TIETOSUOJAVALTUUTETUN TOIMISTO

Dnro 7767/183/21

15.11.2021

Hyvä rekisterinpitäjä

Tietosuojavaltuutetun toimisto on havainnut, että sosiaali- ja terveydenhuollon toimialalla on tarve tarkentavalle ohjeistukselle tietoturvaloukkauksista ilmoittamisesta viranomaiselle tai loukkauksen kohteeksi joutuneille henkilöille.

Tarve on noussut esille esimerkiksi Kelan toteuttamassa selvityspyynnössä reseptipalvelun toiminnasta. Olemme myös kiinnittäneet huomiota siihen, että tietoturvaloukkausten tunnistamisessa ja käsittelyssä on toimijakohtaisia eroja.

Lähetämme teille[1] tämän kirjeen edistääksemme tietoisuutta ja ymmärrystä henkilötietojen tietoturvaloukkauksista ja niihin liittyvistä lakisääteisistä velvoitteista. Kirjeen tarkoituksena on ohjeistaa terveydenhuollon toimialalla toimivia rekisterinpitäjiä, jotta toimintamallit tietoturvaloukkauksista ilmoittamisessa olisivat yhdenmukaisia.

Rekisterinpitäjän ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksesta

Henkilötietojen tietoturvaloukkauksien käsittelystä sekä niihin liittyvistä ilmoitusvelvollisuuksista säädetään EU:n yleisessä tietosuoja-asetuksessa. Rekisterinpitäjällä on tietyissä tilanteissa velvollisuus ilmoittaa havaitsemastaan tietoturvaloukkauksesta viranomaiselle sekä tietoturvaloukkauksen kohteena oleville henkilöille.

Ilmoita viranomaiselle tietoturvaloukkauksesta

Rekisterinpitäjän tulee ilmoittaa havaitsemastaan tietoturvaloukkauksesta viranomaiselle eli tietosuojavaltuutetun toimistolle, kun tietoturvaloukkaus todennäköisesti aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Jos tietoturvaloukkaukseen ei todennäköisesti liity riskiä, ilmoitusta viranomaiselle ei tarvitse tehdä. Riskin arvioinnista voit lukea lisää alempana kohdassa Arvioi tietoturvaloukkauksesta aiheutuva riski rekisteröidylle.

Ilmoitus tulee tehdä viranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on havaittu. Jos ilmoitusta ei tehdä tässä määräajassa, rekisterinpitäjän tulee toimittaa tietosuojavaltuutetun toimistolle selitys ilmoituksen viivästymisen syistä.

Rekisterinpitäjä voi tehdä ilmoituksen tietosuojavaltuutetun toimistolle sähköisellä lomakkeella verkkosivujemme kautta. Kun ilmoituksen tekee sähköistä lomaketta käyttäen, lähettää tietosuojavaltuutetun toimisto ilmoittajalle paluuviestinä vastaanottokuittauksen, josta käy ilmi ilmoituksen tekemisen päivämäärä, asian diaarinumero sekä rekisterinpitäjän asialle ilmoittama viite. Vastaanottokuittausta on mahdollista hyödyntää esimerkiksi tietoturvaloukkauksen asianmukaisessa dokumen-

[1] Kirje on lähetetty sosiaali- ja terveydenhuollon toimialan tietosuojavastaaville ja itsenäisille ammatinharjoittajille. Yhteystiedot on saatu TSV:n tietosuojavastaavien rekisteristä sekä Kelan asiakasrekisteristä. Lisätietoja tietosuojavastaavien rekisteristä: https://tietosuoja.fi/tietosuojavastaavien-henkilotietojen-kasittely

toinnissa. Lisäksi vastaanottokuittauksesta ilmi käyvä asian diaarinumero helpottaa mahdollista yhteydenpitoa tietosuojavaltuutetun toimistoon.

Lomakkeen huolellinen täyttäminen ja loukkauksen tapauskohtainen arviointi on tärkeää. Jos kaikki tiedot eivät ole saatavilla, rekisterinpitäjä voi tehdä ilmoituksen vaiheittain. Tällöin rekisterinpitäjän tulee toimittaa ensin alustava ilmoitus ja myöhemmin täydentävä ilmoitus. Tietoturvaloukkauksen kohteena olevien henkilöiden ja henkilötietojen lukumäärästä voi antaa myös arvion, jos tarkkaa lukumäärää ei ole tiedossa.

Ilmoita tietoturvaloukkauksesta rekisteröidylle

Jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin loukkauksen kohteena oleville henkilöille, tulee rekisterinpitäjän ilmoittaa tietoturvaloukkauksesta myös heille. Ilmoitus pitää tehdä ilman aiheetonta viivytystä.

Päätös tietoturvaloukkauksen kohteeksi joutuneille henkilöille ilmoittamisesta tulee tehdä mahdollisimman pian, jotta rekisteröityjen oikeus saada tieto tietoturvaloukkauksesta ilman aiheetonta viivytystä ei vaarannu. Rekisteröidyille ilmoittaminen tietoturvaloukkauksesta viipymättä auttaa heitä varautumaan mahdollisiin seuraksiin, joita loukkauksesta voi aiheutua.

Viranomainen voi myös antaa rekisterinpitäjälle erikseen määräyksen ilmoittaa rekisteröidylle tietoturvaloukkauksesta.

Ilmoituksen viivästäminen voi joissakin tilanteissa olla perusteltua. Esimerkiksi rekisteröidyn heikko terveydentila voi olla syy viivästää tietoturvaloukkauksesta ilmoittamista. Rekisterinpitäjällä on kuitenkin velvollisuus osoittaa tällaisen tilanteen olemassaolo. Osoitusvelvollisuudesta voit lukea lisää kohdasta Dokumentoi tietoturvaloukkaus ja osoita noudattavasi tietosuojalainsäädäntöä.

Ilmoituksen sekä siihen liittyvän viestinnän tulee olla selkeää ja yksinkertaista. Rekisterinpitäjän on kerrottava rekisteröidylle mm. tietoturvaloukkauksen luonteesta ja todennäköisistä seurauksista sekä tehdyistä toimenpiteistä. Lisäksi rekisterinpitäjän tulee antaa tietosuojavastaavan yhteystiedot tai muu yhteyspiste, josta loukkauksen kohteeksi joutuneet voivat saada lisätietoa.

Kaikissa tilanteissa rekisteröidylle ei tarvitse ilmoittaa tietoturvaloukkauksesta. Jos tapahtuma ei todennäköisesti aiheuta korkeaa riskiä loukkauksen kohteelle, siitä ei tarvitse ilmoittaa hänelle. Muut tilanteet, joissa ilmoitusta ei vaadita, on määritelty tietosuoja-asetuksen 34 artiklan 3 kohdassa.

Arvioi tietoturvaloukkauksesta aiheutuva riski rekisteröidylle

Rekisterinpitäjän on arvioitava, millainen riski tietoturvaloukkauksesta on aiheutunut tietoturvaloukkauksen kohteena olevalle henkilölle. Viranomainen kiinnittää erityistä huomioita rekisterinpitäjän tekemään riskiarviointiin, kun se käsittelee tietoturvaloukkausilmoituksia.

Riskejä voidaan arvioida kolmella tasolla:

1. tietoturvaloukkaus ei aiheuta mitään riskiä rekisteröidylle,
2. loukkaus aiheuttaa todennäköisesti **riskin** tai

3. loukkaus aiheuttaa todennäköisesti **korkean riskin** rekisteröidyn oikeuksille tai vapauksille.

Tietoturvaloukkaukset voivat aiheuttaa rekisteröidylle monenlaisia haitallisia seurauksia. Tällaisia voivat olla esimerkiksi terveydelliset haitat, taloudelliset menetykset, salassa pidettävien henkilötietojen luottamuksellisuuden menetys, syrjintä, maineen vahingoittuminen tai identiteettivarkauden tai petoksen uhriksi joutuminen.

Kun tietoturvaloukkaukseen liittyvää riskiä arvioidaan, tulee huomioida tietoturvaloukkauksesta mahdollisesti aiheutuvan seurauksen vakavuus ja todennäköisyys. Riski on sitä suurempi, mitä vakavampi seuraus on yksilön kannalta ja mitä todennäköisemmin se toteutuu. Silloin kun tietoturvaloukkaus koskee terveystietoja, korkea riski on todennäköisesti olemassa, ellei rekisterinpitäjä osoita, että riskiä on pienennetty.

Lue käytännön esimerkkejä tietoturvaloukkauksista liitteestä 1 (Esimerkkejä tietoturvaloukkauksista sosiaali- ja terveydenhuollossa).

Tee korjaavat toimenpiteet tietoturvaloukkauksen pysäyttämiseksi

Rekisterinpitäjän tulee toteuttaa korjaavia toimenpiteitä tietoturvaloukkauksen pysäyttämiseksi ja rekisteröidyille aiheutuvien vahinkojen pienentämiseksi.

Rekisterinpitäjän on tärkeää ryhtyä korjaaviin toimenpiteisiin heti. Esimerkkejä toimenpiteistä ovat tietojen poistaminen pysyvästi sivullisten saatavilta, tietojen eheyden korjaaminen, tekniset toimenpiteet loukkauksen pysäyttämiseksi tai rajaamiseksi, järjestelmien haavoittuvuuksien korjaaminen, salasanojen ja käyttäjätunnusten vaihtaminen, käyttäjäoikeuksien muuttaminen, tietoverkkojen poiskytkentä sekä ohjeistusten ja salassapitositoumusten päivittäminen.

Kyberturvallisuuskeskus on koonnut sivuilleen ohjeita ja oppaita tietoturvan toteuttamiseksi.

Dokumentoi tietoturvaloukkaus ja osoita noudattavasi tietosuojalainsäädäntöä

Rekisterinpitäjän on dokumentoitava tietoturvaloukkaus. Tämä tarkoittaa sitä, että rekisterinpitäjä kerää ja tallentaa mm. tietoturvaloukkauksen kuvauksen (kuten sen luonne ja kohteena olevat tiedot), ilmoitusvelvoitteiden täyttämiseksi tarvittavat tiedot, tiedot loukkauksen vaikutuksista ja seurauksista, riskiarvioinnin sekä tehdyt toimenpiteet ja tietoturvaloukkaukseen liittyvät päätökset.

Dokumentointi on suositeltava säilyttää riittävän pitkään, jotta tietoihin voidaan tarpeen vaatiessa palata. Viranomaisen on pystyttävä dokumentoinnin avulla tarkistamaan, että tietosuoja-asetusta on noudatettu. Myös rekisteröidyn on voitava saada dokumentoinnin kautta lisätietoa tietoturvaloukkauksesta jälkeenpäin.

Tietoturvaloukkauksen dokumentointi on osa rekisterinpitäjän osoitusvelvollisuutta. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan, että se noudattaa tietosuojalainsäädäntöä (TSA 5 artiklan 2 kohta). Osoitusvelvollisuus koskee sekä rekisterinpitäjän tekemiä päätöksiä että sen toimintaa.

Täältä löydät lisätietoja

- Lue tietoturvaloukkauksista lisää tietosuojavaltuutetun toimiston verkkosivuilta
- Euroopan tietosuojaneuvoston ohjeita tietoturvaloukkauksista:
  - Suuntaviivat asetuksen (EU) 2016/679 mukaisesti henkilötietojen tietoturvaloukkauksen ilmoittamisesta (pdf)
  - Guidelines 01/2021 on examples regarding data breach notification (pdf)[2]

Apulaistietosuojavaltuutettu Pihamaa Heljä-Tuulia 912487203

Asiakirja on allekirjoitettu sähköisesti. Allekirjoituksen oikeellisuuden voi tarvittaessa tarkistaa tietosuojavaltuutetun toimiston kirjaamosta.

Tietosuojavaltuutetun toimiston yhteystiedot

Postiosoite: PL 800, 00531 Helsinki

Sähköposti: tietosuoja@om.fi

Puhelinvaihde: 029 566 6700

Verkkosivut: www.tietosuoja.fi

[2] Kyseinen versio ohjeesta on käynyt läpi Euroopan tietosuojaneuvostossa julkisen kuulemisen, mutta ohjetta ei ole vielä hyväksytty.

Liite 1: Esimerkkejä tietoturvaloukkauksista sosiaali- ja terveydenhuollossa

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Alle on koottu esimerkkejä tietoturvaloukkauksesta ilmoittamisen tueksi.

Esimerkit ovat yleisiä, eivätkä ota huomioon tapauskohtaisia erityispiirteitä. Rekisterinpitäjän tulee siksi aina arvioida kyseistä tietoturvaloukkausta ja ilmoittamiskynnystä tapauskohtaisesti.

Esimerkki	Riski-kynnys	Ilmoita vi-ranomai-selle	Ilmoita rekiste-röidylle	Huomautukset / suosi-tukset
Työntekijä on lähettänyt sähköpostitse tai kirjeitse väärään osoitteeseen asiakkaan / potilaan terveydentilatietoja (esimerkiksi päihdekuntoutus-suunnitelma tai sairausloma-todistus). Tiedot ovat päätyneet sivulliselle.	Korkea riski	✓	✓	Suojaamatonta sähköpostia ei tule käyttää salassa pidettävien tietojen viestimiseen.
Kokouksessa äänilaitteen kaiutin oli ollut Bluetoothin kautta yhteydessä viereisen huoneen laitteisiin. Tämä johti siihen, että puhelun kuuli sivullinen. Kokouksessa käsiteltiin asiakkaan / potilaan tietoja. Ei ole tietoa, kuinka kauan sivullinen oli ollut mukana puhelussa.	Korkea riski	✓	✓	Henkilökunnan ohjeistuksessa voidaan esimerkiksi huomioida se, että kokouslaitteiden yhdistämisessä ei käytetä Bluetoothia.
Sairaalan potilastiedot ovat poissa käytöstä 30 tunnin ajan verkkohyökkäyksen vuoksi.	Korkea riski	✓	✓	Rekisterinpitäjällä tulee olla kyky palauttaa nopeasti tietojen saatavuus fyysisen tai teknisen vian sattuessa.
Rekisterinpitäjä on käytönvalvonnan yhteydessä havainnut, että yksikön työntekijä on sivullisen asemassa käsitellyt (ns. urkkinut) yksittäisen potilaan / asiakkaan tietoja omiin tarkoituksiinsa.	Korkea riski	✓	✓	

Työntekijä on ladannut sosiaaliseen mediaan valokuvan, jossa näkyy myös erään potilaan tiedot. Kuvankäsittelyohjelmalla voi tarkentaa potilaan tietoja, vaikka kuva on epätarkka. Ei ole tietoa, onko sivullinen ladannut kuvan.	Korkea riski	✓	✓	Tieto loukkauksen kohteena olevasta henkilöstä on dokumentoitava ennen kuvan hävittämistä ilmoitusvelvollisuuden toteuttamista varten.
Työntekijä on hukannut parkkipaikalle asiakaslistan, joka sisältää tietoja asiakkaiden terveydentilasta. Työntekijä huomasi virheen, mutta hän ei löytänyt listaa. Ei ole tietoa, onko asiakaslista päätynyt sivulliselle.	Korkea riski	✓	✓	
Osa järjestelmässä olevista potilastiedoista tuhoutui lopullisesti inhimillisen virheen johdosta. Varmuuskopioita ei ole, eikä tietoja voida palauttaa.	Korkea riski	✓	✓	
Lääkärin vastaanotolta tullut asiakas (hlö A) ilmoitti vastaanotossa saaneensa toiselle henkilölle (hlö B) kuuluneen sairauspäiväraha-lomakkeen.	Korkea riski	✓	✓	
Työterveyshuollon laskun erittelyssä oli kirjattu työntekijän käynnin syy, joka paljasti tarpeettomasti terveydentilatietoja. Laskun vastaanottaja oli työnantajan edustaja.	Korkea riski	✓	✓	
Kotihoidon työntekijä oli vahingossa jättänyt asiakkaan (A) kotiin toisen asiakkaan (B) tietolomakkeen. Asiakkaan (A) omainen oli löytänyt tiedot omaisensa papereiden joukosta.	Korkea riski	✓	✓	
Terveydenhuollon ammattilainen merkitsi potilaan A:n tiedon lääke-allergiasta vahingossa potilaan B tietoihin. Potilaan A tietoihin ei siis merkitty lainkaan allergiatietoja. Potilaalla B ei ole allergiaa. Toinen terveydenhuollon ammattilainen (tietämättä A:n allergiasta) antaa sairaan-hoidossa potilas A:lle lääkettä, jolle A on allerginen. A:lle	Korkea riski	✓	✓	Ilmoitusta tietoturvalouk-kauksesta ei välttämättä tarvitse tehdä potilas B:lle, jos korkeaa riskiä ei hänelle ole syntynyt.

aiheutuu terveydellistä haittaa.				
On herännyt epäily siitä, että henkilö A on esiintynyt henkilö B:nä (identiteettivarkaus), tehnyt hänen nimissään ajanvarauksen ja saapunut lääkärin vastaanotolle. Lääkäri on hoitanut asiakasta ilmoitetuilla henkilötiedoilla ja tehnyt kirjauksen B:n potilastietoihin. Henkilö B on ottanut itse yhteyttä rekisterinpitäjään huomattuaan Omakannassa merkintöjä, jotka eivät ole hänen. Rekisterinpitäjä on poistanut virheelliset tiedot B:n tiedoista.	Korkea riski	✓	✓	Potilaan henkilöllisyys on syytä varmistaa kunkin asioinnin yhteydessä.
Järjestelmävian takia potilaan (A) lähete toimenpiteeseen oli tallentunut hetkellisesti väärän potilaan (B) tietoihin. Vika oli paikallinen ja väärä tieto ei kulkeutunut Kantaan. Lähetteen vastaanottava laboratorio oli tietoinen viasta. Vika sekä tietojen eheys korjattiin nopeasti. Potilaille ei aiheutunut haittaa.	Riski	✓		Jos potilas A ei olisi päässyt toimen-piteeseen, korkea riski olisi saattanut täyttyä.
Siivooja tyhjensi vuodeosaston jäteastian huolimattomasti väärään astiaan, joka oli rekisterinpitäjän hallussa. Osaston työntekijät käyttivät jäteastiaa tuhottavan potilaspaperin säilytykseen. Rekisterinpitäjällä ei ollut tietoa kenen potilaiden tiedoista on kysymys. Rekisterinpitäjä varmistui yhteistyössä jätehuollon kanssa, että tiedot tuhottiin, ja että tiedot eivät päässeet sivullisen haltuun.	Riski	✓		Rekisterinpitäjän tulee huomioida prosesseissaan se, että potilastietoja ei tule säilyttää avoimissa jäteastioissa, vaan ne tulee säilyttää vain lukituissa astioissa.
Terveydenhuollon toiminta-yksikkö (A) lähetti useiden potilaiden leikkaushoitoa koskevia tietoja toiseen terveydenhuollon toimintayksikköön (B). Tietojen lähettämisen tarkoitus oli tieteellinen tutkimus. Yksiköiden välillä ei ollut vielä laadittu sopimusta, eikä potilailta ollut hankittu	Riski	✓		

suostumusta tutkimukseen osallistumiseksi. Lähetetyt tiedot eivät sisältäneet suoria tunnistetietoja, mutta osa potilaista oli mahdollista tunnistaa tietojen yhdistelyllä ja päättelyllä. Tiedot päätyivät vain tutkimusta suorittaville terveydenhuollon ammattilaisille, jotka ovat salassapitovelvollisia. Vastaanottaja tuhosi tiedot.				
Apteekista toimitettiin organisaatioon A tarkoitettu useiden potilaiden lääkkeitä sisältänyt tilaus organisaatioon B. Apteekki tekee yhteistyötä kummankin organisaation kanssa. Lääkkeet saatiin toimitettua ajoissa oikeille potilaille.	Riski	✓		
Luotettavalle/turvalliselle vastaanottajalle, jonka kanssa yhteistyösuhde, on jaettu potilastietoa samalla osastolla. Vastaanottajalla on lakisääteinen salassapitovelvollisuus ja hän käsittelee työtehtävissään kyseistä tietoa. Tilanteessa ei ole syytä epäillä, että tietoja on käytetty tai tullaan käsittelemään lainsäädännön tai rekisterinpitäjän ohjeiden vastaisesti.	Ei riskiä			Potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvat saavat käsitellä potilasasiakirjoja vain siinä laajuudessa kuin heidän työtehtävänsä ja vastuunsa sitä edellyttävät.
Rekisterinpitäjän työntekijä lähettää suojaamattomassa sähköpostissa henkilötietoja. Ei ole syytä epäillä, että tiedot olisivat päätyneet sivulliselle.	Ei riskiä			Suojaamatonta sähköpostia ei tule käyttää salassa pidettävien tietojen viestimiseen.
Järjestelmätoiminnon vuoksi pääkäyttäjällä on ollut mahdollisuus nostaa käyttöoikeustasonsa liian laajaksi, jolloin hän olisi saanut pääsyn tehtäviensä kannalta tarpeettomiin tietoihin. Rekisterinpitäjä pystyi teknisin toimin varmistumaan, että pääkäyttäjä ei ollut nostanut käyttöoikeustasoansa.	Ei riskiä			Potilastietojärjestelmässä tulee olla käyttöoikeuksien hallintajärjestelmä, jonka avulla käyttäjälle voidaan määritellä tehtävien mukaiset käyttöoikeudet.
Rekisterinpitäjä on tallentanut salatun varmuuskopion asiakastietoja sisältävästä arkistosta USB-muistitikulle.	Ei riskiä			

Muistitikku varastetaan tiloihin tehdyn murron yhteydessä. Tiedot on salattu uusimman tekniikan mukaisella algoritmilla, tiedoista on varmuuskopiot, yksilöllinen salausavain ei vaarannu ja tiedot voidaan palauttaa ajoissa.				
Tekstiviesti ajanvarauksesta oli mennyt väärään puhelinnumeroon. Viesti ei sisältänyt tunnisteellisia henkilötietoja, eikä myöskään terveyttä koskevia tietoja.	Ei riskiä			
Apteekin työntekijä antoi asiakkaalle B asiakirjan, jossa oli nähtävillä asiakkaan A nimi ja henkilötunnus. Asiakas huomasi tapahtuneen heti, ja palautti asiakirjan välittömästi apteekin työntekijälle.	Ei riskiä			
Potilas A ilmoitti terveydenhuoltoon, että hänen potilastietoihinsa oli kirjattu toisen henkilön (B) potilastietoja. A ei pysty kirjattujen tietojen perusteella päättelemään, kuka B on. Kun asia varmistui, B:n tiedot poistettiin A:n potilastiedoista ja kirjattiin tiedot B:n omiin potilastietoihin. A:n hoitoon liittyviä ratkaisuja ei ehditty tehdä henkilöä B koskevien tietojen perusteella, eikä tapahtuneella ollut vaikutusta B:n hoitoon.	Ei riskiä			On varmistettava, että A:n kanssa käytävässä kommunikaatiossa ei paljasteta, kuka B on. Jos A kykenee tunnistamaan B:n suoraan tai yhdistämällä muita tietoja, on riski todennäköisesti korkea, ja B:lle ilmoitettava. Jos jommankumman potilaan hoitoa koskevia ratkaisuja on ehditty tehdä virheellisten tietojen perusteella, on riski todennäköisesti korkea tämän potilaan osalta.