Käytännön neuvoja tietosuojan toteuttamiseen

Tietosuoja-asetusta (EU) 2016/679 ryhdyttiin soveltamaan toukokuussa 2018, mistä lähtien henkilötietoja käsittelevien organisaatioiden on tullut täyttää toiminnassaan tietosuoja-asetuksen vaatimukset. Tietosuojan käytännön toteutus on yksi merkittävä keino, jolla organisaatio voi erottua kilpailijoistaan. Toisaalta tietosuojaan liittyvien velvoitteiden ja rekisteröityjen oikeuksien laiminlyöminen muodostaa organisaatiolle merkittävän riskin, jonka realisoituminen voi aiheuttaa huomattavia taloudellisia seurauksia sekä mainevahinkoa. Sisäiselle tarkastukselle tietosuojaseikat tuovat tarkastuksiin mielenkiintoisen lisän, minkä huomioimalla sisäinen tarkastus voi tarjota hyödyllistä tietoa ja näkemystä organisaation toiminnalle.

Käytännössä tietosuojan toteuttaminen edellyttää jatkuvaa tietosuojaseikkojen huomioimista sekä koko organisaation läpäisevää tietosuojakulttuuria. Käytännön toteutuksen kannalta ensisijaisen tärkeää on johdon tuki tietosuojan edistämiseksi. Ilman riittäviä resursseja ja organisointia tietosuojan toteuttaminen jää helposti ohueksi, jolloin tietosuojavelvoitteiden laiminlyömisestä aiheutuvia riskejä ei pystytä torjumaan samalla kun resursseja viedään muulta toiminnalta. Tietosuojan toteuttamiseen onkin järkevää suhtautua yhtenä kilpailuetua luovana tekijänä, jolla torjutaan samalla organisaatioon kohdistuvia riskejä.

Tarkasteltaessa tietosuojan toteuttamista organisaatiossa, merkittäviä osa-alueita ovat mm. käsittelyn yleinen laillisuus, rekisteröityjen oikeudet, rekisterinpitäjään ja henkilötietojen käsittelijään kohdistuvat vaatimukset sekä henkilötietojen siirtäminen kolmansiin maihin.

Jokainen osa-alue sisältää paljon erilaisia velvoitteita, jotka on huomioitava omassa toiminnassa mutta joiden varsinainen toteuttamistapa on organisaation muotoiltavissa ja päätettävissä. Kantavana ajatuksena tietosuoja-asetuksessa on rekisteröidyn oikeuksille käsittelystä aiheutuvan riskin arvioiminen sekä riskiä vastaavien tietosuojatoimien toteuttaminen. Jotta rekisterinpitäjä voi arvioida rekisteröityjen oikeuksille aiheutuvaa riskiä, on sen tiedettävä mitä, missä, milloin ja miten henkilötietoja käsitellään.

Keskeistä tietosuojan käytännön toteuttamisessa on selvittää, mitä henkilötietoja organisaatio käsittelee. Ainoastaan tunnistamalla käsiteltävät henkilötiedot on mahdollista jatkossa kehittää organisaation tietosuojaa. Käsiteltävät henkilötiedot voidaan tunnistaa esimerkiksi tarkastelemalla organisaation tietovirtoja ja prosesseja. Selvittämällä käsiteltäviä henkilötietoja saadaan samalla selville missä ja milloin sekä monesti myös miten henkilötietoja käsitellään.

Olennaista on, että käsiteltäville henkilötiedoille on johdettu asianmukainen oikeusperuste käyttötarkoitussidonnaisuuden ja tietojen minimoinnin periaatteet huomioiden. Jos käsittelylle ei ole löydettävissä oikeusperustetta tai henkilötiedot eivät ole tarpeellisia käyttötarkoitukseensa nähden, henkilötietoja ei tule käsitellä.

Henkilötietojen kartoituksen jälkeen voidaan tarkastella, mitkä rekisteröidyn oikeudet ovat organisaation toiminnan ja rekisteröityjen kannalta merkittävimpiä. Erityisesti kannattaa kiinnittää huomiota esimerkiksi rekisteröidyn pääsyyn omiin tietoihinsa ja oikeuteen tulla unohdetuksi. Henkilötietojen käsittelystä informointi on keskeinen osa tietosuojan toteuttamista,

koska käytännössä sillä, miltä tietosuojan toteutuminen rekisteröidylle näyttää, on suuri merkitys. Läpinäkyvyyden periaatteen mukaisesti hyvällä viestinnällä luodaan kilpailuetua ja pienennetään riskejä.

Rekisterinpitäjällä on henkilötietojen käsittelystä viimesijainen vastuu. Tietosuoja-asetuksessa säädetyn sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi rekisterinpitäjän tulee järjestää toimintansa niin, että kaikki organisaation suorittama henkilötietojen käsittely tapahtuu oletusarvoisesti tietosuoja-asetuksen periaatteita noudattaen. Käytännön toiminnassa olennaista on toimittajien hallinta. Rekisterinpitäjän on arvioitava toimittajan kyky tietosuojan toteuttamiseksi toiminnassaan. Yhtä olennaista organisaatiolle, joka toimii henkilötietojen käsittelijänä, on pystyä osoittamaan oma kykynsä tietosuojavaatimusten täyttämiseksi. Sopimukset ovat riskienhallintakeino sekä rekisterinpitäjälle että henkilötietojen käsittelijälle. Organisaation riskienhallinnan näkökulmasta keskeistä on tietää, milloin organisaatio toimii rekisterinpitäjänä ja milloin henkilötietojen käsittelijänä.

Rekisterinpitäjän on hallittava henkilötietojen käsittelyn koko elinkaari. Tämän vuoksi tietosuojan käytännön toteuttamisessa tulee hallita myös henkilötietojen siirtoihin liittyvät kysymykset eli siirretäänkö henkilötietoja kolmansiin maihin. Henkilötietojen siirtoihin liittyvät seikat ilmenevät samoja kysymyksiä selvittämällä kuin käsiteltävät henkilötiedotkin eli missä, milloin ja miten henkilötietoja käsitellään.

Tiivistäen voidaan todeta, että tietosuojan käytännön toteuttamisessa on kyse henkilötietojen luokittelusta, riskiarvioinneista, tarpeellisen dokumentaation laatimisesta sekä tehtävien organisoinnista niin, että henkilötietojen käsittelyä koskevat tehtävät ja vastuut ovat selkeitä kullekin organisaatiossa työskentelevälle henkilölle sekä henkilötietojen käsittelijöille. Korostamatta ei voi olla organisaation sisäisen viestinnän ja tietosuoja-asioiden säännöllisen kouluttamisen tärkeyttä.

Leevi Simola, OTM, CIPP/E, Verohallinto