**Ohjeet tietomurtoihin reagoimiseksi**

Rekisteröidyn oikeuksista säädetään erityisesti tietosuoja-asetuksessa seuraavasti. Alle on koottu TYYn kannalta olennaisimmat artiklat:

Art. 32: Käsittelyn turvallisuus
Art. 33: Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle
Art. 34: Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Lisäksi kannattaa huomioida tietosuojavaltuutetun ohjeet tietoturvaloukkauksista: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietoturvaloukkaukset.html

**Mitä tietoturvaloukkauksella tarkoitetaan?**

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt USB-tikku, varastettu tietokone, hakkerointi, haittaohjelmatartunta, kyberhyökkäys, tulipalo datakeskuksessa tai tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksen seurauksena saattaa tapahtua esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen tai salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys.

**Rekisterinpitäjän velvollisuus varautua mahdollisten tietoturvaloukkausten varalta**

Rekisterinpitäjän ja henkilötietojen käsittelijän on suojattava henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Sen lisäksi rekisterinpitäjän on varauduttava mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet tietoturvaloukkaustilanteita varten. Tietoturvaloukkauksiin on pystyttävä reagoimaan mahdollisimman nopeasti.

Tietoturvaloukkaus edellyttää rekisterinpitäjältä kykyä arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu tietoturvaloukkauksen kohteena olleille henkilöille. Arvion johtopäätös voi olla esimerkiksi se, että tietoturvaloukkauksesta ei aiheudu riskiä, aiheutuu riski tai aiheutuu korkea riski. Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä (esimerkiksi tietoturvaloukkauksen dokumentointi, ilmoitus valvontaviranomaiselle tai ilmoitus rekisteröidylle).

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä

tietoturvaloukkauksesta lopulta seuraa. Dokumentointivelvollisuuden tai ilmoituksen tekemisen laiminlyöminen on tietosuoja-asetuksen vastaista ja voi johtaa tietosuoja-asetuksessa määritettyihin seuraamuksiin.

**Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle (art. 33)**

*Olennainen sisältö*: Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin riskiä. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

Ilmoituksessa on vähintään a) kuvattava henkilötietojen tietoturvaloukkaus, ml. mahdollisuuksien mukaan rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät; 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.

Jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, ml. henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa, että tätä artiklaa on noudatettu.

**Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle (art. 34)**

*Olennainen sisältö*: Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä. Ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava ainakin b) tietosuojavastaan 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.

Ilmoitusta rekisteröidylle ei kuitenkaan vaadita, jos jokin seuraavista edellytyksistä täyttyy: a) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettava 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 rekisteröidyn oikeuksiin ja vapauksiin todennäköisesti 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.

Jos rekisterinpitäjä ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä tai päättää, että jokin aiemmin mainituista ilmoitusvelvollisuuden kumoavista edellytyksistä täyttyy, arvioituaan, kuinka todennäköisesti henkilötietojen tietoturvaloukkaus aiheuttaa suuren riskin.

***Toimenpiteet käytännössä tietomurron tapahtuessa:***

1. Selvitetään loukkauksen laatu
    a. Aiheutuuko tietoturvaloukkauksesta todennäköisesti luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Asian arvioinnissa kannattaa käyttää varovaisuutta ja maalaisjärkeä. Huomioon olisi otettava tietoturvarikkomuksen tyyppi; henkilötietojen luonne, arkaluonteisuus ja määrä; tunnistamisen helppous; rekisteröidyn ominaisuudet; rekisterinpitäjän ominaisuudet; tietovuodon seurauksien vakavuus. Tarkemmin huomioon otettavista seikoista ks. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietoturvaloukkaukset.html
        i. Jos vastaus on ei, ilmoitusvelvollisuutta viranomaiselle tai rekisteröidylle ei lähtökohtaisesti ole.
        ii. Jos vastaus on kyllä, pitää tietoturvaloukkauksesta ilmoittaa tietosuojavaltuutetun toimistoon.
    b. Aiheutuuko tietoturvaloukkauksesta todennäköisesti korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille.
        i. Jos vastaus on ei, ilmoitusvelvollisuutta rekisteröidylle ei ole.
        ii. Jos vastaus on kyllä, pitää tietoturvaloukkauksesta ilmoittaa lähtökohtaisesti myös rekisteröidylle. Ilmoitusta ei kuitenkaan tarvitse tehdä, jos jokin seuraavista edellytyksistä täyttyy:
            1. rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettava kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;
            2. rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin todennäköisesti kohdistuva korkea riski ei enää todennäköisesti toteudu;
            3. se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidylle tiedotetaan yhtä tehokkaalla tavalla.
2. Ilmoitetaan loukkauksesta tarvittaessa viranomaiselle ja/tai rekisteröidylle. Tietosuojavaltuutetun toimistolle tiedot on annettava viimeistään 72 tunnin kuluessa

loukkauksen ilmitulosta ja rekisteröidylle ilman aiheetonta viivytystä. Jos tietoja viranomaiselle ei ole mahdollista toimittaa samanaikaisesti, voidaan ne toimittaa vaiheittain ilman aiheetonta viivytystä. Ilmoituksessa on vähintään

   a. kuvattava henkilötietojen tietoturvaloukkaus, ml. mahdollisuuksien mukaan rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät (tämä tarvitsee selvittää vain viranomaiselle, muttei rekisteröidylle);
   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.

3. Tehdään asiasta rikosilmoitus poliisille, jos epäillään, että kyseessä voisi olla rikollinen teko. Rikoslain 38 luvussa on määritelty erityisesti tieto- ja viestintärikoksia. Esimerkiksi luvun 8 §:ssä säädetään tietomurrosta.
4. Suoritetaan korjaavia toimenpiteitä, joilla voidaan ehkäistä tietoturvaloukkausten riskiä tulevaisuudessa ja ehkäistä loukkauksesta mahdollisesti aiheutuvia haitallisia seurauksia rekisteröidylle.
5. Dokumentoidaan tietoturvaloukkaus ja siihen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet siten, että valvontaviranomainen voi tarkistaa asetusta noudatetun.