Ovatko yrityksenne henkilötietojen siirrot EU:n tietosuojalainsäädännön mukaisia? Transfer-työkalumme avulla suoritat pakollisen arvioinnin

Sami Rintala
Partner

Onko yrityksellänne käytössä pilvipalveluita? Hyödyntääkö yrityksenne kolmannen osapuolen palveluita tai tuotteita kuten Google Analytics tai Salesforce? Ylläpidättekö itse SaaS-palvelua? Viimeaikaisten EU:n tietosuojalainsäädännön vaatimusten muutosten johdosta yritykset ympäri EU:ta joutuvat arvioimaan tekemiään henkilötietojen siirtoja EU:n ja ETA:n ulkopuolisiin niin sanottuihin kolmansiin maihin. Arvio tulee toteuttaa, jotta voidaan varmistaa EU:n takaaman tietosuojan tason säilyvän myös tietojen siirtojen yhteydessä. Arvio tulee toteuttaa palvelu- ja maakohtaisesti, ja sen tulee sisältää kohdemaan lainsäädännön arviointi.

Kokosimme yhteen tietojen siirtoihin liittyviä yleisimpiä kysymyksiä. Vaadittavan arvion tekeminen on haastavaa, myös organisaatioille, joilla on omaa tietosuoja- ja tietoturvaosaamista talon sisällä. Arvioinnin laajuuden ja haastavuuden vuoksi olemme myös kehittäneet työkalun auttamaan yrityksiä arvion toteuttamisessa. Transfer-työkalumme avulla voit toteuttaa arvion sekä tehokkaasti että velvoitteiden mukaisesti.

1. Mikä on muuttunut EU:n tietosuojalainsäädännön vaatimuksissa ja keitä se koskee?

Euroopan Unionin tuomioistuimen niin sanotun Schrems II -tuomion myötä tietojen siirroille kolmansiin maihin asetettiin tiukempia vaatimuksia. Jos tietojen siirron kohdemaalla ei ole EU:n komission vastaavuuspäätöstä, tietojen viejinä toimivien yritysten tulee valita tietojen siirroille GDPR:n V luvun mukainen siirtomekanismi. Siirtomekanismin valinnan ja käyttöönoton lisäksi yritysten tulee tehdä tietojen siirron vaikutustenarviointi (Transfer Impact Assesment, TIA), arvioidakseen säilyykö tietosuojan taso EU:n tasoa vastaavana. Jos arviossa todetaan, että tietojen siirron yhteydessä tietosuojan taso laskee, yrityksen tulee ottaa käyttöön täydentäviä suojatoimia, tai jos täydentävien suojatoimienkaan avulla ei voida taata EU:n tietosuojaa vastaavaa tasoa, tietoja ei tulisi siirtää.

Tämä koskee kaikkia yrityksiä, jotka siirtävät henkilötietoja kolmansiin maihin. Valtaosassa nykyisistä pilvipalveluista ja SaaS-palveluista tapahtuu henkilötietojen siirtoja EU:n ja ETA:n ulkopuolelle.

2. Mikä on Schrems II -tuomio?

Itävaltalainen tietosuoja-aktivisti Maximillian Schrems teki kantelun Irlannin tietosuojavaltuutetulle siitä, että Facebook siirsi henkilötietoja Yhdysvaltoihin. Kantelussa oli kyse siitä, ettei Yhdysvallat takaa henkilötiedoille EU:n tietosuojaa vastaavaa tietosuojan tasoa, erityisesti Yhdysvalloissa lainsäädännössä sallitun viranomaisten tiedustelutoiminnan vuoksi. Asia päätyi EU:n tuomioistuimen arvioitavaksi, ja tuomioistuin kumosi ns. Privacy Shield -järjestelyn, jonka nojalla henkilötietoja voitiin aiemmin siirtää EU:sta Yhdysvaltoihin. Tuomion myötä tietojen siirrot kolmansiin maihin vaativat aiempaa kattavamman riskiarvioinnin ja mahdollisia täydentäviä suojatoimia. Schrems II -tuomion seurauksena Euroopan tietosuojaneuvosto julkaisi ohjeistuksen tietojen siirron yhteydessä tehtävästä riskiarviosta sekä täydentävistä suojatoimista.

3. Yrityksemme tietosuoja-asiat päivitettiin jo vuonna 2018 GDPR:n mukaisiksi. Pitääkö vielä tehdä jotain?

Vaikka yrityksenne tietosuoja-asiat päivitettiin vuonna 2018 GDPR:n mukaisiksi, Schrems II -tuomio ja uudet vakiosopimuslausekkeet aiheuttavat uusia velvoitteita yrityksille, jotka siirtävät henkilötietoja kolmansiin maihin. Tämän johdosta yritysten tulee kartoittaa tietojen siirtonsa, päivittää mahdolliset vakiosopimuslausekkeet uusiin 27.12.2022 mennessä sekä tarvittaessa suorittaa tietojen siirtoja koskeva vaikutustenarviointi, jonka perusteella voidaan arvioida ja ottaa käyttöön tiedon siirtoihin liittyviä lisäsuojatoimenpiteitä.

DLA Piperin Suomen tietosuojatiimin osakas Sami Rintala kommentoi: ”Schrems II edellyttää, että organisaatiot arvioivat ja perustelevat tiedonsiirrot. Usein kysymys on, joudutaanko jostain jo laajassa käytössä olevasta esim. SaaS-ratkaisusta luopumaan, tai millä edellytyksin sen käyttöä voidaan jatkaa. Moni suomalainen organisaatio on jo havahtunut siihen, että arvioiden tekeminen edellyttää sellaista juridista ja teknistä osaamista sekä tietoturvaratkaisujen ymmärtämistä, mitä organisaatiossa ei ole. Monissa organisaatioissa ei ole vielä tiedostettu, mistä oikein on kyse, mitä tulisi tehdä, tai mistä kannattaa lähteä liikkeelle.”

4. Mitä ovat vakiosopimuslausekkeet?

Henkilötietojen siirto EU:n ja ETA:n ulkopuolelle voidaan tehdä käyttäen EU:n komission hyväksymiä vakiosopimuslausekkeita (standard contractual clauses, SCC) siirtomekanismina. Vakiosopimuslausekkeet solmitaan tietojen viejän ja tietojen tuojan välillä. Komissio päivitti vakiosopimuslausekkeet 4.6.2021. Päivitettyjen vakiosopimuslausekkeiden käyttöönotolle on säädetty 18 kuukauden siirtymäaika, joka päättyy 27.12.2022. Yrityksen solmiessa uusia sopimuksia, joihin liittyy tietojen siirto kolmansiin maihin, on siis tullut jo käyttää uusia vakiosopimuslausekkeita ja vanhojen sopimuksien vakiosopimuslausekkeet tulee päivittää uusiin 27.12.2022 mennessä.

5. Mitä jos yrityksemme ei ota käyttöön uusia vakiosopimuslausekkeita eikä tee tietojen siirron vaikutustenarviointia?

Jos yritys ei ota vakiosopimuslausekkeita lainkaan käyttöön tietojen siirron yhteydessä eikä myöskään vakiosopimuslausekkeiden sijasta käytä mitään muuta GDPR:n mukaista siirtomekanismia, yritys rikkoo GDPR:ää ja voi tämän seurauksena saada käsittelykiellon, seuraamusmaksun ja korvausvaatimuksia. Seuraamuksia voi yhtä lailla saada tietojen siirron vaikutustenarvioinnin tekemättä jättämisestä. Yhtenä suurimmista uhista yrityksille voi pitää viranomaisen määräämää käsittelykieltoa, jonka seurauksena yritys ei voisi tarjota palveluitaan.

6. Meillä on käytössä kolmannessa maassa sijaitseva SaaS-palvelu, jossa on asiakastietojamme. Miten yrityksemme tulee toimia tilanteen suhteen?

Yritysten kannalta olisi helpointa puhtaasti tietosuojanäkökulmasta, ettei henkilötietoja siirrettäisi lainkaan EU:n ja ETA:n ulkopuolelle, mutta usein tämän toteuttaminen ei ole mahdollista, tai se ei ole järkevää kaupallisista tai operatiivisista syistä. Monelle tulee yllätyksenä, että ”siirroksi” katsotaan tietosuojalainsäädännön mukaan myös tilanne, jossa data fyysisesti sijaitsee EU:n ja ETA:n alueella, mutta siihen on pääsy kolmansista maista, kuten usein on esim. huolto- ja tukitilanteissa. Käytännössä valtaosassa nykyisistä pilvipalveluista ja SaaS-palveluista tapahtuu henkilötietojen siirtoja EU:n ja ETA:n ulkopuolelle.

Tilanteessa, jossa tietoja siirretään kolmanteen maahan, yrityksen tulee käyttää GDPR V luvun mukaista siirtomekanismia ja tehdä tietojen siirron vaikutustenarviointi. Tilanteesta riippuen tietojen siirron vaikutustenarviointi voi osoittaa, että yrityksen tulee ottaa käyttöön täydentäviä suojatoimia, jotka voivat olla teknisiä, organisatorisia tai sopimuksellisia.

7. Yrityksemme myy SaaS-palvelua, jossa käsitellään henkilötietoja. Miten yrityksemme tulee toimia tässä tilanteessa?

Yrityksen käsitellessä muiden yritysten henkilötietoja käsittelijän roolissa tarjoamassaan SaaS-palvelussa yritys on velvollinen huomioimaan mm. käyttämänsä alikäsittelijät tietojen siirron osalta. Jos tietojen siirto tapahtuu

käsittelijältä käsittelijälle, on tietojen viejänä toimiva käsittelijä velvollinen huomioimaan GDPR V luvun velvoitteet. Lisäksi on tehtävä tietojen siirron vaikutustenarviointi, sekä tilanteesta riippuen ottaa käyttöön täydentäviä suojatoimia.

8. Miten yrityksenne tulisi tehdä tietojen siirron vaikutustenarviointi eli *transfer impact assessment*?

Tietojen siirron vaikutustenarviointi koostuu viidestä vaiheesta:

1. Tunnista ja dokumentoi siirtosi

2. Arvioi kohdemaan lainsäädännön tietosuojan taso

3. Arvioi täydentävät suojatoimet

4. Arvioi rekisteröidyille koituvan haitan vakavuus ja todennäköisyys

5. Lopullinen riskiarvio

DLA Piper on kehittänyt työkalun nimeltä Transfer, joka toimii yritysten apuna tietojen siirron vaikutustenarvioinnin tekemisessä. Työkalu luo kattavan dokumentaation ja raportin, jonka avulla yritykset voivat täyttää tietojen siirtoihin liittyvät velvoitteensa.

Lisäksi DLA Piperilla on valmiina laaja ja edullinen kirjasto tarvittavia maa-analyysejä yli 60 EU:n ja ETA:n ulkopuolisesta maasta, joiden avulla yritys voi täyttää tietojen siirron vaikutustenarvioinnin vaiheen 2 velvoitteen arvioida kohdemaan lainsäädännön tietosuojan tasoa. Tämä helpottaa huomattavasti paikallisen lainsäädännön arviointia ja saatavilla on aina päivitetty versio maa-analyyseistä.

9. Koska tietojen siirron vaikutustenarvioinnin pitää olla tehty?

Uudet vakiosopimuslausekkeet tulee ottaa käyttöön vanhoissa sopimuksissa 27.12.2022 mennessä. Viimeistään vakiosopimuslausekkeiden päivityksen yhteydessä yritysten tulisi ottaa huomioon myös muut tietojen siirtoihin liittyvät velvollisuudet, kuten tietojen siirtojen vaikutustenarvioinnin tekeminen, jos tätä työtä ei ole vielä aloitettu.

10. Kuinka laaja projekti tietojen siirron vaikutustenarviointi on?

Projektin laajuus riippuu siitä, kuinka moneen maahan tietojen siirtoja tapahtuu ja kuinka monen eri palvelun kautta.

“Schrems II -tuomion myötä ristiriitaisten säännösten tulkinnan vaivaa ja vastuuta on siirretty instituutioilta tiedonsiirtoja tekeville organisaatioille. Schrems II:n vaatimusten täyttäminen on haastavaa niillekin organisaatioille, joilla resurssit ja tiedot ovat hyvät. Monet keskisuuret ja pienet yritykset eivät siitä selviydy”, toteaa DLA Piperin Ewa Kurowska-Tober, Global Co-Chair of Data Protection & Security Group.

DLA Piperin *Transfer*-työkalu on rakennettu tukemaan yrityksiä tietojen siirtojen vaikutustenarvioinnissa. Sen avulla tietojen siirron vaikutustenarvioinnin tekemiselle on selvä rakenne, joka auttaa huomioimaan siirtoon liittyvät olennaiset seikat tarjoten samalla tehokkaan tavan tietojen siirtojen vaikutustenarvioinnin toteuttamiseen.

Transfer-työkalun palvelukokonaisuus räätälöidään asiakkaan tarpeiden mukaan, ilman piilokustannuksia. Työkalu toimii yhtä hyvin monikansalliselle yritykselle, joka siirtää tietoja maailmanlaajuisessa verkostossa, kuin pienemmälle organisaatiolle, joka hallinnoi kertaluonteisia siirtoja.

Projekti voidaan aloittaa pilottiprojektilla, jossa henkilötietojen siirron arvioinnin tekemistä tukee DLA Piperin asiantuntijatiimi. Pilottiprojektin jälkeen organisaatiollanne on prosessi, työkalut ja osaaminen viimeistellä arvioinnit itsenäisesti.

Tarvittaessa DLA Piperin tietosuoja-asiantuntijat hoitavat tietojen siirron vaikutustenarvioinnin teille palveluna alusta loppuun.

Jos ette ole vielä aloittaneet arviointia tai epäröitte, miten hanketta kannattaisi parhaalla tavalla edistää, olkaa toki yhteydessä meihin! Tehokas puolen tunnin tapaaminen voi parhaassa tapauksessa olla tämän vuoden paras investointisi yritykseenne.