

MITEN HENKILÖTIETOJA VOIDAAN SIIRTÄÄ JATKOSSA YHDYSVALTOIHIN JA MITÄ OPPIA VIIMEAIKAISISTA VIRANOMAISPÄÄTÖKSISTÄ?

Markus Myhrberg ja Ville Kukkonen

1.10.2020

LEXIA
Legal Excellence



KESKEINEN TIETOSUOJASÄÄNTELY

Yleinen tietosuoja-asetus (GDPR)



Tietosuoja laki

Työelämän
tietosuoja laki

Laki sähköisen
viestinnän
palveluista

Erityislainsäädäntö

KÄSITTELYSSÄ NOUDATETTAVAT PERIAATTEET

- **Noudatettava** henkilötietojen käsittelyssä

1. Lainmukaisuus, kohtuullisuus, läpinäkyvyys

2. Käyttötarkoitussidonnaisuus

3. Tietojen minimointi

- Pystyttävä **osoittamaan** noudattaminen

4. Täsmällisyys

5. Säilytyksen rajoittaminen

6. Eheys ja luottamuksellisuus

KÄSITTELYPERUSTE

Määrittele etukäteen
Muista osoitusvelvollisuus

Suostumus

Sopimus

Oikeutettu etu

Julkisen
vallan
käyttäminen

Lakisääteinen
velvoite

Elintärkeiden
etujen
suojaaminen

INFORMOINTI- JA OSOITUSVELVOLLISUUS

→ KESKEINEN OSA VIRANOMAISEN ARVIOIDESSA KÄSITTELYN LAINMUKAISUUTTA

- ? TIEVARANTOJEN JA TIEVIRTOJEN DOKUMENTOINTI
- ? ULKOISET TIEOSUOJAKÄYTÄNNÖT JA KÄSITTELYTOIMIA KOSKEVAT SELOSTEET
- ? HENKILÖTIEOJEN KÄSITTELYÄ KOSKEVAT SOPIMUKSET
- ? TIEOSUOJA- JA TIEOTURVAPOLITIIKAT, SISÄISET OHJEISTUKSET
- ? PROSESSIKUVAUKSET
- ? RISKIARVIOIDEN JA PÄÄTÖSTEN DOKUMENTOINTI
- ? VAIKUTUSTENARVIOINNIT (DPIA)
- ? TIEOSUOJAORGANISAATION TOIMINNAN DOKUMENTOINTI

MITÄ OPPIA VIIMEAIKAISISTA VIRANOMAISPÄÄTÖKSISTÄ?

LEXIA
Legal Excellence



CASE 1 - REKISTERÖITYJEN INFORMOINTI JA KÄSITTELYN LÄPINÄKYVYYS



- Posti ei ollut riittävällä tavalla informoinut rekisteröityjä tietosuojalainsäädännön mukaisista oikeuksista muuttoilmoituksen tekemisen yhteydessä.
- Rekisteröityjä ei mm. ollut informoitu oikeudesta kieltää Postia luovuttamasta rekisteröityjen tietoja sellaisille tahoille, jotka harjoittivat suoramarkkinointia. Tämän seurauksena muuttoilmoituksen tehneet henkilöt saivat suoramarkkinointiin liittyviä yhteydenottoja eri yrityksiltä.
- Oikeudesta vastustaa henkilötietojen käsittelyä oli ilmoitettu vain niille henkilöille, jotka muuttoilmoituksen tekemisen lisäksi olivat ostaneet lisäpalveluita.
- Rekisterinpitäjän katsottiin laiminlyöneen tietosuojalainsäädännössä rekisteröityjen informoinnille asetettuja vaatimuksia ja samalla myös henkilötietojen käsittelyn läpinäkyvyyden periaatteen noudattaminen.
- Rikkomus koski 161 000 asiakasta pelkästään vuoden 2019 aikana.
- Seuraamusmaksun suuruus 100 000 euroa (päätös ei ole lainvoimainen).

CASE 2 - VAIKUTUSTENARVIOINTI



- Tapauksessa Kymen Vesi Oy käsitteli työntekijöidensä sijaintitietoja paikantamalla ajoneuvoja ajotietojärjestelmän avulla.
 - Sijaintitietoja käytettiin muun muassa työajanseurantaan.
- Tapauksessa katsottiin olevan kyse sijaintitietojen järjestelmällisestä valvonnasta. Valvonnan kohteena olevien työntekijöiden katsottiin olevan heikommassa asemassa suhteessa rekisterinpitäjänä olevaan työnantajaan.
- Vaikutustenarviointi on suoritettava esimerkiksi ennen sijaintitietojen käsittelyä, jos sijaintitietoja käytetään järjestelmälliseen valvontaan, ja käsittely kohdistuu rekisterinpitäjään nähden heikommassa asemassa olevien rekisteröityjen sijaintitietoihin.
- Yritys ei ollut tehnyt yleisen tietosuoja-asetuksen mukaista vaikutustenarviointia ennen sijaintitietojen käsittelyn aloittamista.
 - Eikä myöskään arviota, että olisi ennalta tunnistanut käsittelytilanteeseen liittyvät riskit ja tehdyt sen perusteella arviota DPIA:n tarpeellisuudesta.
- Seuraamusmaksun suuruus 16 000 euroa (päätös ei ole lainvoimainen).

CASE 3 - TARPEETTOMIEN HENKILÖTIETOJEN KERÄÄMINEN

- Tapauksessa yritys oli käsitellyt henkilötietoja työelämän tietosuojalain keskeisten säännösten vastaisesti, sillä useiden kerättyjen henkilötietojen osalta niiden käsittelyyn oikeuttava käsittelyperuste oli puuttunut.
- Kyseinen yritys oli kerännyt henkilötietolomakkeella tietoja mm. henkilön uskonnollisesta vakaumuksesta, terveydentilasta, mahdollisesta raskaudesta ja perhesuhteista.
 - Tällaiset tiedot ovat tietosuoja-asetuksen nojalla erityisiin henkilötietoryhmiin katsottavia tietoja, joiden käsittely on sallittua vain tietosuoja-asetuksen mukaisella poikkeusperusteella.
- Tietojen minimoinnin periaatteen rikkomisen lisäksi tapauksessa havaittiin puutteita myös tietosuoja-asetuksen noudattamiseen liittyvässä dokumentoinnissa.
- Yrityksen olisi tullut laatia ja ylläpitää tietosuoja-asetuksen mukaista selostetta käsiteltävänä olevien henkilötietojen käsittelytoimista, sillä tapauksessa henkilötietojen käsittely oli säännöllistä ja kohdistui erityisiin henkilötietoryhmiin.
 - Seloste käsittelytoimista on keskeinen asiakirja, kun arvioidaan rekisterinpitäjän henkilötietojen käsittelyn lainmukaisuutta ja osoitusvelvollisuuden täyttymistä.
- Yritys ei kyennyt osoittamaan noudattavansa tietosuoja-asetusta työntekijöiden ja työnhakijoiden henkilötietoja käsiteltäessä.
- Tietosuojavaikuttettu määräsi yrityksen poistamaan tarpeettomat tiedot ja antoi huomautuksia puutteellisesta dokumentoinnista.
- Seuraamusmaksun suuruus 12 500 euroa (päättös ei ole lainvoimainen).

CASE 4 - RISKIEN TUNNISTAMINEN, TIETOSUOJAPERIAATTEIDEN NOUDATTAMINEN JA VAIKUTUSTENARVIOINTI

- Tapauksessa havaittiin useita vakavia puutteita riskien tunnistamisessa sekä tietosuojaan peruskysymyksissä, kuten rekisteröityjen informoinnissa, dokumentoinnissa ja henkilötietojen käsittelyn roolien määrittelyssä.
- Taksi Helsinki oli ottanut takseissa käyttöönsä ääntä ja kuvaa tallentavan kameravalvontajärjestelmän, mutta ei ollut arvioinut henkilötietojen käsittelyyn liittyviä riskejä ja vaikutuksia ennen järjestelmän käyttöönottoa.
- Takseissa olevissa ilmoituksissa ei kerrottu äänen tallentamisesta tai siitä, mistä asiakkaat olisivat voineet saada tiedon. Tämän vuoksi yhtiön ei katsottu informoineen henkilötietojen käsittelystä tietosuojalainsäädännön edellyttämällä tavalla.
- Yhtiö ei ollut kertonut kanta-asiakasohjelman yhteydessä suoritetusta automaattisesta päätöksenteosta ja profiloinnista tietosuojaselosteessaan. Tietojen ei voitu katsoa olevan rekisteröityjen helposti saatavilla.
- Äänitietojen käsittely ei myöskään ollut tietosuoja-asetuksen tietojen minimoinnin periaatteen mukaista.
- Oikeutetun edun käyttöä käsittelyperusteena ei oltu dokumentoitu
- Yhtiön olisi tullut tehdä tietosuojaa koskeva vaikutustenarviointi turvakameravalvonnasta, sijaintitietojen käsittelystä sekä kanta-asiakasohjelman yhteydessä harjoitetusta automaattisesta päätöksenteosta ja profiloinnista.
- Apulaistietosuojavaalautettu määräsi korjaavia toimenpiteitä, kuten dokumentoimaan oikeutetun edun käsittelyperusteena ja laatimaan vaikutustenarvioinnin.
- Seuraamusmaksun suuruus 72 000 euroa (päätös ei ole lainvoimainen).

CASE 6 - SÄHKÖINEN SUORAMARKKINOINTI JA REKISTERÖIDYN OIKEUDET

- Tapauksessa yritys oli lähettänyt sähköisiä suoramarkkinointiviestejä ilman ennalta annettua suostumusta. Lisäksi yritys ei ollut noudattanut rekisteröidyn oikeuksia, sillä yritys ei ollut vastannut rekisteröityjen oikeuksia koskeviin pyyntöihin tai toteuttanut niitä, eikä se pystynyt osoittamaan käsitelleensä henkilötietoja lainmukaisesti.
- Suoramarkkinointiviestejä oli lähetty ilman ennakkolupaa. Lisäksi osa vastaanottajista oli pyytänyt suoramarkkinoinnin lopettamista, mutta he olivat kielloista huolimatta saaneet markkinointiviestejä.
 - Tietosuoja-asetuksen mukainen vastustamisoikeus suoramarkkinointiin ei ollut toteutunut.
- Rekisterinpitäjä oli katsonut kohdistaneensa sähköistä suoramarkkinointia yhteisöihin, jolloin sähköisen viestinnän palveluista annetun lain mukaan sähköiseen suoramarkkinointiin ei olisi vaadittu ennalta annettua suostumusta. Rekisterinpitäjän olisi tullut selvittää kyseisen henkilön asema yrityksessä ja arvioida, liittyykö suoramarkkinointi olennaisesti henkilön työtehtäviin.
 - Rekisterinpitäjän olisi pitänyt pyytää suostumus rekisteröidyltä sähköiseen suoramarkkinointiin.
- Lisäksi muihin rekisteröidyn oikeuksia koskeviin pyyntöihin ei ollut vastattu ilman aiheetonta viivettä ja enintään kuukauden kuluessa pyynnön vastaanottamisesta. Rekisterinpitäjä ei ollut myöskään toteuttanut pyyntöjä (tai ei pystynyt osoittamaan tätä)
- Apulaistietosuoja-valtuutettu antoi yritykselle huomautuksen henkilötietojen käsittelystä ilman suostumusta sekä rekisteröidyn oikeuksien laiminlyömisestä ja toteuttamatta jättämisestä. Lisäksi rekisterinpitäjä veloitettiin korjaamaan toimintatapansa yhteisölle kohdistetun suoramarkkinoinnin osalta sekä määrättiin toteuttamaan rekisteröidyn oikeudet tietosuoja-asetuksen mukaisesti.
- Seuraamusmaksun suuruus 7000 euroa (päätös ei ole lainvoimainen).

CASE 7 - SUOSTUMUS EVÄSTEIDEN KÄYTTÖÖN



- Tapauksessa yritys ilmoitti evästeiden käytöstä verkkosivustonsa evästebannerin kautta. Yritys ilmoitti keräävänsä tietoja yritykselle sekä kolmansille osapuolille palveluiden käytöstä ja käyttäjien IP-osoitteista, jotta palveluita voidaan personoida ja mainontaa kohdentaa.
- Apulaistietosuoja-valtuutettu katsoi, etteivät vapaaehtoisen suostumuksen edellytykset täyty annettaessa suostumusta bannerin kautta. Suostumuksesta kieltäytyminen tai peruuttaminen tulee olla yhtä helppoa kuin suostumuksen antaminen. Aktiivisena ja nimenomaisena tahdonilmaisuna ei voida pitää sitä, että käyttäjälle kerrottiin mahdollisuudesta kieltää evästeiden tallentaminen ja käyttö selainasetuksista.
- Suostumusta ei voida antaa siten, että käyttäjä jättää tekemättä muutoksia selainasetuksiinsa, sillä käyttäjällä on oltava tilaisuus valita, hyväksyykö vai hylkääkö hän suostumusta koskevat ehdot.
- Suostumuksen voi antaa erilaisilla tavoilla, mutta pätevää suostumusta ei voi antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta.
- Apulaistietosuoja-valtuutettu määräsi yrityksen muuttamaan toimintatapojaan suostumuksen keräämisessä tietosuoja-asetuksen mukaisiksi.
- Päätös ei ole lainvoimainen.

MITEN HENKILÖTIETOJA VOIDAAN SIIRTÄÄ JATKOSSA YHDYSVALTOIHIN?

HENKILÖTIETOJEN SIIRTÄMINEN EU/ETA:N ULKOPUOLELLE



HENKILÖTIETOJEN SIIRTÄMINEN EU/ETA:N ULKOPUOLELLE



SUOJAN RIITTÄVYYTTÄ KOSKEVA PÄÄTÖS

Euroopan komission tietosuojan
riittävyyttä koskeva päätös
(Argentiina, Kanada, Israel,
Japani, Uusi-Seelanti, Sveitsi,
Uruguay

Privacy Shield -mekanismi



ASIANMUKAISET SUOJATOIMET

Mallisopimuslausekkeet (SCCs)
Yrityksiä sitovat säännöt (BCR)
Hyväksytyt käytäntesäännöt /
sertifikaatit



POIKKEUKSET

Nimenomainen suostumus
Sopimusliitännäinen (tai
sopimuksentekoa edeltävä
välttämättömyys)
Välttämättömyys elintärkeiden
etujen suojaamiseksi
Välttämättömyys oikeudellisten
vaateiden vuoksi

Henkilötietojen siirto Yhdysvaltoihin vastatuulella

- Euroopan unionin tuomioistuin (EUT) antoi heinäkuussa 2020 ratkaisun koskien tietosuoja ja henkilötietojen siirtoa Yhdysvaltoihin ("Schrems II").
- EUT:n ratkaisun mukaan Yhdysvaltojen kanssa sovittu Privacy Shield- järjestelmä ei täytä tietosuoja-asetuksessa asetettuja vaatimuksia.
- Henkilötietojen siirtäminen Privacy Shield- järjestelmän perusteella ei ole sallittua 16.7.2020 lähtien.
- Tuomioistuin otti ratkaisussa kantaa myös mallisopimuslausekkeisiin henkilötietojen siirtojen perusteena kolmansiin maihin.



HENKILÖTIETOJEN SIIRTO YHDYSVALTOIHIN VASTATUULESSA

- Henkilötietojen siirto mallisopimuslausekkeitä hyödyntäen on edelleen sallittua.
- Mallisopimuslausekkeiden käyttöä sellaisenaan ei kuitenkaan välttämättä voida nähdä riittävänä ratkaisuna.
- Arvio tietosuojan toteuttamisesta tulisi tehdä tapauskohtaisesti huomioiden kohdemaan lainsäädäntö ennen mallisopimuslausekkeiden käyttöä.
- Euroopan tietosuojaneuvosto on korostanut Schrems II- ratkaisun jälkeisessä kannanotossaan myös sitä, että ensisijainen vastuu tietosuojan tason varmistamisesta on henkilötietoja siirtävällä taholla.
- Henkilötietojen siirto on keskeytettävä tai lopetettava, jos yritys toteaa, ettei asianmukaisia suojatoimia ja riittävän tietosuojan tasoa voida varmistaa.
- Privacy Shield -järjestelyn kumoamisen myötä tulee varmistaa, että henkilötietojen siirto perustuu jatkossa johonkin muuhun suojamekanismiin.

MITÄ TULISI TEHDÄ NYT?

- Käy läpi sopimuskumppanit ja palveluntarjoajat sen selvittämiseksi, mitkä näistä tahoista siirtävät henkilötietoja Yhdysvaltoihin tai muutoin käsittelevät niitä siellä.
 - Henkilötietojen siirroksi luokitellaan myös pääsyn tarjoaminen henkilötietoihin Yhdysvalloista tai pelkkä passiivinen säilyttäminen Yhdysvalloissa. Tietosuojalainsäädännön mukainen henkilötietojen määritelmä on hyvin laaja.
- Selvitä, perustuuko tietojen siirto Privacy Shield -menettelyyn vai johonkin muuhun tietosuoja-asetuksen mukaiseen suojamekanismiin.
- Siirry Privacy Shield -menettelystä muihin tietosuoja-asetuksen suojamekanismeihin, kuten mallisopimuslausekkeisiin ja mahdollisesti tarvittaviin lisätoimenpiteisiin.
 - Keskustele tarvittavista lisätoimenpiteistä Yhdysvalloissa henkilötietojen käsittelevän sopimuskumppanisi kanssa.
- Huomioi, että muutokset tietojen siirtoja koskeviin menettelyihin voivat edellyttää muutoksia esimerkiksi asiakassopimuksiin.
- Päivitä tietosuojaselosteet ja muu tietosuojainformaatio.
 - Henkilötietojen siirtämisestä Euroopan talousalueen ulkopuolelle ja siirroissa käytetyistä suojamekanismeista on informoitava käsittelyn kohteena olevia rekisteröityjä.
- Seuraa viranomaisten ohjeistuksia asian suhteen.

Brexit ja henkilötietojen siirto Isoon-Britanniaan?



Iso-Britannian EU-ero astui voimaan 1.2.2020.

Siirtymäkausi kestää vuoden 2020 loppuun. Siirtymäkauden aikana jatketaan EU:n nykysäännöillä ja neuvotellaan tulevasta suhteesta.

Euroopan unionin yleistä tietosuoja-asetusta sovelletaan siirtymäkauden ajan.

Henkilötietoja voidaan siirtää Britanniaan samoilla perusteilla kuin EU:n sisällä vuoden 2020 loppuun asti.

• •

LISÄTIETOJA

- Euroopan tietosuojaneuvoston vastauksia yleisimpiin kysymyksiin Schrems II -tuomiosta
- Yhdysvaltojen kauppaministeriön lausunto henkilötietojen siirrossa edellytettävistä lisätoimenpiteistä



LEXIA ASIANAJOTOIMISTO

MARKUS MYHRBERG

+358 40 5055343

markus.myhrberg@lexia.fi

VILLE KUKKONEN

+358 40 7456784

ville.kukkonen@lexia.fi