Pilveteenuse valik ja vastutus – kuidas maandada riske

Isikuandmete töötlemisel ehk isikuandmetega toimingute tegemisel, näiteks kogumisel, säilitamisel, kasutamisel jne võib töötlejaks olla nii füüsiline kui ka juriidiline isik, kui ta töötleb andmeid või tema ülesandel töödeldakse andmeid. Töötlejad jagunevad omakorda **vastutavaks ja volitatud töötlejateks**. Pilveteenuse puhul on **pilveteenuse pakkuja üldjuhul volitatud töötlejaks**, kes vastutava töötleja ülesandel andmeid töötleb.

Uus andmekaitsemäärus kohustab vastutavat töötlejat volitatud töötlejaga **üsna spetsiifilist lepingut sõlmima**, et tagada isikuandmete töötlemise osas selgus. Samas ei ole leping oluline mitte üksnes määruse nõuete täitmiseks, vaid pigem ikka nii vastutava kui ka volitatud töötleja huvides, et tagada selgus pooltevahelises vastutuses.

Uus andmekaitsemäärus näeb teatud juhtudel ette ka volitatud töötleja vastutuse, kuid kuna isiku ees jääb vastutavaks siiski vastutav töötleja, peab ta enne pilveteenuse kasutamiseks lepingu sõlmimist, juba pilveteenuse valikul, **väga põhjalikult riske hindama**. Riskide hindamise olulisuse toob välja ka, peamiselt küll avalikule sektorile mõeldud, ISKE. Majandus- ja kommunikatsiooniminister kinnitas 30. jaanuaril 2017 ISKE rakendusjuhendi uue versiooni 8.0, mis uuendusena käsitleb ka pilveteenuseid. Pilveteenuste osas toob rakendusjuhend välja mitmeid riske, millega tuleb arvestada. Riigi poolt pilvede osas ulatuslike riskide nägemine kinnitab, et kergemalt ei saa suhtuda ka **erasektor, kes samuti peab andmeid kaitsma ja tagama nende turvalisuse.**

Riskide hindamine eeldab vastuse leidmist küsimusele, kas on võimalik olla täiesti kindel, et teenusepakkuja töötleb andmeid vastavalt andmekaitse reeglitele ja kokkulepitule. See hõlmab nii teenusetingimuste põhjalikku analüüsi kui ka tehniliste ja organisatsiooniliste turvameetmete hindamist. Võib juhtuda, et teenusetingimuste kohaselt on teenus küll vastav, kuid tegelikkuses võib esineda pilveteenuse serverite osas mõni tehniline risk, mis muudab teenuse sobimatuks.

Puudusi võib esineda ka teenusetingimustes, mistõttu tuleb teenusetingimuste lugemisel ja analüüsimisel olla väga tähelepanelik. **Tihtipeale on pilveteenuste tingimused võrdlemisi pikad, kuid arvestades, millised tagajärjed võivad andmekaitserikkumised kaasa tuua, tasub see aeg võtta ja tingimused põhjalikult läbi uurida või hankida selleks professionaalset abi.**

Erilist tähelepanu tuleb pöörata sellistele pilveteenustele, mille teenusepakkujad on pärit Euroopa Liidu ja Euroopa majanduspiirkonna välistest riikidest – tihtipeale asuvad ka nende serverid seal ning sellisel juhul tuleb eraldi analüüsida, kas on täidetud on Euroopa Liidus kehtestatud andmekaitsenõuded. Näiteks Dropbox sätestab oma tingimustes, et hoiab andmeid serverites üle kogu maailma. Olles Euroopa Liidu vastutav töötleja, peaks selline tingimus tähelepanu äratama, kuna võib juhtuda, et andmeid ei hoita Euroopa Liidu liikmesriikides. Võimalik, et sellist tingimust saaks läbi rääkida, kuid juhul, kui see ei õnnestu, tuleb hinnata, kas vastutav töötleja on valmis sellise riski võtma.

Andmete töötlemine pilves tingib mitmeid riske, kuid teenuste põhjalikul ja ammendaval hindamisel ning sobilike ja nõutud lepingute sõlmimisel, võimaldab siiski tagada isikuandmete turvalise ja õiguspärase töötlemise.

Artikkel on esialgsel kujul avaldatud portaalis IT-uudised.

(Autor: Siiri Vello)

LIISI JÜRGEN
VANDEADVOKAAT, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE