ETELÄ-
KARJALAN
hyvinvointialue

Ohje

22.4.2026

Ohje palveluntuottajille henkilötietojen tietoturvaloukkaustilanteita varten

Tämän dokumentin tarkoituksena on antaa palveluntuottajille ohjeet tilaajan henkilötietojen tietoturvaloukkauksiin reagoimiseksi. Dokumentti on tarkoitettu käytettäväksi hankinnoissa, joissa palveluntuottaja (henkilötietojen käsittelijä) käsittelee tilaajan henkilötietoja tilaajan (rekisterinpitäjän) lukuun osana palvelusetelillä järjestettävää sosiaali- ja/tai terveydenhuollon palvelua. Dokumentti täydentää palvelusetelituottajien sääntökirjan liitteenä olevia ”Henkilötietojen käsittelyn ehtoja”.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi salassa pidettävien tietojen lähettäminen suojaamattomassa sähköpostissa, asiakas-, potilas- tai henkilöstötietojen luovutus tai postitus väärälle henkilölle, hävinnyt tai varastettu tietokone tai tiedonsiirtoväline, kuten USB-tikku, hakkerointi tai haittaohjelmatartunta ja kyberhyökkäys. Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Palveluntuottaja toteuttaa ennakolta kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet sen varmistamiseksi, että henkilötietojen tietoturvaloukkaukset paljastuvat viipymättä ja niihin reagoidaan asianmukaisesti. Palveluntuottaja ryhtyy tilaajan henkilötietojen tietoturvaloukkauksen havaittuaan viipymättä riittäviin toimenpiteisiin henkilötietojen tietoturvaloukkauksen poistamiseksi ja sen haittavaikutusten rajoittamiseksi ja korjaamiseksi. Palveluntuottaja dokumentoi ja raportoi selvityksen tulokset ja suoritetut toimenpiteet tilaajalle.

Palveluntuottajan on ilmoitettava tilaajalle kirjallisesti kaikista tietoonsa tulleista tilaajan henkilötietojen tietoturvaloukkauksista. Ilmoitus on tehtävä viipymättä ja mahdollisuuksien mukaan viimeistään 24 tunnin kuluessa loukkauksen ilmitulosta mahdollisesti sovitusta palveluajasta riippumatta.

Kirjallisessa ilmoituksessa on oltava vähintään seuraavat tiedot tilaajan henkilötietojen tietoturvaloukkauksesta:

- tapahtuneen henkilötietojen tietoturvaloukkauksen kuvaus ja henkilötietojen tietoturvaloukkauksen kohteena olleiden tietojen yksilöiminen, mukaan lukien asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat ilmoitusta tehtäessä tiedossa;

- palveluntuottajan tietosuojavastaavan tai muun vastuuhenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;

- kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista; ja

- kuvaus toimenpiteistä, joita palveluntuottaja ehdottaa tai joita se on jo toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Palveluntuottajan tulee täydentää ilmoitusta viipymättä ja oma-aloitteisesti, mikäli se saa tehdyn ilmoituksen jälkeen lisätietoja tilaajan henkilötietojen

tietoturvaloukkauksesta. Ilmoituksen mahdollinen täydentäminen tehdään kirjallisesti.

Palveluntuottaja lähettää edellä mainitut ilmoitukset salatulla sähköpostilla sopimuksessa mainitulle tilaajan yhteyshenkilölle sekä tilaajan tietosuojavastaavalle (tietosuoja@ekhva.fi).

Lisäksi palveluntuottajan tulee ilmoittaa tilaajalle viipymättä muista palvelun häiriö- tai ongelmatilanteista, joilla on tai voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin. Palveluntuottaja selvittää viipymättä kaikissa tietoturvapoikkeamissa, onko tilaajan henkilötietoja vaarantunut sekä ryhtyy välittömästi tarvittaviin korjaaviin toimenpiteisiin. Palveluntuottajan tulee auttaa tilaajaa varmistamaan, että käsittelyn turvallisuuteen ja henkilötietojen tietoturvaloukkauksiin liittyviä velvollisuuksia noudatetaan.

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.