

Korvaushakemukset henkilötietojen tietoturvaloukkauksissa

(EU:n tietosuoja-asetuksen (EU 2016/679) 82 artikla)

Strateginen tietoturva- ja
tietosuojatyöryhmä
18.8.2025

18.8.2025

Sisällys

1. Johdanto.....	3
2. Rekisteröidyn informointi.....	3
2.1 Tietosuoja-asetuksen velvoitteet	3
2.2 Korvaushakemuksen käsittelyä ohjaavat tiedot Pohteella	4
3. Henkilötietojen käsittelyn vastuut Pohteella.....	4
4. Vahingonkorvauksen maksamisesta päättäminen Pohteella	5
4.1 Korvauksen määrä /korvausperusteet	5
4.2 Valtuudet korvauksen myöntämiseen.....	6
4.3 Korvausvastuun välttäminen	7
5. Pohteen vahingonkorvausprosessi EU:n tietosuoja-asetuksen 82 artiklan mukaisissa vahingonkorvauksissa	8
5.1 Prosessikuvaus	8
5.2 Prosessikaavio	11

18.8.2025

1. Johdanto

Tämä toimintaohje on laadittu EU:n tietosuoja-asetuksen (EU 2016/679) mukaisiin tilanteisiin, joissa rekisteröidylle on aiheutunut tietosuoja-asetuksen rikkomuksen johdosta aineellista tai aineetonta vahinkoa siinä määrin, että joko rekisterinpitäjälle tai henkilötietojen käsittelijälle syntyy korvausvelvollisuus aiheutetusta vahingosta. Tietosuoja-asetuksen 34 artiklan mukaan rekisterinpitäjän on ilmoitettava rekisteröidylle tietoturvaloukkauksesta, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Ohjeen perustana ovat EU:n tietosuoja-asetuksen artikkelit 33, 34 ja 82 sekä vahingonkorvauslaki (412/1974) ja Pohjois-Pohjanmaan hyvinvointialueen hallintosääntö.

Ohjeessa kuvataan tietosuoja-asetuksen mukaisten rekisteröidylle tehtävien ilmoitusten ja maksettavien korvausten normiperustaa sekä Pohteen sisäinen toimintamalli vahingonkorvaushakemusten käsittelyssä.

2. Rekisteröidyn informointi

2.1 Tietosuoja-asetuksen velvoitteet

EU:n tietosuoja-asetuksen (EU 2016/679) 34 artiklan mukaan henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. **Ilmoitusta ei vaadita**, jos jokin seuraavista edellytyksistä täyttyy;

- rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta.
- rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu.
- se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla tiedotetaan rekisteröidylle tehokkaalla tavalla.

Mikäli ilmoitus on tehtävä, niin rekisteröidylle tehtävän ilmoituksen sisältö määräytyy EU:n tietosuoja-asetuksen 33 artiklan mukaan. Tietosuoja-asetuksen 33 artiklan 3 kohdan b, c ja d -alakohtien mukaiset tiedot. Nämä tiedot ovat;

- b) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa
- c) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset

18.8.2025

- d) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

TARKEMMAT TIEDOT ILMOITTAMISESTA POHTEEN TIETOSUOJAHOJEISSA

Tietosuoja-asetuksen 82 artiklassa säädetään vastuusta ja rekisteröidyn oikeudesta vahingonkorvaukseen. Rekisteröidyllä on oikeus saada vahingonkorvausta, jos hänelle aiheutuu tietosuoja-asetuksen rikkomisesta aineellista tai aineetonta vahinkoa.

2.2 Korvaushakemuksen käsittelyä ohjaavat tiedot Pohteella

Korvaushakemuksen käsittelyn tehostamiseksi rekisteröidylle tehtävän ilmoituksen on syytä sisältää seuraavia tietoja tietosuoja-asetuksen vaatimusten lisäksi. Vahingonkorvauksen hakijaa on ohjeistettava liittämään nämä käsittelyä ohjaavat tiedot vahingonkorvaushakemukseen; 1) Mistä toimintayksiköstä (Terveystieteiden tutkimuskeskus, sosiaalihuolto, pelastustoimi) on kyse, 2) Kyseisen toimintayksikön vastuhenkilö (johtajaylilääkäri, sosiaalijohtaja, pelastusjohtaja), 3) Pohteen kirjaamon yhteystiedot, 4) Vahingonkorvausvaatimus perusteluineen.

Ohjeistuksella vastataan hallintolain (434/2003) velvoitteisiin hallinnon oikeusperiaatteista ja neuvonnasta. Hallintolain 6 §:n mukaan viranomaisen on kohdeltava hallinnossa asioivia tasapuolisesti sekä käytettävä toimivaltaansa yksinomaan lain mukaan hyväksyttäviin tarkoituksiin. Viranomaisen toimien on oltava puolueettomia ja oikeassa suhteessa tavoiteltuun päämäärään nähden. Niiden on suojattava oikeusjärjestyksen perusteella oikeutettuja odotuksia. Lain 8 § 1 momentin mukaan viranomaisen on annettava asiakkailleen tarpeen mukaan hallintoasian hoitamiseen liittyvää neuvontaa sekä vastattava asiointia koskeviin kysymyksiin ja tiedusteluihin.

3. Henkilötietojen käsittelyn vastuut Pohteella

Tietosuoja-asetuksen 1 luvun 4 artiklassa määritellään rekisterinpitäjä. Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä,

18.8.2025

rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

Hyvinvointialuelain (611/2021) 95 § määrittää hyvinvointialueen hallintosäännön sisällöstä. Pykälän I kohdan mukaan hallintosäännössä on oltava määräykset tiedonhallinnan ja asiakirjahallinnon järjestämisestä. Tiedonhallintalaki (906/2019) määrittää tiedonhallintamallin (5§) sisällöstä. Tiedonhallintamallissa on mm. määriteltävä tietovarannosta vastaavasta viranomaisesta. Pohteen hallintosäännön mukaan Aluehallitus huolehtii hyvinvointialueen rekisterinpitäjän velvollisuuksista (Hallintosääntö 2 §).

Aluehallitus on päättänyt henkilötietojen vastuuhenkilöt 20.12.2022 518 §:

Hyvinvointialueen toiminnassa syntyneiden henkilötietojen käsittelytarkoitus määritellään toimintayksikkökohtaisesti. Hyvinvointialueella on terveydenhuollon, sosiaalihuollon ja pelastustoimen toimintayksiköt. Aluehallitus määrittää toimintayksikkökohtaisesti henkilötietojen käsittelyn vastuuhenkilöt.

1. Terveydenhuollon toimintayksikön henkilötietojen käsittelyn vastuuhenkilö on johtajaylilääkäri, joka vastaa potilasrekisteristä
2. Sosiaalihuollon toimintayksikön henkilötietojen käsittelyn vastuuhenkilö on sosiaalijohtaja, joka vastaa asiakasrekisteristä
3. Pelastustoimen toimintayksikön henkilötietojen käsittelyn vastuu henkilö on pelastusjohtaja
4. Muiden henkilötietojen käsittelytarkoitusten osalta, esimerkiksi henkilöstöhallintoa tai tietojohdantamista varten käsiteltävät henkilötiedot, vastuuhenkilöitä ovat toimialue/palvelualuejohtajat omilla toimi- ja palvelualueillaan tai muu määritelty viranhaltija.
5. Vastuuhenkilö voi päättää käsittelytarkoituksen kokonaisuuden jakamisesta esimerkiksi tehtävittäin tai palveluittain ja määrittää näille käsittelytoimille omat osavastuuhenkilöt.

4. Vahingonkorvauksen maksamisesta päättäminen Pohteella

4.1 Korvauksen määrä /korvausperusteet

Tietosuoja-asetuksen 82. art.: ”1. Jos henkilölle aiheutuu tämän asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta.” Rekisteröidylle aiheutuvan vahingon käsite olisi tulkittava laajasti unionin tuomioistuimen oikeuskäytännön perusteella ja tavalla, jossa tietosuoja-asetuksen

18.8.2025

tavoitteet otetaan kaikilta osin huomioon. Rekisteröityjen olisi saatava täysi ja tosiasiallinen korvaus aiheutuneesta vahingosta.

Edellä todetun mukaisesti 82 artiklan mukainen korvausvastuu voi aiheutua myös tilanteissa, joissa Pohde toimii henkilötietojen käsittelijänä esim. yhteistyösopimusten mukaisesti.

Vahingonkorvauksen määrä perustuu näyttöön; vahingonkorvauksen vaatijan tulee pystyä erittelemään ja perustelemaan hänelle aiheutuneen vahingon määrä ja esittämään mahdolliset tositteet aiheutuneista vahingoista.

Korvauksia maksetaan esim. seuraavista kuluista:

- toimenpiteiden aiheuttamista kuluista, joilla rekisteröity on suojautunut suuremmilta vahingoilta, esimerkiksi luottokiellosta (Vahingonkorvauslaki 5 luku 1§)
- henkisestä kärsimyksestä (Vahingonkorvauslaki 5 luku 6§)
- rekisteröidyn henkilötietojen väärinkäytön aiheuttamista taloudellisista vahingoista, kuten pikavippien ottamisesta rekisteröidyn nimiin (Vahingonkorvauslaki 5 luku 1§)
- Korvausvelvollisuus ei rajoitu vahingonkorvauslaissa eriteltyihin vahinkoihin (tietosuoja-asetuksen mukaan laajasti aineettomiin ja aineellisiin vahinkoihin)

[Vahingonkorvaukset tietosuojarikoksen tai tietomurron uhreille - Rikosuhripäivystys](#)

[Linkki tietosuojavaikuttetun asiaa koskevalle sivustolle](#)

Korvaushakemuksessa esitetyn vaatimuksen ja rekisteröidylle maksettavan korvauksen määrittelyssä tulee konsultoida oikeudellisia palveluita sekä tietosuojatiimiä. Korvauksen määrää määrittäessä voidaan hyödyntää [henkilöasiain neuvottelukunnan](#) suosituksia (suositukset korvausten määrästä maksettaessa vahingonkorvauksia kärsimyksestä rikosten yhteydessä)

4.2 Valtuudet korvauksen myöntämiseen

Vahingonkorvauksen myöntämisen/päättämisen valtuudet hallintosäännön ja muiden sääntöjen mukaan:

Hallintosääntö:

- 12 §: Aluehallitus päättää vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta- vaaditun arvon ylittäessä 20 000 euroa.
- 32 §: konsernipalvelujen johtaja päättää vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta vaaditun arvon ollessa enintään 20 000 euroa.

18.8.2025

- 33 §: sosiaali- ja terveydenhuollon järjestämisjohtaja päättää vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta vaaditun arvon ollessa enintään 20 000 euroa.
- 34: Toimialuejohtajat päättävät vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta vaaditun arvon ollessa enintään 20 000 euroa.
- 35 §: Tehtävälajohtajat päättävät vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta vaaditun arvon ollessa enintään 20 000 euroa.
- 36 §: Yliopistosairaalajohtaja päättää vahingonkorvausten ja vahingonkorvausluonteisten korvausten maksamisesta vaaditun arvon ollessa enintään 20 000 euroa.
- **Näistä tehty delegointipäätökset toimialueittain:**
- Pohteen vakuutusturva; Vakuutussopimus 16-766-439-0 Vakuutus kattaa tietosuojalain tai EU:n yleisen tietosuoja-asetuksen mukaisen korvausvastuun (tapauskohtainen; yhteys riskienhallintapäällikköön) kattaa 3 000 000 euroon asti julkista valtaa käytettäessä tai muutoin kuin julkista valtaa käyttämällä.

Hyödyllisiä linkkejä:

<https://www.riku.fi/opaat-ja-ohjeet/vahingonkorvaukset-rikosvahingoissa/vahingonkorvaukset-tietovuodon-uhreille/>

<https://tietosuoja.fi/vahingonkorvausten-vaatiminen>

4.3 Korvausvastuun välttäminen

82 artiklan 2 kohdan mukaan ”kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut käsittelystä, jolla on rikottu tätä asetusta. Henkilötietojen käsittelijä on vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijöille osoitettuja tämän asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti”

Mikäli rekisterinpitäjä tai henkilötietojen käsittelijä voi osoittaa, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta, niin se on vapautettava korvausvastuusta edellä mainitun 82 artiklan toisen kohdan nojalla. Tämän takia tietoturvaloukkauksen ilmetessä on selvitettävä mm. tehty turvaamistoimenpiteet, riskikartoitukset (rekisterinpitäjän osoitusvelvollisuus). Jos henkilötietojen tietoturvaloukkaus havaitaan, rekisterinpitäjä voi osoitusvelvollisuuden avulla näyttää, että se on aktiivisesti pyrkinyt tunnistamaan tietosuojaan liittyviä riskejä ja ottanut käyttöön tarvittavia toimenpiteitä henkilötietojen suojaamiseksi. Jos rekisterinpitäjä ei pysty osoittamaan noudattavansa tietosuoja-asetuksen velvoitteita, se voi aiheuttaa rekisteröidyn oikeuksille ja

18.8.2025

vapauksille kohdistuvan riskin lisäksi maineriskin rekisterinpitäjälle tai hallinnollisia seuraamuksia.
(<https://tietosuoja.fi/osoitusvelvollisuus>).

5. Pohteen vahingonkorvausprosessi EU:n tietosuoja-asetuksen 82 artiklan mukaisissa vahingonkorvauksissa

5.1 Prosessikuvaus

Henkilötietojen tietoturvaloukkauksen ilmi tullessa on tärkeää aloittaa tapauksen selvittäminen. 1) Tietosuoja-asetuksen 34 artiklan mukaan rekisterinpitäjän on ilmoitettava rekisteröidylle tietoturvaloukkauksesta, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. 2) Tietosujaloukkauksen selvittäminen on tärkeää myös rekisterinpitäjän kannalta, sillä tietosuoja-asetuksen 82 artiklan 3 kohdan mukaan rekisterinpitäjä tai henkilötietojen käsittelijä on vapautettava 82 artiklan 2 kohdan mukaisesta vastuusta, mikäli rekisterinpitäjä/käsittelijä osoittaa, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.

Alkuarvion pohjalta tehdään ilmoitukset sekä rekisteröidylle/rekisteröidyille että tietosuojavaltuutetulle. Tässä ohjeessa ei [käsitellä ilmoitusta tietosuojavaltuutetulle](#).

Rekisteröidylle tehtävän ilmoituksen sisältö määräytyy EU:n tietosuoja-asetuksen 33 artiklan mukaan. Ilmoituksessa on annettava ainakin 33 artiklan 3 kohdan b, c ja d alakohdissa tarkoitetut tiedot ja toimenpiteet.

- 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.

Tämä ohjeistus on laadittu EU:n tietosuoja-asetuksen 82 artiklan 1 kohdan mukaisiin tilanteisiin. Artiklan 1 kohdan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvausta, jos henkilölle aiheutuu aineellista tai aineetonta vahinkoa.

18.8.2025

Korvaushakemuksen käsittelyn tehostamiseksi rekisteröidylle tehtävän ilmoituksen on syytä sisältää seuraavia tietoja tietosuoja-asetuksen vaatimusten lisäksi. Vahingonkorvauksen hakijaa on ohjeistettava liittämään nämä käsittelyä ohjaavat tiedot vahingonkorvaushakemukseen; 1) Mistä toimintayksiköstä (Terveystieteiden tutkimuskeskus, sosiaalihuolto, pelastustoimi) on kyse, 2) Kyseisen toimintayksikön vastuuhenkilö (johtajaylilääkäri, sosiaalijohtaja, pelastusjohtaja), 3) Pohteen kirjaamon yhteystiedot, 4) Vahingonkorvausvaatimus perusteluineen. Vahingonkorvauksen määrä perustuu näyttöön; vahingon kärsijällä on velvollisuus osoittaa vahingon määrää koskevat todisteet.

Korvaushakemuksen saavuttua Pohteen kirjaamoon vahingonkorvaushakemus kirjataan Pohteen diariin ja kirjaamo toimittaa saapuneen vahingonkorvaushakemuksen sekä rekisterinvastuuhenkilölle että kyseiselle toimintayksikölle. Toimintayksiköissä hakemus ohjataan delegointisäännösten mukaisesti viranhaltijapäätöksen tekijälle.

Viranhaltijapäätöksen tulee perustua selvitykseen, jonka perusteella mm. kartoitetaan mahdollisuutta vapautua korvausvastuusta (82 artikla 2 kohta). Viranhaltijapäätöksen tueksi on hankittava rekisterin vastuuhenkilön lausunto korvauksen maksamisen perusteista. Rekisterinvastuuhenkilöä ja korvauksesta päättävää viranhaltijaa avustavat korvauksen määrän selvittelyssä lakiyksikkö ja tietosuojatiimi. Korvauksen määrää määrittäessä voidaan hyödyntää henkilöasiain neuvottelukunnan suosituksia (suositukset korvausten määrästä maksettaessa vahingonkorvauksia kärsimyksestä rikosten yhteydessä)

Viranhaltijapäätös annetaan tiedoksi asianosaiselle. Päätöksessä on oltava oikaisuvaatimusosoitus. Asian yksityisoikeudellisen luonteen johdosta viimeistään Aluehallituksen asiaa koskevan päätöksen jälkeen asianosaista on ohjattava mahdollisuudesta käynnistää yksityisoikeudellinen vahingonkorvausprosessi haastehakemuksella käräjäoikeudessa¹.

Mikäli tietosuojaloukkaus on ollut vakava, niin Pohteen sisäisen käsittelyn rinnalla/sijaan on kulkenut rikosprosessi, johon vahingonkorvausvaatimukset on voitu kytkeä/yhdistää. Rikosprosessissa käräjäoikeuden vahingonkorvauspäätöksestä aukeaa normaalit yksityisoikeuden mahdollistamat

¹ Ylimmät laillisuusvalvojat ovat ratkaisukäytännössään katsoneet, että kunnan tulisi hallintolain (434/2003) 8 §:n mukaisen viranomaisen neuvontavelvollisuuden täyttääkseen ohjeistaa vahingonkärsijää mahdollisuudesta saattaa yksityisoikeudellinen vahingonkorvausvaatimus haastehakemuksella käräjäoikeuden käsiteltäväksi. Kunnallisvalitusosoituksessa tulisi mainita, ettei hallinto-oikeus ota tutkittavakseen vahingonkorvausta koskevaa valitusperustetta (esimerkiksi apulaisoikeusasiamiehen päätös 11.9.2017, EOAK/4661/2016 ja apulaisoikeuskanslerin päätös 27.11.2011, OKV/595/1/2010).

18.8.2025

muutoksenhaut ylempiin oikeusasteisiin. Pohteen sisäisen käsittelyprosessin aikana selvitetään myös Pohteen vastuuvakuutuksen 16-766-439-0 kattavuus tapauskohtaisesti.

18.8.2025

5.2 Prosessikaavio

