Toimintaohje EU:n tietosuoja-asetuksen hallintaan

EU:n tietosuoja-asetus tulee voimaan 25.5.2018. Asetus velvoittaa myös pieniä yrityksiä henkilötietojen tarkempaan suojaamiseen. Nykyiseen henkilötietolakiin verrattuna tietosuoja-asetus sisältää yrityksille uusia velvoitteita.

Asiakas- ja työntekijärekisteri

Useimmilla yrityksillä on jonkinlainen **asiakasrekisteri**. Vaikka asiakaskunta koostuisi pelkästään yrityksistä, on rekisterissä yleensä tietoa myös asiakasyritysten yhteyshenkilöistä. Teidän kannattaa käydä läpi, mitä tietoa sinne on henkilöistä tallennettu.

Yleensä asiakasrekisterit eivät sisällä kovinkaan arkaluontoisia henkilötietoja, joten niiden suhteen ei kannata tehdä kärpäsestä härkästä. Maanläheinen toimintatapojen kartoitus ja sopiminen ovat kuitenkin paikallaan. Esimerkiksi asiakastietojärjestelmän asianmukainen käyttäjähallinta on tärkeää myös liikesalaisuuksien, eikä yksinomaan henkilötietojen turvallisuuden näkökulmasta.

Työntekijärekisterinne sen sijaan sisältää arkaluontoista henkilötietoa. Palkanlaskennan tarpeisiin tarvitaan tietoa henkilön sairaspoissaoloista, ay-jäsenyyksistä sekä toisinaan myös ulosotosta. Myös henkilötunnusta käytetään palkanlaskennassa säännönmukaisesti.

Mikäli palkanlaskentanne tapahtuu meillä:
Olemme sopineet/tulemme sopimaan kanssanne palkanlaskentaa varten seuraavat yhteyskäytännöt:

- Yrityksessänne hoitaa palkanlaskentaan liittyviä asioita nimetty yhteyshenkilö
- Toimitatte meille palkanlaskentaa varten tarvittavat tiedot sovitulla tavalla
- Toimitamme teille palkanlaskennassa tuotetut tiedot sovitulla tavalla
- Palautamme tai hävitämme sovittavalla tavalla palkanlaskennan aineistot, kun niitä ei enää tarvita kirjanpitolain tai muun lainsäädännön perusteella

Tärkeintä on se, että teillä on selkeä toimintatapa, miten säilytätte meiltä vastaanottamanne henkilötietoja sisältävän aineiston. **Aineisto tulee säilyttää paperilla lukkojen takana tai tiedostomuodossa sellaisissa hakemistoissa, jotka on rajattu käyttöoikeuksin henkilöille, jotka tietoja työssään tarvitsevat.**

Käytännön toimia pk-yrityksissä

- Arkistoi työntekijöiden lääkärintodistukset, ulosottodokumentaatio, AY-jäsenyystiedot ja vastaavat omaan mappiinsa lukkojen taakse tai sähköisessä muodossa hakemistoon, jonka käyttöoikeudet on rajattu.

- Harkitse, voiko arkaluontoiset tiedot lähettää suojaamattomassa sähköpostissa. Hyvin monet sähköpostipalvelut käyttävät jo salattua yhteyttä ja tarvittaessa löytyy ilmaisia sovelluksia sähköpostin sisällön suojaamisen.

- Laadi ohjeet henkilötietojen käsittelyyn ja kouluta henkilöstö. Muista arkijärki siinä, mikä on oikeasti arkaluontoista. Tarvittaessa voit kysyä meiltä ohjausta tai apua.

- **Muista, että jos et ole sopinut kanssamme toisin, työntekijäsi eivät saa kysellä palkka-asioitaan suoraan meiltä. Meillä ei yleensä ole mahdollisuutta tunnistaa kyselijää luotettavasti.**

- Asiakasrekisteriinne rekisteröidyillä henkilöillä, samoin kuin työntekijöillänne, on oikeus tarkastaa omat tietonsa ja korjauttaa virheet. Mieti menettely, jolla kysyjä (esimerkiksi asiakkaan henkilö) tunnistetaan ja miten tiedot annetaan.

- Hävitä aineistot, kun ne eivät enää ole tarpeen. Palkanlaskennan aineistojen lakisääteinen säilytysaika on 6 tai 10 vuotta. Jos esimerkiksi lääkärintodistusten perusteella on haettu ja saatu KELA-korvauksia, ovat lääkärintodistukset tositteita, jotka tulee säilyttää 6 vuotta. Ne tulee hävittää säilytysvelvollisuuden umpeuduttua, koska säilytyksellä ei ole enää lakisääteistä tai muuta perustetta.

Tietosuoja-asetukseen liittyviä käsitteitä

Rekisteröity tarkoittaa henkilötietojen pohjalta tunnistettavissa olevaa ihmistä, jonka henkilötiedot ovat käsittelyn kohteena. Tietosuoja-asetus ei siis säätele esimerkiksi yrityksen asiakasrekisterin pitoa muuten kuin asiakkaiden yhteyshenkilöiden osalta.

Henkilötiedot tarkoittavat kaikkia rekisteröityä koskevia tietoja, joiden perusteella tämä on suoraan tai epäsuorasti tunnistettavissa. Osa tiedoista on asetuksessa säädetty erityisen arkaluontoiseksi. Esimerkkinä voidaan mainita ihmisen terveystiedot ja ay-jäsenyystiedot.

Rekisteri tarkoittaa mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa. Tietokantojen lisäksi esimerkiksi Excel-taulukko voi siis muodostaa rekisterin. Tyypillisiä rekistereitä pk-yrityksissä ovat asiakasrekisteri sekä työntekijärekisteri henkilöstöhallinnon ja palkanlaskennan tarpeisiin.

Rekisterinpitäjä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Pk-yritys on työntekijärekisterinsä pitäjä, vaikka palkanlaskenta olisikin ulkoistettu tilitoimistolle ja vaikka tilitoimisto hoitaisi rekisterin tietojen ylläpidon ja käyttäisi rekisteriä palkanlaskennan hoitoon.

Henkilötietojen käsittelijä tarkoittaa luonnollista henkilöä tai oikeushenkilöä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi tilitoimisto, joka käsittelee asiakkaiden työntekijöiden tietoja laskeakseen palkat, on henkilötietojen käsittelijä.

Riskiperusteisuus tarkoittaa sitä, että yrityksen toimet on suunniteltava sen mukaan, mikä riski tietojen vuotamisella tai häviämisellä on. Esimerkiksi asiakasrekisterissä oleva tieto siitä, että Ville Virtanen (insinööri) toimii tuotantopäällikkönä yrityksessä X ja käyttää tiettyä puhelinnumeroa ja sähköpostiosoitetta ei aiheuta samanlaista riskiä kuin terveydenhuoltoalan yrityksen tieto asiakkaan terveydentilan kehityksestä tai palkanlaskentaa varten rekisteröity tieto Pekka Pekkalan sairaspoissaolojen suuresta määrästä.