mida andmekaitse reform kaasa toob?

GDPR sisaldab mitmeid uuendatud põhimõtteid, mis võivad ettevõtja jaoks kaasa tuua vajaduse suures mahus muuta seniseid protseduure ja süsteeme. Mõned näited andmetöötaja uuenenud kohustustest, mis annavad aimu ettevõtja ees seisvate muudatuste mahukusest:

- ✓ Isikuandmete töötlemisel on **teavitamiskohustus**, mille puhul tuleb õiguseid ja vabadusi kahjustada võivatest isikuandmetega seotud rikkumistest teavitada järelevalveasutust ning teatud juhtudel ka andmesubjekti ennast.
- ✓ Isikuandmete töötlemine peab olema korrastatud ja süsteemne ning andmesubjekti kohta kogutud **andmestik peab olema teisaldatav ühest elektroonilisest töötlemisest süsteemist teise**.
- ✓ Kohustus määrata **andmekaitseametnik**, kui isikuandmete töötlemise laad ja ulatus

seda nõuavad, näiteks kui ettevõtte põhitegevus nõuab regulaarset ja süstemaatilist isikuandmete töötlemist või erikategooriasse kuuluvate isikuandmete laiapõhjalist töötlemist.

- ✓ Isikuandmete töötlemisel tuleb tagada isikuandmete **töötlemise toimingute dokumenteerimine** ning olukorras, kus andmete töötlemisega võib tekkida füüsilistele isikute õigustele ja vabadustele suur oht, tuleb andmete töötlemisel teha **andmekaitsealane mõjuhinnang**.

Lisaks eelnevale võib ettevõtjal olla keeruline kustutada isikuandmed olukorras, kus andmete töötlemise eesmärk on lõppenud ning andmesubjekt ei soovi edasise töötlemise jätkamist. Samuti võib keerukaks osutuda kohustus tagada ning vajadusel tõendada andmesubjekti selgesõnalise, teadliku ja vabatahtliku nõusoleku olemasolu olukordades, kus see on nõutav.

Tagamaks ELi eeskirjade täitmine liikmesriikides, suurendatakse GDPRiga riiklike andmekaitseasutuste volitusi ning seatakse karmid karistused GDPRi rikkumise eest, mis võivad ulatuda väikeste eksimuste puhul kuni 2%ni ja suurte eksimuste puhul kuni 4%ni ettevõtte eelmise aasta ülemaailmsest käibest või kuni 20 000 000 euronit, sõltuvalt sellest, kumb summa on suurem.

Mida teha, et isikuandmete töötlemine vastaks uuenenud nõuetele?

Kuna GDPRi mõju ettevõtetele on ulatuslik ning trahvid rikkumise eest märkimisväärsed, tuleks isikuandmete kaitsega seotud tegevused seada prioriteediks ning alustada ettevalmistustöödega juba nüüd.

Soovitame kaardistada, millistes süsteemides ja milliseid isikuandmeid ettevõttes töödeldakse ning kes omavad isikuandmetele ligipääsu. Kasulik oleks läbi viia andmekaitse õigus- ja infosüsteemide audit, mis võimaldab tuvastada andmete töötlemisega seotud puudused ja riskikohad. Kindlasti tuleks analüüsida ja kasutusele võtta tehnilised meetmed andmekaitsereeglite järgimiseks. Soovituslik oleks äriprotsessidest ja auditi tulemustest lähtudes töötada välja isikuandmete töötlemise juhendid ja strateegia ning koolitada töötajaid, tagamaks vastavus GDPRi nõuetele.

Sõltuvalt ettevõtja tegevuslaadist ning isikuandmete töötlemise mahust ja viisist võivad ettevalmistustööd kujuneda väga ajamahukaks. Kindlasti on protsessi eduka läbiviimise eelduseks, et tegevusse on kaasatud lisaks juhtkonnale kõik osakonnad ja tugiteenused, kes isikuandmete töötlemisega kokku puutuvad. Soovitame kaaluda kogunud piiriülest teenust pakkuva multidistsiplinaarse

välise nõustaja kaasamist, kes aitab viia andmetöötluse protsessi vastavusse uuendatud andmekaitse reeglistiku ja ELi andmekaitsemäärusega.

KPMGs on kogunud professionaalid nii õigus- kui ka IT-nõustamise vallas, kes mitme valdkonna spetsialistidest koosneva ühtse meeskonnana saavad aidata nii isikuandmete kaitse reformiga kaasnevate muudatusvajaduste kaardistamisel kui ka uute lahenduste juurutamisel. Oleme nõustanud mitut Eesti suuretevõtjat ning hea meelega toome oma kogemuse ka oma teiste klientideni. Kuivõrd äri on tihti piiriülene ja nõuded riigiti mõnevõrra erinevad, siis koostöös KPMG võrgustiku teiste riikide kolleegidega saame leida sobivad lahendused ka terve kontserni vajadustele isikuandmete kaitse reformi nõuetele vastavuse tagamisel. KPMG Põhjamaade küberturvalisuse meeskond on üks regiooni suuremaid, olles nõustanud kümneid isikuandmete kaitse vastavuskontrolli projekte, ja piiriülestes küsimustes saame pakkuda parimat rahvusvahelist kogemust ja oskusteavet.

Sirli-Kristi Käpa

KPMG Advokaadibüroo
vanemjurist
Tel 667 6805
sirli-kristi.kapa@kpmglegal.ee



Laura Saks

KPMG Advokaadibüroo
jurist
Tel 667 6804
laura.saks@kpmglegal.ee



Teet Raidma

IT nõustamisteenuste juht
KPMG Baltics
Tel 667 6814
traidma@kpmg.com

