

EU:n tietosuoja-asetus tulee, oletko valmis?

Paljon uutisoitu EU:n tietosuoja-asetus on ollut laajamittainen uudistus, joka asettaa uusia vaatimuksia henkilötietojen käsittelylle kaikissa yrityksissä, yhteisöissä ja muissa organisaatioissa. Nykyisin asiaa käsittelee pääasiassa kunkin EU-maan oma kansallinen lainsäädäntö sekä kunkin maan viranomaisten tulkinnat.

Mikä tietosuoja-asetus?

Asetus koskee kaikkia henkilötietojen käsittelyä EU:ssa. Henkilötietoja ovat kaikenlaiset luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavat merkinnät, jotka voidaan tunnistaa häntä tai hänen perhettään koskeviksi. Niitä ovat esimerkiksi nimi, henkilötunnus, osoite, sähköpostiosoite, asiakas- tai työsuhteen liittyvät tiedot, paikkatiedot sekä internet-osoitteet. Käytännössä kaikki yritykset käyttävät henkilötietoja mm asiakasrekistereissään.

Asetus hyväksyttiin virallisesti 14. huhtikuuta 2016 ja se astuu voimaan kahden vuoden siirtymäajalla toukokuussa 2018. Yritysten tulee tutustua uudistukseen ja saattaa omat toimintatapansa sekä dokumentit kuntoon hyvissä ajoin ennen asetuksen voimaantuloa. Asetuksen myötä yrityksille henkilötietojen rekisterienpitäjinä sekä tietoja käsittelevinä toimijoina tulee uusia oikeuksia ja velvollisuuksia suhteessa rekisteröityihin ja suhteessa toisiin yrityksiin.

Yrityksen vastuu ja aktiivinen rooli korostuu

Yrityksillä on rekisterinpitäjänä tilivelvollisuus henkilötietojen käsittelystä. Se tarkoittaa sitä, että yritys on ennakkoon riskiperusteisesti suunnitellut tietosuojatoimintansa ja pystyy tarvittaessa todentamaan velvollisuuksien täyttämisen viranomaiselle. Tämä koskee myös mahdollisten henkilötietojen käsittelijöitä eli alihankkijoita ja yhteistyötahoja. Täten yrityksen sopimukset ja ohjeistukset tulee käydä läpi ennen asetuksen voimaantuloa.

Mikäli yrityksen ydintoimintoihin kuuluu henkilötietojen järjestelmällinen seuranta taikka arkaluontoisten henkilötietojen, esimerkiksi terveystietojen käsittely, tulee yrityksen nimetä tietosuojavastaava. Hänen tehtävänsä on suunnitella, kehittää ja valvoa tietosuojaa. Tietosuojavastaava voi olla oma työntekijä taikka ulkopuolinen henkilö. Vaikka yrityksellä ei olisikaan velvollisuutta nimetä tietosuojavastaavaa, on suositeltavaa, että nimetään vastuuhenkilö huolehtimaan tietosuojasta tarvittaessa yhdessä ulkopuolisen asiantuntijan tukemana.

Tietosuoja-asetuksella pyritään parantamaan rekisteröityjen oikeuksia. Yrityksille tulee ilmoitusvelvoite henkilötietojen tietoturvaloukkauksista. Yrityksen on ilmoitettava viranomaiselle epäillyistä loukkauksista 72 tunnin kuluessa. Mikäli loukkauksesta on todennäköisesti haitallisia vaikutuksia rekisteröidylle, on yrityksen ilmoitettava rekisteröidylle tapahtuneesta. Täten yrityksen työntekijän henkilötietoja sisältävän tietokoneen varastaminen tai USB-muistitikun katoaminen voi laukaista tämän ilmoitusvelvoitteen.

Yrityksen vastuu ja aktiivinen rooli korostuu

Rekisteröidyllä on oikeus tulla unohdetuksi. Jos henkilötietojen käsittely ei ole enää alkuperäisen perusteensa mukaan taikka käsittelylle ei enää ole laillista muuta perustetta, on rekisteröidyllä oikeus vaatia tietojensa poistamista.

Eniten asetuksen uutisoinnissa on tuotu esiin se, että asetuksen säännösten rikkomisesta voivat viranomaiset määrätä sakon, jonka suuruus voi olla maksimissaan neljä prosenttia yrityksen maailmanlaajuisesta liikevaihdosta. Tämän lisäksi viranomaiset voivat antaa mm. huomautuksia, korjauskehoituksia ja muita määräyksiä.

Mitenkä yrityksen tulee valmistautua muutokseen?

Yrityksen tulee siis valmistautua riittävän ajoissa tulevaan asetukseen. Lyhyesti tämä tapahtuu seuraavasti:

Yritys selvittää, millaisia henkilötietoja se käsittelee, millä perusteella ja miten. Jatkossa kerättävää henkilötietojen määrää pitää minimoida. Kerättävien tietojen tulee olla myös täsmällisiä. Niiden tulee olla välttämättömiä palvelun ja liiketoiminnan käytön kannalta. Virheelliset tiedot tulee poistaa viipymättä ja tietojen oikeellisuutta tulee ylläpitää. Rekisteröityjen vaatimuksiin tulee vastata ripeästi.

Tässä yrityksen muutokseen valmistautumisessa on keskeistä prosessien ja sopimusten sekä erilaisten yritysten käyttöehtojen analysointi ja läpikäynti. Käytännössä on usein todettu, että sopimukset eivät ole riittävästi huomioineet tietosuoja-asioita nykyisenkään sääntelyn tasolla. Riskikartoituksessa voidaan määrittää riskit ja minimoida niitä sopimusmuutoksin. Viimeistään nyt rekistereistä tulee olla asianmukaiset rekisteriselosteet.

Yrityksen pitää toimia tietosuoja-asiaissa myös teknisesti. Sen tulee lisätä sisäistä valvontaa ja käyttöönottaa menettely, jossa yritys säännöllisesti testaa ja arvioi omien teknisten ja organisatoristen toimenpiteiden tehokkuutta henkilötietojen turvallisuuden varmistamiseksi. Tämä tekninen suojaaminen tulee olla ennakoivaa.

Yrityksen henkilökunnan ohjeistaminen ja kouluttaminen on tärkeä suorittaa ja tämä koulutus tulee dokumentoida riittävästi. Tietosuoja viimekädessä rakennetaan ihmisten toiminnalla.

Valmistautumisprosessi sisältää monta erilaista osatehtävää ja edellyttää erityisosamista ja dokumentaatiota. Mikäli yritys ei pysty toteuttamaan valmistautumista omilla resursseillaan, on suositeltavaa käyttää asiantuntijoita. Näin varmistetaan oikea lopputulos nopeasti ja kustannustehokkaasti.



Teresa Laine-Puhakainen, Legal Counsel

Teresa (OTK) työskentelee KPMG:llä liikejuridiikan ja työoikeuden asiantuntijana. Hänellä on yli kahdenkymmenen vuoden käytännön kokemus yritysten juridiikkaan liittyvistä kysymyksistä ja neuvonnasta. Teresan toimenkuvaan kuuluu asiakasyritysten avustaminen oikeudellisissa toimeksiannoissa sekä asiakkaiden toiminnan juridisten riskien hallinnoiminen sopimuksilla.

KPMG tarjoaa tilintarkastus-, vero- ja lakipalveluja sekä liikkeenjohdon konsultointia ja yritysjärjestelypalveluja. KPMG on toistuvasti nostettu tietoturvapalvelujen markkinajohtajaksi kansainvälisissä selvityksissä. Toimimme 197 000 henkilön voimin 154 maassa ympäri maailmaa. Suomessa meitä on yli 1100 henkilöä 22 paikkakunnalla. Meillä on myös noin 110 hengen toimisto Tallinnassa. | www.kpmg.fi

