Tietosuoja-asetus sisäisen tarkastuksen näkökulmasta

EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation, GDPR) sovelletaan 25.5.2018 lähtien kaikissa EU:n jäsenmaissa lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä sekä yhdenmukaistaa EU:n jäsenvaltioiden tietosuojaa koskevia säännöksiä. Asetuksen tavoitteena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä.

Nykyisen henkilötietolain pääperiaatteet säilyvät uudessa tietosuoja-asetuksessa, jossa on lisäksi määritelty uusia velvoitteita rekisterinpitäjälle. Myös rekisteröidylle henkilölle on määritelty uusia oikeuksia, kuten esimerkiksi oikeus siirtää tietoja järjestelmästä toiseen.

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia rekisterinpitäjiä ja henkilötietojen käsittelijöitä sekä yksityisellä että julkisella sektorilla. Tietosuoja-asetuksen myötä useampaan eri EU:n jäsenvaltioon etabloitunut rekisterinpitäjä voi jatkossa olla tekemisissä vain yhden johtavan valvontaviranomaisen kanssa.

Henkilötietojen käsittelylle on aina oltava laissa määritelty käsittelyn oikeusperuste. Henkilön oikeus kontrolloida omia tietojaan tuo uusia velvoitteita käytännön asiakaspalvelutilanteisiin ja tiedon käytön dokumentointiin. Rekisterinpitäjän tulee voida selittää asiakkaalle mihin tarkoitukseen hänen henkilökohtaisia tietojaan käytetään ja suoda asiakkaalle pyynnöstä pääsy tietoihin sekä mahdollisuus rajoittaa tietojen käyttöä tai poistaa tietoja.

Tietosuoja-asetuksen keskeinen sisältö

Henkilötietoa on kaikki tieto, joka voidaan suoraan tai epäsuorasti liittää yksityishenkilöön, kuten nimi, henkilötunnus ja osoite, mutta myös esimerkiksi transaktiotiedot, IP osoite ja verkkotunnukset.

Tietosuoja-asetuksen riskiperusteinen lähestymistavan mukaan tietosuojavelvoitteet ja suojatoimet on suhteutettava rekisteröidyn henkilön oikeuksille aiheutuvaan riskiin. Rekisterinpitäjän on tehtävä arvio henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvista vahingoista esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai taloudellisiin menetyksiin.

Tiettyjen rekisterinpitäjien ja henkilötietojen käsittelijöiden on nimitettävä tietosuojavastaava. Tämä velvoite koskee kaikkia viranomaisia ja julkishallinnon elimiä sekä sellaisia muita organisaatioita, kuten rahoituslaitokset, joiden ydintehtäviin sisältyy henkilöiden järjestelmällinen ja laajamittainen seuranta tai erityisiin henkilötietoryhmiin kohdistuva laajamittainen käsittely.

Kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi. Riskin tasoa arvioitaessa on otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Vaikutustenarvioinnissa on tarkasteltava suunniteltuja toimenpiteitä sekä suojatoimia ja mekanismeja, joiden avulla voidaan lievittää tietojenkäsittelyyn kohdistuvaa riskiä ja varmistaa henkilötietojen suoja sekä asetuksen vaatimusten toteutuminen rekisterinpitäjän toiminnassa. Rekisterinpitäjän on aina tarvittaessa varmistettava, että henkilötietojen käsittely tosiasiallisesti tapahtuu vaikutustenarvioinnin mukaisesti ja annettava riittävät takeet siitä, että henkilötietojen käsittely täyttää tietosuoja-asetuksen vaatimukset esimerkiksi noudattamalla hyväksyttyjä käytännesääntöjä.

Tietojen suojaamisesta on huolehdittava kaikissa käsittelyn vaiheissa. Käsittelyn turvallisuus edellyttää esimerkiksi kykyä taata järjestelmien ja palveluiden jatkuva luottamuksellisuus ja käytettävyys sekä kykyä palauttaa tietojen saatavuus ja taata nopea pääsy tietoihin teknisen vian sattuessa. Tietojen suojaaminen edellyttää myös henkilötietojen käsittelyn tehokasta seuraamista ja valvontaa.

Tietosuoja tarkastustoiminnassa

Sisäisellä tarkastuksella on lähtökohtaisesti pääsy kaikkeen informaatioon, jota se tarvitsee tehtäviensä hoitamisessa, mukaan lukien yrityksen asiakas- ja henkilöstötietokannat. Yleisen luottamuksellisuusvelvoitteen lisäksi sisäiset tarkastajat eivät saa avoimesti keskustella saamistaan henkilötiedoista ja käsitellä niitä yrityksen muun henkilöstön kanssa, paitsi jos tiedot koskevat suoraan ao. henkilöstön tehtäviä.

Tarkastusprojektin valmistuttua mahdolliset asiakkaiden ja henkilöstön henkilötiedot tulisi poistaa tarkastustietokannoista ja työpapereista.

Tietosuojan implementoinnin tarkastaminen

Tarkastuksen tavoitteena on arvioida yrityksen tietosuojaohjelmaa ja sen organisointia sekä miten tietosuojaan liittyviä riskejä on identifioitu, priorisoitu ja lievennetty. Keskeisenä tarkastuskohteena on myös raportointi yrityksen johdolle ja hallitukselle.

Rekisterinpitäjät ovat perustaneet prosesseja hallinnoidakseen tietosuojaa ja varmistaakseen asiakkaan oikeuksien toteutumisen. Näiden prosessien tulee olla riittävän kattavia ja tehokkaita ja sisältää tarpeellinen tietotekninen tukirakenne. Myös tietosuojarikkomusten raportoinnin tulee olla täsmällistä ja välitöntä. Yrityksen sisäisen ohjeistuksen tulee kuvata, miten henkilötietoja kerätään, käytetään, säilytetään ja jaetaan yrityksen sisällä. Henkilöstön koulutuksen tulee myös riittävästi kattaa tietosuojanäkökohdat päivittäisessä liiketoiminnassa. Tietosuojan toteutumisen sisäisen valvonnan tulee olla tehokkaasti organisoitu.

Osa henkilötietojen käsittelyä koskevasta toiminnasta, kuten esimerkiksi tietojen säilytys- ja analysointipalveluja, on saatettu ulkoistaa tietojen käsittelyyn erikoistuneille yrityksille. Ulkoistuksiin liittyvien sopimusten ja valvonnan tulee olla riittävän kattavia, jotta ulkoistavan yrityksen lopullisen vastuun valvonta ja arviointi ovat mahdollisia. Tietosuoja-asetuksessa on yksityiskohtainen lista siitä, mitä henkilötietojen käsittelyä koskevan sopimuksen tulee sisältää.

Jim Johansson, CIA, CFSA, Nordea