TIETOSUOJAVALTUUTETUN TOIMISTO

31.5.2023

Dnro 7684/171/22

Apulaistietosuojavaltuutetun päätös henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa

Asia Verkkosivustolla käytettäviin seurantateknologioihin liittyvä henkilötietojen käsittely

Asiassa on annettu samalla asianumerolla (7684/171/22) päätös 27.4.2023. Tämä päätös korvaa kyseisen aiemman päätöksen.

Rekisterinpitäjä Ilmatieteen laitos

Rekisterinpitäjän tietoturvaloukkausilmoitus

Ilmatieteen laitos[1] on tehnyt tietosuojavaltuutetun toimistolle tietoturvaloukkausilmoituksen 16.9.2022. Ilmoituksen mukaan rekisterinpitäjä on käyttänyt verkkopalveluissaan evästeitä hyödyntäviä verkkopalvelun liitännäisiä, joissa on kyse Googlen tuotteista.

Rekisterinpitäjän mukaan tietoturvaloukkaus havaittiin, kun julkisten sivujen käyttäjä oli rekisterinpitäjään yhteydessä Google Analytics ja reCAPTCHA-palveluiden käytöstä.

Tietoturvaloukkauksen alkamispäivä on rekisterinpitäjän mukaan ollut 1.1.2010, ja analytiikka on poistettu käytöstä syyskuussa 2022. Tietoturvaloukkauksen kohteena olevien rekisteröityjen määräksi rekisterinpitäjä arvioi 330 000 henkilöä.

Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä selvitystä 22.9.2022 päivätyllä selvityspyynnöllä. Rekisterinpitäjä on antanut asiassa kirjallisen selvityksen 7.10.2022.

Rekisterinpitäjä on selvityksessään vahvistanut, että verkkosivuilla on käytetty Google Analytics ja reCAPTCHA-palvelua.

ReCAPTCHA-tunnistusta on selvityksen mukaan käytetty palautelomakkeen yhteydessä, ja tarkoituksena on ollut erottaa tietokoneohjelmat ihmisistä. Google Analytics -palvelua on käytetty kävijämäärän seurantaan.

[1] Ilmatieteen laitos on liikenne- ja viestintäministeriön hallinnonalalle kuuluva palvelu- ja tutkimuslaitos, joka tuottaa havainto- ja tutkimustietoa ilmakehästä ja meristä sekä sää-, meri- ja ilmastopalveluita yleisen turvallisuuden, elinkeinoelämän ja kansalaisten tarpeisiin.

Rekisterinpitäjän mukaan EU-tuomioistuimen asiassa C-311/18 antamassa ratkaisussa (ns. Schrems II -ratkaisu) tarkoitettuja täydentäviä suojatoimia ei ole otettu käyttöön, eikä henkilötietojen siirroille ole ollut yleisen tietosuoja-asetuksen V-luvun mukaista siirtoperustetta.

Sovellettavasta lainsäädännöstä

Euroopan parlamentin ja neuvoston yleistä tietosuoja-asetusta (EU) 2016/679 (yleinen tietosuoja-asetus) on sovellettu 25.5.2018 alkaen. Säädös on asetuksena jäsenvaltioissa välittömästi sovellettavaa oikeutta. Yleistä tietosuoja-asetusta täsmentää kansallinen tietosuojalaki (1050/2018).

Yleisen tietosuoja-asetuksen 44 artiklassa säädetään henkilötietojen siirtoja koskevasta yleisestä periaatteesta. Artiklan mukaan sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain, jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat yleisen tietosuoja-asetuksen V-luvussa vahvistettuja edellytyksiä, ja ellei yleisen tietosuoja-asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia yleisen tietosuoja-asetuksen V-luvun säännöksiä on sovellettava, jotta varmistetaan, että yleisen tietosuoja-asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.

Yleisen tietosuoja-asetuksen 45 artiklassa säädetään henkilötietojen siirrosta tietosuojan riittävyyttä koskevan päätöksen perusteella. Artiklan 1 kohdan mukaan henkilötietojen siirto johonkin kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Tällaiselle siirrolle ei tarvita erityistä lupaa.

Yleisen tietosuoja-asetuksen 46 artiklassa säädetään henkilötietojen siirrosta kolmanteen maahan tai kansainväliselle järjestölle asianmukaisia suojatoimia soveltaen. Jollei yleisen tietosuoja-asetuksen 45 artiklan 3 kohdan mukaista päätöstä ole tehty, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Artiklan kohdissa 2 ja 3 on avattu, mitä asianmukaiset suojatoimet voivat olla. Artiklan 2 kohdan mukaan asianmukaisia suojatoimia voivat olla: a) viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline; b) 47 artiklan mukaiset yritystä koskevat sitovat säännöt; c) komission 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen antamat tietosuojaa koskevat vakiolausekkeet; d) tietosuojaa koskevat vakiolausekkeet, jotka tietosuojaviranomainen vahvistaa ja jotka komissio hyväksyy 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen; e) 40 artiklassa tarkoitetut hyväksytyt käytännesäännöt yhdessä kolmannen maan rekisterin-pitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin; f) 42 artiklassa tarkoitettu hyväksytty sertifiointimekanismi yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin. Artiklan 3 kohdan mukaan toimivaltaisen valvontaviranomaisen luvalla

asianmukaisia suojatoimia voivat olla myös erityisesti seuraavat: a) rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön rekisterinpitäjän, henkilötietojen käsittelijän tai vastaanottajan väliset sopimuslausekkeet; tai b) säännökset, jotka sisällytetään viranomaisten tai julkisten elinten välisiin hallinnollisiin järjestelyihin ja joihin sisältyy rekisteröityjen täytäntöönpanokelpoisia ja tehokkaita oikeuksia.

Oikeudellinen kysymys

Apulaistietosuojavaltuutettu arvioi ja ratkaisee asian edellä mainitusti yleisen tietosuoja-asetuksen (EU) 2016/679 ja tietosuojalain (1050/2018) pohjalta.

Apulaistietosuojavaltuutetun on ratkaistava:

1) Onko rekisterinpitäjän kansainvälisiä tiedonsiirtoja koskeva menettely ollut nyt arvioiduilta osin yleisen tietosuoja-asetuksen 44 ja 46 artiklojen mukaista, ja onko henkilötietojen siirtoihin Yhdysvaltoihin ollut olemassa pätevä siirtoperuste.

Apulaistietosuojavaltuutetun päätös

Päätös

Rekisterinpitäjällä ei ole ollut käsiteltävänä olevassa asiassa pätevää siirtoperustetta henkilötietojen siirtoihin Yhdysvaltoihin, eikä rekisterinpitäjän menettely ole ollut yleisen tietosuoja-asetuksen 44 ja 46 artiklojen mukaista. Yleisen tietosuoja-asetuksen 44 artiklan mukaan henkilötietojen siirrot kolmanteen maahan voidaan toteuttaa vain, jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat yleisen tietosuoja-asetuksen V-luvussa vahvistettuja edellytyksiä. Henkilötietojen siirrolle on oltava olemassa yleisen tietosuoja-asetuksen V-luvun mukainen siirtoperuste, ja silloin, jos rekisterinpitäjä ei voi toteuttaa tiedonsiirtoja yleisen tietosuoja-asetuksen 45 artiklassa tarkoitetun tietosuojan riittävyyttä koskevan päätöksen perusteella, rekisterinpitäjän tulee toteuttaa yleisen tietosuoja-asetuksen 46 artiklan mukaiset suojatoimet. EU-tuomioistuimen asiassa C-311/18 antaman ratkaisun mukaisesti rekisterinpitäjä ei nyt arvioidussa asiassa ole voinut käyttää siirtoperusteena tietosuojan riittävyyttä koskevaa päätöstä, eikä rekisterinpitäjä ole reCAPTCHA ja Google Analytics -palveluiden kohdalla määritellyt tai soveltanut lainmukaista henkilötietojen siirtoperustetta (rikotut artiklat: 44 ja 46).

Määräys

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58(2)(d) artiklan mukainen määräys huolehtia siitä, että tässä asiassa arvioituja palveluita käytettäessä Yhdysvaltoihin ilman lainmukaista siirtoperustetta siirretyt henkilötiedot poistetaan. Asiassa saadun selvityksen perusteella rekisterinpitäjä on jo ryhtynyt toimenpiteisiin reCAPTCHA- ja Google Analytics -palveluiden poistamiseksi verkkosivuiltaan, eikä asiassa ole tämän vuoksi tarpeen antaa edellä mainittujen palveluiden verkkosivuilta poistamista koskevaa määräystä käsittelytoimien saattamiseksi tietosuojasääntelyn mukaisiksi.

Apulaistietosuojavaltuutettu jättää rekisterinpitäjän harkintaan asianmukaiset toimenpiteet, mutta määrää toimittamaan selvityksen tehdyistä toimenpiteistä tietosuojavaltuutetun toimistolle **30.6.2023** mennessä, ellei rekisterinpitäjä hae määräyksen osalta muutosta tähän päätökseen.

Huomautus

Rekisterinpitäjä on Google Analytics -analytiikkatyökalua ja reCAPTCHA-palvelua käyttäessään siirtänyt henkilötietoja Yhdysvaltoihin ilman pätevää henkilötietojen siirtoperustetta. Menettelyllään rekisterinpitäjä on rikkonut yleisen tietosuoja-asetuksen 44 ja 46 artiklaa. Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58(2)(b) artiklan mukainen huomautus yleisen tietosuoja-asetuksen säännösten vastaisista henkilötietojen käsittelytoimista koskien henkilötietojen siirtoja Yhdysvaltoihin.

Muiden verkkosivuilla mahdollisesti käytössä olevien palveluiden osalta rekisterinpitäjälle annetaan ohjausta (ks. tämän päätösasiakirjan sivu 6).

Perustelut

Henkilötietojen siirroista Yhdysvaltoihin

Unionin ja Yhdysvaltojen välillä on aiemmin voitu toteuttaa tiedonsiirtoja niin kutsutun Privacy Shield -järjestelyn nojalla. Järjestelyllä on ollut tarkoitus turvata riittävä tietosuojan taso siirrettäville henkilötiedoille. EU-tuomioistuin on 16.7.2020 asiassa C-311/18 antamassaan ratkaisussa kumonnut komission päätöksen koskien Privacy Shield -järjestelyä ja todennut, että tietosuojan riittävyyttä Yhdysvalloissa koskeva Privacy Shield -päätös on pätemätön.[2] Ratkaisun mukaan, mikäli Euroopan unioniin sijoittautunut rekisterinpitäjä tai sen henkilötietojen käsittelijä ei voi toteuttaa riittäviä lisätoimenpiteitä riittävän henkilötietojen suojan varmistamiseksi, sen on keskeytettävä tai lopetettava henkilötietojen siirto asianomaiseen kolmanteen maahan.[3]

reCAPTCHA ja Google Analytics

CAPTCHA[4]-palveluita käytetään erottamaan, onko sivuston käyttäjä ihminen vai tietokone. Yleensä CAPTCHA-palveluiden tarkoituksena on mahdollistaa esimerkiksi niin kutsuttujen bottien automatisoidun toiminnan estäminen, kuten palautteiden massalähettäminen palautelomakkeella. CAPTCHA-testi voi käytännössä olla esimerkiksi kuvanvarmennus, jossa ruudukosta tulee valita tietyn sisältöisiä kuvia (kuten ajoneuvoja tai liikennevaloja), tai testissä saattaa olla kyse näkymättömästä, sivustolla vierailijan käyttäytymisen arviointiin perustuvasta menetelmästä.

Nyt arvioitavassa asiassa käytetyn CAPTCHA-palvelun kohdalla on kyse yhdysvaltalaisyritys Googlen reCAPTCHA-palvelusta. Palvelu on ollut käytössä rekisterinpitäjän sivustolta löytyvän palautelomakkeen yhteydessä. Rekisterinpitäjän verkkosivustolla on lisäksi ollut käytössä Google Analytics -analytiikkatyökalu.

Google Analytics ja reCAPTCHA-palveluissa on kyse ulkoisista palveluista. Ulkoisia palveluja käytettäessä henkilötietoja käsitellään ulkoisen palveluntarjoajan palvelussa, kyseisen palveluntarjoajan (eli tässä tapauksessa Googlen) toimesta. Tässä yhteydessä palveluntarjoajalle välittyy verkkosivuilla vierailijoista yleisen tietosuoja-asetuksen 4 artiklassa tarkoitettuja henkilötietoja, kuten IP-osoitteita ja muita tietoja, joita voidaan käyttää rekisteröidyn tunnistamisessa.

[2] Asia C-311/18, ratkaisun kohta 201.
[3] Asia C-311/18, ratkaisun kohta 135.
[4] Completely Automated Public Turing test to tell Computers and Humans Apart.

Palveluntarjoajalle välittyvät tiedot voivat käsittää esimerkiksi tietoja verkkosivustolla vierailijan selaimesta ja käyttäjästä (kuten sivustolla vierailijan käytössä oleva selain ja selainruudun koko, kielivalinnat, aikavyöhyke ja asennetut fontit) ja tietoja päätelaitteesta (kuten vierailijan päätelaitteen tyyppi, käyttöjärjestelmä, näytön resoluutio ja koko sekä näytönohjaimen tyyppi). Näistä tiedoista muodostettujen yhdistelmien vertailu mahdollistaa rekisteröityjen laajamittaisen, automatisoidun tunnistamisen ja profiloinnin, ja samanlaisena toistuva yhdistelmä eri sivustovierailujen yhteydessä kertoo siitä, että kyseessä on todennäköisesti aina sama käyttäjä.[5] Tietoja voidaan näin käyttää rekisteröidyn tunnistamiseksi, ja niitä voidaan tunnistamis- ja profilointitarkoituksessa yhdistää myös muihin, samasta käyttäjästä kerättyihin tietoihin. Palveluntarjoajalle välittyviin tietoihin lukeutuu edellä todetusti myös henkilötiedoksi katsottava ja rekisteröidyn tunnistamisen mahdollistava IP-osoite.[6]

Nyt arvioitavassa asiassa on kyse yhdysvaltalaispalveluntarjoajasta (Google), jonka tässä asiassa arvioituja palveluita käytettäessä henkilötietoja siirtyy Yhdysvaltoihin ja jonka palveluiden kohdalla rekisterinpitäjän olisi tullut tehdä asianmukainen arvio siitä, ovatko tiedonsiirrot tietosuojasääntelyn mukaisia. Tietosuojavaltuutetun toimistolle antamansa selvityksen mukaan rekisterinpitäjä ei ole määritellyt asiassa yleisen tietosuoja-asetuksen V-luvun mukaista siirtoperustetta, eikä arvioinut mahdollisten täydentävien suojatoimien tarvetta tai ottanut käyttöön täydentäviä suojatoimia, joilla yhdysvaltalaisen palveluntarjoajan ja Yhdysvaltojen tiedusteluviranomaisen pääsy kaikkiin henkilötietoihin estettäisiin tehokkaasti.

Rekisterinpitäjä on edellä esitetysti laiminlyönyt yleisen tietosuoja-asetuksen 44 ja 46 artiklojen mukaiset velvollisuutensa. Rekisterinpitäjä ei reCAPTCHA ja Google Analytics -palveluiden kohdalla ole huolehtinut asianmukaisesti siitä, että henkilötietojen siirroille on olemassa pätevä siirtoperuste, eikä rekisterinpitäjä ole myöskään siirtoperusteen puuttuessa keskeyttänyt tai lopettanut tiedonsiirtoja viipymättä EU-tuomioistuimen asiassa C-311/18 antaman ratkaisun jälkeen. Rekisterinpitäjälle annetaan tämän menettelyn osalta huomautus sekä määräys poistaa Yhdysvaltoihin ilman lainmukaista siirtoperustetta siirretyt henkilötiedot.

Seurannan käytöstä yleisemmin

Apulaistietosuojavaltuutettu toteaa tässä yhteydessä yleisellä tasolla, että verkkosivuilla tapahtuvaa henkilötietojen käsittelyä toteutettaessa on syytä huomioida, ettei rekisterinpitäjä voi siirtää vastuutaan tiedonsiirtojen lainmukaisuuden varmistamisesta rekisteröidyille, vaan rekisterinpitäjän on huolehdittava, ettei verkkosivustolla seurantateknologioita käytettäessä siirretä henkilötietoja esimerkiksi Yhdysvaltoihin ilman pätevää ja rekisterinpitäjän hyödynnettävissä olevaa riittävyyspäätöstä tai ilman asianmukaisia täydentäviä suojatoimia. Tämä on huomioitava myös evästebannereita käytettäessä. Vaikka rekisteröidyllä olisi mahdollisuus kieltää evästeitä evästebannerissa, rekisteröidyn henkilötietoja voi päätyä lainvastaisesti esimerkiksi Yhdysvaltoihin.

Lisättäköön, etteivät rekisterinpitäjät voi myöskään siirtää vastuutaan rekisteröidyille ohjaamalla rekisteröityjä esimerkiksi asentamaan selaimeensa Googlen tarjoama lisäosa, jolla Googlen seurantateknologian, kuten Google Analytics -palvelun, käyttö

[5] Henkilötietoja ovat myös sellaiset tiedot, jotka voidaan yhdistää luonnolliseen henkilöön lisätietoja käyttämällä, tietoja yhdistelemällä.
[6] Ks. IP-osoitteesta henkilötietona tarkemmin esim. unionin tuomioistuimen asiassa C-582/14 (Breyer) antama ratkaisu.

voidaan estää. Kyseinen Googlen tarjoama lisäosa[7] ei tämänhetkisten tietojen mukaan täysin estä rekisteröidyn tietojen välittymistä Googlelle, sillä se ei estä Google Analytics -skriptien lataamista Googlen palvelimilta. Skriptien lataamisessa Googlelle välittyy rekisteröidyn tunnistamisen mahdollistavia tietoja kuten IP-osoite ja tietoa käyttäjän selaimesta.

Sovelletut lainkohdat

Perusteluissa mainitut.

Muutoksenhaku

Tietosuojalain (1050/2018) 25 §:n mukaan tähän päätökseen voi hakea muutosta valittamalla hallinto-oikeuteen noudattaen mitä laissa oikeudenkäynnistä hallintoasioissa (808/2019) säädetään. Valitus tehdään hallinto-oikeuteen.

Tiedoksianto

Päätös annetaan tiedoksi hallintolain (434/2003) 60 §:n mukaisesti postitse saantitodistusta vastaan.

Lisätietoja tästä päätöksestä antaa asian esittelijä

Ylitarkastaja Niina Miettinen puh. 029 566 6774 niina.miettinen@om.fi

Tämän päätöksen on tehnyt apulaistietosuojavaltuutettu Annina Hautala.

Apulaistietosuojavaltuutetun ohjaus

Apulaistietosuojavaltuutettu ohjaa rekisterinpitäjää käymään huolellisesti läpi myös muut sen verkkosivustolla käytössä olevat palvelut sen varmistamiseksi, ettei henkilötietoja siirretä tietosuojasääntelyn vastaisesti EU-/ETA-alueen ulkopuolelle. Tässä arvioinnissa tulee huomioida, etteivät EU-tuomioistuimen asiassa C-311/18 antamassa ratkaisussa toteamat tiedonsiirtoihin liittyvät ongelmat rajoitu yhden palveluntarjoajan, kuten Googlen, palveluihin, sekä se, että esimerkiksi suomalaisten palvelutarjoajien palveluissa saatetaan hyödyntää joiltain osin muita palveluntarjoajia siten, että henkilötietoja siirtyy tietosuojasääntelyn vastaisesti EU-/ETA-alueen ulkopuolelle.

Tähän apulaistietosuojavaltuutetun ohjaukseen ei voi hakea valittamalla muutosta.

[7] Google Analytics Opt-out Browser Add-on.