
TIETOTURVALLISSUUSSOPIMUS

Liite 1: SOPIMUS POHJANMAAN HYVINVOINTIALUEEN JA KUNTIEN VÄLISESTÄ
LIIKUNTANEUVONNAN PALVELUKETJUN TOTEUTTAMISESTA

Sisällysluettelo

1. OSAPUOLET	2
2. MÄÄRITELMÄT	2
3. TAUSTA JA TARKOITUS.....	3
4. TIETOTURVALLISUUDEN HALLINTA	4
5. TIETOAINESTOJEN KÄSITTELY	4
6. PÄÄSY TIETOJÄRJESTELMIIN JA TIETOIHIN	4
7. LOKITIEDOT	5
8. TIETOSUOJA.....	5
9. SELOSTE KÄSITTELYTOIMISTA	5
10. OHJE HENKILÖTIETOJEN TIETOTURVALOUKKAUKSIEN SELVITTÄMISESTÄ.....	6
11. SALASSAPITO JA HUOMIOON OTETTAVA LAINSÄÄDÄNTÖ.....	7
12. MUUT OIKEUDET JA VELVOLLISUUDET	8
13. SEURAAMUKSET	9
14. ALIHANKKIJAT	9
15. RAPORTOINTI.....	9
16. VOIMAAN JÄÄVÄT EHDOT	9
17. SOPIMUKSEN VOIMASSAOLO	10
18. ALLEKIRJOITUKSET.....	10

1. OSAPUOLET

Pohjanmaan Hyvinvointialue (Myöhemmin "Tilaaaja" tai "Osapuoli")

Y-tunnus: 3221324-6

Osoite: PL 101, 65101 Vaasa

Kunta:

Y-tunnus:

Osoite:

2. MÄÄRITELMÄT

"Alihankkija" tarkoittaa mitä tahansa Palvelun tuottamiseen tai yhteistyöhön muuten osallistuvaa osapuolta, jota Toimittaja käyttää omien velvoitteidensa täyttämiseksi.

Henkilötietojen käsittely tarkoittaa Tietosuoja-asetuksen 4 artiklan mukaisesti toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, tietojen luovuttamista, siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

"Henkilötietojen tietoturvaloukkaus" (Personal Data Breach) tarkoittaa tietosuoja-asetuksen 14 artiklan 12) kohdan mukaan Tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

"Palvelu" tarkoittaa Palvelua, josta Osapuolet ovat Pääsopimuksessa sopineet.

"Pääsopimus" tarkoittaa Tilaaajan ja Toimittajan välistä sopimusta, jonka liitteenä tämä Tietoturvallisuussopimus-dokumentti on.

"Tietoaineisto" tarkoittaa tähän Palveluun liittyvää Tilaaajan asiakirjoista ja muista tiedoista muodostuvaa tietokokonaisuutta.

"Tietojärjestelmä" tarkoittaa tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä.

Tietosuoja-asetus: tarkoittaa Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

”Tietosuojalainsäädäntö” tarkoittaa, rajoituksetta ja soveltuvin osin, kaikkea kulloinkin voimassa olevaa henkilötietojen suojaan liittyvää EU-lainsäädäntöä ja kansallista lainsäädäntöä, kuten EU:n yleistä tietosuoja-asetusta (TSA, 679/2016) sekä kansallista tietosuojalakia (1050/2018).

”Tietoturvatapahtuma” on yksittäinen tapahtuma, joka saattaa vaikuttaa tietoturvaan

”Tietoturvapoikkeama” tai **”Tietoturvahäiriö”** on yksi tai useampi tietoturvatapahtuma, vaarantaen tietoturvan ja vaikuttaen organisaation toimintaan

”Tietoturvaloukkaus” oikeudeton puuttuminen tietoon.

”Tilaja” osapuoli (Pohjanmaan hyvinvointialue), joka asettaa vaatimukset ja hyväksyy niiden täyttymisen.

”Tilaajan aineisto” tai **”Tilaajan tieto”** tarkoittaa kaikkea Tilaajan luovuttamaa tai toisen osapuolen laatimaa tietoa, joka liittyy hankinnan kohteena olevan palvelun tuottamiseen.

”Tilat” tarkoittavat sellaisia Toimittajan tai sen Alihankkijan tiloja, joissa säilytetään tai muutoin käsitellään Tietoaineistoja.

Sopimukseen sovelletaan lisäksi EU:n yleisen tietosuoja-asetuksen (2016/679, myös TSA) ja Pääsopimuksen määritelmiä.

3. TAUSTA JA TARKOITUS

Tässä Tietoturvallisuussopimuksessa sovitaan Pääsopimuksen kohteen mukaisen Palvelun tietoturvallisuuteen, tiedonhallintaan, tietosuojaan ja salassapitoon liittyvät periaatteet, toimintatavat ja ehdot, joita Osapuolet soveltavat Pääsopimuksen voimassaoloaikana tai soveltuvin osin sen jälkeen. Ehtoja sovelletaan Pääsopimuksen sisältämien Palveluiden tuottamisessa sekä kaikessa Sopimukseen liittyvässä Osapuolten välisessä yhteistyössä.

Jos toisin ei ole sovittu, ovat tämän Sopimuksen yhteyshenkilöt samat kuin Pääsopimuksella.

4. TIETOTURVALLISUUDEN HALLINTA

Osapuolella (kunta) on ylimmän johdon hyväksymät tietoturvallisuusperiaatteet, jotka kuvaavat tietoturvaluustoimenpiteiden kytkeytymisen organisaation toimintaan. Tietoturvallisuuden hoitamiseen liittyvät tehtävät ja vastuut on määritelty sekä henkilöstölle järjestetään säännöllisesti tietoturvaluuskoulutusta. Tietoturvaluuteen liittyvien poikkeamatilanteiden käsittelyyn on määritelty prosessit ja toimintaohjeet.

5. TIETOAINEISTOJEN KÄSITTELY

Tässä Tietoturvaluussopimuksessa kuvattuja järjestelyjä noudatetaan aina käsitellessä Tilaajaan, Pääsopimuksen Palvelun tuottamiseen liittyvää tai muuta Tilaajalta saatua Tietoaaineistoa. Tietoaaineistoja käsitellään vain Palvelun tuottamisen edellyttämässä laajuudessa.

Tilaajan tietoja annetaan vain niille henkilöille, jotka tarvitsevat tietoja Palvelun tuottamiseen liittyvissä työtehtävissään. Osapuolen (kunta) tulee pystyä osoittamaan, että sen Palvelun tuottamiseen osallistuvat henkilöt ovat tietoisia tämän Sopimuksen mukaisista vaatimuksista ja vaitiolovelvollisuudesta. Tilaajan pyynnöstä toimitetaan selvitys tämän kohdan mukaisen velvollisuuden täyttämisestä.

Sopimuksen päättyttyä Tilaajan Tietoaaineisto palautetaan yleisesti käytössä olevassa muodossa tai Tietoaaineisto tuhoetaan siten, ettei tietoja ole enää mahdollista palauttaa luettavaan muotoon. Osapuolella (kunta) on oikeus säilyttää tietoaaineistoja säädösten ja viranomaismääräysten edellyttämällä tavalla.

6. PÄÄSY TIETOJÄRJESTELMIIN JA TIETOIHIN

Osapuolen (kunta) ja sen Alihankkijan Tilojen tulee olla asianmukaisesti suojattu siten, etteivät ulkopuoliset pääse käsiksi Tilaajan tietoihin.

Osapuolen (kunta) tulee huolehtia sille annetuista salasanoista, tunnistautumisvälineistä ja pääsystä Tilaajan hallinnassa oleviin tietojärjestelmiin, verkkoihin tai sähköisiin ratkaisuihin siten, että vain niillä henkilöillä on pääsy näihin käsiksi, joiden Tilaajan kanssa solmitun Sopimuksen mukaiset tehtävät välttämättä tätä edellyttävät. Tilaajan luovuttamia tunnuksia käytetään vain niihin tarkoituksiin, joita Tilaajalle suorittaman Palvelun mukaiset tehtävät edellyttävät. Tilaajan järjestelmiin ei saa liittyä muutoin, kuin erikseen Tilaajan tälle osoittamin henkilökohtaisin tunnuksin ja/tai tunnistautumisvälinein.

7. LOKITIEDOT

Lokitiedot ovat Tilaajan aineistoa siltä osin kuin lokituksen kohteena on Tilaajan aineiston käsittely tai luovuttaminen. Mikäli lokitiedot sisältävät henkilötietoja, lokitietojen käsittelyyn sovelletaan Tietolainsäädäntöä. Siltä osin kuin lainsäädännössä tai viranomaismääräyksissä on säädetty lokitietojen käsittelystä, sovelletaan ensisijaisesti kyseisiä säädöksiä ja viranomaismääräyksiä.

Lokitiedot ovat viranomaisen toiminnan julkisuudesta annetun lain (621/1999) 24 § 1 mom 7 kohdan 24 §:n mukaisesti salassa pidettäviä.

8. TIETOSUOJA

Toimittajan tulee kaikessa Pääsopimuksen mukaisten velvoitteidensa täyttämisessä noudattaa voimassa olevaa Tietosuojalainsäädäntöä.

Osapuolet vastaavat siitä, että Pääsopimuksen mukainen Palvelu on kulloinkin voimassa olevan Tietosuojalainsäädännön vaatimusten mukainen, ottaen erityisesti huomioon oletusarvoisen ja sisäänrakennetun tietosuojan periaatteet. Osapuolet huolehtivat käsittelemiensä tietojen asianmukaisesta suojaamisesta varmistaakseen Tilaajan aineiston luottamuksellisuuden, eheyden ja saatavuuden.

Selvyyden vuoksi todetaan, että tässä Sopimuksessa mainittu Tilaaja on Pääsopimuksen mukaista Palvelua koskevien henkilötietojen osalta tietosuoja-asetuksessa tarkoitettu Rekisterinpitäjä ja Osapuoli (kunta) Henkilötietojen käsittelijä.

Henkilötietojen käsittelijän tulee avustaa Rekisterinpitäjää varmistamaan, että tietosuoja-asetuksen 3 luvussa sekä 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan. Henkilötietojen käsittelijän tulee esimerkiksi avustaa Rekisterinpitäjää tietosuoja-asetuksen 33 ja 34 artiklan edellyttämien ilmoitusten tekemisessä tietosuoja-asetuksen mukaisessa määräajassa valvontaviranomaiselle ja rekisteröidylle. Henkilötietojen käsittelijän tulee myös pyynnöstä tehdä tietosuoja-asetuksen 31 artiklan mukaista yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.

9. SELOSTE KÄSITTELYTOIMISTA

Henkilötietojen käsittelijä ylläpitää tietosuoja-asetuksen 30 artiklan mukaista sähköistä selostetta Sopimuksen perusteella Rekisterinpitäjän lukuun suorittamastaan henkilötietojen käsittelystä.

Henkilötietojen käsittelijän selosteen tulee sisältää vähintään seuraavat tiedot:

1. Rekisterinpitäjän ja sen tietosuojavastaavan nimi ja yhteystiedot;
2. Henkilötietojen käsittelijän ja sen tietosuojavastaavan nimi ja yhteystiedot;
3. kuvaus Henkilötietojen käsittelijän Rekisterinpitäjän lukuun käsittelemistä rekisteröityjen ryhmistä ja henkilötietoryhmistä;
4. tiedot mahdollisista henkilötietojen siirroista EU- tai ETA-alueen ulkopuolelle;
5. lista henkilötietojen käsittelyssä käytetyistä alikäsittelijöistä; sekä
6. kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista toimenpiteistä.

Rekisterinpitäjä ja Henkilötietojen käsittelijä käyvät edellä mainittua selostetta yhdessä läpi tarvittaessa.

10. OHJE HENKILÖTIETOJEN TIETOTURVALOUKKAUKSIEN SELVITTÄMISESTÄ

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. Henkilötietojen käsittelijän tulee ilmoittaa kirjallisesti tietoturvaloukkauksesta Rekisterinpitäjälle (Pohjanmaan hyvinvointialue) ilman aiheetonta viivytystä saatuaan sen tietoonsa ja 36 h määräajassa, jollei ole erikseen sovittu, että Henkilötietojen käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan valvontaviranomaiselle asetuksen edellyttämällä tavalla. Vastuu ilmoitusvelvollisuuden toteuttamisesta säilyy kuitenkin Rekisterinpitäjällä.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt USB-tikku, varastettu tietokone, hakkerointi, haittaohjelmatartunta, arkaluontoisia henkilötietoja löytyy roskalavalta, kyberhyökkäys, tulipalo datakeskuksessa tai henkilötietoja sisältävän kirjeen postitus väärälle henkilölle.

11. SALASSAPITO JA HUOMIOON OTETTAVA LAINSÄÄDÄNTÖ

Tietojen käsittelyoikeus koskee vain työtehtävien edellyttämiä tietoja. Henkilötietojen käsittely perustuu aina Pääsopimukseen tai toimeksiantoon. Henkilötietoja ei saa käsitellä muuhun kuin laissa tai Pääsopimuksessa määriteltynä käyttötarkoitukseen.

Pääsopimuksen taikka toimeksiantosuhteen aikana tai sen päätyttyä sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja Pohjanmaan hyvinvointialuetta tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia lain mukaan salassa pidettäviä tai muuten vaitiolovelvollisuuden piirissä olevia tietoja. Tällaisia tietoja ovat mm. Pohjanmaan hyvinvointialueen ja sen sopimustoimittajien liikesalaisuudet, kaikki arkaluonteiset ja erityisiä henkilötietoryhmiä koskevat henkilötiedot sekä mahdollisesti tietoon tulleet käyttäjien sähköpostien sisällöt, lokitiedot tms. Näitä tietoja ei saa väärinkäyttää tai jättää paikkaan, jossa ne ovat sivullisten nähtävillä tai saatavilla.

Hyvinvointialueen ulkopuolinen taho, jolla on Pohjanmaan hyvinvointialueen kanssa tehtyyn Pääsopimukseen perustuva pääsy hyvinvointialueen tietojärjestelmiin ja/tai salassa pidettävään tietoon, noudattaa tätä Sopimusta ja laissa säädettyjä kulloinkin voimassa olevia vaitiolovelvollisuus- ja hyväksikäyttökieltosäännöksiä sekä muita salassapitoa, tietosuojaa ja tietoturvaa koskevia säännöksiä. Näitä säännöksiä on erityisesti seuraavissa laeissa ja määräyksissä:

- EU yleinen tietosuojasetus (2016/679)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Tietosuojalaki (1050/2018)
- Tiedonhallintalaki (906/2019)
- Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023), lisäksi
 - THL määräys 3/2024
 - THL määräys 4/2024
 - THL määräys 5/2024
- Liikesalaisuuslaki (595/2018)
- Laki sähköisen viestinnän palveluista (917/2014)
- Rikoslaki, 38 luku (39/1889)
- Tekijänoikeuslaki (404/1961)
- Lakiammatillisesta koulutuksesta (531/2017)
- Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
- Laki vesi- ja energiahuollon, liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja käyttöoikeussopimuksista (1398/2016)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki potilaan asemasta ja oikeuksista (785/1992)

- Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018)
- Turvallisuusluokitteluasetus (1011/2019)
- Varhaiskasvatuslaki (540/2018)

Selvyyden vuoksi todetaan, että em. lakien osalta toimitaan vain soveltuvilta osin eli huomioiden yhteistyön luonne.

12. MUUT OIKEUDET JA VELVOLLISUUDET

- Tietojärjestelmää saa käyttää vain henkilökohtaisella käyttäjätunnuksella.
- Tietojärjestelmän käyttö on rajattu liikuntaneuvojan erilliselle välilehdelle
- Tietojärjestelmään pääsee erillisellä virtuaalityöpöytäratkaisulla (Citrix), jossa käytetään kaksivaiheista tunnistautumista
- Tunnistautumisen tulee tapahtua Tilaajan hyväksymällä vahvalla tunnistautumisella.
- Tilaajan erillisellä luvalla vahvasta tunnistautumisesta voidaan poiketa.
- Jokainen työntekijä vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja toimenpiteistä.
- Käyttäjätunnusta ja salasanaa ei saa antaa muiden tietoon.
- Käyttöoikeuksiin liittyvissä tehtävissä lokitietoja on käsiteltävä siten, ettei yksityisyyden suoja tai tietosuojaa miltään osin vaarannu.
- Tietojärjestelmien käyttöä seurataan ja niiden käytöstä kertyy lokitietoja.
- Ylläpitäjä saattaa ylläpitotehtäviä hoitaessaan saada tietoja viesteistä ja tunnistamistiedoista. Viestin sisältöä tai tietoa viestin olemassaolosta ei saa ilmaista muille tai käyttää hyväksi ilman viestinnän osapuolen suostumusta, ellei laissa toisin säädetä.
- Ylläpitäjällä on oikeus tutustua tai muulla tavoin puuttua käyttäjien verkkoliikenteen sisältöön ja tiedostoihin ilman käyttäjältä saatua lupaa vain Palvelun toteuttamiseksi tai käyttämiseksi ja tietoturvasta huolehtimiseksi, viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi, väärinkäytösten havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi.
- Sopimussuhteen päättyessä kaikki Pohjanmaan hyvinvointialuetta tai sen asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevat tiedot tai asiakirjat ja tietovälineet sekä niiden mahdolliset kopiot luovutetaan Pohjanmaan hyvinvointialueelle, ellei lainsäädännöstä muuta johdu tai asiasta muuta sovita.
- Kun tiedot tai asiakirjat on luovutettu Pohjanmaan hyvinvointialueelle ja Pohjanmaan hyvinvointialueen osalta luovutus on hyväksytty, Henkilötietojen käsittelijän on hävitettävä kaikki omat kappaleensa, ellei lainsäädännöstä muuta johdu, tiedoista ja asiakirjoista tietokannoistaan ja muista tietovälineistä todennetusti siten, että Pohjanmaan hyvinvointialue on sen hyväksynyt.

13. SEURAAMUKSET

Sääntöjen ja periaatteiden rikkomisesta tietojärjestelmien käyttöoikeudet voidaan peruuttaa. Rikkomuksista tiedotetaan aina sopimusosapuolelle ja ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli rikkomuksesta aiheutuu välitöntä tai välillistä taloudellista vahinkoa tai henkilötietojen vuotoja, sovelletaan Sopimuksen mukaisia oikeussuojakeinoja. Tietojen väärinkäyttö voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

14. ALIHANKKIJAT

Mitä tässä liitteessä on sovittu henkilöstöstä, sovelletaan myös Alihankkijan Palvelun tuottamiseen osallistuvaan henkilöstöön. Alihankkijan tulee toimia tämän liitteen vaatimusten mukaisesti. Tilaajan pyynnöstä tulee toimittaa selvitys tämän kohdan mukaisen velvollisuuden täyttämisestä.

15. RAPORTOINTI

Osapuolen (kunta) on ilmoitettava Tilaajalle välittömästi, jos sen keskeisissä turvallisuustoiminnoissa tai henkilöstö- tai turvallisuusjärjestelyissä tapahtuu muutoksia. Tämän Sopimuksen ehtojen toteutumista toiminnassa valvotaan säännöllisesti, mahdolliset poikkeamat kirjataan ja merkittävistä poikkeamista raportoidaan Tilaajalle viivytyksettä sekä aloitetaan korjaustoimet ensi tilassa.

Osapuoli (kunta) toimittaa Tilaajan pyynnöstä selvityksen tämän Tietoturvasopimuksen mukaisten velvollisuuksien täyttämisestä.

16. VOIMAAN JÄÄVÄT EHDOT

Sopimuksen ehdot ovat voimassa viisi (5) vuotta Pääsopimuksen päättymisen jälkeen, ellei lainsäädännöstä muuta johdu.

Sopimuksen salassapitoa koskevat ehdot jatkuvat Sopimuksen päättymisen jälkeen pysyvästi.

17. SOPIMUKSEN VOIMASSAOLO

Sopimuksen voimassaolo on Pääsopimuksen mukainen.

18. ALLEKIRJOITUKSET

Sopimus on allekirjoitettu sähköisesti Pääsopimuksen yhteydessä.