



27.4.2018

## OHJE: TIETOTURVA- TAI TIETOSUOJAPOIKKEAMIEN KÄSITTELYSTÄ HENKILÖTIETOJA SISÄLTÄVISSÄ PALVELUISSA

### 1 Taustaa

Tämä ohje kuvaa VRK:n ja palvelun toimittajan/alihankkijan välisen ilmoitus- ja yhteistyömenettelyn tietoturva- tai tietosuojapoikkeaman yhteydessä.

### 2 Määritelmät

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

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

### 3 Toiminta tietoturva- tai tietosuojasuojapoikkeaman yhteydessä

Havainnon poikkeamasta voi tehdä henkilötietojen käsittelijänä toimiva toimittaja/alihankkija, VRK tai joku ulkopuolinen taho. Havainto on vahvistettava oikeaksi.

Henkilötietojen käsittelijän tulee ilmoittaa tapahtuneesta poikkeamasta VRK:lle välittömästi. VRK ilmoittaa asiasta valvontaviranomaiselle huomioiden EU:n yleisen tietosuojasetuksen asettaman 72 tunnin aikarajan.

Ilmoitus poikkeamasta VRK:lle tehdään ensisijaisesti sähköpostilla Turvapostilla osoitteessa <https://securemail.vrk.fi/>:

Vastaanottaja: [tietoturvallisuus@vrk.fi](mailto:tietoturvallisuus@vrk.fi)

Vaihtoehtoisesti palvelun toimittaja voi tehdä ilmoituksen myös yhteyshenkilölleen VRK:ssa.





27.4.2018

**Ilmoituksessa on mainittava:**

- Milloin ja miten tapahtuma on havaittu.
- Kuvaus mitä on tapahtunut ja mitkä ovat tapahtuman osapuolet yhteystietoineen.
- Mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa.
- Millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille.
- Kuvaus niistä toimenpiteistä, joita aiotaan toteuttaa tai jotka on jo toteutettu haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi.
- Siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Tästä on sovittava VRK:n kanssa.

VRK kirjaa tapahtuneen oman poikkeamanhallintaprosessinsa mukaisesti. Tarvittaessa järjestetään osapuolten (VRK, palvelun toimittaja) kesken puhelinneuvottelu (Skype).

VRK vastaa tarvittaessa ilmoituksesta valvontaviranomaiselle sekä rekisteröidyille. Kun poikkeama on VRK:n osalta loppuun käsitelty, siitä ilmoitetaan palvelun toimittajalle.

**4 Yhteystiedot (VRK)**

Tuomo Hakala  
Sopimuksen tietoturvayhteyshenkilö  
[tuomo.hakala@vrk.fi](mailto:tuomo.hakala@vrk.fi), 0295 535 211

Noora Kallio  
Tietosuojavastaava  
[noora.kallio@vrk.fi](mailto:noora.kallio@vrk.fi), 0295 535 079

Pekka Ristimäki  
Tietoturvapäällikkö  
[pekka.ristimaki@vrk.fi](mailto:pekka.ristimaki@vrk.fi), 040 1394828