



DPA:t ja SCC:t – Ymmärrätkö mihin olet sitoutunut?



Katariina Koski
Senior Associate



Aleks Nieminen
Senior Associate

Euroopan komissio päivitti henkilötietojen siirtotilanteissa käytettävät vakiosopimuslausekkeet kesällä 2021 ja päivitettyjen vakiosopimuslausekkeiden käyttönotolle säädetty 18 kuukauden siirtymäaika päättyy 27.12.2022 ([aiheesta tarkemmin](#) henkilötietojen siirtoa koskevassa artikkelissamme). Näin ollen henkilötietojen käsittelyä koskevia sopimuksia ollaan laajalti päivittämässä ja esimerkiksi Microsoft on 15.9.2022 päivittänyt henkilötietojen käsittelyyn liittyvän tietojenkäsittelysopimuksensa. Olennaisin muutos päivitetystä sopimuksessa liittyy roolituksiin, joiden puitteissa henkilötietoja siirretään ETA:n ulkopuolelle. Aiemmin Microsoftin sopimuskokonaisuus oli rakennettu siten, että tiedonsiirto tapahtui Euroopan komission vakiosopimuslausekkeiden turvin asiakkaan toimissa henkilötietojen viejänä ja Microsoft Corporationin toimiessa henkilötietojen vastaanottajana. Nyt Microsoft on arvioinut roolitusta uudelleen ja uusi sopimus on rakennettu sen pohjalta, että tietojen viejänä toimii asiakkaan sijaan Microsoft Ireland Operations Limited.

Microsoftin päivitetty näkemys tietojen viejän ja vastaanottajan rooleista vaikuttaa olevan linjassa esimerkiksi aiemmin samaan roolitukseen päätyneiden muiden globaalien pilvipalveluiden toimittajien kanssa (esim. Google). Käytännössä Microsoftin asiakkaiden on syytä huomioida tämä muutos toiminnassaan, sillä tiedon siirtäjän rooli siirtyy asiakkaalta Microsoftille. Teoriassa tietosuoja-asetuksen ja vakiosopimuslausekkeiden perusteella velvollisuus henkilötietojen siirron vaikutusten arvioinnin, eli ns. *transfer impact assessment* (TIA-arviointi), suorittamiseen kuuluu vain tietojen viejän ja vastaanottajan vastuulle. Käytännössä Microsoftin asiakkaat eivät kuitenkaan voi huokaista helpotuksesta ja ajatella täysin vapautuvansa velvollisuudesta arvioida tietojen siirtoja, sillä rekisteripitäjällä on yleinen velvollisuus arvioida henkilötietojen käsittelyyn, mukaan lukien käsittelijöiden toimintaan, liittyviä riskejä. Henkilötietojen siirtoihin liittyvien **riskien arviointi on siis edelleen rekisteripitäjän vastuulla** ja tässä kontekstissa TIA-arvioinnin suorittaminen jossain laajuudessa on paikallaan.

Kansainvälisiin pilvipalveluntarjoajiin liittyvän keskustelun ja valvontaviranomaisten kritiikin keskiössä on ollut problematiikka koskien asiakkaiden tietojen luovuttamista kolmansien maiden viranomaisille. Microsoftin

edellisessä sopimusversiossa annettujen sitoumusten (mm. luovutuspyyntöjen ohjaaminen rekisterinpitäjälle, velvollisuus arvioida ja haastaa pyyntöjen laillisuus) lisäksi Microsoft sitoutuu päivitetyn sopimuksen mukaisesti luovuttamaan tai antamaan pääsyn asiakkaan tietoihin vain, jos EU:n lainsäädännön rajoitusedellytykset täyttyvät. Microsoftin uudistetun sopimuksen mukaisesti *"Microsoft paljastaa Käsiteltäviä tietoja tai antaa niihin pääsyn laissa vaaditun mukaisesti edellyttäen, että lait ja käytännöt noudattavat perusoikeuksia ja -vapauksia koskevia periaatteita eivätkä ylitä sitä, mikä on välttämätöntä ja oikeasuhteista demokraattisessa yhteiskunnassa, ja tapauksen mukaan yleisen tietosuoja-asetuksen 23 artiklan 1 kohdassa lueteltujen tavoitteiden turvaamiseksi"*. Näin Microsoft selvästi asettaa tietojen luovuttamisen lähtökohtaiseksi standardiksi EU:n lainsäädännön, tarkemmin yleisen tietosuoja-asetuksen takaaman tason. Valitettavasti nämä ylimääräiset sitoumukset eivät todennäköisesti täysin poista riskiä siitä, että Yhdysvaltain viranomaisilla on mahdollisuus päästä henkilötietoihin, jos Microsoftin suorittamaan käsittelyyn sovelletaan asiaankuuluvaa Yhdysvaltain (tiedustelu)lainsäädäntöä.

Päivitetysssä sopimuksessa Microsoft on myös tarkentanut, mitä tietoja käsitellään sen omiin tarkoituksiin. Uuden sopimuksen puiteissa asiakas valtuuttaa Microsoftin muun muassa luomaan asiakkaan pseudonyymistä tiedosta yhdisteltäviä tilastollisia tietoja Microsoftin omiin tarkoituksiin, kuten laskutus, tilinhallinta sekä sisäinen raportointi ja liiketoiminnan simulointi. Aiemmin mainittuja tarkoituksia, kuten petosten ja kyberrikollisuuden torjuntaa ei ole päivitetysssä versiossa mainittu osana Microsoftin roolia rekisterinpitäjänä. Asiakkaan on hyvä tunnistaa nämäkin muutokset omien rekisterinpitäjävelvoitteiden toteuttamisessa.

Kaiken kaikkiaan muutokset eivät ole käytännön tasolla järin yllättäviä tai mullistavia. Henkilötietojen luovuttamiseen (viranomaisille) liittyvien, eurooppalaiseen tietosuojasäätelyyn nojaavan rajoitusedellytyksen merkitys ja käytännön vaikutukset jäävät osittain epäselväksi. Päivityksessä kyseessä on lähinnä uusien vakiosopimuslausekkeiden myötä tehty tekninen muutos, jonka myötä ja henkilötietojen siirtoihin liittyvät roolit asetetaan uuteen asentoon ja vakiosopimuslausekkeet solmitaan käsitelijöiden välisessä suhteessa.

Mikäli yrityksenne ei vielä täytä henkilötietojen siirtoihin liittyviä velvoitteitaan, [ole yhteydessä meihin](#). DLA Piperin kehittämän [Transfer-metodologian](#) avulla hoidamme henkilötietojen siirtoja koskevat arvioinnit kerralla kuntoon.