

TIETOSUOJA - JA TIETOTURVALIITE

1 JOHDANTO

Tämä henkilötietojen käsittelysopimus ("Liite") on erottamaton osa **Pirkanmaan Voimia Oy:n, y-tunnus 2938704-2 ("Palveluntarjoaja")** ja **Vesilahden kunta 0157711-9 ("Rekisterinpitäjä")** välillä olevaa sopimusta 'Ruokapalvelusopimus koulu- ja päiväkotiruoan toimittamisesta Vesilahden kunnalle' ja sen mukaisia tai liitteenä olevia sopimusehtoja ("**Sopimus**").

Tämän Liitteen tarkoituksena on sopia Rekisterinpitäjän henkilötietojen tietosuojasta ja tietoturvasta Palveluntarjoajan palveluissa sen käsitellessä Rekisterinpitäjän henkilötietoja. Tämä Liite muodostaa osapuolten välille EU:n yleisen tietosuoja-asetuksen ("**GDPR**", (EU) 679/2016) mukaisen kirjallisen sopimuksen henkilötietojen käsittelystä.

Jos tämän Liitteen ja Sopimuksen henkilötietojen käsittelyä koskevat ehdot ovat ristiriidassa keskenään, osapuolet soveltavat ensisijaisesti tämän Liitteen ehtoja.

2 MÄÄRITELMÄT

Tässä Liitteessä tarkoitetaan GDPR:n ja soveltuvan tietosuojalainsäädännön mukaisesti

"Rekisterinpitäjällä" sitä, joka määrittelee Henkilötietojen Käsittelyn tarkoitukset ja keinot ja joka voi olla tässä Liitteessä määritelty Rekisterinpitäjä tai Rekisterinpitäjän toimeksiantaja.

"Käsittelijällä" Palveluntarjoajaa, joka Käsittelee Henkilötietoja Rekisterinpitäjän lukuun Sopimuksen perusteella.

"Käsittelyllä" ja **"Käsittelytoimilla"** 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, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

"Henkilötiedoilla" kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä **"Rekisteröityyn"**, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

"Henkilötietojen tietoturvaloukkauksella" tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten Käsiteltyjen Henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

3 HENKILÖTIETOJEN KÄSITTELY

3.1 Palveluntarjoajan ja Rekisterinpitäjän vastuut

Palveluntarjoaja Käsittelee Rekisterinpitäjän Henkilötietoja Rekisterinpitäjän lukuun ja tämän toimeksiannosta Sopimuksen perusteella. Palveluntarjoaja saa käsitellä henkilötietoja vain Rekisterinpitäjän tässä Liitteessä tai muutoin antamien kirjallisten ohjeiden mukaisesti ja tietosuojalainsäädännön edellyttämin tavoin. Rekisterinpitäjä tai tämän toimeksiantaja on palvelussa Käsiteltävien Henkilötietojen Rekisterinpitäjä ja Palveluntarjoaja Käsitteijä.

Osapuolet sitoutuvat noudattamaan Suomessa ja Euroopan unionissa kulloinkin voimassa olevaa Henkilötietojen Käsitelyä koskevaa lainsäädäntöä, asetuksia sekä viranomaisten määräyksiä ja ohjeistuksia ja tarvittaessa muuttamaan tämän Liitteen ehtoja niiden mukaiseksi.

Rekisterinpitäjä on vastuussa siitä, että sillä on tarvittavat oikeudet ja suostumukset Sopimuksen mukaiseen Henkilötietojen Käsitelyyn. Rekisterinpitäjä vastaa tietosuojaselosteen laatimisesta ja saatavilla pidosta sekä Rekisteröityjen informoinnista ja ilmoituksista tietosuojaviranomaisille. Rekisterinpitäjä vastaa Palveluntarjoajalle antamiensa Henkilötietojen oikeellisuudesta.

Rekisterinpitäjällä on oikeus ja velvollisuus määrittää Henkilötietojen tyypit ja rekisteröityjen ryhmät sekä Henkilötietojen Käsitelyn tarkoitus ja keinot. Nämä on määritelty tämän Liitteen alaliitteessä 1. Alaliitteen 1 tietoja on voitu täsmentää Sopimuksessa ja/tai muissa osapuolten välisissä sopimusasiakirjoissa.

Palveluntarjoajalla on oikeus Käsitellä Rekisterinpitäjän Henkilötietoja ja muita Rekisterinpitäjän tietoja vain Sopimuksen ja tämän Liitteen mukaisesti ja vain siltä osin ja siten kuin on tarpeellista palveluiden toimittamiseksi.

Palveluntarjoaja ylläpitää palvelun kuvausta tai muuta GDPR:n vaatimaa selostetta palvelussa suoritettavista Käsitelytoimista.

Rekisterinpitäjä voi antaa Palveluntarjoajalle tarvittaessa tarkentavia ohjeita kirjallisesti ja Palveluntarjoaja on velvollinen niitä noudattamaan. Rekisterinpitäjällä on oikeus muuttaa ohjeita tarvittaessa. Palveluntarjoajalla on oikeus laskuttaa muutoksista aiheutuvat kohtuulliset kustannukset Rekisterinpitäjältä.

3.2 Alihankkijat, jotka osallistuvat henkilötietojen käsittelyyn

Palveluntarjoaja saa yleisen kirjallisen ennakkoluvan käyttää kolmansien tahojen, kuten alihankkijoiden, palveluksia rekisterinpitäjän henkilötietojen käsittelyssä (jäljempänä myös ”**alikäsitteijä**”). Palveluntarjoajan tulee informoida Rekisterinpitäjää kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat alikäsitteijöiden lisäämistä tai vaihtamista hyvissä ajoin ennen alikäsitteijän lisäämistä tai vaihtamista ja annettava siten Rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

Rekisterinpitäjällä on oikeus vastustaa tällaisia ehdotettuja muutoksia perustellusti tietosuojaan liittyvillä perusteilla. Mikäli Rekisterinpitäjä ei reklamoi ilmoitetusta muutoksesta 30 päivän kuluessa Palveluntarjoajan ilmoituksesta, Rekisterinpitäjän katsotaan hyväksyneen muutoksen. Mikäli Rekisterinpitäjä ei hyväksy ehdotettua muutosta, kummallakin osapuolella on oikeus irtisanoa Sopimus ja tämä Liite päätymään 30 päivän irtisanomisajalla.

Palveluntarjoaja vastaa joka tapauksessa käyttämiensä alikäsitteijöiden toimista täysimääräisesti kuin omistaan suhteessa Rekisterinpitäjään. Palveluntarjoaja on velvollinen varmistamaan, että sen käyttämät alikäsitteijät sitoutuvat noudattamaan sisällöllisesti tätä Liitettä vastaavia ehtoja ja Rekisterinpitäjän kulloinkin antamia käsittelyä koskevia kirjallisia ohjeita sekä käsitteijälle tietosuojalainsäädännön nojalla kuuluvia velvoitteita.

3.3 Palveluntarjoajan avustamisvelvollisuus

Palveluntarjoaja siirtää välittömästi Rekisterinpitäjälle kaikki Rekisteröidyiltä saamansa Henkilötietojen

tarkastamista, oikaisemista, poistamista tai niiden Käsittelyn kieltämistä koskevat pyynnot tai muut Rekisteröidyltä saamansa pyynnot, jotka koskevat kulloinkin voimassaolevan lainsäädännön sekä GDPR:n mukaisten Rekisteröidyn oikeuksien käyttämistä. Rekisterinpitäjän velvollisuutena on huolehtia ko. pyyntöihin vastaamisesta. Palveluntarjoaja ei ole oikeutettu vastaamaan Rekisterinpitäjän Henkilötietoja koskeviin ulkopuolisten tahojen pyyntöihin tai vaatimuksiin, ellei Rekisterinpitäjä toisin ohjeista tai pakottavasta lainsäädännöstä muuta johdu. Ottaen huomioon Käsittelytoimen luonteen, Palveluntarjoaja auttaa Rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään Rekisterinpitäjän velvollisuuden vastata Rekisteröidyn pyyntöihin.

Palveluntarjoaja on velvollinen, ottaen huomioon Henkilötietojen Käsittelyn luonteen ja sen saatavilla olevat tiedot, auttamaan Rekisterinpitäjää varmistamaan, että sille laissa asetettuja velvollisuuksia noudatetaan. Nämä velvollisuudet voivat käsittää tietoturvallisuutta, tietoturvaloukkauksista ilmoittamista, tietosuojaa koskevaa vaikutustenarviointia ja ennakkokuulemista koskevia velvoitteita. Palveluntarjoaja on velvollinen avustamaan Rekisterinpitäjää sovellettavan tietosuojalainsäädännön Henkilötiedon Käsittelijälle asettamien velvoitteiden mukaisessa laajuudessa (kuten Rekisterinpitäjän sekä Palveluntarjoajan osoitusvelvollisuuden täyttäminen, vaikutustenarvioinnin ja ennakkokuulemisen suorittaminen).

Palveluntarjoajan tulee ilmoittaa Rekisterinpitäjälle viipymättä, mikäli Palveluntarjoaja katsoo, että Rekisterinpitäjän ohjeistus rikkoo tietosuojalainsäädäntöä tai mikäli Palveluntarjoaja tulee tietoiseksi siitä, että Käsiteltävät Henkilötiedot ovat joltain osin epätasällisia tai vanhentuneita.

Siltä osin, kun käsiteltävänä on GDPR:n 9 artiklan tarkoittamia erityisiä henkilötietoryhmiä koskevia Henkilötietoja ("**arkaluonteiset tiedot**"), tulee Palveluntarjoajan lisäksi toteuttaa asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi tietosuojalainsäädännön edellyttämin tavoin ja Rekisterinpitäjän mahdollisten erikseen antamien kirjallisten ohjeiden mukaisesti.

Palveluntarjoaja ohjaa kaikki tietosuojaviranomaisten tiedustelut suoraan Rekisterinpitäjälle, eikä Palveluntarjoajalla ole valtuuksia edustaa Rekisterinpitäjää tai toimia Rekisterinpitäjän puolesta Rekisterinpitäjää valvovien tietosuojaviranomaisten kanssa.

Selvyden vuoksi todetaan, että Rekisterinpitäjän ohjeet tai tämä Liite eivät sido Palveluntarjoajaa siltä osin, kuin ne mahdollisesti ovat pakottavan lainsäädännön tai viranomaismääräysten vastaisia. Palveluntarjoaja on kuitenkin tällaisissa tilanteissa velvollinen ilmoittamaan asiasta viipymättä Rekisterinpitäjälle, ellei pakottava lainsäädäntö kiellä ilmoituksen tekoa. Mikäli Rekisterinpitäjä ei reagoi Palveluntarjoajan ilmoitukseen 14 päivän kuluessa, Palveluntarjoajalla on oikeus jättää noudattamatta ko. ohjetta, kunnes se on saanut Rekisterinpitäjältä vastauksen ja Rekisterinpitäjä on muokannut ko. ohjetta pakottavan lainsäädännön tai viranomaismääräysten mukaiseksi tai luopunut ko. ohjeesta.

4 KÄSITTELY EU:N/ETA:N ULKOPUOLELLA

Ellei sovellettavasta lainsäädännöstä muuta johdu, Palveluntarjoaja saa siirtää Henkilötietoja ETA:n ulkopuolelle ("**Kolmannet maat**") vain tietosuojalainsäädännön sekä Rekisterinpitäjän antamien kirjallisten ohjeiden mukaisesti. Palveluntarjoaja vastaa siitä, että siirrot Kolmansiin maihin ovat tietosuojalainsäädännön mukaisia.

Palveluntarjoajan on ilmoitettava kaikista Henkilötietojen siirroista Kolmansiin maihin Rekisterinpitäjälle kirjallisesti etukäteen. Ilmoitus on annettava siten, että Rekisterinpitäjälle jää kohtuullinen aika tarvittaessa vastustaa siirtoa. Palveluntarjoajan on tässä yhteydessä ilmoitettava Rekisterinpitäjälle Rekisterinpitäjän pyytämät lisätiedot ko. siirrosta ja vähintään seuraavat tiedot:

- (i) kuvaus siitä, miten Henkilötietoja käsitellään Kolmansissa maissa;
- (ii) kuvaus siitä, millä toimenpiteillä Kolmansissa maissa tapahtuvan käsittelyn varmistetaan täytävän tietosuojalainsäädännön turvaaman Henkilötietojen suojan tason; ja
- (iii) kuvaus niistä teknisistä ja organisatorisista keinoista, joilla varmistetaan siirron tietosuoja- ja tietoturvasuus.

5 AUDITOINTI

Rekisterinpitäjällä tai tämän valtuuttamalla auditoijalla (ei kuitenkaan Palveluntarjoajan kilpailija) on oikeus auditoida tämän Liitteen alainen toiminta. Osapuolet sopivat auditoinnin ajankohdasta ja muista yksityiskohdista hyvissä ajoin ja vähintään 14 työpäivää ennen tarkastusta. Auditointi tulee suorittaa tavalla, joka ei haittaa Palveluntarjoajan ja sen alihankkijoiden sitoumuksia kolmansiin osapuoliin nähden. Rekisterinpitäjän edustajien ja auditoijan on allekirjoitettava tavanomaiset salassapitositoumukset. Tarkastus voidaan suorittaa enintään kerran kalenterivuodessa tai tarvittaessa useammin, mikäli Rekisterinpitäjällä on perusteltu syy epäillä rikkomusta.

Kumpikin osapuoli vastaa itse tarkastuksen aiheuttamista kustannuksista.

6 TIETOTURVA

Palveluntarjoaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet Rekisterinpitäjän Henkilötietojen suojaamiseksi ottaen huomioon Käsittelyn sisältämät riskit, joita ovat erityisesti luovutettujen, siirrettyjen, tallennettujen tai muuten Käsiteltyjen Henkilötietojen tahaton tai laiton tuhoaminen, hävittäminen, muuttaminen, luvaton (tahallinen tai tahaton) luovuttaminen tai Henkilötietoihin pääsy. Palveluntarjoajan vähimmäistasona noudatettavat tekniset ja organisatoriset tietoturvatyömenpiteet on kuvattu [alaliitteessä 2](#) ja/tai osapuolten välisessä Sopimuksessa.

Palveluntarjoaja tiedostaa sille luovutettujen Rekisterinpitäjän Henkilötietojen luonteen (salassa pidettäviä ja luottamuksellisia tai erittäin luottamuksellisia tietoja). Palveluntarjoajan velvollisuutena on varmistaa, että (i) Henkilötietojen Käsitteilyyn osallistuva Palveluntarjoajan tai Palveluntarjoajan käyttämän alihankkijan henkilöstö noudattaa asianmukaista salassapitovelvollisuutta ja/tai että (ii) niitä koskee asianmukainen lakisääteinen salassapitovelvollisuus ja että se on tietoinen tämän Liitteen velvoitteista. Palveluntarjoajan ja sen mahdollisesti käyttämien alihankkijoiden on käsiteltävä Henkilötietoja luottamuksellisesti, huolellisesti, ammattimaisesti ja hyvän tietojenkäsittelytavan mukaisesti. Palveluntarjoajan on myös rajoitettava pääsy Henkilötietoihin vain sellaisille henkilöstönsä jäsenille, joiden on tarpeen käsitellä Henkilötietoja tässä Liitteessä määriteltyjen tarkoitusten täyttämiseksi tai joiden työtehtävät välittömästi edellyttävät Henkilötietojen Käsitteilyä.

7 TIETOTURVALOUKKAUKSESTA ILMOITTAMINEN

Palveluntarjoajan on ilmoitettava Rekisterinpitäjälle kaikista Henkilötietoihin kohdistuneista tietoturvaloukkauksista ilman aiheetonta viivytystä loukkauksesta tiedon saatuaan tai kun Palveluntarjoajan käyttämä alihankkija on saanut loukkauksen tietoonsa [alaliitteessä 3](#) määritellyille yhteystahoille.

Rekisterinpitäjän pyynnöstä Palveluntarjoajan tulee ilman aiheetonta viivytystä toimittaa Rekisterinpitäjälle kaikki asiaankuuluva tietoturvaloukkaukseen liittyvä tieto. Siltä osin kuin kyseinen tieto on Palveluntarjoajan saatavilla, Palveluntarjoajan on Rekisterinpitäjälle tehtävässä ilmoituksessa kuvattava vähintään:

- (i) tapahtunut tietoturvaloukkaus,
- (ii) mahdollisuuksien mukaan rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät,
- (iii) kuvaus tietoturvaloukkauksen aiheuttamista todennäköisistä seurauksista, ja
- (iv) kuvaus korjaavista toimenpiteistä, jotka Palveluntarjoaja on suorittanut tai tulee suorittamaan tietoturvaloukkausten ennaltaehkäisemiseksi jatkossa, sekä tarvittaessa myös toimenpiteet mahdollisten tietoturvaloukkauksen haittavaikutusten minimoimiseksi.

Palveluntarjoaja dokumentoi ja raportoi selvityksen tulokset ja suoritettavat toimenpiteet Rekisterinpitäjälle. Rekisterinpitäjä vastaa tarvittavista ilmoituksista tietosuojaviranomaisille ja/tai Rekisteröidyille, ellei osapuolten kesken muuta erikseen sovita. Palveluntarjoaja on velvollinen avustamaan Rekisterinpitäjää tarvittaessa erillisen pyynnön mukaisesti tietoturvaloukkauksen selvittämisessä ja jatkotoimenpiteissä.

8 TIETOJEN POISTO/PALAUTTAMINEN SOPIMUKSEN PÄÄTTYESSÄ

Sopimuksen päätyttyä Palveluntarjoajan tulee viipymättä Rekisterinpitäjän ilmoituksen mukaisesti joko palauttaa Rekisterinpitäjälle tai poistaa kaikki tallennetut Henkilötiedot kaikkine kopioineen, ellei sovellettava lainsäädäntö edellytä Palveluntarjoajaa säilyttämään Henkilötietoja. Palveluntarjoajan tulee ilmoittaa viipymättä Rekisterinpitäjälle tällaisesta velvollisuudestaan säilyttää Rekisterinpitäjän Henkilötietoja. Palveluntarjoajan tulee Rekisterinpitäjän pyynnöstä antaa kirjallinen vakuutus siitä, että se on poistanut tai palauttanut kaikki Rekisterinpitäjän sille luovuttamat missä tahansa muodossa olevat Henkilötiedot kaikkine kopioineen.

9 MUUT EHDOT

Tämä Liite on voimassa siihen asti kun (i) Sopimus on voimassa tai (ii) osapuolilla on Henkilötietojen Käsittelytoimiin perustuvia velvoitteita toisiaan kohtaan. Palveluntarjoaja tiedottaa Rekisterinpitäjää kirjallisesti kaikista muutoksista, jotka saattavat vaikuttaa sen kykyyn tai mahdollisuuksiin noudattaa tätä Liitettä.

Mikäli Palveluntarjoaja rikkoo tämän Liitteen mukaisia velvoitteitaan, Rekisterinpitäjällä on oikeus määrätä Palveluntarjoaja keskeyttämään Henkilötietojen Käsittely, kunnes Palveluntarjoaja on korjannut rikkomuksensa.

Rekisterinpitäjällä on oikeus purkaa Sopimus siltä osin, kun kyse on tämän Liitteen mukaiseen Henkilötietojen Käsittelyyn liittyvästä osasta, jos

- (i) Rekisterinpitäjä on keskeyttänyt Käsittelyn yllä todetusti, eikä Palveluntarjoaja ole korjannut rikkomustaan 30 päivän kuluessa siitä, kun Rekisterinpitäjä on vaatinut Käsittelyn keskeyttämistä; tai
- (ii) Palveluntarjoaja rikkoo olennaisesti tai jatkuvasti tätä Liitettä ja/tai tietosuojalainsäädäntöä tai Palveluntarjoajaa velvoittavaa tuomiota tai viranomaispäätöstä.

Osapuolten välisessä Sopimuksessa sovittua vastuunrajoituslauseketta sovelletaan myös tähän Liitteeseen ja siinä asetettuihin velvollisuuksiin. Selvyyden vuoksi todetaan, että mikäli Palveluntarjoaja suorittaisi vahingonkorvausta rekisteröidyille tämän Liitteen mukaisiin toimenpiteisiin liittyen toisen osapuolen puolesta, on korvauksen suorittaneella osapuolella tällöin oikeus periä toisen osapuolen korvausvastuuta vastaava määrä osapuolelta, joka rikkomukseen on syyllistynyt. Lisäksi kumpikin osapuoli vastaa mahdollisista hallinnollisista seuraamusmaksuista, jotka viranomainen tai tuomioistuin on sille määrännyt.

Ellei Sopimuksessa ole sovittu vastuunrajoituksesta, noudatetaan silloin jäljempänä sovittua. Kumpikaan osapuoli ei vastaa välillisestä tai epäsuorasta vahingosta. Välillisenä vahinkona pidetään esimerkiksi saamatta jäänyttä voittoa tai vahinkoa, joka johtuu tuotannon tai liikevaihdon vähentymisestä tai keskeytymisestä. Palveluntarjoajan vastuu rajoittuu kaikissa tapauksissa yhteensä enintään Sopimuksen mukaiseen keskimääräiseen kuukausihintaan kerrottuna kolmella (3).

Veloitteet, joiden on niiden luonteen vuoksi tarkoitus säilyä voimassa tämän Liitteen voimassaolon päättymisestä riippumatta, jäävät voimaan Liitteen päättymisen jälkeen.

10 YHTEYSTIEDOT

Kaikissa tämän Liitteen mukaisissa ilmoitus- ja muissa kommunikaatiotilanteissa noudatetaan alaliitteen 3 mukaisia yhteystietoja.

Mikäli näissä yhteystiedoissa tapahtuu muutoksia, ovat Osapuolet velvollisia ilmoittamaan muutoksista kirjallisesti viipymättä toiselle Osapuolelle.

ALALIITE 1 – KÄSITELTÄVÄT HENKILÖTIEDOT

1. Henkilötietojen tyypit ja rekisteröityjen ryhmät

Osapuolet ovat sopineet, että Palveluntarjoaja käsittelee Rekisterinpitäjän puolesta Sopimuksessa sovitun palvelun tuottamiseksi seuraavia Rekisterinpitäjän Henkilötietoja:

- henkilön nimi
- syntymäaika
- toimipaikka, jossa ruokailee

Rekisteröidyt, joiden Henkilötietoja käsitellään ovat:

- asiakkaat

Käsiteltävät arkaluonteiset tiedot:

- erityisruokavalio terveydentilan perusteella
- eettisen vakaumuksen mukainen ruokavalio

2. Käsittelyn kohde, luonne ja tarkoitus

Osapuolet ovat sopineet, että Palveluntarjoaja tuottaa Rekisterinpitäjälle ruokapalvelua koulujen ja päiväkotien tarpeisiin. Henkilötietoja käytetään em. palveluiden tuottamiseksi Sopimuksen mukaisesti.

Henkilötietoihin kohdistetaan seuraavia käsittelytoimenpiteitä:

Rekisterinpitäjä ylläpitää asiakaskohtaisesti nimellä erityisruokavalioita Palveluntarjoajan tilausjärjestelmässä. Tilauksen jälkeen Palveluntarjoajan tilausjärjestelmä tarkastaa automaattisesti lakisääteisiin ruokavalioihin ja allergeeneihin perustuvat ruokavaliot. Loput ruokavaliot jäävät dieettipöydälle, jossa dieetikokki/-esimies käsittelee tilausta. Dieetikokit valmistavat tilauksen mukaiset erityisruokavaliot ja ne toimitetaan Rekisterinpitäjän palvelukeittiöihin joko yksittäisinä nimellä merkittynä ruokatuoteannoksena tai useampi ruokavalion mukainen ruokatuoteannos isompana eränä.

Vaativien erityisruokavalioiden toteutuksessa Rekisterinpitäjän edustajan toimittaa Palveluntarjoajan ravitsemusasiantuntijalle hoitavan tason yksityiskohtaisen toteutusohjeen ruokavaliosta. Rekisterinpitäjän edustaja ja Palveluntarjoajan ravitsemusasiantuntija suunnittelevat yhteistyössä näiden erityisruokavalioiden toteuttamisohjeet.

3. Henkilötietojen käsittelyn kesto

Palveluntarjoaja käsittelee tässä liitteessä yksilöityjä Henkilötietoja Liitteen sopimuskauden ajan. Liitteen sopimuskausi on sidottu Sopimuksen voimassaoloon ja Liitteen kohdassa 8 sovittuun.

ALALIITE 2 – TIETOTURVAVAATIMUKSET

Tässä tietoturvaliitteessä määritellyt vaatimukset asettavat vähimmäistason Henkilötietojen käsittelyn ja Sopimuksen kohteen tietoturvallisuudelle. Mikäli Rekisterinpitäjä katsoo, että Sopimuksen kohde vaatii tarkempia tietoturvavaatimuksia, tätä liitettä täydennetään tarvittaessa erikseen sovittavilla palvelukohtaisilla tietoturvavaatimuksilla.

Alla on tarkempi kuvaus teknisistä ja organisatorisista turvatoimenpiteistä asianmukaisen turvallisuustason varmistamiseksi ja ottaen huomioon käsittelyn luonne, soveltamisala, asiayhteys ja tarkoitus sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit:

1. Hallinnollinen ja fyysinen tietoturva

Palveluntarjoaja toteuttaa asianmukaiset toimenpiteet, joita tarvitaan luottamuksellisten tietojen suojaamiseksi luvattomalta tietoihin pääsylvä tai tietojen tuhoutumiselta tai muuttumiselta. Palveluntarjoaja varmistaa fyysisen pääsynvalvonnan asianmukaisin ja riittävin toimenpitein. Toimitilat on lukittu ja varmistettu varmuuslukolla. Fyysinen pääsy Palveluntarjoajan järjestelmiin on suojattu asianmukaisin pääsynvalvontakeinoin. Ulkoisten palveluntarjoajien isännöimien, ylläpitämien ja tarjoamien järjestelmien osalta Palveluntarjoaja on varmistanut, että vastaavat turvatoimenpiteet pannaan täytäntöön ja ylläpidetään ulkoisten palveluntarjoajien toimesta.

Palveluntarjoajalla on käytössään tietoturvan hallintamalli, jonka avulla toteutetaan Rekisterinpitäjän kulloinkin asettamia tietoturvatavoitteita ja vaatimuksia. Palveluntarjoaja määrittelee ja nimittää organisaatiossaan tietoturvallisuuteen liittyvät roolit ja vastuut yleisesti tai osapuolten välisen Sopimuksen toteuttamiseksi. Palveluntarjoajan sisäinen organisaatio tulee järjestää siten, että se vastaa tietojen minimointia ja sisäänrakennettua ja oletusarvoista tietosuojaa koskevia erityisiä vaatimuksia.

Palveluntarjoaja tunnistaa ja dokumentoi Sopimuksen kohteeseen liittyvät järjestelmät ja huolehtii niiden sisältämien tietojen luottamuksellisuuden, eheyden, saatavuuden, käytettävyyden ja kiistämättömyyden toteuttamisesta Sopimuksen vaatimusten mukaisesti. Palveluntarjoaja sitoutuu jatkuvasti kehittämään ja vastaa tuottamansa palvelun tietoturvallisuuden ja jatkuvuuden jatkuvasta kehittämisestä.

Jos Sopimuksen kohteeseen liittyvä työ suoritetaan Palveluntarjoajan tai sen alihankkijan tiloissa, tulee Palveluntarjoajan varmistaa tilojen tarkoituksenmukainen fyysinen turvallisuus tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden ja muiden vastaavien erityistilanteiden varalta. Lisäksi henkilöt, joille ei ole myönnetty oikeutta Rekisterinpitäjän luottamuksellisena pidettävään tietoon, saavat oleskella tiloissa ainoastaan valvonnan alaisina. Valvontaa ei edellytetä, mikäli luottamuksellista tietoa säilytetään tai käsitellään tiloissa siten, että nämä henkilöt eivät voi päästä niihin käsiksi. Palveluntarjoaja arvioi ja toteuttaa riittävän valvontaratkaisun kuhunkin tarpeeseen.

Palveluntarjoaja varmistaa tietojen saatavuuden ja pääsyn valvonnan asianmukaisin toimenpitein. Palveluntarjoaja on etenkin huolehtinut ja pannut täytäntöön tietojen varmuuskopiointi- ja palauttamiskäytännön. Varmuuskopioita luodaan säännöllisesti. Palveluntarjoaja noudattaa asianmukaisia menetelmiä poistaakseen henkilötiedot turvallisesti silloin, kun niitä ei enää käytetä ja pitää huolen, että henkilötietoja, jotka on tallennettu käytöstä poistettuihin tietolaitteisiin, ei voida palauttaa tai noutaa.

Palveluntarjoaja toteuttaa henkilötietojen pseudonymisoinnin ja anonymisoinnin aina tarvittaessa ja erikseen niin sovittaessa riittävin teknisin ja organisatorisin toimenpitein.

Palveluntarjoaja varmistaa tietojen siirron hallinnan asianmukaisin toimenpitein, hyödyntäen salattua yhteyttä erityisesti julkisessa verkossa tapahtuvaan tietojen siirtoon.

Erityisesti käyttötarkoitukseen, henkilötietojen tyyppiin ja ryhmiin liittyen Palveluntarjoajan tulee ryhtyä asianmukaisiin toimenpiteisiin soveltuvan käsittelyajan noudattamiseksi tietosuojalainsäädännön

edellyttämin tavoin. Palveluntarjoajan tulee toimenpiteillään varmistaa käsiteltävien henkilötietojen täsmällisyys ja ajantasaisuus.

2. Alihankkijat

Palveluntarjoaja huolehtii, että Palveluntarjoajan alihankkijoihin ja heidän palveluksessaan oleviin henkilöihin sovelletaan samoja tai sisällöllisesti saman sisältöisiä ehtoja kuin tässä tietoturvaliitteessä on Palveluntarjoajalle asetettu.

3. Palveluntarjoajan henkilöstö

Rekisterinpitäjällä on oikeus teettää sille nimetyistä asiantuntijoista turvallisuusselvitys sikäli ja kuten sovellettava voimassa oleva lainsäädännön menettely sallii sen. Palveluntarjoaja sitoutuu varmistamaan, että kaikki henkilöt, joilla on oikeus Sopimuksen kohteen toteuttamiseksi käsitellä luottamuksellista tietoa, käsittelevät niitä ainoastaan Rekisterinpitäjän antamien ohjeiden mukaisesti.

Henkilön, joka toimii Palveluntarjoajan lukuun Rekisterinpitäjän tiloissa, on tarvittaessa todistettava henkilöllisyytensä ja pyynnöstä esitettävä Palveluntarjoajan työ määräys tai valtuutus ennen tehtävän suorittamista. Palveluntarjoaja estää järjestelmien käytön teknisesti ilman tarpeetonta viivytystä, kun henkilön peruste luottamuksellisen tiedon käsittelylle on päättynyt.

Palveluntarjoajan sisäinen organisaatio tulee järjestää siten, että se vastaa tietojen minimointia ja sisäänrakennettua ja oletusarvoista tietosuojaa koskevia erityisiä vaatimuksia.

4. Pääsy järjestelmiin

Palveluntarjoajan tulee huolehtia sille annetuista salasanoista, tunnistautumisvälineistä ja pääsystä Rekisterinpitäjän hallinnassa oleviin tietojärjestelmiin, verkkoihin tai sähköisiin ratkaisuihin siten, että vain niillä Palveluntarjoajan henkilöllä on pääsy näihin käsiksi, joiden Rekisterinpitäjän kanssa solmitun Sopimuksen mukaiset tehtävät välttämättä tätä edellyttävät.

Palveluntarjoaja on pannut täytäntöön asianmukaiset tietojensalaustoimet ja käyttää asianmukaisia haittaohjelmien ja virusten torjuntaohjelmia estääkseen vahingollisten ohjelmien luvattoman pääsyn henkilötietoihin. Palveluntarjoaja huolehtii siitä, että käyttöoikeudet tietoihin osoitetaan ainoastaan tietoja tarvitseville ja tietoihin luvan saaneille henkilöille. Palveluntarjoaja pitää huolen, että tietojenkäsittelyjärjestelmiin luvan saaneilla henkilöillä on pääsy vain sellaisiin tietoihin, jotka kuuluvat luvan saaneiden henkilöiden käyttöoikeuden alle. Palveluntarjoaja pitää huolen, että luvattomien henkilöiden ei ole mahdollista saada pääsyä, lukea, kopioida, muuttaa tai poistaa henkilötietoja tietojen prosessointi- tai käyttövaiheessa taikka niiden säilytyksen jälkeen.

Palveluntarjoaja huolehtii siitä, että Rekisterinpitäjän sille luovuttamia tunnuksia käytetään vain niihin tarkoituksiin, joita Palveluntarjoajan Rekisterinpitäjälle suorittamat tehtävät edellyttävät. Palveluntarjoaja ei saa liittyä Rekisterinpitäjän järjestelmiin muutoin, kuin erikseen Rekisterinpitäjän tälle osoittamien henkilökohtaisin tunnuksin ja/tai tunnistautumisvälinein.

Palveluntarjoaja varmistaa riittävien teknisten ja organisatoristen toimenpiteiden täytäntöönpanon estääkseen luvattomien henkilöiden pääsyn tietojenkäsittelyjärjestelmiin, joissa henkilötietoja käsitellään tai käytetään (pääsynvalvonta) ja estääkseen tietojenkäsittelyjärjestelmien luvattoman käytön (käytönvalvonta).

Palveluntarjoaja varmistaa tietojen tallentamisen ja käytön valvonnan asianmukaisin lokitiedoin tai muin toimenpitein. Järjestelmien tulee dokumentoida erityisesti, milloin ja kenen toimesta tietoja on syötetty, muutettu tai luovutettu ja kenelle. Aikaisempi dokumentoitu versio on voitava tarvittaessa palauttaa. Palveluntarjoaja ylläpitää lisäksi erillistä pöytäkirjaa tietomurroista.

ALALIITE 3 – YHTEYSTIEDOT

Tietosuoja-asioista vastaavat yhteyshenkilöt

Rekisterinpitäjän tämän Liitteen mukaisista tietosuoja-asioista vastaavan yhteystiedot sekä yhteystiedot tietoturvaloukkausten ilmoittamiseksi:

- Tarja Heino, hallinnon suunnittelija, 040 586 6140, tarja.heino@vesilahti.fi

Palveluntarjoajan tämän Liitteen mukaisista tietosuoja-asioista vastaavan yhteystiedot sekä yhteystiedot tietoturvaloukkausten ilmoittamiseksi:

- Joni Talvitie, johtaja, ICT, 045 651 5376, joni.talvitie@voimia.fi