TIETOSUOJAVALTUUTETUN TOIMISTO

13.12.2022

Dnro 4672/161/22

# Apulaistietosuojavaltuutetun päätös käsittelyn lainmukaisuutta, käsittelyn turvallisuutta, sisäänrakennettua ja oletusarvoista tietosuojaa, rekisteröityjen informointia ja henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa

## Asia

Kirjastojen verkkosivustolla käytettäviin seurantateknologioihin liittyvä henkilötietojen käsittely

## Rekisterinpitäjä

Pääkaupunkiseudun Helmet-kirjastot: Helsingin, Espoon, Vantaan ja Kauniaisten kaupunki

## Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on 7.6.2022 päivätyllä selvityspyynnöllä pyytänyt pääkaupunkiseudun kirjastoilta selvitystä Helmet.fi-verkkosivustolla käytettävistä seurantateknologioista.

Helsingin, Espoon ja Kauniaisten kaupunki on antanut asiassa yhteisen kirjallisen selvityksen 23.6.2022. Vantaan kaupunki on antanut oman, samansisältöisen selvityksensä 21.6.2022.

Antamassaan selvityksessä rekisterinpitäjät ovat kertoneet, että välttämättömien evästeiden, kuten esimerkiksi aineiston varaamiseen ja lainojen uusimiseen käytettävien evästeiden lisäksi Helmet-sivustolla on käytössä seurantateknologioita, joiden tarkoituksena on kävijäseuranta ja verkkosivujen kehittäminen.

Selvityksen mukaan analytiikkaevästeinä on käytössä Google Analytics ja Matomo, ja Google Analytics on ollut käytössä vain sisältösivuilla, ei aineistohaussa tai käyttäjän Omat tiedot -osiossa. Google Analyticsin käyttö on selvityksen mukaan päätetty lopettaa.

Verkkosivujen seurantateknologioita koskeva informaatio on ollut rekisteröityjen löydettävissä Helmet.fi-sivustolla ”Tietoa sivustosta” -linkin takaa. Seurantateknologioista kerrotaan otsikon ”Evästeet” alla seuraavasti:

> Sivustolla käytetään niin sanottuja evästeitä ("cookies"). Evästeillä voidaan kerätä tietoja esimerkiksi miltä sivulta olet siirtynyt osoitteeseen, mitä www-sivujamme olet selannut ja milloin, mitä selainta käytät, mikä on näyttösi resoluutio ja käyttöjärjestelmä,

> sekä mikä on tietokoneesi IP-osoite eli mistä internet-osoitteesta lähettämäsi tiedot tulevat ja minne ne vastaanotetaan.
>
> Osa Helmet-sivustolla käytetyistä evästeistä on palvelun toiminnan kannalta välttämättömiä evästeitä, jotka mahdollistavat esimerkiksi aineiston varaamisen ja lainojen uusimisen. Et voi estää välttämättömiä evästeitä.
>
> Käytämme sivustolla myös esimerkiksi tilastollisia evästeitä verkkosivujen kehittämiseen. Voit hylätä nämä ja muut palvelun käytön kannalta ei-välttämättömät evästeet evästetyökalun avulla. Voit muokata omia evästevalintojasi milloin tahansa. Siirry evästeasetuksiin.[1]

Tietoa sivustosta -linkin takaa löytyy puolestaan linkki Helmet-kirjastojen asiakasrekisteriin, jossa kerrotaan tiedonsiirtojen osalta, että ”*Osa palveluntarjoajista toimii myös EU:n tai ETA:n ulkopuolella*”.

Helmet-kirjastot ovat 4.8.2022 täydentäneet kesäkuussa 2022 annettua selvitystä. Rekisterinpitäjien mukaan seurantateknologioita tullaan elo-syyskuun aikana poistamaan Helmet.fi-verkkosivustolta, ja Google Analytics korvataan Matomon palvelulla.

## 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. Tietosuoja-asetus sisältää kansallista liikkumavaraa, minkä perusteella kansallisella lainsäädännöllä voidaan täydentää ja täsmentää asetuksessa nimenomaan määriteltyjä seikkoja. Yleistä tietosuoja-asetusta täsmentää kansallinen tietosuojalaki (1050/2018).

Yleisen tietosuoja-asetuksen 5(1)(a) artiklassa säädetään läpinäkyvyyden periaatteesta. Periaate edellyttää, että henkilötietoja käsitellään rekisteröidyn kannalta läpinäkyvästi. Yleisen tietosuoja-asetuksen 5(1)(a) artiklassa säädetään myös lainmukaisuusperiaatteesta, jonka mukaan henkilötietoja on käsiteltävä lainmukaisesti. Läpinäkyvyysperiaate ja lainmukaisuusperiaate ovat osa yleisen tietosuoja-asetuksen lähtökohtana olevaa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusta (yleisen tietosuoja-asetuksen 25 artikla), jota noudattaakseen rekisterinpitäjän tulee ottaa tietosuoja huomioon toiminnassaan alusta alkaen. Sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen edellyttää, että rekisterinpitäjä panee tietosuojaperiaatteet, kuten läpinäkyvyysperiaatteen ja lainmukaisuusperiaatteen, täytäntöön tehokkaasti.[2]

Yleisen tietosuoja-asetuksen johdantokappaleessa 39 todetaan henkilötietojen käsittelyn läpinäkyvyyden vaatimuksesta seuraavaa: Henkilötietojen käsittelyn olisi oltava laillista ja asianmukaista. Luonnollisille henkilöille olisi oltava läpinäkyvää, miten heitä koskevia henkilötietoja kerätään ja käytetään ja niihin tutustutaan tai niitä käsitellään muulla tavoin sekä selvillä siitä, missä määrin henkilötietoja käsitellään tai on määrä käsitellä. Läpinäkyvyyden periaatteen mukaisesti kyseisten henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä ja niissä on käytettävä selkeää ja yksinkertaista kieltä. Tämä periaate koskee erityisesti rekisteröityjen tietoja rekisterinpitäjän identiteetistä ja käsittelyn tarkoituksista sekä lisätietoja,

[1] Verkkosivustolla vierailtu 5.8.2022.

[2] Ks. Euroopan tietosuojaneuvoston lausunto: EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, s. 6.

joilla varmistetaan kyseisiä luonnollisia henkilöitä koskevan käsittelyn asianmukaisuus ja läpinäkyvyys, sekä heidän oikeuttaan saada vahvistus ja ilmoitus heitä koskevien henkilötietojen käsittelystä. Luonnollisille henkilöille olisi tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää tällaista käsittelyä koskevia oikeuksiaan. Varsinkin henkilötietojen käsittelyn nimenomaiset tarkoitukset olisi määritettävä ja ilmoitettava henkilötietojen keruun yhteydessä yksiselitteisesti ja lainmukaisesti.

Yleisen tietosuoja-asetuksen 6 artiklassa säädetään käsittelyn lainmukaisuudesta. Artiklan mukaan henkilötietojen käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi artiklan 1 kohdassa luetelluista edellytyksistä, kuten rekisteröidyn suostumuksen olemassaolo, täyttyy.

Yleisen tietosuoja-asetuksen 12–14 artikloissa säädetään rekisteröityjen informoinnista, jonka toteuttaminen lukeutuu rekisterinpitäjän velvollisuuksiin. Rekisteröityjä henkilötietojen käsittelystä informoimalla rekisterinpitäjä toteuttaa myös yleisen tietosuoja-asetuksen 5(1)(a) artiklan läpinäkyvyyden periaatetta.

Yleisen tietosuoja-asetuksen 13 artiklassa säädetään toimitettavista tiedoista, kun henkilötietoja kerätään rekisteröidyltä. Artiklan 1 kohdan mukaan kerättäessä rekisteröidyltä häntä koskevia henkilötietoja rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle kaikki 13 artiklan 1 kohdan a–e-alakohdan mukaiset tiedot. Näihin tietoihin lukeutuvat esimerkiksi tiedot henkilötietojen vastaanottajista tai vastaanottajaryhmistä (d-alakohta), sekä tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville (e-alakohta). Artiklan 2 kohdan a-alakohdan mukaan rekisteröidyille tulee myös toimittaa tieto henkilötietojen säilytysajasta, tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit.

Yleisen tietosuoja-asetuksen 25 artiklassa säädetään sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Artiklan 1 kohdan mukaan ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet. Artiklan 2 kohdan mukaan rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.

Yleisen tietosuoja-asetuksen 32 artiklassa säädetään käsittelyn turvallisuudesta. Artiklan 1 kohdan mukaan ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Artiklan 2 kohdan mukaan asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen,

tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

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.

## Tietosuojavaltuutetun toimivallasta evästeasioissa

Evästeiden ja muiden palvelun käyttöä kuvaavien tietojen tallentamisesta käyttäjän päätelaitteelle ja näiden tietojen käytöstä säädetään sähköisen viestinnän palveluista annetun lain (917/2014) 205 §:ssä. Tämän säännöksen noudattamista valvoo Liikenne- ja viestintävirasto Traficom.[3] Toimivalta ottaa kantaa esimerkiksi siihen, onko evästeitä voitu tallentaa käyttäjän päätelaitteelle ja minkälaisiin evästeisiin tulee hankkia käyttäjän suostumus, kuuluu näin ollen Liikenne- ja viestintävirasto Traficomille.

Tietosuojavaltuutettu valvoo tietosuojasääntelyn noudattamista. Esimerkiksi verkkosivustolla käytettävien seurantateknologioiden avulla kerättyjen henkilötietojen käsittelyn valvonta kuuluu tietosuojavaltuutetun toimistolle.

Verkkosivujen seurantateknologioihin, kuten evästeisiin, liittyvää suostumuksenhankintaa ja tallentamista seuraavasta henkilötietojen käsittelystä käytetään tässä päätöksessä toimivallanjaon selkeäksi esille tuomiseksi termiä jatkokäsittely. Jatkokäsittelyä valvoo tietosuojavaltuutetun toimisto.

[3] Ks. Sähköisen viestinnän palveluista annetun lain 303.1 §.

## 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 rekisterinpitäjillä ollut pätevä, yleisen tietosuoja-asetuksen 6 artiklan mukainen käsittelyperuste verkkosivujen seurantateknologioiden kautta kerättyjen henkilötietojen jatkokäsittelylle, ja onko rekisterinpitäjien menettely näiltä osin ollut lainmukaisuusperiaatteen ja sisäänrakennetun tietosuojan vaatimusten (yleisen tietosuoja-asetuksen 5(1)(a) artikla ja 25 artiklan 1 kohta) mukainen.

2) Onko rekisterinpitäjien aineistohakutietojen käsittelyä koskeva menettely ollut tässä päätöksessä arvioiduilta osin yleisen tietosuoja-asetuksen 25 ja 32 artiklojen mukainen.

3) Onko rekisteröityjen informointi verkkosivujen seurantateknologioiden käyttöön liittyvästä henkilötietojen käsittelystä, mukaan lukien kansainvälisistä tiedonsiirroista, ollut yleisen tietosuoja-asetuksen 5(1)(a) artiklan, 13 artiklan ja 25(1) artiklan mukainen.

4) Onko rekisterinpitäjien kansainvälisiä tiedonsiirtoja koskeva menettely ollut yleisen tietosuoja-asetuksen 44 ja 46 artiklojen mukainen, ja onko henkilötietojen siirtoihin Yhdysvaltoihin ollut olemassa pätevä siirtoperuste.

## Apulaistietosuojavaltuutetun päätös

### Päätös

Helmet-kirjastoilla ei ole ollut lainmukaista henkilötietojen käsittelyperustetta Helmet.fi-sivustolla seurantateknologioiden kautta kerättyjen henkilötietojen jatkokäsittelylle, vaan ne ovat käsitelleet näitä henkilötietoja esimerkiksi verkkosivujen kehittämistarkoituksessa ilman lainmukaista käsittelyperustetta (rikotut artiklat: 5(1)(a), 6(1) ja 25(1)).

Helmet-kirjastojen menettely koskien aineistohakutietojen käsittelyä ei myöskään ole ollut tietosuojasääntelyn mukainen, vaan Helmet-kirjastot ovat toimineet siten, että aineistohakutietoja on voinut vuotaa sivullisille (rikotut artiklat: 25 ja 32 artiklan 1 ja 2 kohta).

Helmet-kirjastot ovat niin ikään informoineet puutteellisesti rekisteröityjä Helmet.fi-sivustolla käytettäviin seurantateknologioihin liittyvästä henkilötietojen käsittelystä, mukaan lukien tiedonsiirroista kolmansiin maihin (rikotut artiklat: 5(1)(a), 13 artiklan 1 ja 2 kohta, 25(1)), eikä henkilötietojen siirtoihin Yhdysvaltoihin ole ollut täydentävien suojatoimien puuttuessa lainmukaista siirtoperustetta (rikotut artiklat: 44 ja 46).

Rekisterinpitäjille annetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d-alakohdan mukainen määräys hävittää verkkosivujen seurantateknologioiden kautta

keräämänsä henkilötiedot niiden rekisteröityjen osalta, joiden henkilötietoja on niiden keräämisen jälkeen säilytetty tai eri tavoin hyödynnetty ilman lainmukaista käsittelyperustetta. Tämä määräys ulottuu myös Yhdysvaltoihin ilman pätevää siirtoperustetta siirrettyihin, seurantateknologioiden kautta kerättyihin henkilötietoihin. Rekisterinpitäjät määrätään tämän lisäksi saattamaan käsittelytoimet tietosuojasääntelyn mukaisiksi rekisteröityjen informoinnin osalta ja huolehtimaan siitä, että rekisteröityjen informointi seurantateknologioihin liittyvästä henkilötietojen käsittelystä (ml. tiedonsiirroista) täyttää tietosuojasääntelystä tulevat edellytykset.

Helmet-kirjastojen tulee toimittaa tietosuojavaltuutetun toimistolle selvitys tämän määräyksen johdosta tehdyistä toimenpiteistä **viimeistään 15.2.2022**, ellei tähän päätökseen haeta muutosta.

Koska Helmet-kirjastot ovat ilmoittaneet ryhtyvänsä viipymättä toimenpiteisiin seurantateknologioiden poistamiseksi Helmet.fi-verkkosivustolta, apulaistietosuojavaltuutettu ei anna rekisterinpitäjille tässä päätöksessään määräystä seurantateknologioiden käyttöön liittyvän henkilötietojen käsittelyn lopettamisen ja tiedonsiirtojen keskeyttämisen osalta.

Rekisterinpitäjille annetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b-alakohdan mukainen huomautus yleisen tietosuoja-asetuksen säännösten vastaisista henkilötietojen käsittelytoimista. Rekisterinpitäjät ovat menettelyllään edellä todetusti rikkoneet yleisen tietosuoja-asetuksen 5(1)(a) artiklaa, 6(1) artiklaa, 13 artiklan 1 ja 2 kohtaa, 25 artiklaa, 32 artiklan 1 ja 2 kohtaa sekä 44 ja 46 artiklaa.

## Perustelut

### Henkilötietojen käsittelyperuste

Nyt arvioitavassa asiassa Helmet-kirjastot ovat käyttäneet Helmet.fi-verkkosivustolla erilaisia seurantateknologioita, kuten Google Analytics -analytiikkatyökalua ja Google Tag Manager -palvelua.

Apulaistietosuojavaltuutettu kiinnittää käsittelyperusteen osalta erityistä huomiota siihen, että Helmet-kirjastot ovat asentaneet seurantateknologioita sivustolla vierailijan päätelaitteelle heti verkkosivustolle saavuttaessa, ennen kuin esimerkiksi evästesuostumuksen hankintaan käytettävää, valintoja sisältävää ikkunaa (ns. evästebanneri) on edes näytetty käyttäjälle. Helmet-kirjastot ovat käyttäneet näitä henkilötietoja esimerkiksi palvelun kehittämistarkoituksessa, ja nämä tiedot ovat päätyneet myös yrityskäyttöön seurantateknologiapalveluiden tarjoajille.

Apulaistietosuojavaltuutettu toteaa, että seurantateknologioiden tallentamisen ja käyttämisen osalta sovellettavaksi tulee sähköisen viestinnän palveluista annetun lain 205 §, jonka soveltamista valvoo Liikenne- ja viestintävirasto Traficom. Jotta suostumuksenhankintaa ja seurantateknologioiden tallentamista seuraava jatkokäsittely voi olla tietosuojasääntelyn mukaista, evästeiden ja muiden seurantateknologioiden asettamiselle sähköisen viestinnän palveluista annetun lain 205 §:ssä asetettujen edellytysten tulee ensin täyttyä.[4] Näiden lähtökohtaisten edellytysten osalta verkkosivujen

[4] Ks. myös Euroopan tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, Annettu 12. maaliskuuta 2019, kohdat 40 ja 41 (”*[…] tietojenkäsittelyn alaryhmän eli evästeiden tallentamisen tai noutamisen on noudatettava kansallisia säännöksiä, joilla saatetaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohta osaksi*

seurantateknologioiden käytön laillisuuden arviointi kuuluu edellä todetusti Traficomille. Koska Helmet.fi-verkkosivuston evästebanneri, jonka kautta suostumus evästeisiin on ollut tarkoitus hankkia, ei ole toiminut asianmukaisesti, asiassa voidaan kuitenkin pitää ilmeisenä, että pätevää suostumusta ei ole saatu, eikä jatkokäsittely ole ollut tietosuojasääntelyn mukaista.

Koska Helmet-kirjastot ovat hyödyntäneet verkkosivujen seurantateknologioiden kautta kerättyjä henkilötietoja ilman lainmukaista käsittelyperustetta, menettely on rikkonut yleisen tietosuoja-asetuksen 5(1)(a) ja 6(1) artikloja, jotka edellyttävät, että henkilötietojen käsittelylle, mukaan lukien verkkosivujen seurantateknologioiden kautta kerättyjen henkilötietojen jatkokäsittelylle, on olemassa lainmukainen ja tosiasiallisesti sovellettava käsittelyperuste. Menettely on niin ikään ollut yleisen tietosuoja-asetuksen 25 artiklan vastaista, eikä henkilötietojen käsittelyssä ole huolehdittu siitä, että tietosuoja huomioidaan rekisterinpitäjien toiminnassa siten että sisäänrakennetun tietosuojan vaatimukset täyttyvät. Yleisen tietosuoja-asetuksen 25(1) artikla (*sisäänrakennettu tietosuoja*) edellyttää, että rekisterinpitäjä panee yleisen tietosuoja-asetuksen 5 artiklan mukaiset tietosuojaperiaatteet, kuten 5(1)(a) artiklan lainmukaisuusperiaatteen, täytäntöön tehokkaasti.

### Aineistohakuja koskevien tietojen päätyminen sivullisille

Helmet-kirjastot ovat kertoneet tietosuojavaltuutetun toimistolle antamassaan selvityksessä, että Google Analytics -analytiikkapalvelu on ollut käytössä vain sisältösivuilla, ei aineistohaussa tai asiakkaan Omat tiedot -sivuilla.

Apulaistietosuojavaltuutettu toteaa asiaa selvitettyään tämän osalta seuraavaa: Helmet.fi -verkkosivustolla voi hakea teoksia aineistohakutoimintoa käyttämällä. Tällöin esimerkiksi haetun kirjan nimi näkyy hakutulossivun URL:ssa, eli verkko-osoiterivillä (esim. https://haku.helmet.fi/iii/encore/record/C__Rb2347993__Smuumi-pappa%20ja%20meri__Orightresult__U__X7?lang=fin&suite=cobalt).

Jos käyttäjä on tämän jälkeen siirtynyt hakutulossivulla olevasta linkistä esimerkiksi Helmet.fi-sivuston pääsivulle, jolla on käytössä Google Analytics -palvelu, tieto haetusta teoksesta on voinut päätyä Googlelle Referer http-otsikkokentän kautta.[5] Huomioitakoon, että Helmet-kirjastot eivät ole esimerkiksi määritelleet niin kutsuttua Referrer-Policya, jolla aineistohakutietojen päätymiseen sivullisille olisi ollut mahdollista puuttua.

Kirjaston teoksiin kohdistuvat hakutiedot voivat paljastaa huomattavan määrän henkilön yksityiselämästä kertovia seikkoja, ja niitä voidaan käyttää esimerkiksi rekisteröityä koskevan henkilöprofiilin luomiseen.[6] Huolimattomuus henkilötietojen käsittelyssä on nyt arvioitavassa asiassa johtanut näiden tietojen välittymiseen tiedettävästi ainakin Googlen käyttöön.

Yleisen tietosuoja-asetuksen 32 artikla (*käsittelyn turvallisuus*) edellyttää rekisterinpitäjältä asianmukaisia teknisiä ja organisatorisia toimenpiteitä muun muassa sen

*kansallista lainsäädäntöä. Henkilötietoja, myös evästeillä hankittuja henkilötietoja, voidaan jatkokäsitellä vain, jos siihen on yleisen tietosuoja-asetuksen 6 artiklaan perustuva oikeusperusta, jotta käsittely on lainmukaista*"). Evästeiden osalta ks. myös Traficomin ja Kyberturvallisuuskeskuksen ohjeistus: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/evasteet.

[5] Tämä riippuu rekisterinpitäjien menettelystä johtuen ennen kaikkea käyttäjän päätelaitteesta.

[6] Erilaiset toimijat saattavat yhdistää näitä tietoja myös muista lähteistä kerättyihin, samaa rekisteröityä koskeviin tietoihin, jolloin henkilöprofiilista saadaan tarkempi.

varmistamiseksi, että sivullisten pääsy henkilötietoihin estyy. Yleisen tietosuoja-asetuksen 25 artikla (*sisäänrakennettu ja oletusarvoinen tietosuoja*) edellyttää, että tietosuoja on sisäänrakennettu rekisterinpitäjän toimintaan ja se huomioidaan kaikessa henkilötietojen käsittelyssä oletusarvoisesti. Silloin, kun henkilötietoja voi päätyä systemaattisella tavalla tarkoituksetta kolmansille osapuolille, sisäänrakennetun ja oletusarvoisen tietosuojan toteutuksessa on ilmeisiä puutteita. Koska Helmet-kirjastojen toiminnassa aineistohakutietoja on voinut vuotaa sivullisille, rekisterinpitäjien menettely ei näiltä osin ole täyttänyt yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdan tai 25 artiklan vaatimuksia.

### Rekisteröityjen informointi

Helmet-kirjastojen käyttämiä seurantateknologioita koskeva tietosuojainformaatio on ollut rekisteröityjen löydettävissä Helmet.fi-sivustolla ”Tietoa sivustosta” -linkin takaa. Tietoa sivustosta -linkin takana on lisäksi ollut linkki Helmet-kirjastojen asiakasrekisteriin, jossa kerrotaan tiedonsiirtojen osalta, että ”*Osa palveluntarjoajista toimii myös EU:n tai ETA:n ulkopuolella*”.

Tietosuojainformaation tulee olla helposti rekisteröidyn löydettävissä. ”Tietoa sivustosta” -linkin nimestä ei käy selkeällä tavalla ilmi, että sen takaa on löydettävissä lain edellyttämä informaatio henkilötietojen käsittelystä. Tietosuojainformaation ei näin ollen voida katsoa olevan helposti rekisteröidyn löydettävissä, eikä henkilötietojen käsittelyn läpinäkyvyyden vaatimus tältä osin täyty.

Seurantateknologioiden osalta rekisteröidyille annettava informaatio ei puolestaan sisällä tietoa siitä, mitä palveluntarjoajia (kuten Google) seurantateknologioiden avulla tapahtuvaan henkilötietojen käsittelyyn liittyy, ja miten pitkään henkilötietoja säilytetään. Yleisen tietosuoja-asetuksen 13 artikla edellyttää, että rekisteröidylle annetaan tieto esimerkiksi henkilötietojen vastaanottajista tai vastaanottajaryhmistä (13(1)(d) artikla) sekä säilytysajasta (13(2)(a) artikla). Esimerkiksi ratkaisussaan C-673/17 EU-tuomioistuin on todennut, että internetsivuston käyttäjälle tulee antaa informaatio evästeiden toiminta-ajasta sekä siitä, onko kolmansilla mahdollisuus käyttää näitä evästeitä.[7]

Yleisen tietosuoja-asetuksen 13 artiklan mukaan rekisteröityjä tulee niin ikään informoida henkilötietojen siirroista kolmansiin maihin sekä siirtoperusteesta (13(1)(e) artikla). Nyt arvioitavassa asiassa annettu informaatio, jonka mukaan ”*Osa palveluntarjoajista toimii myös EU:n tai ETA:n ulkopuolella”* ei ole riittävä, jotta sen pohjalta pystyisi muodostamaan käsityksen esimerkiksi siitä, mistä palveluntarjoajista mainitussa on kyse, ja minkä siirtoperusteen nojalla henkilötietoja on katsottu mahdolliseksi siirtää EU- ja ETA-alueen ulkopuolelle. Informaatio on lisäksi laitettu asiakasrekisterilinkin taakse, eikä se siten ole rekisteröityjen helposti löydettävissä.

Rekisteröityjen informointi seurantateknologioiden käyttöön liittyvästä henkilötietojen käsittelystä, mukaan lukien tiedonsiirroista, on edellä esitetysti puutteellista, eikä rekisteröity voi annettujen tietojen perusteella saada selkeää käsitystä siitä, miten ja millaisten edellytysten täyttyessä hänen henkilötietojaan tosiasiallisesti tässä kontekstissa käsitellään.

### Seurantateknologioiden käyttöön liittyvät tiedonsiirrot kolmansiin maihin

[7] Ratkaisun kohta 81.

Helmet.fi-verkkosivustolla on ollut käytössä seurantateknologioita, joiden kautta kirjastosivuston käyttäjien henkilötietoja on välittynyt myös kolmansiin maihin. Käytössä on ollut esimerkiksi yhdysvaltalaisyritys Googlen palveluita kuten Google Analytics ja Google Tag Manager.

### Yhdysvaltojen viranomaisten pääsy henkilötietoihin

Vuonna 2013 kävi ilmi, että eräät maailman suurimmista teknologiayrityksistä, kuten Microsoft, Facebook (Meta), Google, Skype ja Apple, olivat mukana Yhdysvaltojen kansallisen turvallisuusviraston, NSA:n, valvontaohjelmissa.

Näihin ohjelmiin lukeutuva PRISM on mahdollistanut NSA:lle suoran pääsyn teknologiayritysten keskuspalvelimille, ja yhdysvaltalaisviranomaisten on näin mahdollista reaaliajassa nähdä ja kerätä esimerkiksi kaikki Googlelle menevä tavallisten kansalaisten tietoliikenne ilman Googlen myötävaikutusta.

Keräämisen kohteena ovat olleet käytännössä esimerkiksi sähköpostiviestit, valokuvat, nettichatit ja puhelutiedot. Tiedonkeruu on kohdistettu erityisesti ulkomaalaisiin, eli käytännössä esimerkiksi Pohjoismaissa Googlen ja muiden teknologiajättien palveluita käyttäviin henkilöihin.

Yhdysvaltalaisyritysten tulee niin ikään viranomaisen oikeudellisesti sitovasta pyynnöstä luovuttaa henkilötietoja viranomaiselle Yhdysvaltojen kansallisen sääntelyn nojalla.[8] Näin ollen viranomaisten pääsy henkilötietoihin ulottuu myös toimijoihin, jotka eivät ole mukana NSA:n valvontaohjelmissa.

Euroopan komissio on julkaissut 27.11.2013 raportin, jonka mukaan Yhdysvallat on vahvistanut PRISM-ohjelman olemassaolon sekä sen oikeuttamisen Foreign Intelligence Surveillance Act 1978 -säädökseen (FISA) nojalla.

### Google ja tiedonsiirrot Yhdysvaltoihin

Nyt arvioitavassa asiassa pääkaupunkiseudun kirjastojen Helmet.fi-verkkosivustolla on ollut käytössä Googlen palveluita, kuten esimerkiksi Google Analytics -analytiikkatyökalu. Google Analytics -palvelu tallentaa ja lukee käyttäjän selaimelle asetettujen evästeiden kautta kerättyjä tietoja, ja kerätyt tiedot välitetään Googlen palvelimille, jotka sijaitsevat Yhdysvalloissa[9]. Helmet.fi-verkkosivustolla kerättyjä henkilötietoja on näin ollen siirretty Yhdysvaltoihin.

Yleinen tietosuoja-asetus edellyttää, että henkilötietojen siirtäminen unionista kolmansissa maissa oleville rekisterinpitäjille, henkilötietojen käsittelijöille tai muille vastaanottajille ei vaaranna yleiseen tietosuoja-asetukseen perustuvaa henkilötietojen suojan tasoa,[10] ja riittävän tietosuojan tason turvaamiseksi EU:n ja Yhdysvaltojen välisissä tiedonsiirroissa on aiemmin käytetty niin kutsuttua Privacy Shield -järjestelyä. Unionin tuomioistuin on kuitenkin todennut ratkaisussaan asiassa C-311/18 (nk. Schrems II -ratkaisu),[11] että EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä annettu päätös 2016/1250 on pätemätön.[12]

[8] Esimerkiksi CLOUD Act -sääntely velvoittaa näiltä osin toimijoita.
[9] Googlen Ranskan tietosuojaviranomaiselle (CNIL) asiassa dnro MDM221005 antama selvitys.
[10] Ks. yleisen tietosuoja-asetuksen 44 artikla ja johdantokappale 101.
[11] Ratkaisu on annettu 16.7.2020.
[12] Ratkaisun kohta 201.

Ratkaisussaan unionin tuomioistuin katsoo, että Yhdysvaltojen sisäisestä säännöstöstä, joka koskee Yhdysvaltojen viranomaisten pääsyä unionista Yhdysvaltoihin siirrettyihin henkilötietoihin ja näiden tietojen käyttöä, johtuvia henkilötietojen suojan rajoituksia ei ole rajattu tavalla, joka täyttäisi unionin oikeudesta tulevat vaatimukset. Rekisteröidyille ei myöskään anneta täytäntöönpanokelpoisia oikeuksia, joihin he voisivat vedota Yhdysvaltojen viranomaisia vastaan tuomioistuimissa.[13] Unionin tuomioistuin on todennut edelleen, että rekisterinpitäjän on keskeytettävä henkilötietojen siirrot kolmanteen maahan, jos se ei voi toteuttaa riittäviä lisätoimenpiteitä henkilötietojen suojan varmistamiseksi.[14]

Nyt arvioitavassa tapauksessa Helmet-kirjastot eivät ole tehdyn selvityksen mukaan huomioineet toiminnassaan asianmukaisesti EU-tuomioistuimen ratkaisussa C-311/18 todettua, vaan ne ovat käyttäneet verkkosivustollaan tiedonsiirtoja Yhdysvaltoihin käsittävää seurantateknologiaa ilman täydentäviä suojatoimia.

Täydentävien suojatoimien, kuten henkilötietojen salauksen, osalta apulaistietosuojavaltuutettu nostaa tässä yhteydessä esille, että FISA-sääntelyn[15] nojalla esimerkiksi Google on velvollinen antamaan Yhdysvaltojen viranomaisille myös salausavaimen. Toisin sanoen, mikäli rekisterinpitäjän käyttöön ottama täydentävä suojatoimenpide on sellainen, joka mahdollistaa esimerkiksi Googlelle pääsyn selkokielisiin tietoihin, täydentävä suojatoimi ei täytä EU-tuomioistuimen ratkaisussaan C-311/18 asettamia vaatimuksia.[16] Rekisterinpitäjän tulee toiminnassaan myös varmistaa, ettei yhdysvaltalaisviranomaisella ole pääsyä henkilötietoihin esimerkiksi Yhdysvaltojen kansallisen lainsäädännön, kuten CLOUD Act -sääntelyn nojalla.[17]

Koska Helmet-kirjastot ovat tietosuojavaltuutetun toimistolle antamassaan selvityksessä kertoneet, että käytössä on ollut myös Matomon palvelu ja että Google Analytics tullaan korvaamaan Matomo-analytiikkapalvelulla, apulaistietosuojavaltuutettu nostaa niin ikään esille, että rekisterinpitäjien tulee myös Matomon kohdalla huolehtia siitä, ettei palvelun käytössä tapahdu tietosuojasääntelyn vastaisia kansainvälisiä tiedonsiirtoja ja että henkilötietojen käsittely on muutoinkin palvelua käytettäessä yleisen tietosuoja-asetuksen mukaista. Kyseinen palvelu ei automaattisesti ole sellainen, etteikö sen käyttöön voisi liittyä tällaisia tiedonsiirtoja.

Helmet-kirjastot ovat edellä kuvatulla menettelyllään rikkoneet yleisen tietosuoja-asetuksen 44 artiklaa, joka edellyttää tiedonsiirtojen toteuttamista yleisen tietosuoja-asetuksen V-luvun edellytyksiä noudattaen, sekä yleisen tietosuoja-asetuksen 46 artiklaa, joka edellyttää asianmukaisia suojatoimia yleisen tietosuoja-asetuksen 45 artiklan mukaisen päätöksen puuttuessa, eikä rekisteröityjen henkilötietojen siirtämiselle Yhdysvaltoihin ole ollut lain edellyttämää siirtoperustetta.

Helmet-kirjastot ovat saadun selvityksen mukaan ryhtyneet toimenpiteisiin seurantateknologioiden poistamiseksi Helmet.fi-verkkosivustolta, ja tietosuojavaltuutetun toimisto on ohjannut Helmet-kirjastoja varmistamaan tässä yhteydessä, että käyttöön ei

[13] Ks. ratkaisun osio *Tietosuojan riittävää tasoa koskeva toteamus* (alkaa ratkaisun kohdasta 168).
[14] Ratkaisun kohta 135.
[15] Foreign Intelligence Surveillance Act 1978.
[16] Ks. tarkemmin Euroopan tietosuojaneuvoston ohje: EDPB Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, Versio 2.0, kohta 81.
[17] CLOUD Act -sääntely saattaa antaa yhdysvaltalaisviranomaiselle pääsyn henkilötietoihin silloinkin, kun henkilötietoja käsitellään EU:ssa.

jää palveluita, joihin liittyy tietosuojasääntelyn vastaisia henkilötietojen siirtoja Yhdysvaltoihin.

### Viranomaisten verkkosivustoilla käytettävistä seurantateknologioista yleisesti

Viranomaisten verkkosivustoillaan käyttämän seurantateknologian osalta apulaistietosuojavaltuutettu toteaa nyt arvioitavana olevaa asiaa yleisemmällä tasolla seuraavaa:

Apulaistietosuojavaltuutettu korostaa, että viranomaisen verkkopalveluita olisi lähtökohtaisesti voitava käyttää ilman, että rekisteröity saattaa altistaa itsensä kolmansien osapuolten omiin tarkoituksiin, seurantateknologiaa hyödyntämällä tapahtuvalle tiedonkeruulle ja ilman, että tietoja verkkosivuvierailusta päätyy esimerkiksi kaupalliseen käyttöön ja ulkopuolisten tahojen profilointitarkoituksiin. Huomioitakoon, että Google ilmoittaa esimerkiksi Google Analytics -palvelun käyttöehdoissaan nimenomaisesti, että se voi käyttää seurantateknologian kautta saatuja tietoja omiin käyttötarkoituksiinsa.[18]

Viranomaisen ei myöskään tulisi käyttää verkkosivustollaan vierailijoiden henkilötietoja maksuvälineenä, ja viranomaisen tulee tämän vuoksi tehdä asianmukainen arviointi siitä, onko kyseessä esimerkiksi maksuton palvelu, jonka käytön vastikkeena voivat tosiasiassa olla rekisteröityjen henkilötiedot.[19]

Viranomaisen tulee niin ikään huomioida jatkokäsittelyn osalta, että silloin, kun henkilötietojen käsittelyperusteena on rekisteröidyn suostumus, suostumuksen tulee olla nimenomainen, informoitu ja sen tulee kattaa kaikki käsittelytarkoitukset, mukaan lukien henkilötietojen mahdollinen luovuttaminen.[20] Kaikkia eri käsittelytarkoituksia varten tulee myöskin hankkia oma, erillinen suostumus, jotta esimerkiksi suostumuksen vapaaehtoisuuden vaatimus tosiasiallisesti täyttyy, eikä eri käyttötarkoituksiin hankittavia suostumuksia voida niputtaa yhden suostumuksen alle. Oikeutettu etu ei ole yleisen tietosuoja-asetuksen 6(1) artiklan mukaisesti viranomaisen toiminnassa sovellettava käsittelyperuste.[21]

Viranomaisen tulee harkita tarkkaan, millaista seurantateknologiaa sen verkkosivustolla on tosiasiallisesti tarpeellista olla, ja voitaisiinko viranomaisen verkkopalvelua esimerkiksi tarjota täysin ilman muita kuin sivuston toiminnan kannalta välttämättömiä seurantateknologioita. Tässä arvioinnissa on perusteltua huomioida, että viranomaisen sivustolla voi myös vierailla heikommassa asemassa olevia henkilöitä, mukaan lukien iäkkäitä henkilöitä ja lapsia, joiden digitaidot voivat olla puutteelliset tai joiden voi olla haastavaa ymmärtää, mistä seurantateknologioiden kautta tapahtuvassa henkilötietojen käsittelyssä on kyse, ja millaiseen käyttöön tiedot saattavat päätyä.

Huomioitakoon, että seurantateknologioita käytettäessä verkkosivustolla vierailijan toimintaa on mahdollista seurata myös eri sivustojen yli, mikä mahdollistaa esimerkiksi

[18] Google Analytics -palvelun käyttöehtojen mukaan Google ja sen omistamat tytäryhtiöt voivat säilyttää ja käyttää palvelussa kerättyjä tietoja (“*Google and its wholly owned subsidiaries may retain and use, subject to the terms of its privacy policy information collected in Your use of the Service*”), ks. Google Analytics Terms of Service, kohta 6.
[19] Rekisterinpitäjillä ei usein ole minkäänlaista näkyvyyttä siihen, miten seurantapalveluntarjoaja tosiasiallisesti käsittelee kerättyjä henkilötietoja.
[20] Ks. EU:n tietosuojatyöryhmän Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat, annettu 28. marraskuuta 2017, kappale 3.1.3. Suostumuksen tulee myös olla esimerkiksi tietoinen ja aktiivinen. Informaatio henkilötietojen käsittelystä tulee puolestaan antaa rekisteröidylle oikea-aikaisesti.
[21] Yleisen tietosuoja-asetuksen 6(1) artiklan mukaan ”*Ensimmäisen alakohdan f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä”*.

internetin käyttäjän selailupolun ja verkkotoiminnan jäljittämisen, sekä yksityiskohtaisen profiilin muodostamisen kyseisestä henkilöstä. Koska seurantateknologioiden kautta voi tapahtua merkittävää henkilötietojen keräämistä kolmansien osapuolten toimesta, viranomaisen tulee toimia erityisen huolellisesti tehdessään päätöksiä siitä, millaista seurantateknologiaa sen verkkosivustolle laitetaan. Seurantateknologian hyödyntäminen verkkosivuilla edellyttää sekä teknistä asiantuntemusta että tietosuojajuridiikan, mukaan lukien henkilötiedon käsitteen, ymmärtämistä.

## 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

Apulaistietosuojavaltuutettu Heljä-Tuulia Pihamaa

**Liitteet** Valitusosoitus

**Jakelu** Rekisterinpitäjät

## Tietosuojavaltuutetun toimiston yhteystiedot

**Tietosuojavaltuutetun toimisto**
PL 800, 00531 Helsinki – puh. 029 566 6700 (vaihde) – tietosuoja@om.fi – www.tietosuoja.fi

**Postiosoite:** PL 800, 00531 Helsinki

**Sähköposti:** tietosuoja@om.fi

**Puhelinvaihde:** 029 566 6700

**Verkkosivut:** www.tietosuoja.fi