Pohde
Pohjois-Pohjanmaan hyvinvointialue

Tietohallinto 19.12.2025

TIETOTURVALIITE

Pohde
Pohjois-Pohjanmaan hyvinvointialue

Tietohallinto 19.12.2025

Dokumentin omistaja: Pohde tietoturvapäällikkö

Versio-nro	Muutokset	pvm.	Muokkaaja	Hyväksyjä
1.0	Julkaisu	21.2.2025	Tietoturvasuunnittelija Antti Junttila	Tietoturvapäällikkö Anssi Huhtala / Pohde
1.4	Tarkennettu raportointiin ja ilmoituksiin liittyviä kohtia ja teknisiä muutoksia.	19.11.2025	Tietoturvapäällikkö / tietoturva-asiantuntija Antti Junttila	Tietoturvapäällikkö
1.5	Terminologisia muutoksia (toimittaja -> toimittaja), teknisiä muutoksia	19.12.2025	Tietoturva-asiantuntija Antti Junttila	
1.6.	Teknisiä muutoksia	6.1.2026	Tietoturva-asiantuntija Antti Junttila	

Tietohallinto 19.12.2025

Sisällysluettelo:

Dokumentin tarkoitus ja soveltaminen 4
A. Määritelmät 4
B. Tietoturvahäiriöiden luokittelu 5
C. Yleiset vaatimukset 6
D. Käyttöoikeudet- ja valtuudet 8
E. Toimittajan ilmoitus- ja raportointivelvollisuus 9
F. Hankittavaa palvelua koskevat erityisehdot 10
G. Toimittajaa, joka käyttää tilaajan järjestelmää, koskevat erityisehdot 10
H. Tietoturvaloukkaustilanteessa toimiminen sekä jatkuvuudenhallinta 10
I. Salassapito 11
J. Muutoshallinta 12
K. Turvallisuusselvitys 13
L. Sopimuksen muuttaminen ja lisätyö 13
M. Allekirjoitukset 14
LIITE 1 Yhteystiedot 15

Pohde
Pohjois-Pohjanmaan hyvinvointialue

Tietohallinto 19.12.2025

Dokumentin tarkoitus ja soveltaminen

Tämä dokumentti on tilaajan (Pohjois-Pohjanmaan hyvinvointialue) ja toimittajan (järjestelmän tai palvelun toimittaja) välisen hankintasopimuksen (jäljempänä *pääsopimus*) liite, jolla sovitaan hankintasopimuksen kohteen tietoturvallisuuteen, tilaajan aineiston käsittelyyn ja salassapitoon liittyvistä seikoista. Tietosuojaan liittyvistä asioista sovitaan tietosuojaliitteissä.

Tätä dokumenttia sovelletaan pääsopimuksessa mainitun sopimusasiakirjojen soveltamisjärjestyksen mukaisesti.

Tietoturvallisuuteen liittyvien määritelmien lähteenä käytetään Turvallisuuskomitean laatimaa Kyberturvallisuuden sanastoa.

Tässä dokumentissa sopimuksen kohteena on järjestelmä tai palvelu riippuen pääsopimuksen sisällöstä.

A. Määritelmät

Sopijapuoli

- Tilaaja ja toimittaja

Tietojärjestelmä

- Tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä, jota käytetään yhtenäisen ja pysyväisluonteisen tietojenkäsittelykokonaisuuden suorittamiseen. Tässä liitteessä tietojärjestelmällä tarkoitetaan myös ohjelmistoa, sovellusta, tietoteknistä tai muuta laitetta, johon hankinta kohdistuu.

Palvelu:

- Toimittajan tarjoamaa organisoidun toiminnan tuloksena syntyvää aineetonta hyödykettä, joka kulutetaan tai koetaan tilaajan tai tilaussopimuksen mukaisen tahon toimesta.

Sopimuksen kohde:

- Pääsopimuksen kohteena olevaa tietojärjestelmää tai palvelua.

Tilaajan aineisto

- Tilaajalle kuuluvia tai tilaajan käsittelemiä tietoja.

Tietoturva; tietoturvallisuus

- järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus

- Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa.

Tilaajan aineisto:

- Palvelun tai tuotteen toimituksen yhteydessä käytettäviä tai niihin sisältyviä tilaajan asiakirjoja, kirjallisia tietoja, tietokantoja, ohjelmistoja sekä muuta aineistoa, joka on luovutettu toimittajalle tietojärjestelmän tai palvelun tuottamista varten, tai jota toimittaja luo tietojärjestelmän tai palvelun tuottamiseksi.

Tietoturvahäiriö; tietoturvapoikkeama:

- yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti

Tietoturvatapahtuma; tietoturvallisuustapahtuma:

- tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan

Tietoturvahäiriön hallinta; tietoturvapoikkeaman hallinta:

- toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi

B. Tietoturvahäiriöiden luokittelu

Tietoturvahäiriöt tai tietoturvatapahtumat käsitellään niiden vakavuuden vaatimalla tavalla. Pelkkä CVSS-pistemäärä ei määritä tietoturvahäiriön vakavuutta, vaan tilaaja arvioi häiriöstä tai tapahtumasta aiheutuvan riskin omassa ict-ympäristössään. Korjaavat toimenpiteet sovitaan tapauskohtaisesti häiriön vakavuuden mukaisesti. Tässä kohdassa CVSS-pistemäärällä tarkoitetaan first.org:in julkaisemaa uusinta voimassa olevaa CVSS-pisteytystä (Common Vulnerability Scoring System).

<u>Kriittinen tietoturvahäiriö</u>

- Haavoittuvuus, jonka CVSS-luokitus on 7.0–10.0

- Tai sellainen tietoturvahaavoittuvuus tai tapahtuma mikä aiheuttaa korkean riskin tai korkeita riskejä tilaajan Euroopan Unionin yleisen tietosuoja-asetuksen 2016/679 mukaisten tilaajan Rekisteröityjen oikeuksille

- Toimittaja aloittaa toimenpiteet välittömästi (viimeistään seuraavana arkipäivänä havainnosta) tietoturvahäiriön tai tapahtuman poistamiseksi yhteistyössä tilaajan kanssa.

Vakava tietoturvahäiriö

- Haavoittuvuus, jonka CVSS-luokitus on 4.0–6.9
- Tai sellainen tietoturvahaavoittuvuus tai tapahtuma mikä aiheuttaa riskin tai riskejä Euroopan Unionin yleisen tietosuoja-asetuksen 2016/679 mukaisten tilaajan Rekisteröityjen oikeuksille
- Toimittaja aloittaa toimenpiteet tietoturvahäiriön tai tapahtuman poistamiseksi neljäntoista vuorokauden kuluessa sen havaitsemisesta yhteisyössä tilaajan kanssa.

Matala tietoturvahäiriö

- Haavoittuvuus, jonka CVSS-luokitus on 0.1–3.9
- Tai sellainen tietoturvahäiriö tai tapahtuma mistä aiheutuu vähäistä riskiä tai ei riskiä ollenkaan tilaajan Euroopan Unionin yleisen tietosuoja-asetuksen 2016/679 mukaisten tilaajan Rekisteröityjen oikeuksille
- Korjaukset toteutetaan tilaajan normaalin päivityssyklin mukaisesti.

C. Yleiset vaatimukset

1. Tässä liitteessä toimittajalle ja toimittajan palveluksessa oleville henkilöille asetetut velvoitteet koskevat myös toimittajan alihankkijoita ja niiden palveluksessa olevia henkilöitä siltä osin kuin he osallistuvat sopimuksen kohteen toteuttamiseen. Toimittajan on tiedotettava alihankkijoille näistä velvoitteista, ja toimittaja vastaa siitä, että alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat niitä. Toimittaja vastaa käyttämänsä alihankkijan osuudesta kuten omastaan.

2. Sopijapuolet (tilaaja ja toimittaja) sitoutuvat noudattamaan tietoturvallisuudesta, tietosuojasta, julkisuudesta ja salassapidosta annettua lainsäädäntöä sekä lainsäädännön nojalla annettuja viranomaismääräyksiä. Sopimuksella ei voi poiketa lainsäädännön sopijapuolelle asettamista pakottavista velvoitteista.

3. Sopijapuolet (tilaaja ja toimittaja) vastaavat siitä, että sopimuksen mukaiset tehtävät tehdään huolellisesti ja ettei tilaajan aineiston tai luottamuksellisten tietojen luottamuksellisuus, saatavuus tai eheys vaarannu sopijapuolten henkilöstön huolimattomuuden, virheellisten työtapojen tai muun sopimuksen vastaisen toiminnan takia.

4. Toimittaja noudattaa tilaajan aineistoa käsitellessään laissa viranomaisten toiminnan julkisuudesta (621/1999) tarkoitettua hyvää tiedonhallintatapaa, laissa julkisen hallinnon tiedonhallinnasta (906/2019) ja tietosuojalain (1050/2018) edellyttämää hyvää tietojen käsittelytapaa, muuta tietojen suojaamista ja tietosuojaa koskevaa lainsäädäntöä sekä tilaajan antamia kohtuullisia ohjeita. Jos toimittaja laatii tai käsittelee sopimuksen perusteella potilasasiakirjoja, toimittaja sitoutuu laatimaan ne ja käsittelemään niitä siten kuin potilasasiakirjojen laatimisesta on erikseen säädetty ja tilaaja rekisterinpitäjänä ohjeistaa. Myös muun muassa toimittajan laatimat potilasasiakirjat ovat tilaajan aineistoa.

5. Tilaajan aineistoa koskevia ehtoja sovelletaan pääsopimuksen päättymisestä huolimatta niin kauan kuin toimittajalla on hallussaan tilaajan aineistoa.

6. Toimittaja saa käyttää tilaajan aineistoa vain sopimuksen kohteen toteuttamiseen ja vain sopimuksen kohteen toteuttamisen edellyttämässä laajuudessa.

7. Toimittajan tulee huolehtia siitä, että tilaajan aineistoa käsittelevät vain ne toimittajan lukuun työskentelevät henkilöt, joiden työtehtäviin tilaajan aineiston käsittely kuuluu.

8. Toimittajan tilaajalle tuottamassa palvelussa tai tuotteessa säilytettävä, siirrettävä ja käsiteltävä tieto on tilaajan omistamaa, ellei toisin sovita.

9. Tilaajalla on oikeus määritellä tilaajan aineistolle eri tietoturvallisuustasoja ja sen mukaisia erityisiä tietoturvatoimenpiteitä ja ohjeita. Toimittaja käsittelee tilaajan aineistoa sen tietoturvallisuustason edellyttämällä tavalla. Tietoturvatoimenpiteiden ja ohjeistuksien noudattamiselle sovitaan tarvittaessa siirtymäaika, jotta toimittajalla on tosiasiallinen mahdollisuus noudattaa ohjeita.

10. Toimittajan tulee ohjata kolmansien osapuolten tekemät tilaajan aineistoa koskevat tietopyynnöt viipymättä tilaajalle.

11. Sopimuksen tai käyttötarpeen päättyessä toimittaja palauttaa ajan tasalla olevan tilaajan aineiston tilaajalle 15 arkipäivän kuluessa tilaajan kirjallisesta pyynnöstä tietoaineiston avoimuusvaatimuksen mukaisesti. Tilaajan aineiston toimituksen yhteydessä toimittajan tulee niin ikään toimittaa datakuvaus, joka täyttää tietoaineiston avoimuusvaatimuksen. Toimittajalla ei ole oikeutta erillisveloitukseen tilaajan aineiston tai datakuvauksen toimittamisesta.

12. Tuotettavaan palveluun liittyvien salassa pidettävien tietojen tiedonsiirron tulee toimittajan toimesta tapahtua yleisessä tietoverkossa VPN-tunnelin avulla salattua tai muuten verrattain yhtä turvallisella suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä.

13. Toimittajalla on velvollisuus omalla kustannuksellaan tietoturvallisella tavalla hävittää mahdolliset jäljennökset tilaajan aineistosta sen jälkeen, kun tilaaja on kirjallisesti hyväksynyt tilaajan aineiston sopimuksen mukaisesti palautetuksi. Toimittaja tulee tilaajan pyynnöstä ilman erillisveloitusta esittää hävittämisestä kohtuullinen selvitys. Toimittajalla ei ole velvollisuutta hävittää aineistoa, jos toimittaja on velvollinen lain tai viranomaismääräyksen perusteella säilyttämään aineiston. Tietoturvallinen hävitystapa on standardin IEEE 2883-2022 ja ISO/IEC 21964 mukainen tai niihin verrattava, vähintään yhtä tietoturvallinen tapa.

14. Jos sopimuksen kohteena on järjestelmä ja se liitetään sopimuksen mukaan Kanta-palveluihin, toimittaja vastaa siitä, että järjestelmä ja toimittaja täyttävät Kanta-auditointikriteerit ja että toimittaja pitää lain sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) vaatiman tietoturvasuunnitelman ajan tasalla.

D. Käyttöoikeudet- ja valtuudet

15. Toimittajan on toteutettava sopimuksen kohde siten, että käyttöoikeudet tilaajan järjestelmiin ja tilaajan aineistoon sekä niihin liittyviin loki-, hallinta- ja konfiguraatiotietoihin annetaan vain henkilöille, jotka tarvitsevat näitä oikeuksia työtehtäviensä suorittamiseen.

16. Kaikilla toimittajan tai tilaajan tietoa sisältäviä järjestelmiä käyttävillä, ylläpitävillä ja operoivilla työntekijöillä tulee olla yksilöivä, vain henkilökohtaiseen käyttöön tarkoitettu käyttäjätunnus. Käyttäjien tunnistaminen on tehtävä asianmukaisesti ja yksilöivästi jokaisen sisäänkirjautumisen yhteydessä.

17. Toimittajan tulee kyetä toimittamaan asiakkaalle lista henkilöistä, joille on annettu järjestelmien pääkäyttöoikeudet. Pääkäyttöoikeudet tulee antaa ainoastaan sellaisille henkilöille, jotka tarvitsevat näitä oikeuksia työtehtävien suorittamiseen.

18. Toimittaja tulee kyetä toimittamaan asiakkaalle ajantasainen luettelo pyydettäessä vähintään seuraavista seikoista:
    a. kenellä on pääsy järjestelmään tai palveluun.
    b. mitkä käyttöoikeudet yksittäisellä henkilöllä on.
    c. millä perusteella oikeus on annettu.

19. Toimittaja ylläpitää ajantasaista luetteloa henkilöiden kulkuoikeuksista tiloihin, joissa on mahdollista päästä käsiksi tilaajan järjestelmiin tai tilaajan aineistoon ja toimittaa luettelon pyydettäessä.

20. Toimittajan tulee poistaa tarpeettomat käyttöoikeudet ja kulkuoikeudet viipymättä esimerkiksi henkilön poistuessa toimittajan tai alihankkijan palveluksesta tai henkilön työtehtävien muuttuessa. Toimittajan tulee lisäksi tarkistaa aktiiviset käyttöoikeudet säännöllisesti.

21. Tilaajalla on oikeus rajoittaa käyttäjän käyttöoikeuksia tai sulkea käyttäjätunnus, jos tilaajalla on esimerkiksi syytä epäillä, että käyttäjätunnus on kaapattu tai sitä käytetään vahingollisella tavalla.

22. Järjestelmä tai palvelu on toteutettava niin, että edellä mainitut ylläpitotoimet voidaan tehdä ohjeistetusti ja tarvittaessa välittömästi joko tilaajan pääkäyttäjän toimesta tai tilaajan palvelupyynnön perusteella.

E. Toimittajan ilmoitus- ja raportointivelvollisuus

23. Toimittajan on viipymättä ilmoitettava tilaajalle sellaisista toimittajan tietoon tulleista seikoista, jotka aiheuttavat, tai voivat aiheuttaa merkittäviä riskejä tilaajan aineiston luottamuksellisuudelle, eheydelle tai saatavuudelle.

    Velvollisuus koskee ainakin:
    a. toteutuneita tietoturvaloukkauksia.
    b. merkittäviä tietoturvariskejä.
    c. CVSS-luokittelun mukaisista tietojärjestelmähaavoittuvuuksista, joita ei voida paikata, tai ole suunniteltu paikattavan kohtuullisessa ajassa.
    d. palvelunestohyökkäyksiä sekä ainakin vastaavia poikkeamia, jotka ovat omiaan nostamaan riskiä tilaajan aineiston luottamuksellisuudelle, eheydelle ja saatavuudelle.
    e. toimittajan tulee ilmoittaa tilaajalle vastuuhenkilö, jolta asiassa saa lisätietoja.
    f. jos seikka liittyy henkilötietoihin, toimitaan siten kuin henkilötietojen käsittelystä on sovittu henkilötietojen käsittelyn ehdoissa.

24. Toimittajan on ilmoitettava tilaajalle tiedossaan olevat tai tietoonsa saamat sopimuksen kohteen tai sen toteutusteknologian tai komponentteja koskevat merkittävät tietoturvariskit sekä niiden korjausmahdollisuudet ja toimenpiteet, joilla tietoturvariskit voidaan minimoida. Merkittäviä tietoturvariskejä ovat ainakin kriittiset haavoittuvuudet, vanhentuneet salausmenetelmät- ja ohjelmistoversiot.

F. Hankittavaa palvelua koskevat erityisehdot

25. Toimittajan on:
    a. Tehtävä ilmoitus tilaajalle viipymättä tietoturvapoikkeamista, jotka aiheuttavat, tai voivat aiheuttaa merkittävän tietoturvariskin tilaajalle toimitettuun palveluun tai tilaajan aineistoille.

26. Tilaajalla on oikeus:
    a. Tarkastaa sopimuksen kohteena olevat palvelun tuottamiseen liittyvät tietoturva- tai tietosuojajärjestelyt. Ilmoitus tarkastuksesta on toimitettava vähintään 30 päivää ennen tarkastusta.

27. Tilaajalla on oikeus saada toimeksiantajalta kuvaus ja dokumentaatio palvelusta ja sen teknisistä toteutustavoista.

G. Toimittajaa, joka käyttää tilaajan järjestelmää, koskevat erityisehdot

28. Toimittajaan lukuun työskentelevät henkilöt, jotka käyttävät tilaajan tietojärjestelmää allekirjoittavat tilaajan salassapito- ja käyttäjäsitoumuksen. Toimittaja selvittää sitoumukseen liittyvät mahdolliset epäselvyydet tilaajan edustajalta.

H. Tietoturvaloukkaustilanteessa toimiminen sekä jatkuvuudenhallinta

29. Toimittajalla tulee olla kirjallinen ohjeistus tietoturvaloukkaustilanteissa toimimiseen, joka on annettu tiedoksi kaikille osallistuville työntekijöille.

30. Toimittaja huolehtii häiriötilanteiden hallinnasta sopimuksen mukaisesti siten, että ongelman rajaus ja korjaus suoritetaan pääsopimuksessa sovittujen aikamääreiden puitteissa ja sovittujen menettelytapojen mukaisesti. Mikäli pääsopimuksessa ei ole sovittu erillisiä aikamääreitä häiriötilanteiden hallintaa, sovelletaan tämän liitteen kohdan B. viitearvoja.

31. Toimittaja on velvollinen auttamaan tilaajaa tietoturvaloukkauksiin liittyvien vahinkojen minimoinnissa sekä asian selvittämisessä viranomaistahojen kanssa. Toimittaja sitoutuu avustamaan parhaan kykynsä mukaan viranomaisia tilatun tuotteen, järjestelmään tai palveluun kohdistuvan tietoturvatapahtuman tai -loukkauksen selvittämisessä viranomaisten pyynnöstä.

32. Toimittaja saa veloittaa tietoturvaloukkauksen sille aiheuttamasta lisätyöstä sopimuksen mukaisen hinnan, jos kaikki seuraavat edellytykset toteutuvat:
    a. tietoturvaloukkaus ei aiheudu toimittajan tai toimittajan alihankkijan, työntekijän tai harjoittelusuhteessa tai verrattavassa suhteessa toimittajaan olevan henkilön vastuulla olevasta syystä
    b. toimittajan virhe tai laiminlyönti ei ole myötävaikuttanut tietoturvaloukkauksen tapahtumiseen
    c. toimittajan toimenpiteet eivät sisälly mahdolliseen jatkuvan palvelun veloitukseen.

33. Tilaajan ja toimittajan yhteinen häiriönhallintaharjoitus voidaan toteuttaa kerran kahdessa vuodessa tilaajan pyynnöstä ilman lisäkustannuksia.

34. Toimittajalla on ennalta määrätty prosessi tuotettavaan palveluun liittyvän toimintaympäristön häiriöiden ja poikkeamien hallintaan.

35. Toimittaja ylläpitää kirjallista toipumissuunnitelmaa, joka kohdistuu tuotettavan palvelun ylläpitoon poikkeamatilanteessa. Toimittaja vastaa toipumissuunnitelman kehityksestä sekä vuosittaisesta päivityksestä ja testauksesta.

I. Salassapito

36. Toimittaja vastaa siitä, että toimittajan lukuun työskentelevät henkilöt, joilla voi olla pääsy tilaajan salassa pidettäviin tietoihin, ovat etukäteen allekirjoittaneet kirjallisen salassapitositoumuksen tai muutoin sitouttaneet työntekijät salassapitoon vähintään kohdan 37 seikkojen osalta. Toimittajan on tilaajan pyynnöstä esitettävä kyseinen salassapitositoumus tai sitouttamisen perusteet tilaajalle.

37. Toimittajan on huolehdittava siitä, että toimittajan lukuun työskentelevät henkilöt ovat tietoisia seuraavista seikoista ja ovat sitoutuneet niitä noudattamaan:
    a. Työntekijä saa käyttää tilaajan aineistoa vain työtehtäviensä mukaiseen tarkoitukseen ja vain siinä laajuudessa kuin työtehtävien hoitaminen edellyttää. Työntekijällä ei ole oikeutta käyttää tilaajan aineistoa muuhun kuin edellä mainittuun tarkoitukseen.
    b. Työntekijän on pidettävä tilaajan aineisto salassa, eikä sitä saa luovuttaa tai muulla tavalla paljastaa sivullisille.
    c. Salassapitovelvollisuus on voimassa pysyvästi, ellei kyseisen tiedon osalta salassapitovelvollisuuden kestoa ole laissa erikseen määrätty.
    d. Salassapitovelvollisuus koskettaa myös tilaajan viranomaisen julkista aineistoa siltä osin, kuin sitä tilaaja ei ole aineistoa saattanut julkisesti saataville.

e. Sivullisina pidetään muun muassa sellaisia toimittajan lukuun työskenteleviä henkilöitä, jotka eivät työtehtäviensä perusteella tarvitse tilaajan aineistoa tietoonsa.
f. Toimittajan työntekijän on ilmoitettava tietoonsa tulleista tietoturvaa tai tietosuojaa vaarantavista seikoista toimittajalle viipymättä.
g. Työntekijän tulee käsitellä tilaajan aineistoa sisältäviä asiakirjoja ja tallenteita huolellisesti ja riittävästä tietoturvasta huolehtien.
h. Tilaajan aineistoa sisältäviä asiakirjoja ei saa viedä pois tilaajan tai toimittajan toimitiloista, elleivät työntekijän työtehtävät sitä nimenomaisesti edellytä.
i. Työntekijän pitää palauttaa tai hävittää hallussaan olevat asiakirjat ja tallenteet luotettavasti ja riittävästä tietoturvasta huolehtien työtehtäviensä mukaisen käyttötarpeen päätyttyä.
j. Tietojärjestelmien käytöstä kertyy lokitietoa, jota käytetään viranomaisen lakisääteisten velvollisuuksien toteuttamiseen sekä tarvittaessa väärinkäytösten selvittämiseen ja asiakastietolain mukaisten tietopyyntöjen toteuttamiseen.
k. Salassapitovelvollisuuden rikkominen saattaa aiheuttaa työntekijälle lainsäädännön mukaisen henkilökohtaisen vastuun.

38. Sopijapuolet pitävät toisiltaan saamansa luottamukselliset tiedot salassa eivätkä käytä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin ja sopimuksen edellyttämässä laajuudessa. Tilaajalla on kuitenkin velvollisuus noudattaa viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisia velvoitteita.

39. Salassapitovelvollisuus ei koske tietoa, joka on yleisesti saatavilla tai julkista tai jonka sopijapuoli on saanut laillisesti haltuunsa muuten kuin toiselta sopijapuolelta eikä jokin muu syy edellytä tiedon salassapitoa.

40. Sopijapuoli palauttaa tai toisen sopijapuolen suostumuksella hävittää tietoturvallisesti toisen sopijapuolen luottamuksellisen aineiston sopimuksen tai käyttötarpeen päättyessä. Aineistoa ei saa hävittää, jos laki tai viranomaisten määräykset vaativat säilyttämistä. Aineisto on hävitettävä kohdan 12 mukaisia standardeja noudattaen.

J. Muutoshallinta

41. Toimittaja ei saa tehdä sopimuksen kohteena olevaan järjestelmään, laitteeseen tai palveluun sellaista muutosta, mistä aiheutuu merkittävä tietoturvariski tilaajan aineistolle, ellei siitä ole kirjallisesti etukäteen sovittu sopijapuolten kesken.

42. Toimenpiteet, jotka vaikuttavat sopimuksen kohteen tai tilaajan järjestelmien tietoturvallisuuteen, on tehtävä tavalla, jolla turvallisuusriskit ovat hallinnassa.

K. Turvallisuusselvitys

43. Tilaaja voi edellyttää turvallisuusselvityslain (726/2014) mukaisen turvallisuusselvityksen, tai tasoltaan vastaavan ulkomaisen turvallisuusselvityksen teettämistä toimittajan lukuun työskentelevistä henkilöistä, joilla saattaa olla pääsy tilaajan salassa pidettäviin tietoihin. Toimittaja vastaa turvallisuusselvityksen kohteena olevan henkilön suostumuksen hankkimisesta ja siitä, että henkilö antaa turvallisuusselvityksen teettämiseksi tarvittavat tiedot. Mikäli turvallisuusselvityksen kohteena oleva henkilö kieltäytyy selvityksestä tai turvallisuusselvityksessä ilmenee seikkoja, joilla on oleellinen vaikutus tilaajan tietojen, omaisuuden tai muiden rinnastettavien seikkojen turvallisuuteen, toimittajan tulee tarjota tilalle toinen henkilö, jolla on vastaava kokemus ja pätevyys.

44. Tilaajalla voi edellyttää turvallisuusselvityslain (726/2014) mukaista yritysturvallisuusselvitystä toimittajalta tai toimittajan lukuun toimivalta turvallisuusselvityslain 1. luvun 3 § 6 kohdan mukaiselta toimijalta. Mikäli yritysturvallisuusselvityksen kohde kieltäytyy selvityksestä tai yritysturvallisuusselvityksessä ilmenee seikkoja, joilla on oleellinen vaikutus tilaajan tietojen, omaisuuden tai muiden rinnastettavien seikkojen turvallisuuteen, toimittajan tulee järjestää toiminta siten, että yritysturvallisuusselvityksen kohteena olevalla taholla ei ole pääsyä tilaajan tietoihin, omaisuuteen tai muihin niihin rinnastettaviin kohteisiin.

45. Sopijapuoli vastaa itse kustannuksista, joita turvallisuusselvityksen teettämisestä sille aiheutuu. Tilaaja maksaa turvallisuusselvityksen teettämiseen liittyvät viranomaismaksut. Jos turvallisuusselvitys tulee uudelleen tehtäväksi sen vuoksi, että toimittajan henkilöstössä tapahtuu tilaajasta riippumaton muutos, toimittaja vastaa uuden henkilön turvallisuusselvityksen teettämisen kustannuksista.

L. Sopimuksen muuttaminen ja lisätyö

46. Tietoturvallisuuteen liittyvän lainsäädännön, tai sen tulkintaa koskevien suositusten, ohjeistusten tai määräysten muuttuessa, sopijapuolet tekevät tarpeelliset sopimusmuutokset. Toimittaja on velvollinen toteuttamaan tietoturvallisuuteen liittyvän lainsäädännön, tai sen tulkintaa koskevien suositusten, ohjeistusten tai määräysten mukaisten muutokset sopimuksen kohteena olevaan palveluun tai järjestelmään.

47. Liitettä 1 Yhteystiedot voidaan päivittää tarpeen mukaan ilman pääsopimuksen tai sen liitteiden uudelleen allekirjoittamista.

Pohde
Pohjois-Pohjanmaan hyvinvointialue

Tietohallinto 19.12.2025

LIITE 1 Yhteystiedot

TILAAJA			TOIMITTAJA		
Nimi ja tehtävä	Puhelinnumero	Sähköposti	Nimi ja tehtävä	Puhelinnumero	Sähköposti