ETELÄ-
KARJALAN
hyvinvointialue

26.1.2023

Ohje: Tietoturvaloukkausten ilmoittaminen ja käsittely, palveluntuottaja

1 Taustaa

Tämä ohje kuvaa Etelä-Karjalan hyvinvointialueen ja palveluntuottajan välisen ilmoitus- ja yhteistyömenettelyn tietoturvaloukkauksen yhteydessä.

2 Määritelmät

Tietoturvapoikkeama: tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.

Tietosuojapoikkeama: seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltävien henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin. Voi johtua myös tarkoituksellisesta toiminnasta. Tietosuojapoikkeama kohdistuu nimenomaisesti yksilöön ja henkilötietojen suojaan.

Tietoturvaloukkaus: seurauksena henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää, muuttuu, luovutetaan luvattomasti tai henkilötietoihin pääsee käsiksi taho, jolla ei ole niihin käsittelyoikeutta. Sisältää tieturvapoikkeaman sekä tietosuojapoikkeaman.

3 Toiminta tietoturva- ja tietosuojapoikkeaman yhteydessä

Havainnon loukkauksesta voi tehdä henkilötietojen käsittelijänä toimiva palveluntuottaja, tämän alihankkija, Etelä-Karjalan hyvinvointialue tai joku ulkopuolinen taho. Havainto on vahvistettava oikeaksi.

Henkilötietojen käsittelijänä toimiva palveluntuottaja on velvollinen ilmoittamaan havaitsemastaan loukkauksesta välittömästi rekisterinpitäjälle Etelä-Karjalan hyvinvointialueelle. Ilmoitus on tehtävä osapuolten välisessä sopimuksessa tai sopimusliitteessä sovittujen määräaikojen sisällä (yl. 24 h), kuitenkin viimeistään EU:n yleisessä tietosuoja-asetuksessa säädetysti ja ilman aiheetonta viivästystä. Siltä osin kuin kaikkia tietoja ei ole mahdollista toimittaa samanaikaisesti, voidaan tiedot toimittaa vaiheittain. Ilmoitus tulee tehdä ensisijaisesti valvonta-asiantuntijalle p. 0400128441 tai sopimuksessa mainitulle Etelä-Karjalan hyvinvointialeen yhteyshenkilölle ja lisäksi tarvittaessa asian kiireellisyydestä riippuen suoraan Etelä-Karjalan hyvinvointialueen tietosuojaorganisaatiolle tietosuoja@ekhva.fi, tietosuojavastaava p. 040 651 1786, tietosuoja-asiantuntija p. 040 651 1974

Siltä osin kuin palveluntuottajan ilmoitus pitää sisällään henkilötietoja, erityisiin henkilötietoryhmiin kuuluvia tai salassa pidettäviä tietoja, ilmoitus tulee tehdä suojattuna sähköpostina. Jos tuottaja ei pysty lähettämään suojattua sähköpostia tai asian kiireellisyys sitä vaatii, asiasta tulee ilmoittaa puhelimitse Etelä-Karjalan hyvinvointialueen sopimusyhteyshenkilölle, joka kirjaa ylös tiedot tapahtuneesta ja on välittömästi yhteydessä em. hyvinvointialueen tietosuojaorganisaatioon. Tärkeää on, että tapahtunutta päästään selvittämään myös Etelä-Karjalan hyvinvointialueella mahdollisimman pian niissäkin tilanteissa, joissa tarvitaan vielä tarkempia lisäselvityksiä eikä palveluntuottaja voi heti ilmoittaa kaikkia tietoja. Suojaamattomassa sähköpostissa saa lähettää vain tiedon siitä, että tietoturvaloukkaus on tapahtunut ja tarkemmat tiedot annetaan alkuvaiheessa puhelimitse.

Lisäksi tämän ilmoituksen tehtyään palveluntuottaja toimittaa ilman aiheetonta viivytystä Etelä-Karjalan hyvinvointialueelle postitse tarkemman kirjallisen dokumentaationsa tai vastaavan raporttinsa tapahtumasta. Tätä ei vaadita, mikäli ilmoitus tietoturvaloukkauksesta on tehty Etelä-Karjalan hyvinvointialueelle kirjallisesti sisältäen kaikki tietosuoja-asetuksen mukaiset sekä hyvinvointialueen ja palveluntuottajan välisissä sopimuksissa ja ohjeistuksissa mainitut tiedot. Jos ilmoitus on tehty Etelä-Karjalan hyvinvointialueelle puhelimitse tai ilmoittamalla salaamattomassa

sähköpostissa tapahtunut ilman tarkempia ilmoituksessa vaadittuja tietoja, postitse toimitettava raportti loukkauksesta on tehtävä aina.

4 Ilmoituksessa tarvittavat tiedot

a) Henkilötietojen käsittelijänä toimivan palveluntuottajan tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot.
b) Kuvaus tietoturvaloukkauksen laajuudesta.
    i. Asianomaisten rekisteröityjen ryhmät.
    ii. Ryhmien arvioidut lukumäärät.
    iii. Henkilötietotyyppien ryhmät ja arvioidut lukumäärät.
c) Kuvaus tietoturvaloukkauksen todennäköisistä seurauksista.
d) Kuvaus toimenpiteistä, joita palveluntuottaja ehdottaa tai jotka se on toteuttanut poikkeaman johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

4.1 Perustiedot poikkeamasta

Mahdollisimman tarkka kuvaus poikkeamasta kaiken saatavissa olevan tiedon perusteella:

a) Milloin tietoturvaloukkaus on tapahtunut?
b) Miten tietoturvaloukkaus on tapahtunut?
c) Mikäli tämä ilmoitus tehdään tietoturva-asetuksessa säädetyn tai sopimuksessa sovitun määräajan ulkopuolella, perustelut tälle.
d) Minkälaisia suojakeinoja (organisatorisia/teknisiä) organisaatiolla oli käytössä tapahtuneen kaltaisten tietoturvaloukkauksen estämiseksi?

4.2 Henkilötiedot, joihin loukkaus kohdistui

a) Mihin henkilötietoryhmiin ja rekisteröityjen ryhmiin tietoturvaloukkaus kohdistui? Kohdistuiko tietoturvaloukkaus erityisiin henkilötietoryhmiin (esim. arkaluonteisiin henkilötietoihin, henkilötunnukseen tai terveystietoihin)?
b) Kuinka montaa rekisteröitynyttä tietoturvaloukkaus koskee?
c) Ovatko ko. rekisteröidyt tietoisia tietoturvaloukkauksen tapahtumisesta?
d) Kuvailu potentiaalisista, rekisteröityjä ja heidän yksityisyyden suojaansa koskevista riskeistä ja haitoista, jotka tietoturvaloukkauksesta johtuvat.
e) Onko palveluntuottajalle tullut yhteydenottoja rekisteröidyiltä tietoturvaloukkauksen johdosta?

f) Onko se ohjeistanut rekisteröityjä mahdollista toimista, joilla he voivat pyrkiä rajaamaan tietoturvaloukkauksen seurauksia? Jos on ohjeistanut, miten?

4.3 Poikkeaman tutkiminen, rajoittaminen ja siitä toipuminen

a) Onko palveluntuottaja ryhtynyt toimenpiteisiin poikkeaman seurausten minimoinniksi tai rajoittamiseksi? Kuvaus toimenpiteistä.
b) Onko altistunut tieto saatu takaisin palveluntuottajan haltuun? Jos kyllä, kuvailu siitä, miten ja milloin tämä tapahtui.
c) Minkälaisiin toimiin palveluntuottaja on ryhtynyt tai aikoo ryhtyä vastaavanlaisten Tietoturvaloukkausten estämiseksi jatkossa?

4.4 Muuta

a) Onko palveluntuottaja tehnyt ilmoituksen tietoturvaloukkauksesta Poliisille?
b) Onko tehnyt ilmoituksen tietoturvaloukkauksesta jollekin muulle viranomaiselle, kuten tietosuojavaltuutetulle?

Etelä-Karjalan hyvinvointialue kirjaa tapahtuneen tietoturvaloukkauksen asianhallintajärjestelmään. Tarvittaessa järjestetään osapuolten kesken selvitystilaisuus tai vastaava neuvottelu. Etelä-Karjalan hyvinvointialue vastaa rekisterinpitäjänä tarvittaessa ilmoituksesta valvontaviranomaiselle sekä rekisteröidylle.

Lisätietoja tietosuojavaltuutetun toimiston verkkosivuilta www.tietosuoja.fi/tietoturvaloukkaukset

Etelä-Karjalan hyvinvointialue

Kirjaamo

Valto Käkelän katu 3

53130 Lappeenranta

Vaihde 05 352 000

Faksi 05 352 7800

etunimi.sukunimi@ekhva.fi

www.ekhva.fi

Y-tunnus: 3221313–1

Asiakirja päättyy tähän.