

Rekisterinpitäjän ohjeistus henkilötietojen käsittelijälle

Tilitoimiston asiakkaan antama liite 1C tilitoimistolle

Tausta ja dokumentin tarkoitus

Ohjeistuksella varmistetaan, että asetuksen velvoite henkilötietojen käsittelyn suojaustoimista toteutetaan huomioiden tietojen riskiperusteisuus. Artiklan 1 mukaisesti ”Tällä asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan.”

Rekisterinpitäjän on ohjeistettava henkilötietojen käsittelijää siitä, kuinka henkilötietoja on käsiteltävä. Tietosuoja-asetus (29 artikla) määrää, että ”Henkilötietojen käsittelijä tai kukaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, ei saa käsitellä niitä muuten kuin rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä niin vaadita.”

Käytännön toimenpiteet ohjeistetaan rekisterinpitäjältä tietojen käsittelijälle:

Kirjallinen toimeksiantosopimus

Rekisterinpitäjä on tehnyt kirjallisen sopimuksen (artikla 28) ulkoistaessaan henkilötietojensa käsittelyn. Sopimuksen mukaisesti käsittelijä huolehtii siinä sovitusta tehtävistä. Tarkempi kuvaus tehtävistä on määritelty sopimuksen palveluerittelyllä. Sopimus määrittelee vastuunjaon osapuolten välillä. Sopimusta päivitetään tarvittaessa.

Salassapitosopimus

Rekisterinpitäjä on varmistanut, että henkilötietojen käsittelijän henkilöstö on sitoutunut noudattamaan salassapitovelvollisuutta (artikla 28). Käytännössä käsittelijä on tehnyt salassapitosopimuksen jokaisen kanssa, joka käsittelee näitä tietoja työssään. Muulla käsittelijän henkilöstöllä ei saa olla pääsyä henkilötietoihin.

Alihankkijoiden käyttäminen

Rekisterinpitäjä antaa ennakkoluvan, että henkilötietojen käsittelijä voi käyttää alihankkijoita toiminnassaan (artikla 28). Asetuksen edellyttämällä tavalla käsittelijän on ilmoitettava suunnitelluista muutoksista rekisterinpitäjälle.

Henkilötietojen käsittelyn turvallisuus -menetelmäkuvaukset

Rekisterinpitäjä on tehnyt henkilötietojen käsittelijän kanssa kuvauksen henkilötietojen toimittamisesta, käsittelystä, säilyttämisestä, säilytysajoista sekä tietojen luovuttamisesta, palauttamisesta ja poistamisesta. Kuvauksessa on huomioitu tietojen käsittelyn riskit ja suojaustoimenpiteet sekä Kirjanpitolain mukainen velvoite kirjanpidon aineiston säilyttämisestä, jota palkanlaskennan aineisto on.

Kuvauksen ajantasaisuus käydään yhdessä käsittelijän kanssa läpi määräajoin, vähintään kerran vuodessa, ja aina kun prosesseissa tai käytettävissä järjestelmissä tapahtuu muutoksia.

Menetelmäkuvauksessa on huomioitu asetuksen vaatimus (artikla 24) ”Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.”

Rekisterinpitäjä noudattaa huolellisuutta henkilöiden tietojen säilyttämisestä ja vastaa siitä, että tietoihin pääsy on rajattu käsittelijöille, joiden tehtävien hoitaminen sitä edellyttää. Rekisterinpitäjä on toimeksiantosopimusta tehtäessä varmistanut, että myös tietojen käsittelijän henkilöstön keskuudessa toimitaan asetuksen mukaisesti ja sillä on asiantuntemus, luotettavuus ja resurssit asetuksen noudattamiseksi. Ns. arkaluonteiset (artikla 9: muun muassa terveystiedot ja ay-jäsenyys) mukaiset tiedot on suojattava erityisellä huolellisuudella ja säilytettävä erillään muusta palkka-aineistosta.

Rekisterinpitäjä ohjeistaa tietojen käsittelijää käyttämään henkilötietojen välittämisessä suojattua sähköpostia tai vaihtoehtoisesti SaaS-järjestelmää, jossa tiedot toimitetaan salasanalla varmistetun palvelun kautta molemmin puolin, tai muuta suojattua tapaa, josta sovitaan erikseen.



Rekisterinpitäjä on varmistanut kirjallisesti järjestelmätoimittajilta, että heidän järjestelmissään noudatetaan tietosuojavelvoitteita teknisissä ratkaisuisa ja, että järjestelmätoimittajien henkilökunta on koulutettu tietosuoja-asetuksen sisällöstä. Rekisterinpitäjä on varmistanut henkilötietojen käsittelijältä, että tämä on toiminut samoin omien järjestelmätoimittajiensa kanssa. Siltä osin kuin järjestelmistä siirretään tietoja toisiin järjestelmiin, on liittymien tietoturvan varmistettava toimivan asianmukaisesti.

Selosteet käsittelytoimista

Rekisterinpitäjä on kuvannut henkilötietojen käsittelytoimet selosteessaan. Tilitoimisto on tehnyt oman selosteen käsittelijänä asiakkaan henkilötietojen käsittelystä. (artikla 30).

Tiedottaminen ja tiedonanto rekisteröidylle

Rekisterinpitäjä on huolehtinut tiedottamisesta henkilöille, joiden henkilötietoja rekisterissä käsitellään. Tiedote on saatavilla yrityksen normaaleissa tiedotuskanavissa, joita ovat sisäinen intranet, yrityksen ilmoitustaulu, jakelu sähköpostilla sekä uusien työntekijöiden perehdyttämisineistossa.

Rekisterinpitäjä on sopimuksessa käsittelijän kanssa ulkoistanut tilitoimistolle rekisteröidyn omien tietojen toimittamisen tämän pyynnöstä. Tietopyynnöt käsittelijälle toimittaa sopimuksella ilmoitettu rekisterinpitäjän yhteyshenkilö. Tästä on ilmoitettu rekisteröidyille tehdyssä tiedotteessa.

Käsittelijän velvollisuus opastaa rekisterinpitäjää

Rekisterinpitäjä ohjeistaa tietojen käsittelijää, että tämän velvollisuus on asetuksen mukaan (artikla 28) opastaa rekisterinpitäjää tietosuoja-asetuksen määräysten noudattamisessa.

Mikäli käsittelijä huomaa rekisterinpitäjän henkilöstön toimivan asetuksen vastaisesti, on käsittelijän ilmoitettava siitä rekisterinpitäjälle. Mikäli rekisterinpitäjä tarvitsee tietosuoja-asetuksen sisältöön ja noudattamiseen liittyen opastusta, se pyytää käsittelijältä ohjeistusta.

Tietoturvaloukkauksista ilmoittaminen

Rekisterinpitäjä edellyttää tietojen käsittelijää tekemään ilmoitukset tietoturvaloukkausten ilmi tullessa asetuksen mukaisesti (artikla 33 ja 34).

Ohjeistuksessa mainitut dokumentit

Tässä ohjeistuksessa mainitut dokumentit säilytetään ohjeistuksen liitteenä. Ohjeistuksen ja muiden asiakirjojen ajantasaisuutta tarkastellaan vähintään kerran vuodessa. Mikäli prosesseihin tai järjestelmiin tulee muutoksia, niiden tietoturvallisuus ja suojaustoimet varmistetaan ennen käyttöönottoa.

Ohjeistuksessa mainitut osapuolet

Tässä ohjeistuksessa asetuksen tarkoittama käsittelijä on *Tili Johanna* ja rekisterinpitäjä *Asiakas*

Dokumentti kertoo *Asiakkaan* ohjeet sen palkka- ja henkilöstöhallinnon tietojen käsittelyn ohjeet *Tili Johannelle* asetuksen edellyttämällä tavalla