TIETOSUOJAVALTUUTETUN TOIMISTO

8.11.2021

Dnro 1506/452/18

Tietosuojavaltuutetun päätös sisäänrakennettua ja oletusarvoista tietosuojaa ja henkilötietojen käsittelyn eheyttä ja luottamuksellisuutta koskevassa asiassa

Asia

Sivullisten pääsy e-laskutukseen liittyviin henkilötietoihin

Vireillesaattajalta saatu selvitys

Vireillesaattaja on 30.4.2018 kertonut tietosuojavaltuutetun toimistolle, että hänen ystävänsä oli yhteishankintaa maksettaessa vahingossa tilannut omaan pankkiinsa vireillesaattajan luottokortin Visa-laskun. Visa-laskusta oli mahdollista nähdä vireillesaattajan henkilötietoja, ja e-laskutilauksen tekeminen vaikutti olevan mahdollista pelkästään laskutiedoista saadulla viitenumerolla.

Rekisterinpitäjältä saatu selvitys

Rekisterinpitäjänä toimivalta pankilta on pyydetty asiassa selvitystä 23.10.2020 päivätyllä selvityspyynnöllä ja 18.12.2020 päivätyllä lisäselvityspyynnöllä. Rekisterinpitäjä on antanut asiassa kirjallisen selvityksen 9.11.2020 ja lisäselvityksen 11.1.2021.

Rekisterinpitäjän mukaan asian vireillesaattaja on kertonut sille luovuttaneensa Visa-luottokorttilaskunsa maksutiedot, mukaan lukien viitenumeron, ystävälleen, jotta tämä voi maksaa osuutensa vireillesaattajan luottokorttilaskusta. Vireillesaattajan kertomien tietojen perusteella ystävä on erehdyksessä tehnyt laskua maksaessaan laskusta e-laskutilauksen omaan pankkiinsa, minkä seurauksena vireillesaattajan luottokorttilasku on päätynyt e-laskuna ystävälle.

Rekisterinpitäjän mukaan luottokorttilaskun (sekä luottolaskun) tilaamiseksi vaaditaan laskun viitenumerotieto. Viitenumero on jokaisella asiakkaalla yksilöllinen, ja se sisältää tarkistenumeron. Ilman viitenumeroa luottokorttilaskua ei voi tilata e-laskuna. Koska tilaamiseen riittää viitenumerotieto, toisen asiakkaan luottokorttilasku on mahdollista tilata e-laskuna viitenumeron syöttämisessä tapahtuneen näppäilyvirheen seurauksena. Edellä kuvattu tilanne on rekisterinpitäjän mukaan mahdollinen mutta harvinainen viitenumerossa olevan tarkistenumeron vuoksi. Rekisterinpitäjä on 6.4.2020 tehnyt tietosuojavaltuutetun toimistolle ilmoituksen tietoturvaloukkauksesta, jossa asiakas on e-laskutilausta tehdessään näppäillyt oman luottolaskunsa viitenumeron virheellisesti ja saanut tämän johdosta toisen asiakkaan luottolaskun e-laskuna.

Rekisterinpitäjän antaman selvityksen mukaan Visa-luottokorttilasku sisältää seuraavat henkilötiedot: etu- ja sukunimi, kotiosoite, luottokortin luottoraja, luoton velkasaldo, luottokortin käyttöä koskevat tiedot ostotapahtumien muodossa (veloittaja, tapahtuman päivämäärä ja summa). Lisäksi luottokorttilasku sisältää maskatun korttinumeron sekä luottokorttilaskun maksutiedot sisältäen tilinumeron, viitenumeron, maksettavan kuukausierän ja eräpäivän. Luottolaskun e-laskun

esilläpitoarkistoversiossa on aiemmin ollut näkyvissä henkilötunnus, mutta se on poistettu laskusta tietosuojasääntelyyn perustuneena kehitystoimenpiteenä vuonna 2018.

Rekisterinpitäjän mukaan käytännössä on tavanomaista, että asiakkaat luovuttavat tietoisesti ja keskinäisen sopimuksen perusteella viitenumeron esimerkiksi perheenjäsenelleen, kuten puolisolleen tai vanhemmalleen, laskujen maksamista varten. Rekisterinpitäjä ei lähtökohtaisesti ole halunnut estää tai vaikeuttaa e-laskun tilaamista, koska tämä voi vaikeuttaa etenkin ikäihmisten pankkiasioiden hoitamista perheen sisällä.

Rekisterinpitäjän mukaan e-laskutilaukselle olisi mahdollista lisätä toinen yksilöintitieto nyt käytettävän viitenumeron lisäksi, ja tämän lisäyksen pystyy tekemään laskuttaja, eli tässä tapauksessa rekisterinpitäjä itse. Rekisterinpitäjä kertoo myös antamassaan selvityksessä, että se on käynnistänyt kehitystyön toisen yksilöintitiedon lisäämiseksi luottolaskun e-laskutilaukseen.

Sovellettavasta lainsäädännöstä

Euroopan parlamentin ja neuvoston yleistä tietosuoja-asetusta (EU) 2016/679 (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). Henkilötietojen käsittelyä koskevista periaatteista on säädetty yleisen tietosuoja-asetuksen 5 artiklassa.

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 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.

Oikeudellinen kysymys

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

Tietosuojavaltuutetun tulee ratkaista, onko rekisterinpitäjän menettely koskien e-laskutukseen liittyviä henkilötietojen suojaustoimenpiteitä ollut yleisen tietosuoja-

asetuksen 5(1)(f) artiklan (*eheyden ja luottamuksellisuuden periaate*) ja 25(1) artiklan (*sisäänrakennettu ja oletusarvoinen tietosuoja*) mukainen.

Tietosuojavaltuutetun päätös ja perustelut

Päätös

Rekisterinpitäjä ei ole noudattanut toiminnassaan yleisen tietosuoja-asetuksen 5(1)(f) artiklaa (*eheyden ja luottamuksellisuuden periaate*) ja 25(1) artiklaa (*sisäänrakennettu ja oletusarvoinen tietosuoja*), eikä rekisterinpitäjän menettely koskien e-laskutukseen liittyviä henkilötietojen suojaustoimenpiteitä ole näin ollen ollut yleisen tietosuoja-asetuksen mukainen.

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58(2)(d) artiklan mukainen määräys noudattaa eheyden ja luottamuksellisuuden periaatetta sekä sisäänrakennettua ja oletusarvoista tietosuojaa koskevaa velvoitetta ja saattaa käsittelytoimet tietosuojasääntelyn mukaisiksi.

Rekisterinpitäjälle annetaan yleisen tietosuoja-asetuksen 58(2)(b) artiklan mukainen huomautus eheyden ja luottamuksellisuuden periaatteen ja sisäänrakennettua ja oletusarvoista tietosuojaa koskevan velvoitteen rikkomisesta.

Tietosuojavaltuutettu jättää rekisterinpitäjän harkintaan asianmukaiset toimenpiteet, mutta määrää toimittamaan selvityksen tehdyistä toimenpiteistä tietosuojavaltuutetun toimistolle **20.12.2021 mennessä**, ellei se hae muutosta tähän päätökseen.

Perustelut

Yleisen tietosuoja-asetuksen 5 artiklassa säädetään eheyden ja luottamuksellisuuden periaatteesta, joka muun muassa edellyttää, että asiamukaisia teknisiä ja organisatorisia toimenpiteitä toteuttamalla estetään asiattomien pääsy henkilötietoihin. Periaate kytkeytyy asetuksen riskiperusteiseen lähestymistapaan, jonka toteuttamiseksi rekisterinpitäjän tulee jatkuvasti arvioida suojaustoimenpiteiden riittävyyttä suhteessa käsittelyyn liittyviin riskeihin, sekä huolehtia riskejä vastaavista teknisistä ja organisatorisista toimenpiteistä henkilötietojen riittävän suojaamisen varmistamiseksi (ks. erityisesti yleisen tietosuoja-asetuksen 24 artikla, *rekisterinpitäjän vastuu*).

Eheyden ja luottamuksellisuuden periaate sisältyy yleisen tietosuoja-asetuksen kokonaisvaltaiseen lähtökohtaan, sisäänrakennettuun ja oletusarvoiseen tietosuojaan (yleisen tietosuoja-asetuksen 25 artikla), jonka toteutuminen edellyttää, että rekisterinpitäjä huomioi toiminnassaan tietosuojan keskeisenä tekijänä alusta alkaen. Sisäänrakennetun ja oletusarvoisen tietosuojan asettamat vaatimukset täyttääkseen rekisterinpitäjän tulee sisällyttää henkilötietojen käsittelyä koskevat periaatteet, kuten eheyden ja luottamuksellisuuden periaate, tehokkaasti kaikkeen henkilötietojen käsittelyyn.[1] Eheyden ja luottamuksellisuuden periaatteen toteutuessa tehokkaasti sivullisten pääsy henkilötietoihin estyy.

Nyt tarkasteltavana olevassa asiassa luottokorttilaskun ja luottolaskun tilaamiseksi e-laskuna on riittänyt viitenumerotieto. Luottokorttilaskun sisältämiin henkilötietoihin

[1] Ks. Euroopan tietosuojaneuvoston ohje: EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, kappaleet 2.1.1 ja 2.1.2.

kuuluvat muun muassa nimi, osoite, luottokortin luottoraja, luoton velkasaldo, luottokortin käyttöä koskevat tiedot ostotapahtumien muodossa ja osittain peitetty korttinumero.

Vireillesaattajan tapauksessa vireillesaattaja on itse edesauttanut ongelmatilanteen synnyssä. Vireillesaattajalle on kuitenkin tullut yllätyksenä, mitä tietoja pelkän viitenumeron avulla asiakkaasta on mahdollista saada. Sama ongelmatilanne on saattanut toistua tapauksissa, joissa vastaavaa myötävaikutusta ei ole ollut käsillä, vaan rekisteröity on e-laskua maksaessaan tehnyt näppäilyvirheen.

Asiassa voidaan huomioida, että rekisterinpitäjä on tehnyt 6.4.2020 tietosuojavaltuutetun toimistolle tietoturvaloukkausilmoituksen, jossa henkilö on näppäilyvirheen seurauksena tilannut toiselle henkilölle kuuluvan e-laskun. Tietosuojavaltuutettu huomioi, ettei epäkohta saatujen tietojen perusteella vaikuta sellaiselta, että se olisi aiheuttanut laaja-alaisia ongelmia.

Tietosuojavaltuutettu katsoo kuitenkin, ettei ole asianmukaista, että sivulliselle mahdollistuu yksittäisen näppäilyvirheen seurauksena pääsy rekisteröidyn henkilötietoihin. Myös aiempi tietoturvaloukkaustilanne on ollut indikaatio rekisterinpitäjälle siitä, että esimerkiksi suojausparametrien lisääminen olisi tarkoituksenmukainen toimenpide sen varmistamiseksi, että henkilötietojen luottamuksellisuus toteutuu. Tietosuojavaltuutettu huomioi tässä kohdin, että luottokorttilaskuun on sisältynyt ostotapahtumatietoja, ja että perustuslakivaliokunta on katsonut yksityiskohtaisten tilitietojen rinnastuvan yksityiselämän suojan ydinalueelle kuuluviin arkaluonteisiin tietoihin, koska tilitapahtumista voi käydä ilmi arkaluonteisia tietoja, kuten tieto terveydenhuoltopalvelujen käytöstä.

Tietosuojavaltuutettu katsoo, että rekisterinpitäjän on perusteltua huolehtia asianmukaiseksi katsomallaan tavalla, ettei näppäilyvirhe yksittäisen tiedon syöttämisessä mahdollista pääsyä toisen henkilön henkilötietoihin. Rekisterinpitäjälle annetaan näin ollen yleisen tietosuoja-asetuksen 58(2)(d) artiklan mukainen määräys saattaa käsittelytoimet yleisen tietosuoja-asetuksen sääntelyn mukaisiksi. Tässä yhteydessä tietosuojavaltuutettu laittaa kuitenkin merkille, että rekisterinpitäjä on jo huomioinut muutostarpeen ja ryhtynyt asiassa vähintäänkin alustaviin toimenpiteisiin.

Tietosuojavaltuutettu huomioi myös, että aiemmin näppäilyvirhe on saattanut johtaa pääsyyn rekisteröidyn henkilötunnukseen.[2] Henkilötunnus on kuitenkin rekisterinpitäjän mukaan poistettu laskusta tietosuojasääntelyyn perustuneena kehitystoimenpiteenä vuonna 2018. Tietosuojavaltuutettu toteaa, että aiempi toimintatapa on asiassa saadun selvityksen perusteella ollut käytössä yleisen tietosuoja-asetuksen soveltamisen alkamista edeltävänä aikana. Tietosuojavaltuutetun käytössä olevista toimenpiteistä on tuolloin säädetty henkilötietolain (523/1999) 40 §:ssä, ja käytännössä tietosuojavaltuutettu on voinut ohjein ja neuvoin pyrkiä siihen, ettei lainvastaista menettelyä jatketa tai uusita. Koska toiminta ei ole jatkunut enää yleisen tietosuoja-asetuksen soveltamisen alkamisen jälkeen, yleisen tietosuoja-asetuksen 58(2) artiklan mukaisten korjaavien toimivaltuuksien käyttö ei tule arvioitavaksi tämän menettelyn osalta.

Sovelletut lainkohdat

[2] Asiassa saadun selvityksen mukaan luottolaskun e-laskun esilläpitoarkistoversiossa on ollut aiemmin näkyvissä henkilötunnus.

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.