TIETOSUOJAVALTUUTETUN TOIMISTO

29.10.2021

Dnro 9024/181/19

Tietosuojavaltuutetun päätös henkilötietojen eheyttä ja luottamuksellisuutta, henkilötietojen käsittelyn turvallisuutta, sisäänrakennettua ja oletusarvoista tietosuojaa ja henkilötietojen siirtoja kolmansiin maihin koskevassa asiassa

Asia

Asiakkaiden henkilötietojen käsittely WhatsApp-pikaviestinpalvelussa

Kantelijalta saatu selvitys

Tietosuojavaltuutetun toimistossa on 21.11.2019 saatettu vireille kantelu, jonka mukaan siivousalan yritys käyttää asiakastietojen välittämiseen yritykseltä työntekijälle WhatsApp-pikaviestinpalvelua. Tietoihin lukeutuvat esimerkiksi asiakkaiden nimet, osoitteet, puhelinnumerot, ovikoodit ja avainboksien numerot.

Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä selvitystä 6.10.2020 päivätyllä selvityspyynnöllä. Rekisterinpitäjä on antanut asiassa selvityksen 19.10.2020 ja lisäselvityksen 19.11.2020.

Rekisterinpitäjä on kertonut, että se on muuttanut käytäntöjään tietosuojavaltuutetun toimiston selvityksen yhteydessä, ja WhatsApp-viesteinä kulkevat enää lähinnä työkohteiden sijaintitiedot, eli asiakkaiden nimet ja osoitteet. Esimerkiksi ovikoodit ilmoitetaan nyt työntekijälle suullisesti. Rekisterinpitäjä on kertonut, että se on käyttänyt WhatsApp-palvelua, koska asiakastietojen käsittelyyn tilattu palvelu on edelleen keskeneräinen, eikä rekisterinpitäjällä ole tietoa uuden palvelun käyttöönottoaikataulusta.

Rekisterinpitäjän mukaan kaikkia entisiä työntekijöitä on jo aiemmin ohjeistettu poistamaan kaikki viestintä, ja heitä on nyt muistutettu uudelleen asiasta. Rekisterinpitäjä on esittänyt tietosuojavaltuutetun toimistolle antamassaan selvityksessä, että kotiasiakkailla on tapana vaihtaa ovikoodeja, jolloin vanha koodi ei enää toimi, ja sisäänpääsy vaatii avaimen. Yritysten hälytyskoodit eivät rekisterinpitäjän mukaan mahdollista sisäänpääsyä, ja tällaisetkin koodit vaihdetaan tietyin aikavälein.

Kantelijan vastine

Kantelija on antanut asiassa vastineen 23.10.2020 ja kertonut, ettei rekisterinpitäjä ole aiemmin ohjeistanut työntekijöitä poistamaan WhatsApp-ryhmiä.

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), jota on sovellettu 1.1.2019 alkaen. Tietosuojalailla kumottiin aiemmin voimassa ollut henkilötietolaki (523/1999).

Yleisen tietosuoja-asetuksen 5(1)(f) artiklassa säädetään eheyden ja luottamuksellisuuden periaatteesta, jonka mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

Yleisen tietosuoja-asetuksen 24 artiklassa säädetään rekisterinpitäjän vastuusta. Artiklan 1 kohdan mukaan ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa. Artiklan 2 kohdan mukaan silloin, kun se on oikeasuhteista käsittelytoimiin nähden, 1 kohdassa tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.

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 (*käsittelyn turvallisuus*) säädetään teknisistä ja organisatorisista toimenpiteistä, jotka rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava henkilötietojen käsittelyyn liittyvää riskiä vastaavan turvallisuustason varmistamiseksi.

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.

Oikeudellinen kysymys

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

Tietosuojavaltuutetun tulee ratkaista, onko WhatsApp-pikaviestinpalvelun käyttäminen asiakkaiden henkilötietojen käsittelyssä ollut yleisen tietosuoja-asetuksen 5(1)(f) artiklan (*eheyden ja luottamuksellisuuden periaate*), 24 artiklan (*rekisterinpitäjän vastuu*), 25 artiklan (*sisäänrakennettu ja oletusarvoinen tietosuoja*) ja 32 artiklan (*käsittelyn turvallisuus*) mukaista.

Tietosuojavaltuutetun päätös

Rekisterinpitäjä ei ole noudattanut toiminnassaan yleisen tietosuoja-asetuksen 5(1)(f) artiklaa (*eheyden ja luottamuksellisuuden periaate*), 24 artiklaa (*rekisterinpitäjän vastuu*), 25 artiklaa (*sisäänrakennettu ja oletusarvoinen tietosuoja*) ja 32 artiklaa (*käsittelyn turvallisuus*). Rekisterinpitäjän menettely koskien WhatsApp-pikaviestinpalvelun käyttöä asiakkaiden henkilötietojen käsittelyssä ei näin ollen ole ollut yleisen tietosuoja-asetuksen mukainen.

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d-alakohdan mukainen määräys saattaa käsittelytoimet asetuksen säännösten mukaisiksi.

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b-alakohdan mukainen huomautus asetuksen säännösten vastaisista käsittelytoimista.

Perustelut

Yleisessä tietosuoja-asetuksessa on lähtökohtana riskiperusteinen lähestymistapa, jonka toteuttamiseksi rekisterinpitäjän tulee jatkuvasti arvioida suojaustoimenpiteiden riittävyyttä suhteessa käsittelyyn liittyviin riskeihin, sekä toteuttaa riskejä vastaavat tekniset ja organisatoriset toimenpiteet henkilötietojen riittävän suojaamisen varmistamiseksi (ks. erityisesti yleisen tietosuoja-asetuksen 24 artikla, *rekisterinpitäjän vastuu*).

Riskiperusteisen lähestymistavan kohdalla on nyt tarkasteltavana olevassa tapauksessa kiinnitettävä erityistä huomiota asetuksen 5 artiklan 1 kohdan f-alakohtaan (*eheyden ja luottamuksellisuuden periaate*) ja 32 artiklaan (*käsittelyn turvallisuus*).

Eheyden ja luottamuksellisuuden periaate edellyttää, että henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Tietoturvaa koskeva artikla 32 puolestaan edellyttää, että rekisterinpitäjä toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet riskiä vastaavan turvallisuustason varmistamiseksi.

Eheyden ja luottamuksellisuuden periaate on 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 eheyden ja luottamuksellisuuden periaatteen, täytäntöön tehokkaasti.[1]

Nyt arvioitavana olevassa asiassa rekisterinpitäjä on välittänyt asiakkaiden henkilötietoja työntekijöille WhatsApp-pikaviestinpalvelun kautta. Tietoihin on saattanut lukeutua esimerkiksi nimi, osoite, puhelinnumero, ovikoodi ja hälytysjärjestelmän koodi.

WhatsApp Messenger on puhelimen internet-yhteyttä käyttävä pikaviestinpalvelu älypuhelimille. Palvelua käytetään tyypillisesti tekstiviestien tapaan. Tietosuojavaltuutettu on katsonut aiemmassa, terveydenhuollon toimintaa koskevassa kannanotossaan (dnro 3013/183/18), että WhatsApp-sovelluksen käyttö johtaa asiakkaan henkilötietojen tietojen siirtoon kolmansiin maihin, eikä tietosuojavaltuutettu suosittele sovelluksen käyttöä ajanvaraukseen liittyvässä asiakasviestinnässä terveydenhuollon toiminnassa.[2] Aiemmassa ratkaisukäytännössään tietosuojavaltuutettu on lisäksi katsonut, ettei työntekijöitä tulisi tietoturvasyistä velvoittaa omien välineidensä käyttöön (dnro 2290/41/12).[3]

Nyt arvioitavana olevassa asiassa rekisterinpitäjä on käyttänyt WhatsApp-sovellusta asiakastietojen välittämiseen. Erityisesti osoitteiden, ovikoodien ja avainboksien numeroiden kohdalla kyse on ollut tiedoista, joiden päätymisestä sivulliselle voi aiheutua rekisteröidylle selkeää haittaa. Rekisterinpitäjä on esittänyt antamassaan selvityksessä, että se on varotoimenpiteenä ohjeistanut entisiä työntekijöitä poistamaan kaiken viestinnän. Tässä yhteydessä rekisterinpitäjä ei selvityksessä saatujen tietojen perusteella ole varmistanut, onko yritystoimintaan liittyvä ryhmä esimerkiksi työsuhteen päättyessä poistettu, tai onko työntekijän varmuuskopiosta poistettu yritystä koskeva osio. Asiassa saadun selvityksen perusteella rekisterinpitäjä ei myöskään ole informoinut rekisteröityjä, eli siivousyrityksen asiakkaita, WhatsApp-sovelluksen käytöstä.

WhatsApp-palvelun kohdalla on huomioitava, että sovellusta käytettäessä sopimussuhde on yksityishenkilön, eli työntekijän ja Facebookin välillä, eivätkä esimerkiksi yksityishenkilön kanssa tehtävään sopimukseen sisältyvät vastuunrajoituslausekkeet ole lähtökohtaisesti yhteensopivia yrityskäytön kanssa.

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

[2] Erityisesti terveydenhuollon osalta voidaan myös todeta, että tieto viestinnästä (ns. metatieto) on sovelluksessa vapaasti hyödynnettävää tietoa, joka paljastaa esimerkiksi arkaluonteiseksi tiedoksi luokiteltavan asiointisuhteen terveydenhuollon kanssa.

[3] Asia on koskenut työntekijän henkilökohtaisten pankkitunnusten käyttämistä työtehtävän hoitoon liittyvässä sähköisessä tunnistautumisessa.

Sovellusta hyödynnettäessä rekisterinpitäjällä ei myöskään ole keinoja valvoa, miten henkilötietoja palvelussa käytetään, tai asettaa muutoinkaan käytölle rajoituksia.[4] Lisäksi asiassa voidaan huomioida sovelluksen käyttämisen riskialttius puhelimen katoamistilanteessa, jolloin puhelimeen pääsy mahdollistaa käytännössä myös WhatsApp-sovellukseen pääsyn.

Edellä todetun perusteella tietosuojavaltuutettu katsoo, ettei WhatsApp-sovelluksen käyttö asiakastietojen välittämisessä yritykseltä työntekijän henkilökohtaiseen puhelimeen ole vastannut eheyden ja luottamuksellisuuden periaatteeseen, sisäänrakennetun ja oletusarvoisen tietosuojan velvoitteeseen ja käsittelyn turvallisuuteen liittyviä vaatimuksia, eikä rekisterinpitäjä ole huomioinut, että sen tulee asetuksen riskiperusteisen lähestymistavan mukaisesti toteuttaa riskejä vastaavat tekniset ja organisatoriset toimenpiteet henkilötietojen riittävän suojaamisen varmistamiseksi.

Nyt arvioitavassa asiassa tietosuojavaltuutettu kiinnittää lisäksi erityistä huomiota siihen, että sovelluksen käyttö on todennäköisesti johtanut tiedonsiirtoihin unionista kolmansiin maihin, mukaan lukien 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.[5] Asian vireilletuloajankohtana[6] riittävän tietosuojan tason turvaamiseksi EU:n ja Yhdysvaltojen välisissä tiedonsiirroissa on käytetty niin kutsuttua Privacy Shield -järjestelyä. Unionin tuomioistuin on kuitenkin todennut ratkaisussaan asiassa C-311/18[7], että EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä annettu päätös 2016/1250 on pätemätön.[8] 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 Yhdysvaltain viranomaisia vastaan tuomioistuimissa.[9] Unionin tuomioistuin toteaa edelleen, että rekisterinpitäjän on keskeytettävä henkilötietojen siirrot kolmanteen maahan, jos se ei voi toteuttaa riittäviä lisätoimenpiteitä henkilötietojen suojan varmistamiseksi.[10]

Euroopan tietosuojaneuvosto on arvioinut edellä sanotun päätöksen seurauksia ja riittäviä suojamekanismeja. Asian tullessa vireille tietosuojavaltuutetun toimistossa Privacy Shield -järjestelmä on ollut yhä käytössä, ja asian selvityksen aikana asiassa C-311/18 annetun päätöksen seurausten arviointi Euroopan tietosuojaneuvostossa on ollut kesken. Tämän vuoksi asian selvittämisen yhteydessä rekisterinpitäjältä ei ole pyydetty erikseen selvitystä koskien yleisen tietosuoja-asetuksen V-luvun mukaisia siirtomekanismeja, joilla turvataan yleisen tietosuoja-asetuksen mukainen henkilötietojen suojan taso. Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä selvitystä ennen kuin Euroopan tietosuojaneuvosto on hyväksynyt tietojen siirtämistä koskevat

[4] Tietosuojanäkökohtien ohella voidaan huomioida, että sovellusta käyttäessään työnantaja-asemassa oleva taho luopuu osittain direktio-oikeudestaan.
[5] Ks. yleisen tietosuoja-asetuksen 44 artikla ja johdantokappale 101.
[6] Asia on saatettu vireille tietosuojavaltuutetun toimistossa 21.11.2019.
[7] Ratkaisu on annettu 16.7.2020.
[8] Ratkaisun kohta 201.
[9] Ks. ratkaisun osio *Tietosuojan riittävää tasoa koskeva toteamus* (alkaa ratkaisun kohdasta 168).
[10] Ratkaisun kohta 135.

suuntaviivat[11] ja Euroopan komissio on hyväksynyt tiedonsiirtoja kolmansiin maihin koskevat vakiolausekkeet[12]. Näin ollen tietosuojavaltuutettu ei käytä asiassa tältä osin yleisen tietosuoja-asetuksen 58(2) artiklan mukaisia korjaavia toimivaltuuksiaan.

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.

Tiedoksianto

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

[11] EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.
[12] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972.