



Tietosuojavaltuutetun vastaus tietoturvaloukkausta koskevaan ilmoitukseen

Viite Tietoturvaloukkausta koskeva ilmoituksenne 9.8.2019

Ilmoittaja

Verohallinto (0245458-3)

Helena Hynynen, tietosuojavastaava, johtava asiantuntija

PL 325

00052 VERO

Tietoturvaloukkauksen kuvaus

Kuvaus tietoturvaloukkauksesta:

"Verohallinnon verotuspäätösten ja muiden asiakaskirjeiden tulostus hoidetaan Edita Prima Oy:ssä. Virhe on tapahtunut Edita Prima Oy:n tulostusjärjestelmässä siten, että järjestelmä on sekoittanut työerän sisällä olevia aineistoja tulostamalla joitakin osia yhden asiakkaan kirjeen tiedoista toisen vastaanottajan kirjeeseen.

Tulostuserän data on siirretty Verohallinnolta Edita Prima Oy:lle 6.8.2019, josta se on koottu järjestelmässä tulostuseräksi 7.8.2019. Erä on toimitettu Postin jakeluun illalla 7.8.2019."

Tietoturvaloukkauksen tyyppi on luvaton luovuttaminen tai luvaton pääsy tietoihin.

Kohteena olleet tiedot

Ilmoituksessa ilmoitettu

Tietoturvaloukkaus olisi käsittänyt 30 000 henkilön seuraavat tiedot:

Yleiset henkilötiedot

- Identiteettitiedot (esim. nimi ja syntymäaika)
- Henkilötunnus
- Yhteystiedot
- Taloudellista asemaa koskevat tiedot
- Ei vielä tiedossa
- Viralliset asiakirjat

Erityiset henkilötietoryhmät

- Uskonnollista tai filosofista vakaumusta koskevat tiedot
- Ammattiliiton jäsenyyttä kuvaavat tiedot
- Terveystilaa koskevat tiedot
- Ei vielä tiedossa

Lisätietoselvityksessä tarkentuneet

Tietoturvaloukkaus on koskenut 2305 henkilöä, mutta tiedot ovat olleet pääosin tunnistamattomassa muodossa ts. niitä ei voi yhdistää tunnistettavaan henkilöön/ verovelvolliseen.

Tunnistettavassa muodossa tulostuneita tietoja oli rekisterinpitäjän tekemän selvityksen mukaan kuuden henkilön osalta seuraavasti:

- Viiden osalta henkilötunnus oli tulostunut viiteen asiakirjaan.
- Henkilötunnus on tulostunut verotusasiakirjalle luoton tunnuksena, koska Kansaneläkelaitos käyttää henkilötunnusta luottojen tunnuksena.
- Kolmeen asiakirjaan on tulostunut henkilötunnus ja pankkitili.
- Kahdessa asiakirjassa oli vain henkilötunnus.

Turvakieltoasiassa ei ollut selkeästi henkilön turvakieltoon yhdistettävää tietoa ja kirjeissä oli kyse samasta henkilöstä.

Toteutetut toimenpiteet

Rekisterinpitäjä on selvittänyt tietoturvaloukkauksen syyn ja henkilötietojen osalta tarkalleen asiaa koskevat henkilötiedot.

Rekisterinpitäjä ja henkilötietojen käsittelijä ovat korjanneet järjestelmässä/ohjelmistossa olleen vian.

Yhteydenotto rekisteröityihin

Rekisterinpitäjä aikoo lähettää ilmoituksen kaikille 2305 henkilölle, joiden tietoja on ollut tunnistamattomassa muodossa kirjeissä.

Rekisterinpitäjä aikoo lähettää ilmoituksen kaikille kuudelle henkilölle, joiden tietoja on ollut tunnistettavassa muodossa kirjeissä.

Rajat ylittävä käsittely

Ei ole.

Yleisen tietosuoja-asetuksen (EU) 2016/679 säännöksiä

A. Tietosuoja-asetuksen 34 artiklan 1 kohdan mukaan, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille

ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

B. Tietosuoja-asetuksen 34 artiklan 1 kohdassa tarkoitettussa rekisteröidylle annettavassa ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava ainakin 33 artiklan 3 kohdan alakohdassa mainitut seuraavat tiedot:

b. Ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa.

c. Kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset.

d. Kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Tietosuoja-asetuksen 33 Artiklan 4 kohdan mukaan, jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

C. Tietosuoja-asetuksen 34 Artiklan 3 kohdan alakohtien mukaan ilmoitusta rekisteröidylle ei vaadita, jos jokin seuraavista edellytyksistä täyttyy:

a. Rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suoja-toimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta.

b. Rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu.

c. Se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidylle tiedotetaan yhtä tehokkaalla tavalla.

D. Tietosuoja-asetuksen 34 Artiklan 4 kohdan mukaan, jos rekisterinpitäjä ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä tai päättää, että jokin tietosuoja-asetuksen 34 Artiklan 3 kohdan edellytyksistä täyttyy, arvioituaan, kuinka todennäköisesti henkilötietojen tietoturvaloukkaus aiheuttaa suuren riskin. Tietosuoja-asetuksen 58 artiklan 2 kohdan e alakohdan perusteella valvontaviranomainen voi määrätä rekisterinpitäjän ilmoittamaan tietoturvaloukkauksesta rekisteröidylle.

Tietosuojavaltuutetun määräys/toimenpiteet

2. Ei määräystä rekisteröidyille ilmoittamisesta

Tietosuojavaltuutettu ei määrää rekisterinpitäjää ilmoittamaan tietoturvaloukkauksesta rekisteröidyille, koska rekisterinpitäjä on ilmoittanut tekevänsä edellä A kohdassa tarkoitetun ilmoituksen rekisteröidyille. Rekisterinpitäjän on kuitenkin varmistettava, että ilmoitus sisältää edellä B kohdassa mainitut asiat ja tarvittaessa täydennettävä ilmoitusta.



Jari Råman,

Apulaistietosuojavaltuutettu



Kalle-Ville Kosteila,

IT-erityisasiantuntija