TIETOSUOJAVALTUUTETUN TOIMISTO

12.3.2024

TSV/29/2020

Apulaistietosuojavaltuutetun päätös

Asia

Henkilötunnuksen ja laboratoriotutkimustietojen lähettäminen potilaalle tekstiviestitse

Rekisterinpitäjä

Hyvinvointialue[1]

Tietosuojavaltuutetun toimistolle tehty ilmoitus

Tietosuojavaltuutetun toimistoon 27.1.2020 yhteyttä ottanut henkilö on kertonut ilmoituksessaan, että hän oli saanut keskussairaalalta tekstiviestin, joka alkoi hänen henkilötunnuksellaan ja jossa hänen PSA-näytteensä kerrottiin epäonnistuneen. Tekstiviestissä kehotettiin olemaan yhteydessä laboratorioon.

Vireillesaattaja tiedustelee toimintatavan tietosuojalainsäädännön mukaisuutta.

Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä selvitystä 2.8.2022 päivätyllä selvityspyynnöllä.[2] Rekisterinpitäjä on 23.8.2022 antanut asiassa kirjallisen selvityksen.

Rekisterinpitäjä on esittänyt selvityksessään, että henkilötunnuksen sisällyttäminen tekstiviesteihin varmistaa sen, että esimerkiksi samannimisille, väärille henkilöille ei ohjaudu vahingossa tietoja.

Rekisterinpitäjän mukaan mobiilipalvelu lähettää potilaalle automaattisesti tekstiviestillä testissä mitattavan arvon, hoito-ohjeen ja ehdotuksen seuraavasta kontrollipäivästä. Automaattisten tekstiviestien sisällöt voivat olla esimerkiksi seuraavanlaisia:

> ”[Potilaan henkilötunnus]: [Testin X] arvonne on [Y] ja kaikki on kunnossa. Seuraava kontrollinne on [päivämäärä]”
>
> ”[Potilaan henkilötunnus]: [Testin X] arvonne on [Y]. Tilanteen tarkistamiseksi ottakaa yhteyttä”

[1] Asian vireillesaattamisajankohtana rekisterinpitäjänä on toiminut sairaanhoitopiiri. Vastuu rekisterinpidosta on 1.1.2023 alkaen siirtynyt sairaanhoitopiiriltä hyvinvointialueelle.
[2] Selvitys on pyydetty sairaanhoitopiiriltä diaarinumerolla 665/182/20.

Rekisterinpitäjän mukaan palvelussa, jossa henkilötunnus välittyy tekstiviestinä potilaan omaan matkapuhelimeen, henkilötunnuksen käsittelyyn liittyvän riskin on arvioitu olevan vähäinen. Sen sijaan tilanteessa, jossa laboratoriokokeen jälkeinen viesti kohdennetaan väärälle henkilölle, rekisteröidyn henkeen ja terveyteen kohdistuvat riskit voivat olla huomattavan suuret.

Sovellettavasta lainsäädännöstä

Asiassa sovelletaan Euroopan parlamentin ja neuvoston yleistä tietosuoja-asetusta (EU) 2016/679 (yleinen tietosuoja-asetus) ja täsmentävää kansallista tietosuojalakia (1050/2018).

Yleisen tietosuoja-asetuksen 5(1)(c) artiklassa säädetään tietojen minimointiperiaatteesta. Artiklan mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

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, kuten tietojen pseudonymisointi ja tarvittavat suojatoimet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi yleisen tietosuoja-asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin. 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. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

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 87 artiklassa säädetään kansallisen henkilötunnuksen käsittelemisestä. Artiklan mukaan jäsenvaltiot voivat määritellä tarkemmin erityiset kansallisen henkilönumeron tai muun yleisen tunnisteen käsittelyn edellytykset. Tässä tapauksessa kansallista henkilönumeroa tai muuta yleistä tunnistetta on käytettävä

ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia yleisen tietosuoja-asetuksen mukaisesti.

Ratkaistavana olevan asian tapahtuma-ajankohtana tietosuojalain 29 §:ssä on säädetty henkilötunnuksen käsittelystä seuraavasti: Henkilötunnusta saa 29 §:n 1 momentin mukaan käsitellä rekisteröidyn suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää: 1) laissa säädetyn tehtävän suorittamiseksi; 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai 3) historiallista tai tieteellistä tutkimusta taikka tilastointia varten. Tietosuojalain 29 §:n 2 momentin mukaan henkilötunnusta saa käsitellä luotonannossa tai saatavan perimisessä, vakuutus-, luottolaitos-, maksupalvelu-, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Tietosuojalain 29 §:n 4 momentin mukaan henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Tietosuojalain 29 §:n sääntelyä on tiukennettu 1.1.2024 voimaan tulleella lakimuutoksella. Tässä apulaistietosuojavaltuutetun päätöksessä sovelletaan tapahtuma-ajankohtana voimassa ollutta sääntelyä.

Oikeudellinen kysymys

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

Apulaistietosuojavaltuutetun on ratkaistava:

> Onko rekisterinpitäjän menettelytapa, jossa se on tavanomaisesti lähettänyt rekisteröidyille automatisoituja, laboratoriokäyntejä koskevia tekstiviestejä, joihin on sisällytetty henkilötunnus, ollut yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdan, 25 artiklan 2 kohdan ja tietosuojalain 29.4 §:n mukainen.
>
> Nyt päätöksen kohteena olevassa asiassa on kyse myös tekstiviestin käyttöön liittyvistä, käsittelyn turvallisuutta koskevista, yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdan mukaisista seikoista. Tekstiviestitse lähetettävien henkilötietojen suojaamisen osalta apulaistietosuojavaltuutettu antaa rekisterinpitäjälle ohjausta.

Apulaistietosuojavaltuutetun päätös

Päätös

Rekisterinpitäjän tavanomainen menettelytapa, jossa se on lähettänyt rekisteröidyille automatisoituja, laboratoriokäyntejä koskevia tekstiviestejä, joihin on sisällytetty henkilötunnus, ei ole ollut tietosuojalain 29.4 §:n (*henkilötunnuksen käsittely*), yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c alakohdan (*tietojen minimointi*) ja 25 artiklan 2 kohdan (*oletusarvoinen tietosuoja*) mukainen.

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d alakohdan mukainen määräys saattaa henkilötunnuksen käsittelyä koskevat käsittelytoimet yleisen tietosuoja-asetuksen ja tietosuojalain säännösten mukaisiksi.

Apulaistietosuojavaltuutettu määrää rekisterinpitäjän toimittamaan selvityksen tehdyistä toimenpiteistä tietosuojavaltuutetun toimistolle **13.5.2024** mennessä, ellei se hae muutosta tähän päätökseen.

Laboratoriotutkimustietojen tekstiviestitse lähettämistä koskevan menettelyn osalta apulaistietosuojavaltuutettu antaa rekisterinpitäjälle ohjausta.

Perustelut

Henkilötunnuksen tarpeellisuus tekstiviesteissä

Nyt arvioitavassa asiassa tietosuojavaltuutetun toimistolle ilmoituksen tehneelle henkilölle on toimitettu tekstiviestitse tieto laboratoriotutkimuksen epäonnistumisesta. Tekstiviestissä on mainittu lisäksi ilmoituksen tehneen henkilön henkilötunnus ja kehotettu häntä olemaan yhteydessä laboratorioon. Tekstiviestissä on ollut kyse potilaalle automatisoidusti, mobiilipalvelun kautta lähetetystä viestistä.

Rekisterinpitäjä on selvityksessään esittänyt, että henkilötunnuksen sisällyttämisellä tekstiviesteihin varmistetaan, että esimerkiksi samannimisille, eri henkilötunnuksen omaaville henkilöille ei ohjaudu virheellisesti tietoja.

Tietosuojalain 29 §:n tarkoituksena on suojata henkilötunnusta ja pyrkiä estämään sen tarpeetonta käsittelyä.[3] Tietosuojalain 29.4 §:n mukaan henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin.

Asiakirjan käsite on laaja. Lainsäädännössä asiakirjan käsitettä on määritelty esimerkiksi julkisuuslain (621/1999) 5.1 §:ssä. Lainkohdan mukaan kyseisessä laissa asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.[4] Tietosuojalain 29.4 §:ssä säädettyä ei ole rajattu koskemaan tiettyjä asiakirjatyyppejä. Nyt arvioitavassa asiassa tekstiviesti on katsottava tietosuojalain 29.4 §:ssä tarkoitetuksi asiakirjaksi, johon henkilötunnusta ei tule tarpeettomasti merkitä.

Tietosuojalain 29 §:n lisäksi henkilötunnuksen käsittelyyn sovelletaan muita yleisen tietosuoja-asetuksen asiaankuuluvia säännöksiä,[5] kuten yleisen tietosuoja-asetuksen 5(1)(c) artiklaa ja 25(2) artiklaa. Edellä mainituista säännöksistä seuraa, että rekisterinpitäjän tulee rakentaa sen tietojärjestelmät niin, että henkilötunnusta käsitellään vain sellaisissa tilanteissa kuin se on tarpeellista.

Apulaistietosuojavaltuutettu toteaa, että rekisterinpitäjän esittämät perustelut henkilötunnuksen käsittelyn tarpeellisuudesta liittyvät olennaisesti rekisteröidyn yksilöintiin siinä vaiheessa, kun tietojärjestelmästä haetaan oikean potilaan tiedot.

---

[3] HE 96/1998, s. 48 (”*Määrittelyllä pyritään estämään henkilötunnuksen tarpeetonta käsittelyä*”).

[4] On myös muistettava, että luonnollisten henkilöiden suojelun olisi oltava teknologianeutraalia, eli se ei saisi riippua käytetystä tekniikasta (ks. esim. yleisen tietosuoja-asetuksen johdantokappale 15).

[5] Kansallista henkilötunnusta on käytettävä ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia yleisen tietosuoja-asetuksen mukaisesti (ks. yleisen tietosuoja-asetuksen 87 artikla ja HE 9/2018 vp, s. 113). Ks. myös esim. Euroopan unionin tuomioistuimen ratkaisu asiassa C-439/19, ratkaisun kohta 96 (”*kaikessa henkilötietojen käsittelyssä on yhtäältä noudatettava tietojen käsittelyä koskevia periaatteita*”).

Rekisterinpitäjän on mahdollista käsitellä henkilötunnusta taustajärjestelmässään potilaan yksilöimistarkoituksessa ja sen varmistamiseksi, että kyse on oikeasta henkilöstä, jolle tekstiviesti tullaan välittämään.

Apulaistietosuojavaltuutettu toteaa, että vaikka henkilötunnusta voidaan käsitellä sen henkilön yksilöimiseksi, jolle tekstiviesti on tarkoitus välittää, henkilötunnusta ei tule kuitenkaan tarpeettomasti merkitä tekstiviestin sisältöön.

Apulaistietosuojavaltuutettu katsoo, että henkilötunnuksen merkitseminen tekstiviestiin ei tosiasiallisesti vaikuta siihen, että viesti ohjautuu oikealle henkilölle. Rekisterinpitäjä ei ole tuonut esille muita perusteita henkilötunnuksen käsitellylle, eikä apulaistietosuojavaltuutetun tiedossa ole muutoinkaan perusteita, joiden nojalla henkilötunnuksen merkitseminen tekstiviestiin olisi tarpeellista. Rekisterinpitäjän menettely ei siten ole edellä esitetyin perustein ollut yleisen tietosuoja-asetuksen 5(1)(c) ja 25(2) artiklojen tai tietosuojalain 29.4 §:n mukaista.

Apulaistietosuojavaltuutettu muistuttaa tässä yhteydessä, että henkilötunnusta ei tule käyttää esimerkiksi pelkästään rekisterinpitäjän toiminnan sujuvoittamistarkoituksessa, eikä rekisterinpitäjän tule käsitellä henkilötunnusta vain siitä syystä, että tietojen käsittely on henkilötunnuksen avulla helpompaa.[6] Tietojärjestelmät on rakennettava siten, että automatisoidusti lähetettäviin tekstiviesteihin ei tarpeettomasi merkitä henkilötunnusta. Henkilötunnusta tulee niin ikään käsitellä siten, ettei se tule asiattomasti sivullisten saataville.

Apulaistietosuojavaltuutettu antaa tämän menettelyn osalta rekisterinpitäjälle määräyksen saattaa käsittelytoimet tietosuojasääntelyn mukaisiksi.

Tekstiviestitse lähetettävien henkilötietojen suojaaminen

Tekstiviestitse lähetettävien henkilötietojen suojaamisen osalta apulaistietosuojavaltuutettu antaa rekisterinpitäjälle yleistä ohjausta.

Asian vireillesaattajalle on toimitettu tekstiviestitse henkilötunnus sekä tieto tietyn, erikseen nimetyn laboratoriotutkimuksen epäonnistumisesta. Kyse on ollut rekisteröidyille tavanomaiseen tapaan lähetettävistä tekstiviesteistä.

Tekstiviestien tietoturvallisuudesta voidaan todeta seuraavaa: SMS-viestit kulkevat matkapuhelinverkossa teleyritysten välillä suojaamattomina. SMS-viestien sisältöä ei suojata välityksen aikana esimerkiksi salakirjoituksella muutoin kuin mobiililaitteen ja matkapuhelinverkon tukiaseman välisen radioliikenteen osalta. SMS-viestijärjestelmä (SS7) ei tarjoa edellytyksiä viestisisällön tai viestin välitystietojen salaamiselle.

Tekstiviestien kohdalla voidaan myös huomioida, että SMS-viestien välitysmekanismit toteuttavasta SS7-protokollarymästä on tunnistettu haavoittuvuuksia, jotka muodostavat uhan viestinnän luottamuksellisuuden toteutumiselle ja joita ei ole mahdollista korjata tai asianmukaisella tavalla hallita. Näiden haavoittuvuuksien vuoksi on esimerkiksi mahdollista ohjata tiettyyn tilaajaliittymään lähetetyt SMS-viestit matkapuhelinverkossa viestinnän välitykseen nähden sivulliselle teleyritykselle ja lukea ne siellä selkokielisenä. Myös mobiililaitteisiin ujutettujen haittaohjelmien kautta on

[6] Ks. myös HE 9/2018 vp, s. 113–114 (”[…] *esimerkiksi pelkkä laissa säädetyn tehtävän helpompi tai nopeampi suorittaminen henkilötunnuksen avulla ei oikeuttaisi henkilötunnuksen käsittelyä, vaan käsittely olisi sallittua ainoastaan silloin, kun rekisteröidyn yksiselitteinen yksilöiminen on tärkeää tehtävästä suoriutumiseksi*”).

mahdollista urkkia tietoja. Lisäksi SS7-protokollaryhmän roaming-ominaisuuden väärinkäyttö saattaa mahdollistaa esimerkiksi mobiililaitteen ja matkapuhelinverkon välisen liikenteen salakuuntelun. SMS-viestit voidaan myös kaapata paikallisesti valetukiasemien tai haittasovellusten avulla.

Henkilötunnuksessa on kyse vahvasti yksilöivästä ja lähtökohtaisesti pysyväksi tarkoitetusta tunnisteesta, jonka päätymisestä sivullisille voi aiheutua rekisteröidylle merkittävää haittaa, kuten joutuminen identiteettivarkauden uhriksi. Henkilötunnusta on käytettävä ainoastaan noudattaen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia yleisen tietosuoja-asetuksen mukaisesti.

Tieto tietylle henkilölle suoritetusta lääketieteellisestä toimenpiteestä on puolestaan terveyttä koskeva, erityisiin henkilötietoryhmiin kuuluva tieto (yleisen tietosuoja-asetuksen 9 artikla). Rekisterinpitäjän tulee suojata erityisiin henkilötietoryhmiin kuuluvia tietoja erityisen hyvin.[7]

Apulaistietosuojavaltuutettu ohjaa rekisterinpitäjää huomioimaan, että rekisterinpitäjän menettelytapaan liittyy edellä esitetysti tietoturvariskejä, jotka sen tulee huomioida, jotta yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdan vaatimukset, kuten henkilötietoihin pääsyyn liittyvien riskien asianmukainen hallinta, täyttyvät. Tekstiviestien suojauksen yleisen toteutustavan vuoksi rekisterinpitäjän ei ole käytännössä mahdollista parantaa tätä suojausta teknisillä toimenpiteillä, vaan sen on huolehdittava henkilötietojen asianmukaisen suojan toteutumisesta rajaamalla rekisteröidyille yksipuolisesti lähetettäviin tekstiviesteihin sisällytettävät henkilötiedot.

Rekisteröidyille lähetettävien tekstiviestien tietosisältö tulee siis muodostaa käsittelyn turvallisuusvaatimuksen sekä sisäänrakennetun ja oletusarvoisen tietosuojan (yleisen tietosuoja-asetuksen 25 artikla) vaatimusten mukaisesti, riskiperusteista lähestymistapaa noudattaen. Niin ikään rekisterinpitäjän tulee tekstiviestien sisältöä määritellessään ottaa asianmukaisesti huomioon tekstiviestien suojaukseen liittyvät puutteet sekä tekstiviestillä toimitettavien tietojen luonne.

Edellä todetun perusteella apulaistietosuojavaltuutettu ohjaa rekisterinpitäjää oletusarvoisena toimintatapanaan rajaamaan tekstiviestien tietosisällön asianmukaisesti. Esimerkiksi tietosuojavaltuutetun toimistolle ilmoituksen tehneen henkilön kohdalla tekstiviestin sisältö olisi ollut mahdollista rajata siten, että tekstiviestissä olisi kerrottu yleisellä tasolla laboratoriotutkimuksen epäonnistumisesta ja pyydetty henkilöä olemaan yhteydessä laboratorioon.

Rekisterinpitäjän olisi menettelytapojaan määrittäessään niin ikään hyvä arvioida mahdollisuuksia vaihtoehtoisille toimintatavoille henkilötietojen tavanomaisessa saattamisessa rekisteröityjen tietoon.

Sovelletut lainkohdat

Yleisen tietosuoja-asetuksen 5(1)(c), 25(1), 25(2), 32(1) ja 32(2) artiklat, tietosuojalain 29.4 §.

[7] Ks. esim. yleisen tietosuoja-asetuksen johdantokappale 51: ”*Henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille*”. Lainsäädännössä on myös säädetty erityisistä salassapitovelvoitteista, kun terveydenhuollon toimintayksikkö käsittelee potilaan terveystietoja.

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 valitusosoituksen mukaiseen 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

Päätöksen on tehnyt apulaistietosuojavaltuutettu Heljä-Tuulia Pihamaa.