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
- henkilökohtaisissa tilauksissa osasto, potilashuone, vuodepaikka (pl. kotiateriapalvelu)
- toimipaikka ja/tai osasto, jossa henkilö ruokailee
- kotiosoite, ovikoodi (kotiateriapalvelu)

Rekisteröidyt, joiden Henkilötietoja käsitellään ovat:

- potilaat, asukkaat, asiakkaat

Käsiteltävät arkaluonteiset tiedot (jos soveltuu):

- erityisruokavalio terveydentilan perusteella
- eettisen vakaumuksen mukainen ruokavalio

2. **Käsittelyn kohde, luonne ja tarkoitus**

Osapuolet ovat sopineet, että Palveluntarjoaja tuottaa Rekisterinpitäjälle ateriapalveluja hyvinvointialueen tarpeisiin. Henkilötietoja käytetään em. palveluiden tuottamiseksi Sopimuksen mukaisesti.

Henkilötietoihin kohdistetaan seuraavia käsittelytoimenpiteitä:

Rekisterinpitäjä ylläpitää ruokavaliokohtaisesti tai asiakaskohtaisesti nimellä erityisruokavalioita Palveluntarjoajan tilausjärjestelmässä. Tilauksen jälkeen Palveluntarjoajan tilausjärjestelmä tarkastaa automaattisesti lakisääteisiin ruokavalioihin ja allergeeneihin perustuvat ruokavaliot. Loput ruokavaliot jäävät dieettipöydälle, jossa dieettikokki/-esihenkilö käsittelee tilausta. Dieettikokit valmistavat tilauksen mukaiset erityisruokavalioruoat ja ne toimitetaan Palveluntuottajan valmistuskeittiöltä suoraan tai Palveluntuottajan palvelukeittiön kautta Rekisterinpitäjän toimituspisteisiin /osastoille / kotipalveluasiakkaiden koteihin joko yksittäisinä nimellä merkittynä ruokatuoteannoksena tai useampi ruokavalion mukainen ruokatuoteannos isompana eränä.

Yksilöllisten erityisruokavalioiden sisällön ja toteutuksen suunnittelee tarvittaessa Palveluntuottajan ravitsemusasiantuntija yhteistyössä Rekisterinpitäjän edustajan kanssa.

3. **Henkilötietojen käsittelyn kesto**

Palveluntarjoaja käsittelee tässä liitteessä yksilöityjä Henkilötietoja Liitteen sopimuskauden ajan. Liitteen sopimuskausi on sidottu Sopimuksen voimassaoloon.

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 turvatoimenpiteitä 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 pääsyltä 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 työmääräys 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 henkilöillä 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 osoittamin 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.