## Henkilötietojen tietoturvaloukkauksia koskevan tiedonantovelvoitteen täyttäminen – MALLIPOHJA

MALLI suunnittelun tueksi, ei viralliseen käyttöön

EU:n yleisen tietosuoja-asetuksen mukaan 33 ja 34 artiklojen mukaan rekisterinpitäjän on ilmoitettava henkilötietoihin kohdistuneesta tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta tietosuojavaltuutetulle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

Jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

Ilmoituksessa annettavat tiedot otsikkotasolla ovat:

1. Tietosuojavastaavan nimi ja yhteystiedot;
2. Kuvaus henkilötietojen tietoturvaloukkauksesta, mukaan lukien mahdollisuuksien mukaan
3. asianomaisten rekisteröityjen ryhmät;
4. ryhmien arvioidut lukumäärät; sekä
5. henkilötietotyyppien ryhmät ja arvioidut lukumäärät;
6. Kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista; sekä
7. Kuvaus toimenpiteistä, joita rekisterinpitäjä ehdottaa tai jotka rekisterinpitäjä on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

### Perustiedot tietoturvaloukkauksesta

(a) Kuvaa tietoturvaloukkausta kaiken saatavissa olevan tiedon perusteella.

(b) Milloin tietoturvaloukkaus tapahtui?

(c) Miten tietoturvaloukkaus tapahtui?

(d) Mikäli tämä ilmoitus tehdään säädetyn määräajan ulkopuolella, ilmoita perustelut tälle.

(e) Minkälaisia suojakeinoja (organisatorisia/teknisiä) organisaatiolla oli käytössä tapahtuneen kaltaisten tietoturvaloukkausten estämiseksi?

(f) Liitä tämän ilmoituksen mukaan edellisen kohdan perusteella relevantit politiikka- ym. dokumentit. Ilmoita myös dokumenttien implementointiajankohdat.

(g) Onko ko. politiikat ja muu ohjaava dokumentaatio koulutettu todistettavasti sellaisille henkilöille, jotka osallistuvat henkilötietojen käsittelyyn?

### Henkilötiedot, joihin tietoturvaloukkaus kohdistui

(a) Mihin henkilötietoryhmiin ja rekisteröityjen ryhmiin tietoturvaloukkaus kohdistui? Kohdistuiko tietoturvaloukkaus erityisiin henkilötietoryhmiin (“arkaluonteisiin henkilötietoihin”)?

(b) Kuinka montaa rekisteröitynyttä tietoturvaloukkaus koskee?

(c) Ovatko ko. rekisteröidyt tietoisia tietoturvaloukkauksen tapahtumisesta?

MALLI suunnittelun tueksi, ei viralliseen käyttöön

(d) Kuvaile potentiaalisia, rekisteröityjä ja heidän yksityisyyden suojaansa koskevia riskejä ja haittoja jotka tietoturvaloukkauksesta johtuvat.

(e) Onko organisaatiolle tullut yhteydenottoja rekisteröidyiltä tietoturvaloukkauksen johdosta?

(f) Onko organisaatio ohjeistanut rekisteröityjä mahdollista toimista, joilla he voivat pyrkiä rajaamaan tietoturvaloukkauksen seurauksia?

### Tietoturvaloukkauksen tutkiminen, rajoittaminen ja siitä toipuminen

1. Onko organisaatio ryhtynyt toimenpiteisiin tietoturvaloukkauksen seurausten minimoinniksi tai rajoittamiseksi? Kuvaile näitä toimenpiteitä.
2. Onko altistunut tieto saatu takaisin organisaation haltuun? Jos kyllä, kuvaile miten ja milloin tämä tapahtui.
3. Minkälaisiin toimiin organisaatio on ryhtynyt vastaavanlaisten tietoturvaloukkausten estämiseksi jatkossa?

### Muuta

1. Onko organisaatio tehnyt ilmoituksen tietoturvaloukkauksesta Poliisille?
2. Onko organisaatio tehnyt ilmoituksen tietoturvaloukkauksesta jollekin muulle viranomaiselle, mukaan lukien tietosuojan valvontaviranomaiset Euroopan unionin jäsenvaltioissa?