TIETOSUOJAVALTUUTETUN TOIMISTO

Päätös

TSV/3/2019
Dnro128/182/19

4.12.2023

Apulaistietosuojavaltuutetun päätös

Asia

Henkilötietojen käsittelyn turvallisuus terveydenhuollon ajanvarauspalvelussa.

Rekisterinpitäjä

Terveydenhuollon toimija

Asian kuvaus

Tietosuojavaltuutetun toimistoon on saatettu vireille asia, joka koskee yleisen tietosuoja-asetuksen ((EU) 2016/679) 32 artiklassa säädettyä henkilötietojen käsittelyn turvallisuutta rekisterinpitäjän verkkoajanvarausjärjestelmässä.

Rekisterinpitäjältä saatu selvitys

Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä selvitystä 14.3.2023. Selvityspyynnön yhteydessä tietosuojavaltuutetun toimisto on antanut rekisterinpitäjälle ohjausta yleisen tietosuoja-asetuksen 32 artiklasta. Samassa yhteydessä rekisterinpitäjälle on annettu tiedoksi apulaistietosuojavaltuutetun päätös[1] koskien toisen terveydenhuollon rekisterinpitäjän verkkoajanvarausjärjestelmää.

Rekisterinpitäjä on vastannut selvityspyyntöön 30.3.2023. Rekisterinpitäjä on todennut, että rekisterinpitäjän verkkoajanvarausjärjestelmässä uuden ajan varaaminen on toteutettu etunimi, sukunimi ja henkilötunnus -yhdistelmällä.

Rekisterinpitäjä on todennut, että verkkoajanvarausjärjestelmän väärinkäyttöä ei ole havaittu. Rekisterinpitäjän mukaan väärinkäyttöä on pyritty havaitsemaan kirjautumisten lukumäärän ja epäonnistuneiden kirjautumisyritysten havainnoinnin avulla. Rekisterinpitäjä on todennut, että kirjautuminen verkkoajanvarausjärjestelmään on estettävissä tarvittaessa selainistunnon ja IP-osoitteen perusteella. Rekisterinpitäjä on todennut, että ajanvarauksen käytön voi yksittäistapauksessa estää.

Rekisterinpitäjä on todennut, että verkkoajanvarausjärjestelmään on mahdollista määrittää salasana. Rekisterinpitäjä ei kuitenkaan ole ottanut salasanatoimintoa käyttöön. Rekisterinpitäjä on kertonut ottavansa

[1] Dnro 5546/163/2019

TIETOSUOJAVALTUUTETUN TOIMISTO

todennäköisesti käyttöön vahvan sähköisen tunnistamisen vuoden 2024 aikana.

Oikeudellinen kysymys

Asiassa on ratkaistavana, onko henkilötietojen käsittely rekisterinpitäjän ylläpitämässä verkkoajanvarausjärjestelmässä täyttänyt yleisen tietosuoja-asetuksen ((EU) 2016/679) 32 artiklan 1 ja 2 kohdassa asetetut vaatimukset siltä osin kuin ajanvaraus rekisterinpitäjän terveyspalveluihin on ollut mahdollista etunimi-, sukunimi- ja henkilötunnusyhdistelmällä.

Mikäli vastaus edellä olevaan kysymyksen on kielteinen, apulaistietosuojavaltuutetun harkittavaksi tulee, onko asiassa tarpeen käyttää yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan b alakohdan mukaisia korjaavia toimivaltuuksia.

Apulaistietosuojavaltuutetun päätös

Määräys saattaa käsittelytoimet yleisen tietosuoja-asetuksen mukaisiksi

Apulaistietosuojavaltuutettu antaa rekisterinpitäjälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d alakohdan mukaisen määräyksen saattaa käsittelytoimet yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdissa säädetyn mukaisiksi.

Apulaistietosuojavaltuutettu määrää toimittamaan selvityksen tehdyistä toimenpiteistä tietosuojavaltuutetun toimistoon viimeistään kuuden viikon kuluttua päätöksen tiedoksisaannista, ellei rekisterinpitäjä hae muutosta tähän päätökseen.

Apulaistietosuojavaltuutetun päätöksen perustelut

Rekisterinpitäjä tuottaa yksityisestä terveydenhuollosta annetun lain (152/1990) [2] mukaisia terveydenhuollon palveluita. Rekisterinpitäjän verkkosivustolla[3] kerrotaan, että rekisterinpitäjä on Pohjois-Suomen johtava gynekologiaan erikoistunut lääkärikeskus. Verkkosivustolla kerrotaan, että ajan voi varata monipuolisesti erilaisiin terveydenhuollon palveluihin, kuten gynekologiaan, psykiatriaan, mammografiaan, syöpähoitoihin ja plastiikkakirurgiaan. Verkkosivuston mukaan soittopyyntöjä, toimenpideaikoja, raskausajan ultraäänitutkimuksia tai muita erikoistutkimuksia ei voi varata sähköisen verkkoajanvarauspalvelun kautta.

Rekisterinpitäjän sähköisessä verkkoajanvarausjärjestelmässä kirjautuminen[4] on toteutettu pelkästään henkilötunnuksen sekä etu- ja sukunimen yhdistelmällä. Rekisterinpitäjä ei tunnista verkossa asioivan henkilöllisyyttä. Verkkoajanvarausjärjestelmä ei myöskään tee nimi- ja henkilötunnusvertailua eli sähköinen ajanvaraus on mahdollista ilman, että nimi- ja henkilötunnustiedot kuuluvat samalle henkilölle.

[2] Uusi laki terveydenhuollon valvonnasta 741/2023 tulee osittain voimaan 1.1.2024.

[3] Rekisterinpitäjän verkkosivu

[4] Verkkoajanvarausjärjestelmän verkkosivu

Apulaistietosuojavaltuutettu katsoo, että pelkästään henkilötunnuksen sekä etu- ja sukunimen kysyminen verkkoajanvarauksen yhteydessä ei todenna henkilöllisyyttä sähköisessä asioinnissa. Henkilötunnusta ei ole tarkoitettu henkilön tunnistamiseen, vaan henkilöiden erottamiseen toisistaan. Henkilötunnuksen käyttö salasanan kaltaisena tietona perustuu oletukseen, ettei henkilötunnus ole ulkopuolisten tiedossa ja henkilötunnuksen tietäminen siten todentaisi henkilön henkilöllisyyden. Tosiasiallisesti henkilötunnus on kuitenkin lähes aina useiden muidenkin henkilöiden tiedossa.

Terveydenhuollossa käsiteltävien ajanvaraustietojen ensisijainen käyttötarkoitus on potilaan terveyspalvelujen järjestäminen ja potilaan hoidon toteuttaminen.[5] Terveydenhuollon ajanvaraustiedot ovat laissa potilaan asemasta ja oikeuksista 1992/785, (potilaslaki) tarkoitettuja potilasasiakirjoja[6], ja laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (2021/784, asiakastietolaki) tarkoitettuja potilastietoja[7]. Terveydenhuollon ajanvaraustiedot sisältyvät yleisen tietosuoja-asetuksen (EU) 2016/679 9 artiklan mukaisiin erityisiin henkilötietoryhmiin.

Tietosuoja-asetuksen 35 johdantokappaleessa määritellään terveyttä koskeva henkilötieto. Kyseisen johdantokappaleen mukaan terveyttä koskevia henkilötietoja ovat kaikki tiedot, jotka koskevat rekisteröidyn terveydentilaa ja paljastavat tietoja rekisteröidyn entisestä, nykyisestä tai tulevasta fyysisen terveyden tai mielenterveyden tilasta. Tiedot, jotka on kerätty terveyspalvelujen saamista varten tai niiden tarjoamisen yhteydessä ovat terveyttä koskevia tietoja. Lisäksi luonnolliselle henkilölle annettu numero, symboli tai erityistuntomerkki, jolla hänet voidaan tunnistaa yksiselitteisesti terveydenhuollon piirissä ovat johdantokappaleen mukaan terveyttä koskevia tietoja. Tiedot sairauksista, vammoista, sairauden riskistä, esitiedoista tai annetuista hoidoista sekä tieto rekisteröidyn fyysisestä tai lääketieteellisestä tilanteesta riippumatta siitä, mistä lähteestä tiedot on saatu ovat terveyttä koskevia yleisen tietosuoja-asetuksen 9 artiklan mukaisia erityisiin henkilötietoryhmiin kuuluvia tietoja.

Terveydenhuollon palveluiden järjestämisessä rekisterinpitäjän vastuu ja huolellisuus ovat korostuneet. Terveydenhuollon palveluja käyttävät voivat olla heikossa asemassa olevia rekisteröityjä, jotka eivät välttämättä kykene arvioimaan sähköiseen ajanvarauspalveluun sisältyviä riskejä.

Kirjautumista huijaustarkoituksessa voi olla vaikea havaita, sillä rekisterinpitäjän ylläpitämässä sähköisessä ajanvarauksessa ei ole käytössä tunnistautumista (heikkoa[8] tai vahvaa). Sähköiset kirjautumisyritykset on voitu esimerkiksi hajauttaa pitkälle aikavälille, useammalle kohteelle ja eri IP-osoitteista tuleviksi. Kun sähköiseen ajanvaraukseen ei vaadita heikkoa tai vahvaa tunnistautumista, ajan varaaminen on mahdollista toisen henkilön henkilötiedoilla. Ilman lupaa toisen henkilön tiedoilla tehtyjä ajanvarauksia kutsutaan ns. haamuajanvarauksiksi. Esimerkiksi kiusantekotarkoituksessa tehty haamuajanvaraus voi aiheuttaa haamuajanvarauksen kohteena olevalle rekisteröidylle monenlaista vahinkoa, kuten mielipahaa asian selvittämisestä,

[5] Potilastietojen käyttötarkoitus on potilaslain (laki potilaan asemasta ja oikeuksista annettu laki 1992/785) 12 § 1 momentista johdettuna potilaan hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan turvaaminen.

[6] Potilaslain 2 § 5 kohdassa säädetyn mukaisesti potilasasiakirjoilla tarkoitetaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettäviä, laadittuja tai saapuneita asiakirjoja taikka teknisiä tallenteita, jotka sisältävät hänen terveydentilaansa koskevia tai muita henkilökohtaisia tietoja.

[7] Uusi asiakastietolaki 703/2023 (laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä) ei ole tätä päätöstä kirjoittaessa voimassa. Uusi asiakastietolaki tulee voimaan 1.1.2024. Hallituksen esitys HE 246/2022 vp.

[8] Heikolla tunnistamisella tarkoitetaan tässä yhteydessä muuta kuin vahvaa tunnistamista, lisätietoja alaviitteessä 11.

sekä taloudellisia vahinkoja (palvelusta seurannut lasku). Henkilö voi joutua identiteettivarkauden kohteeksi, jos hänen henkilötunnustaan käytetään identiteettivarkauden[9] täyttävän teon tunnusmerkistön mukaisesti.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain eli asiakastietolain (784/2021)17 §:n 1 momentin mukaan asiakas on asiakastietojen sähköisessä käsittelyssä tunnistettava luotettavasti.[10] Etäpalveluiden yhteydessä luotettavana tunnistamismenetelmänä pidetään Sosiaali- ja terveysalan lupa- ja valvontaviraston ja Asiakas- ja potilasturvallisuuskeskuksen mukaan ainakin vahvaa tunnistamista.[11] Vahvalla sähköisellä tunnistamisella voi todentaa henkilöllisyyden sähköisessä asioinnissa.

Yleisen tietosuoja-asetuksen 32 artikla edellyttää rekisterinpitäjän toteuttavan teknisiä ja organisatorisia toimenpiteitä, joiden avulla rekisterinpitäjä voi varmistaa, että henkilötietojen käsittelyn turvallisuus vastaa henkilötietojen käsittelystä rekisteröityjen oikeuksille ja vapauksille aiheutuvia riskejä. Asianmukaisen turvallisuustason arvioimisessa rekisterinpitäjän on kiinnitettävä huomiota muun ohella luvattomasta luovuttamisesta tai henkilötietoihin pääsystä rekisteröidyille aiheutuviin riskeihin (yleisen tietosuoja-asetuksen 32 artiklan 2 kohta). Rekisterinpitäjä voi pyrkiä pienentämään riskejä esimerkiksi kyvyllä taata henkilötietojen käsittelyyn käytettävien tietojärjestelmien ja palveluiden jatkuva luottamuksellisuus (yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan b-alakohta).

Apulaistietosuojavaltuutettu katsoo, että henkilötietojen käsittelyn turvallisuuden tasoa ei voida rekisterinpitäjän verkkoajanvarausjärjestelmän osalta pitää yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdassa tarkoitetulla tavalla asianmukaisena. Verkkoajanvarausjärjestelmän heikkoudet ovat rekisterinpitäjän antaman selvityksen perusteella mahdollista korjata esimerkiksi ottamalla käyttöön salasana ja/tai siirtymällä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (2009/617) 2 §:n 1 momentin mukaiseen vahvaan sähköiseen tunnistautumiseen.

Edellä mainituilla perusteilla apulaistietosuojavaltuutettu antaa rekisterinpitäjälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan d alakohdan mukaisen määräyksen saattaa käsittelytoimet yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdissa säädetyn mukaisiksi. Rekisterinpitäjän tulee jatkossa tunnistaa verkkoajanvarausjärjestelmän käyttäjä luotettavalla tavalla siten, että yleisen tietosuoja-asetuksen 32 artiklan 1 ja 2 kohdan

---

[9] Rikoslain (19.12.1889/39) 38 luvun 9 a § (10.4.2015/368) mukaan, joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.

[10] Uusi asiakastietolaki 703/2023 tulee voimaan 1.1.2024. Uuden asiakastietolain 8.1 §:ssä säädetään samasta vaatimuksesta.

[11] Lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 2 § 1 momentin 1 kohdan mukaan *vahvalla sähköisellä tunnistamisella* tarkoitetaan sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen (EU) N:o 910/2014, (eIDAS-asetus) 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset. eIDAS-asetuksen 8 artiklan 2 kohdan b-alakohdan mukaan *korotettu varmuustaso* tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa merkittävän luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on vähentää merkittävässä määrin henkilöllisyyden väärinkäytön tai muuttamisen riskiä. eIDAS-asetuksen 8 artiklan 2 kohdan c-alakohdan mukaan *korkea varmuustaso* tarkoittaa sähköisen tunnistamisen järjestelmän yhteydessä sähköisen tunnistamisen menetelmää, joka tarjoaa korkeamman luottamustason henkilön väitetyn tai esitetyn henkilöllisyyden osalta kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä ja jota luonnehditaan suhteessa siihen liittyviin teknisiin eritelmiin, standardeihin ja menettelyihin sekä teknisiin tarkastuksiin, joiden tarkoituksena on estää henkilöllisyyden väärinkäyttö tai muuttaminen. Asetuksessa määritellään lisäksi matala varmuustaso.

TIETOSUOJAVALTUUTETUN TOIMISTO

edellytykset täyttyvät. Apulaistietosuojavaltuutettu määrää toimittamaan selvityksen tehdyistä toimenpiteistä tietosuojavaltuutetun toimistoon viimeistään kuuden viikon kuluttua päätöksen tiedoksisaannista, ellei rekisterinpitäjä hae muutosta tähän päätökseen.

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 Pohjois-Suomen hallinto-oikeuteen.

Tiedoksianto

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

Päätöksen on tehnyt apulaistietosuojavaltuutettu Heljä-Tuulia Pihamaa.