

## Liite 1

### Rekisterinpitäjän ja henkilötietojen käsittelijän välinen

# HENKILÖTIETOJEN KÄSITTELYSOPIMUS

#### SISÄLLYSLUETTELO

1	OSAPUOLET, YHTEYS- JA TIETOSUOJAVASTUUHENKILÖT .....	2
2	SOPIMUKSEN PERUSTEET JA SOVELTAMISALA .....	2
3	SOPIMUKSEN TARKOITUS .....	3
4	HENKILÖTIETOJEN KÄSITTELYN KUVAUS.....	3
5	REKISTERINPITÄJÄN OIKEUKSIA JA VELVOLLISUUKSIA .....	4
6	HENKILÖTIETOJEN KÄSITTELIJÄN OHJEET, OIKEUDET JA VELVOLLISUUDET .....	5
7	HENKILÖTIETOJEN KÄSITTELIJÄN TEKNISET JA ORGANISATORISET TOIMENPITEET .....	11
8	SOPIMUKSEN NOUDATTAMATTA JÄTTÄMINEN JA SOPIMUKSEN PURKAMINEN .....	11
9	VASTUU JA VAHINGONKORVAUS.....	13
10	SOPIMUKSEN MUUTTAMINEN JA PÄIVITTÄMINEN .....	13
11	SOPIMUSLIITTEET .....	13
12	SOPIMUKSEN VOIMASSAOLO JA ALLEKIRJOITUKSET .....	14
13	LIITE 1.1: HENKILÖTIETOJEN KÄSITTELYN KUVAUS.....	15
14	LIITE 1.2: KÄSITTELIJÄN TEKNISET JA ORGANISATORISET TOIMENPITEET .....	16
15	LIITE 1.3: HENKILÖTIETOJEN ALIKÄSITTELIJÖIDEN LUETTELO .....	17
16	LIITE 1.4 KESKEISIÄ TIETOSUOJASÄÄNTELYN MÄÄRITELMIÄ .....	18

## 1 OSAPUOLET, YHTEYS- JA TIETOSUOJAVASTUUHENKILÖT

<b>1.1. Rekisterinpitäjä:</b>	Hyvinvointilomat ry (myös "Tilaaaja")
Osoite	
Organisaation y-tunnus	2440730-7
<u>A. Yhteyshenkilö</u> nimi, asema ja yhteystiedot	[täydennetään]
<u>B. Tietosuojavastaava (tai tietosuojavastuuhenkilö)</u> nimi ja yhteystiedot	[täydennetään]

<b>1.2 Henkilötietojen käsittelijä:</b>	[täydennetään] (myös "Palveluntuottaja")
Osoite	[täydennetään]
Organisaation y-tunnus	[täydennetään]
<u>A. Yhteyshenkilö</u> nimi, asema ja yhteystiedot	[täydennetään]
<u>B. Tietosuojavastaava tai tietosuojavastuuhenkilö</u> nimi ja yhteystiedot	[täydennetään]

## 2 SOPIMUKSEN PERUSTEET JA SOVELTAMISALA

- 2.1 Hyvinvointilomat ry:n puitesopimuksen liitteenä 1 on tämä Henkilötietojen käsittelysopimus alaliitteineen (myös "DPA-sopimus"). Hyvinvointilomat ry on tehnyt Palveluntuottajan kanssa puitesopimuksen, jossa lomapalvelun asiakkaiden henkilötietojen rekisterinpitäjä on Hyvinvointilomat ry ja henkilötietojen käsittelijä on Palveluntuottaja.
- 2.2 Tämän DPA-sopimuksen perusteena on EU:n yleinen tietosuoja-asetus (EU 2016/679, myös "GDPR"). GDPR täydentää tietosuojalaki (1050/2018, "TiSL"). DPA-sopimuksessa yksilöidään käsiteltävät henkilötiedot ja niiden käsittelyyn oikeutetut.
- 2.3 Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (jäljempänä "rekisteröity") liittyvät tiedot, jonka henkilötietoja kulloinkin käsitellään. Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, osoitteen, henkilötunnuksen, kuvan, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, biometrisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. GDPR:ssa, tietosuojalainsäädäntö ja muissa tietosuojasäätelyssä ("Tietosuojalainsäädäntö") ja DPA-sopimuksessa käytettyjä käsitteitä ja määritelmiä on liitteessä 1.4.

- 2.4 DPA-sopimuksessa määritetään tietosuojalainsäädännön mukaisesti rekisterinpitäjän ja henkilötietojen käsittelijän sekä mahdollisten henkilötietojen alikäsittelijöiden (myös "alikäsitelijä") oikeudet ja velvollisuudet suhteessa käsiteltäviin henkilötietoihin.
- 2.5 Henkilötietojen käsittelijän suorittamaa käsittelyä määritetään tällä DPA-sopimuksella ja sen henkilötietojen käsittelyn kuvauksella Liitteessä 1.1 vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän sekä käsittelijän velvollisuudet ja oikeudet.
- 2.6 DPA-sopimus sääntelee henkilötietojen käsittelijän rekisterinpitäjän puolesta tekemää henkilötietojen käsittelyä ja määrittelee sen, miten käsittelijä osaltaan varmistaa yksityisyyden rekisterinpitäjän ja sen rekisteröityjen puolesta teknisillä ja organisatorisilla toimenpiteillä Liitteessä 1.2. Osapuolten tarkoituksena ei ole tällä DPA-sopimuksella siirtää mitään rekisterinpitäjän lakisääteisiä velvollisuuksia henkilötietojen käsittelijälle.

### 3 SOPIMUKSEN TARKOITUS

- 3.1 DPA-sopimuksen tarkoituksena on varmistaa GDPR:n noudattaminen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä (GDPR 28 artikla 3 ja 4 kohdat). DPA-sopimuksessa käytetään muiden ehtojen lisäksi EU 2021/915 päätöksen mukaisia rekisterinpitäjän ja henkilötietojen käsittelijöiden välisiä vakiosopimuslausekkeita ("vakiosopimuslausekkeet", 28 artikla 7 kohta). Vakiosopimuslausekkeet eivät vaikuta velvoitteisiin, joita rekisterinpitäjään sovelletaan GDPR:ssa.
- 3.2 DPA-sopimusta ja sen sisältämiä vakiosopimuslausekkeita on luettava ja tulkittava GDPR:n säännösten valossa. DPA-sopimusta ja vakiolausekkeita ei saa tulkita tavalla, joka on ristiriidassa GDPR:ssa säädettyjen oikeuksien ja velvoitteiden kanssa tai tavalla, joka loukkaa rekisteröityjen perusoikeuksia tai -vapauksia. Jos DPA-sopimus ja sen vakiolausekkeet ovat ristiriidassa osapuolten välisen asiaa koskevien sopimusten määräysten kanssa, jotka ovat olemassa silloin kun DPA-sopimuksesta ja sen vakiolausekkeista sovitaan tai tulevat voimaan sen jälkeen, niin DPA-sopimus ja sen vakiolausekkeet ovat ensisijaisia.
- 3.3 Henkilötietojen käsittelijän on välittömästi ilmoitettava rekisterinpitäjälle, jos henkilötietojen käsittelijä katsoo, että rekisterinpitäjän antamat ohjeet ovat GDPR:n taikka sovellettavien unionin tai jäsenvaltioiden tietosuojasäännösten vastaisia.

### 4 HENKILÖTIETOJEN KÄSITTELYN KUVAUS

- 4.1 Henkilötietojen käsittelijä saa käsitellä rekisterinpitäjän puolesta ja lukuun liitteessä 1.1 kohdassa 1.1 kuvattuja rekisterinpitäjän henkilörekisteriin kuuluvia henkilötietoja.
- 4.2 Henkilötietojen käsittelijä saa käsitellä rekisterinpitäjän puolesta ja lukuun liitteessä 1.1 kohdassa 1.2 kuvattuja rekisterinpitäjän henkilörekisteriin kuuluvia *arkaluonteisia henkilötietoja*.

## 5 REKISTERINPITÄJÄN OIKEUKSIA JA VELVOLLISUUKSIA

	<b><u>Rekisterinpitäjä:</u></b>
<b>1. Rekisterinpitäjä</b>	<p>a) toimii henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön tarkoitettuna rekisterinpitäjänä, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.</p> <p>b) sitoutuu huolehtimaan henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön mukaisista rekisterinpitäjän velvollisuuksista.</p> <p>c) huolehtii Tietosuojalainsäädäntöä noudattaen tietoturvallisuudesta koko henkilötietojen elinkaaren ajan. Henkilötietojen elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon</p> <p>d) vastaa GDPR:n mukaan siitä, että käyttämänsä henkilötiedon käsittelijät noudattavat soveltuvaa lainsäädäntöä.</p> <p>e) on lopullinen vastuu henkilötietojen käsittelyn lainmukaisuudesta.</p>
<b>2. Rekisteröidyn oikeuksien toteuttaminen</b>	<p>a) yksi päävelvollisuuksista on rekisteröityjen oikeuksien toteuttaminen.</p> <p>b) huolehtii siitä, että Tietosuojalainsäädännön mukaiset rekisteröidyn oikeudet toteutuvat, joiden peruseriaatteena on henkilötietojen suojan takaaminen valtuudettomalta tai henkilöä vahingoittavalta tietojen käytöltä.</p> <p>c) ei pääsääntöisesti luovuta arkaluontoisia henkilötietoja käsittelijälle, ellei luovutus perustu lainsäädäntöön ja/tai rekisteröidyn nimenomaiseen suostumukseen.</p> <p>d) arkaluontoisten tietojen käsittelystä on aina laadittava DPA-sopimukseen oma liite 1.2, jonka salassa pidettävyys arvioidaan tapauskohtaisesti.</p>
<b>3. Henkilötietojen käsittelijän käyttö</b>	<p>a) saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi (Liite 1.2) niin, että käsittely täyttää voimassa olevan henkilötietojen käsittelyyn ja Tietosuojalainsäädännön vaatimukset, ja että sillä varmistetaan rekisteröidyn oikeuksien suojele.</p>
<b>4. Tietojen muuttaminen ja ohjeiden anto käsittelijälle</b>	<p>a) saa muuttaa, täydentää ja päivittää Käsittelijälle antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita:</p> <p>b) ohjeet voivat olla henkilötietojen käsittelyä tai tietosuojaa koskeviin teknisiin tai organisatorisiin toimenpiteisiin liittyviä muutoksia, täydennyksiä tai päivityksiä.</p> <p>c) Käsittelijä ja muut alikäsittelijät sitoutuvat noudattamaan näitä muutettuja, täydennettyjä tai päivitettyjä ohjeita.</p>
<b>5. Tietosuojaseloste/ Tietosuojailmoitus</b>	<p>a) vastaa tietosuojaselosteiden/tietosuojailmoitusten laatimisesta ja saatavilla pidosta sekä päättää tietojen käsittelyssä noudatettavasta menettelystä ja tietojen luovuttamisesta.</p>
<b>6. Tietosuojavastaava /tietosuoja - vastuuhenkilö</b>	<p>a) tietosuojavastaavan tai tietosuojavastuuhenkilön (kohta 1.1) tehtävänä on seurata ja edistää Tietosuojalainsäädännön toteutumista DPA-sopimuksen mukaisten rekisteröityjen henkilötietojen käsittelyssä.</p> <p>b) tietosuojavastaavan tai tietosuojavastuuhenkilön on tiedotettava ja koulutettava DPA-sopimukseen liittyvistä tietosuoja-asioista ja rekisteröityjen henkilötietojen tietosuojasäädännön mukaisesta käsittelystä.</p> <p>c) osapuolen on ilmoitettava toiselle osapuolelle viivytyksettä nimettyjen tietosuojavastaavan tai tietosuojavastuuhenkilön vaihtumisesta.</p>

## 6 HENKILÖTIETOJEN KÄSITTELIJÄN OHJEET, OIKEUDET JA VELVOLLISUUDET

	<b><u>Henkilötietojen käsittelijä:</u></b>
<b>1. Käsittelijän rooli</b>	<p>a) toimii henkilötietojen käsittelyä ja tietosuojaa koskevan lainsäädännön tarkoitamana henkilötietojen käsittelijänä, joka käsittelee rekisterinpitäjän henkilötietoja rekisterinpitäjän puolesta ja lukuun.</p> <p>b) suojelee niiden henkilöiden eli rekisteröityjen oikeuksia, jotka luovuttavat henkilötietojaan rekisterinpitäjälle ja joka luovuttaa henkilötietoja Käsittelijälle.</p> <p>c) ei käsittele eikä muulla tavoin hyödynnä DPA-sopimuksen perusteella käsittelemiään henkilötietoja muutoin kuin DPA-sopimuksen täyttämisen mukaisessa tarkoituksessa ja laajuudessa.</p> <p>d) on käsiteltävä henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, paitsi jos henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaaditaan. Tässä tapauksessa henkilötietojen käsittelijä tiedottaa rekisterinpitäjälle kyseisestä oikeudellisesta vaatimuksesta ennen käsittelyä, paitsi jos se kielletään lainsäädännössä yleistä etua koskevien tärkeiden syiden vuoksi. Rekisterinpitäjä voi myös antaa myöhemmin ohjeita koko henkilötietojen käsittelyn ajan. Nämä ohjeet on aina dokumentoitava.</p> <p>e) on välittömästi ilmoitettava rekisterinpitäjälle, jos henkilötietojen käsittelijä katsoo, että rekisterinpitäjän antamat ohjeet ovat GDPR:n taikka sovellettavien unionin tai jäsenvaltioiden tietosuojasäännösten vastaisia.</p>
<b>2. Käyttö - tarkoituksen rajaaminen</b>	<p>a) saa käsitellä henkilötietoja ainoastaan tässä DPA-sopimuksessa ja sen <u>Liitteessä 1.1</u> esitettyjä käsittelyn erityistarkoituksia varten, ellei rekisterinpitäjä anna lisäohjeita.</p>
<b>3. Henkilötietojen käsittely ja aika</b>	<p>a) käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien ohjeiden ja Sopimuksen mukaisesti.</p> <p>b) suorittama käsittely saa kestää ainoastaan <u>Liitteessä 1.1</u> täsmennetyin ajan.</p>
<b>4. Käsittelyn turvallisuus</b>	<p>a) on toteutettava ainakin <u>Liitteessä 1.2</u> eritellyt tekniset ja organisatoriset toimenpiteet henkilötietojen turvallisuuden varmistamiseksi. Tähän sisältyy tietojen suojaaminen tietoturvaloukkauksilta, jotka johtavat vahingossa tapahtuvaan tai laittomaan tietojen tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai käyttöön (henkilötietojen tietoturvaloukkaus). Asianmukaista turvallisuustasoa arvioidessaan osapuolten on otettava asianmukaisesti huomioon uusien tekniikka, täytäntöönpanokustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröidyille aiheutuvat riskit.</p> <p>b) antaa käsiteltävät henkilötiedot henkilöstönsä jäsenille vain siinä määrin kuin se on ehdottoman välttämätöntä sopimuksen täytäntöönpanoa, hallinnointia ja seurantaa varten.</p> <p>c) varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.</p>
<b>5. Arkaluonteiset tiedot /Henkilötietojen erityiset tietoryhmät</b>	<p>a) on sovellettava erityisiä rajoituksia ja/tai täydentäviä suojatoimia, jotka on kuvattu <u>Liitteessä 1.2</u>, jos käsittelyyn liittyy henkilötietoja, joista käy ilmi rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja tai biometrisiä tietoja luonnollisen henkilön yksiselitteistä tunnistamista varten, terveyttä tai henkilön seksuaalista käyttäytymistä tai seksuaalista suuntautumista koskevia tietoja taikka rikostuomioihin ja rikoksiin liittyviä tietoja.</p>

<b>6. Dokumentointi ja vaatimusten – mukaisuus</b>	<p>a) on käsiteltävä nopeasti ja asianmukaisesti rekisterinpitäjän kyselyt, jotka koskevat tietojen käsittelyä näiden lausekkeiden mukaisesti.</p> <p>b) on asetettava rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen sen osoittamiseksi, että näissä lausekkeissa vahvistettuja velvoitteita on noudatettu ja jotka johtuvat suoraan GDPR:sta.</p> <p>c) on rekisterinpitäjän pyynnöstä myös sallittava DPA-sopimuksen kattamien käsittelytoimien tarkastukset ja osallistuttava niihin kohtuullisin väliajoin tai kun on viitteitä vaatimusten noudattamatta jättämisestä. Päättyessään uudelleentarkastelusta tai tarkastuksesta rekisterinpitäjä voi ottaa huomioon henkilötietojen käsittelijällä olevat asiaankuuluvat sertifioinnit. Rekisterinpitäjä voi päättää suorittaa tarkastuksen itse tai valtuuttaa riippumattoman tarkastajan. Tarkastuksiin voi sisältyä myös käynnejä henkilötietojen käsittelijän toimitiloissa tai muissa fyysisissä tiloissa, ja niistä on tarvittaessa ilmoitettava riittävän ajoissa. Osapuolten on asetettava tässä tarkoitetut tiedot, mukaan lukien tarkastusten tulokset, pyynnöstä toimivaltais(t)en valvontaviranomais(t)en saataville. Osapuolten on voitava osoittaa noudattavansa näitä lausekkeitä.</p>
<b>7. Henkilötietojen alikäsittelijöiden käyttö ja rekisterinpitäjän luvat</b>	<p>a) Jos henkilötietojen käsittelijä kutsuu toisen henkilötietojen käsittelijän suorittamaan tiettyjä toimintoja, on sovellettava GDPR:n 28 artiklan 2 ja 4 kohdassa tarkoitettuja erityisiä vaatimuksia. Erityisesti vaaditaan erityinen tai yleinen kirjallinen ennakkolupa. Riippumatta siitä, onko tämä ennakkolupa erityinen vai yleinen, ensimmäisen henkilötietojen käsittelijän on pidettävä ajan tasalla luettelo muista henkilötietojen käsittelijöistä.</p> <p>b) <b>VAIHTOEHTO 1: ERILLINEN ENNAKKOLUPA:</b> Henkilötietojen käsittelijä ei saa antaa mitään rekisterinpitäjän puolesta DPA-sopimuksen nojalla suorittamista käsittelytoimista alihankintana henkilötietojen alikäsittelijälle ilman rekisterinpitäjän erillistä kirjallista ennakkolupaa. Henkilötietojen käsittelijän on toimitettava erillistä lupaa koskeva pyyntö vähintään <b>[MÄÄRITÄ AJANJAKSO]</b>/sopimuskausi] ennen asianomaisen henkilötietojen alikäsittelijän palkkaamista sekä tarvittavat tiedot, jotta rekisterinpitäjä voi päättää luvasta. Rekisterinpitäjän erillisen ennakkoluvan mukainen luettelo rekisterinpitäjän valtuuttamista henkilötietojen alikäsittelijöistä on <u>Liitteessä 1.3</u>, jota Osapuolten on pidettävä ajan tasalla.</p> <p>c) <b>VAIHTOEHTO 2: YLEINEN KIRJALLINEN LUPA:</b> Henkilötietojen käsittelijällä on rekisterinpitäjän yleinen lupa, joka koskee henkilötietojen alikäsittelijöiden palkkaamista <b>sovitusta luettelosta</b>. Henkilötietojen käsittelijän on ilmoitettava kirjallisesti rekisterinpitäjälle kaikista kyseiseen luetteloon suunnitelluista muutoksista lisäämällä tai vaihtamalla henkilötietojen alikäsittelijöitä vähintään <b>[MÄÄRITÄ AJANJAKSO]</b> aiemmin ja annettava näin rekisterinpitäjälle riittävästi aikaa vastustaa tällaisia muutoksia ennen asianomaisen henkilötietojen alikäsittelijän (alikesittelijöiden) palkkaamista. Henkilötietojen käsittelijän on annettava rekisterinpitäjälle tiedot, jotka ovat tarpeen, jotta rekisterinpitäjä voi käyttää vastustamisoikeuttaan.</p> <p>d) Jos henkilötietojen käsittelijä käyttää henkilötietojen alikäsittelijää suorittamaan tiettyjä käsittelytoimia rekisterinpitäjän puolesta, käsittelijän on tehtävä sopimus, jossa henkilötietojen alikäsittelijälle asetetaan DPA-sopimuksen nojalla olennaisilta osin samat tietosuojavelvoitteet kuin henkilötietojen käsittelijälle. Henkilötietojen käsittelijän on varmistettava, että henkilötietojen alikäsittelijä noudattaa velvoitteita, joita henkilötietojen käsittelijään sovelletaan näiden lausekkeiden ja GDPR:n nojalla.</p>

	<p>e) Henkilötietojen käsittelijä on rekisterinpitäjän pyynnöstä toimitettava jäljennös tällaisesta henkilötietojen alikäsittelijän sopimuksesta ja mahdollisista myöhemmistä muutoksista rekisterinpitäjälle. Jos se on tarpeen liikesalaisuuksien tai muiden luottamuksellisten tietojen (mukaan lukien henkilötiedot) suojaamiseksi, henkilötietojen käsittelijä voi poistaa sopimuksesta tekstiä ennen jäljennöksen toimittamista.</p> <p>f) Henkilötietojen käsittelijä on edelleen täysin vastuussa rekisterinpitäjälle henkilötietojen alikäsittelijän velvoitteiden täyttämisestä alikäsittelijän kanssa tekemänsä sopimuksen mukaisesti. Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle, jos henkilötietojen alikäsittelijä ei täytä sopimusvelvoitteitaan.</p> <p>g) Henkilötietojen käsittelijä on sovittava henkilötietojen alikäsittelijän kanssa kolmatta osapuolta suojaavasta edunsaaja lausekkeesta, jonka mukaan jos henkilötietojen käsittelijä on tosiasiallisesti kadonnut, lakannut olemasta oikeudellisesti tai tullut maksukyvyttömäksi, rekisterinpitäjällä on oikeus purkaa henkilötietojen alikäsittelijän sopimus ja ohjeistaa alikäsittelijää poistamaan tai palauttamaan henkilötiedot.</p>
<p><b>8. Kansainväliset tiedonsiirrot</b></p>	<p>a) voi siirtää tietoja kolmanteen maahan tai kansainväliselle järjestölle ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden perusteella tai henkilötietojen käsittelijään sovellettavan unionin tai jäsenvaltion lainsäädännön mukaisen erityisen vaatimuksen täyttämiseksi, ja siirron on tapahduttava GDPR:n V luvun mukaisesti.</p> <p>b) Rekisterinpitäjä hyväksyy sen, että jos henkilötietojen käsittelijä käyttää kohdan 6 alakohdan 7 mukaisesti henkilötietojen alikäsittelijää suorittamaan tiettyjä käsittelytoimia (rekisterinpitäjän puolesta) ja kyseisiin käsittelytoimiin liittyy GDPR V luvussa tarkoitettu henkilötietojen siirto, henkilötietojen käsittelijä ja henkilötietojen alikäsittelijä voivat varmistaa GDPR V luvun säännösten noudattamisen käyttämällä GDPR 46 artiklan 2 kohdan nojalla hyväksymiä vakiosopimuslausekkeitä edellyttäen, että kyseisten vakiosopimuslausekkeiden käytön edellytykset täyttyvät.</p>
<p><b>9. Rekisterinpitäjän avustaminen</b></p>	<p>a) on viipymättä ilmoitettava rekisterinpitäjälle kaikista rekisteröidyltä saamistaan pyynnöistä. Henkilötietojen käsittelijä ei saa itse vastata pyyntöön, paitsi jos rekisterinpitäjä on antanut siihen luvan.</p> <p>b) on avustettava rekisterinpitäjää sen velvollisuuksien täyttämässä, jotka koskevat rekisteröityjen oikeuksien käyttämistä koskeviin pyyntöihin vastaamista, ottaen huomioon käsittelyn luonne.</p> <p>c) on edellä olevan 9. a) ja b) kohdan mukaisia velvollisuuksia täyttäessään noudatettava rekisterinpitäjän ohjeita.</p> <p>d) sen lisäksi, että henkilötietojen käsittelijä on 9. b) kohdan nojalla velvoitettu avustamaan rekisterinpitäjää, henkilötietojen käsittelijän on lisäksi avustettava rekisterinpitäjää seuraavien velvoitteiden noudattamisessa ottaen huomioon käsittelyn luonne ja henkilötietojen käsittelijän käytettävissä olevat tiedot:</p> <ol style="list-style-type: none"> <li>1) velvoite arvioida suunniteltujen käsittelytoimien vaikutusta henkilötietojen suojaan, jäljempänä <i>'tietosuojaa koskeva vaikutustenvarviointi'</i>, jos tietyn tyyppinen käsittely todennäköisesti aiheuttaa suuren riskin luonnollisten henkilöiden oikeuksille ja vapauksille;</li> <li>2) velvoite kuulla ennen käsittelyä toimivaltaista valvontaviranomaista / toimivaltaisia valvontaviranomaisia, jos <i>tietosuojaa koskeva vaikutustenvarviointi</i> osoittaa, että käsittely aiheuttaisi korkean riskin, jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi;</li> </ol>

	<p>3) velvollisuus varmistaa henkilötietojen oikeellisuus ja ajantasaisuus ilmoittamalla rekisterinpitäjälle viipymättä, jos henkilötietojen käsittelijä havaitsee, että sen käsittelemät henkilötiedot ovat virheellisiä tai vanhentuneita;</p> <p>4) GDPR 32 artiklassa säädetty velvoitteet.</p> <p>e) Osapuolet vahvistavat <u>Liitteessä 1.2</u> asianmukaiset <i>tekniset ja organisatoriset toimenpiteet</i>, joita henkilötietojen käsittelijän on noudatettava avustaessaan rekisterinpitäjää tämän lausekkeen soveltamisessa, sekä tarvittavan avun soveltamisalan ja laajuuden.</p>
<p><b>10. Tietoturva - loukkauksista ilmoittaminen</b></p>	<p>a) on tehtävä tietoturvaloukkauksen tapauksessa yhteistyötä rekisterinpitäjän kanssa ja avustettava rekisterinpitäjää, jotta tämä voi täyttää tapauksen mukaan GDPR 33 ja 34 artiklan mukaiset velvoitteensa, ottaen huomioon käsittelyn luonne ja henkilötietojen käsittelijän käytettävissä olevat tiedot.</p> <p>a) on ilmoitettava kirjallisesti henkilötietojen tietoturvaloukkauksesta Rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa ja viimeistään <b>36</b> tunnin kuluessa. Rekisterinpitäjä arvioi riskit ja mahdollisen ilmoituksen tekemisen valvontaviranomaiselle.</p> <p>b) on annettava Rekisterinpitäjälle vähintään seuraavat tiedot tietoturvaloukkauksesta:</p> <ol style="list-style-type: none"> <li>1) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;</li> <li>2) ilmoitettava tietosuojavastaava tai muu vastuuhenkilö, jolta voi saada asiassa lisätietoja;</li> <li>3) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset; sekä</li> </ol> <p>b) kuvattava toimenpiteet, joita kyseinen henkilötietojen käsittelijä ehdottaisi tai joita se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta ja tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.</p>
<p><b>11. Tietoturva - loukkaus rekisterinpitäjän käsittelemien tietojen osalta</b></p>	<p>Jos henkilötietojen tietoturvaloukkaus koskee <u>rekisterinpitäjän käsittelemiä tietoja</u>, henkilötietojen käsittelijän on avustettava rekisterinpitäjää</p> <p>a) ilmoitettaessa tapauksen mukaan henkilötietojen tietoturvaloukkauksesta toimivaltaiselle valvontaviranomaiselle / toimivaltaisille valvontaviranomaisille ilman aiheetonta viivytystä sen jälkeen, kun rekisterinpitäjä on saanut sen tietoonsa /, (paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä);</p> <p>b) hankittaessa seuraavat tiedot, jotka on GDPR 33 artiklan 3 kohdan mukaisesti mainittava rekisterinpitäjän ilmoituksessa, ja joihin on sisällytettävä vähintään seuraavat:</p> <ol style="list-style-type: none"> <li>1) henkilötietojen luonne, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotietueiden ryhmät ja arvioidut lukumäärät;</li> <li>2) henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;</li> <li>3) toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.</li> </ol> <p>Jos ja siltä osin kuin kaikkia tietoja ei ole mahdollista toimittaa samaan aikaan, alkuperäisen ilmoituksen on sisällettävä saatavilla olevat tiedot, ja lisätiedot on sen jälkeen toimitettava ilman aiheetonta viivytystä, kun ne tulevat saataville;</p>

	<p>c) noudatettaessa GDPR 34 artiklan mukaisesti velvoitetta ilmoittaa henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä rekisteröidylle, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin luonnollisten henkilöiden oikeuksille ja vapauksille.</p>
<p><b>12. Tietoturva - loukkaus henkilötietojen käsittelijän käsittelemien tietojen osalta</b></p>	<p>Kun kyseessä on <u>henkilötietojen käsittelijän käsittelemiin tietoihin liittyvä henkilötietojen tietoturvaloukkaus</u>, henkilötietojen käsittelijän on ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan tietoturvaloukkauksen tietoonsa. Kyseisen ilmoituksen on sisällettävä vähintään seuraavat:</p> <ul style="list-style-type: none"> <li>a) kuvaus tietoturvaloukkauksen luonteesta (mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ja henkilötietotietueiden ryhmät ja arvioitu lukumäärä);</li> <li>b) tiedot yhteyspisteestä, josta saa lisätietoja henkilötietojen tietoturvaloukkauksesta;</li> <li>c) tietoturvaloukkauksen todennäköiset seuraukset ja toimenpiteet, jotka on toteutettu tai joita ehdotetaan toteutettavaksi tietoturvaloukkauksen korjaamiseksi, mukaan lukien sen mahdollisten haitallisten vaikutusten lieventämiseksi.</li> </ul> <p>Jos ja siltä osin kuin kaikkia tietoja ei ole mahdollista toimittaa samaan aikaan, alkuperäisen ilmoituksen on sisällettävä saatavilla olevat tiedot, ja lisätiedot on sen jälkeen toimitettava ilman aiheetonta viivytystä, kun ne tulevat saataville. Osapuolet esittävät Liitteessä 1.2 (organisatoriset ja tekniset toimet) kaikki muut tiedot, jotka henkilötietojen käsittelijän on toimitettava avustaessaan rekisterinpitäjää GDPR 33 ja 34 artiklan mukaisten rekisterinpitäjän velvoitteiden noudattamisessa.</p>
<p><b>13. Salassapito - velvollisuus</b></p>	<ul style="list-style-type: none"> <li>a) varmistaa, että sen henkilötietojen käsittelyyn oikeutetut henkilöt kuten käsittelijän työntekijät, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.</li> <li>b) varmistaa, että jokainen henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan DPA-sopimuksen ja rekisterinpitäjän ohjeiden mukaisesti.</li> <li>c) huolehtii, että sen henkilöstö ei paljasta saamiaan salassa pidettäviä tietoja DPA-sopimuksen ulkopuolisille tahoille ilman rekisterinpitäjän kirjallisesti annettua lupaa.</li> <li>d) varmistaa, että salassa pidettäviä tietoja käsittelevät ja niihin pääsevät vain henkilöt, joiden työtehtävien kannalta se on välttämätöntä.</li> <li>e) tiedottaa henkilöstölleen, että vaitiolo- ja salassapitovelvollisuus on voimassa tämän DPS-sopimuksen päättymisen jälkeenkin.</li> <li>f) tekee tarpeen mukaan salassapitolausekkeet työsopimukseen ja mahdollisten ulkopuolisten konsulttien tai vastaavien kanssa salassapitosopimukset.</li> </ul>
<p><b>14. Vaitiolo velvollisuus</b></p>	<ul style="list-style-type: none"> <li>a) varmistaa, että sen henkilötietojen käsittelyyn oikeutetut henkilöt kuten käsittelijän työntekijät, ovat sitoutuneet noudattamaan vaitiolo velvollisuutta: <i>Tietosuojalaki 35 §: ”Joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta taikka toisen liikesalaisuudesta, ei saa oikeudettomasti ilmaista sivulliselle näin saamiaan tietoja eikä käyttää niitä omaksi tai toisen hyödyksi tai toisen vahingoksi.”</i></li> </ul>

<p><b>15. Tietosuoja - vastaava tai tietosuoja - vastuu henkilö</b></p>	<p>a) käsittelijän tietosuojavastaavan tai tietosuojavastuuhenkilön (kohta 1.2 B) tehtävänä on seurata ja edistää Tietosuojalainsäädännön toteutumista erityisesti DPA-sopimuksen mukaisten rekisteröityjen henkilötietojen käsittelyssä.</p> <p>b) tietosuojavastaavan tai tietosuojavastuuhenkilön on tiedotettava ja koulutettava DPA-sopimukseen liittyvistä tietosuoja-asioista ja Rekisteröityjen henkilötietojen tietosuojasäädännön mukaisesta käsittelystä.</p> <p>c) Osapuolen on ilmoitettava toiselle osapuolelle viivytyksettä nimettyjen tietosuojavastuuhenkilöiden vaihtumisesta.</p>
<p><b>16. Tietoturva tekniset ja organisatoriset toimenpiteet</b></p>	<p>a) toteuttaa riittävät <i>turvatoimet</i> henkilötietojen suojaamiseksi.</p> <p>b) toteuttaa tarvittavat <i>tekniset, fyysiset ja organisatoriset toimenpiteet</i> asianmukaisen tietoturvatason varmistamiseksi ja henkilötietojen suojaamiseksi asiattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta, vahingoittumiselta, muutattamiselta tai luovuttamiselta. Käsittelijän turvatoimien tulee täyttää soveltuvat Tietosuojasäätelyn vaatimukset. Kyse voi olla teknisistä toimista, kuten tietokoneiden virustorjunnasta ja palomuureista, toimitilojen kulunvalvonnasta tai organisatorisista toimista, kuten riittävästä ja asiantuntevista resursseista.</p> <p>c) sitoutuu toteuttamaan <i>riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet</i> henkilötietojen käsittelyn turvallisuuden varmistamiseksi ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit sekä noudattamaan rekisterinpitäjän ohjeita ja mahdollisia rekisterinpitäjän ohjeiden päivityksiä.</p>
<p><b>17. Avustamis – velvollisuus ja rekisteröityjen oikeudet</b></p>	<p>a) avustaa rekisterinpitäjää täyttämään tämän rekisteröityjen oikeuksiin liittyvät velvollisuudet. Rekisteröidyillä on lukuisia oikeuksia, kuten oikeus saada pääsy itseään koskeviin henkilötietoihin ja saada virheelliset tiedot oikaistuiksi.</p> <p>d) auttaa rekisterinpitäjää varmistamaan, että GDPR:n 32-36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot;</p> <p>e) auttaa rekisterinpitäjää käsittelytoiminnan luonteen mukaisesti asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat GDPR:n III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä.</p>
<p><b>18. Luettelo rekisteröityjen henkilötietojen muutoksista</b></p>	<p>a) on velvollinen ylläpitämään luetteloa rekisteröityjen henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista.</p> <p>b) on luovutettava luettelo pyydettyä Rekisterinpitäjälle.</p> <p>c) on luovutettava luettelossa mainittuja tietoja Rekisterinpitäjän pyytämässä laajuudessa Rekisterinpitäjän yksilöimille kolmansille tahoille.</p>
<p><b>19. Tietojen siirto</b></p>	<p>a) huolehdittava siitä, että sen käsittelemät henkilötiedot ovat sellaisessa yleisesti käytetyssä ja koneellisesti luettavassa muodossa, että ne voidaan <i>automaattisesti irrottaa järjestelmästä siirrettäväksi toiseen järjestelmään</i>.</p>
<p><b>20. Tietojen luovutus - rajoitukset</b></p>	<p>a) on oltava valmius asettaa ja hallinnoida tietojen luovutuksia koskevia rajoituksia, jollaisia voi aiheutua esimerkiksi väestötietolain mukaisesta rekisteröidyn turvakiellosta.</p> <p>b) tulee pystyä rajoittamaan rekisteröidyn henkilötietojen käsittelyä osittain tai kokonaan rekisterinpitäjän vaatimalla tavalla. Rekisteröidyn henkilötietojen rajoittaminen ei saa johtaa muiden rekisterissä olevien</p>

	luonnollisten henkilöiden henkilötietojen rajoittamiseen, ellei osapuolten kesken kirjallisesti toisin sovita.
<b>21. Tiedonanto – velvollisuus rekisterinpitäjälle</b>	<p>a) sitoutuu ilman aiheetonta viivästystä ilmoittamaan rekisterinpitäjälle kaikista <i>rekisteröityjen pyynnöistä</i>, jotka koskevat Tietosuojalainsäädännön mukaisten <i>rekisteröidyn oikeuksien käyttämistä</i>.</p> <p>b) sitoutuu ilmoittamaan <b>72 tunnin</b> sisällä rekisterinpitäjälle muista Käsittelijän tuottaman palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.</p> <p>c) on saatettava rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen, jotta voidaan osoittaa rekisterinpitäjän toimineen oikein.</p> <p>d) on välittömästi ilmoitettava rekisterinpitäjälle, jos Käsittelijä katsoo, että Rekisterinpitäjän ohjeistus rikkoo GDPR:ä tai muita tietosuojasäännöksiä.</p>
<b>22. Reagointiaika Rekisterinpitäjän yhteydenottoihin</b>	a) on reagoitava viimeistään 72 tunnin kuluessa rekisterinpitäjän yhteydenotosta ja vastaamaan viimeistään yhden (1) viikon kuluessa rekisterinpitäjän tietosuojaa koskeviin ilmoituksiin, reklamaatioihin tai muihin viesteihin.
<b>23. Auditointioikeus ja tarkastukset</b>	a) sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin. Tilaajalla on oikeus tarkistaa ja arvioida henkilötietojen käsittelijän menettelyt tietosuojan noudattamisesta kerran vuodessa. Tilaaja vastaa auditoinnin kustannuksista. Mikäli auditoinnin seurauksena havaitaan, että henkilötietojen käsittelijän tietoturvajärjestelyt eivät ole DPA-sopimuksen mukaiset, henkilötietojen käsittelijä sitoutuu tekemään tarvittavat korjaukset omalla kustannuksellaan.
<b>24. Käsittely EU:n tai ETA:n ulkopuolelle</b>	a) ei saa siirtää henkilötietoja EU:n tai ETA-alueen ulkopuolelle.
<b>25. Tietojen poistaminen ja palauttaminen Rekisterinpitäjälle</b>	<p>a) tulee poistaa tai palauttaa kaikki henkilötiedot rekisterinpitäjälle</p> <p>b) tulee poistaa olemassa olevat jäljennökset, jollei käsittelijällä ole lakisääteistä velvollisuutta säilyttää henkilötietoja, kun käsittelyyn liittyvien palveluiden tarjoaminen on päättynyt.</p>

## 7 HENKILÖTIETOJEN KÄSITTELIJÄN TEKNISET JA ORGANISATORISET TOIMENPITEET

7.1 Liitteessä 1.2 on oltava kuvaus henkilötietojen käsittelijän/käsittelijöiden toteuttamista teknisistä ja organisatorisista turvatoimenpiteistä (mukaan lukien asiaankuuluvat sertifioinnit) asianmukaisen turvallisuustason varmistamiseksi ja ottaen huomioon käsittelyn luonne, soveltamisala, asiayhteys ja tarkoitus sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.

## 8 SOPIMUKSEN NOUDATTAMATTA JÄTTÄMINEN JA SOPIMUKSEN PURKAMINEN

8.1 Jos henkilötietojen käsittelijä rikkoo näiden DPA-sopimuksen mukaisia velvoitteitaan, rekisterinpitäjä voi määrätä henkilötietojen käsittelijän *keskeyttämään* henkilötietojen käsittelyn, kunnes henkilötietojen käsittelijä noudattaa näitä lausekkeitä tai sopimus puretaan, sanotun kuitenkaan rajoittamatta GDPR säännösten soveltamista. Henkilötietojen käsittelijän on viipymättä ilmoitettava rekisterinpitäjälle, jos se ei mistä tahansa syystä pysty noudattamaan DPA-sopimusta.

8.2 Rekisterinpitäjällä on oikeus purkaa sopimus siltä osin kuin on kyse henkilötietojen käsittelystä DPA-sopimuksen mukaisesti, jos

- 1) rekisterinpitäjä on keskeyttänyt henkilötietojen käsittelijän suorittaman henkilötietojen käsittelyn kohdan 8.1 mukaisesti eikä DPA-sopimuksen noudattamista palauteta kohtuullisessa ajassa ja joka tapauksessa kuukauden kuluessa keskeyttämisestä;
- 2) henkilötietojen käsittelijä rikkoo olennaisesti tai jatkuvasti DPA-sopimusta tai GDPR:n mukaisia velvoitteitaan;
- 3) henkilötietojen käsittelijä ei noudata toimivaltaisen tuomioistuimen tai toimivaltais(t)en valvontaviranomais(t)en sitovaa päätöstä DPA-sopimuksen tai GDPR:n mukaisista

velvoitteistaan.

- 8.3 Henkilötietojen käsittelijällä on oikeus purkaa sopimus siltä osin kuin se koskee henkilötietojen käsittelyä DPA-sopimuksen nojalla, jos rekisterinpitäjä vaatii ohjeiden noudattamista sen jälkeen, kun käsittelijä

on kohdan 3.3 mukaisesti ilmoittanut rekisterinpitäjälle, että sen ohjeet ovat sovellettavien oikeudellisten vaatimusten vastaisia.

- 8.4 Kun sopimus on purettu, henkilötietojen käsittelijän on rekisterinpitäjän valinnan mukaan poistettava kaikki rekisterinpitäjän puolesta käsitellyt henkilötiedot ja todistettava rekisterinpitäjälle, että se on tehnyt niin, tai palautettava kaikki henkilötiedot rekisterinpitäjälle ja poistettava olemassa olevat jäljennökset, jollei unionin tai jäsenvaltion lainsäädännössä edellytetä henkilötietojen säilyttämistä. Henkilötietojen käsittelijän on varmistettava, että näitä lausekkeitä noudatetaan, kunnes tiedot poistetaan tai palautetaan.

## **9 VASTUU JA VAHINGONKORVAUS**

- 9.1 Osapuolen vastuu vahingoista ja oikeus korvaukseen määräytyy tietosuojalainsäädännön mukaan.
- 9.2 Jos rekisteröidylle aiheutuu vahinkoa tietosuojalainsäädännön rikkomisesta, Osapuolet vastaavat rekisteröidylle aiheutuneesta vahingosta tietosuojalainsäädännön mukaisesti. Osapuolet vastaavat tietosuojalainsäädännön mukaisesti valvontaviranomaisen mahdollisesti määräämistä hallinnollisista sakoista.
- 9.3 Käsittelijä on velvollinen puolustamaan kustannuksellaan rekisterinpitäjää, jos rekisteröity väittää, että rekisterinpitäjä on loukannut rekisteröidyn yksityisyyden suojaa, ja loukkauksen katsotaan johtuvan henkilötietojen käsittelijästä.

## **10 SOPIMUKSEN MUUTTAMINEN JA PÄIVITTÄMINEN**

- 10.1 Osapuolet sitoutuvat olemaan muuttamatta DPA-sopimusta ja sen lausekkeitä, lukuun ottamatta tietojen lisäämistä täytettäviin kohtiin tai niissä olevien tietojen päivittämistä.
- 10.2 Tämä ei estä osapuolia sisällyttämästä ja päivittämästä DPA-sopimukseen vakiosopimuslausekkeitä ja lisäämästä muita lausekkeitä tai täydentäviä suojatoimia edellyttäen, että ne eivät ole suoraan tai välillisesti ristiriidassa DPA-sopimuksen kanssa eivätkä rajoita rekisteröityjen perusoikeuksia tai vapauksia.
- 10.3 Jos jokin tämän DPA-sopimuksen ehto osoittautuu pätemättömäksi, se ei vaikuta DPS-sopimuksen muiden ehtojen voimassaoloon. Osapuolet korvaavat pätemättömän ehdon laillisella ehdolla, jonka tarkoitus vastaa pätemättömää ehtoa.

## **11 SOPIMUSLIITTEET**

- 11.1 DPA-sopimuksen liitteitä ovat muun muassa henkilötietojen käsittelystä, arkaluontoisten tietojen käsittelystä, alikäsittelijöistä laaditut liitteet:

LIITE 1.1 Henkilötietojen käsittelyn kuvaus

LIITE 1.2 Henkilötietojen käsittelijän tekniset ja organisatoriset toimet

LIITE 1.3 Henkilötietojen alikäsittelijöiden luettelo

LIITE 1.4 Keskeisiä tietosuojasäätelyn käsitteitä ja määritelmiä

## 12 SOPIMUKSEN VOIMASSAOLO JA ALLEKIRJOITUKSET

- 12.1 Tämä DPA-sopimus tulee voimaan, kun kumpikin osapuoli on sen allekirjoittanut.
- 12.2 DPA-sopimus on voimassa niin kauan kuin henkilötietojen käsittelijä käsittelee DPA-sopimuksen mukaisesti henkilötietoja. DPA-sopimuksen päättyessä henkilötietojen käsittelijä poistaa tai palauttaa rekisterinpitäjän puolesta käsittelemänsä henkilötiedot DPA-sopimuksen ehtojen mukaisesti.
- 12.3 Tätä DPA-sopimusta on tehty kaksi (2) samasanaista kappaletta, yksi kummallekin osapuolelle. Tämä DPA-sopimus voidaan allekirjoittaa sähköisesti.

**Rekisterinpitäjä:**

**HYVINVOINTILOMAT ry**

Helsingissä \_\_\_\_\_.2022

\_\_\_\_\_  
[tarkennetaan]  
toiminnanjohtaja

**Henkilötietojen käsittelijä:**

[nimi]

[Paikka] \_\_\_\_\_

\_\_\_\_\_  
[nimi/asema]

### 13 LIITE 1.1: HENKILÖTIETOJEN KÄSITTELYN KUVAUS

LIITE 1.1 Henkilötietojen käsittelijä saa käsitellä rekisterinpitäjän puolesta ja lukuun seuraavia rekisterinpitäjän henkilörekisteriin kuuluvia henkilötietoja:	
A. Henkilötietojen käsittelyn kohde/ henkilörekisterin nimi	[tarkennetaan]
B. Rekisteröityjen ryhmät, joiden henkilötietoja käsitellään	yhteyshenkilön tiedot: Nimi, Yhteystiedot lomalaisten tiedot: Nimi, Yhteystiedot, Terveystiedot ja erityistarpeet, Avustajan Nimi, Avustajan Yhteystiedot
C. Mitä henkilötietoja käsitellään eli käsiteltävät henkilötietoryhmät	ks. kohta B
D. Henkilötietojen käsittelyn luonne ja tarkoitus/ tarkoitukset, jota/joita varten henkilötietoja käsitellään rekisterinpitäjän puolesta	lomajaksojen tilaus ja hallinnointi lomajaksojen suunnittelu ja toteutus lomalaisten laskutus ja lomajärjestelyt lomalaisten majoitus tms.
E. Käsittelyaika	lomajakson päättymisen jälkeen, kunnes palautteet on kerätty [tarkennetaan]

LIITE 1.2 Käsiteltävät arkaluonteiset tiedot (jos sellaisia on)		
Arvioi aina liitteen <b>salassa pidettävyys</b> tapauskohtaisesti.		
Henkilötietojen käsittelijä saa käsitellä Rekisterinpitäjän puolesta ja lukuun seuraavia rekisterinpitäjän henkilörekisteriin kuuluvia <b>arkaluonteisia henkilötietoja</b> :	<b>Kyllä</b>	<b>Ei</b>
A. rotu tai etninen alkuperä		x
B. poliittiset mielipiteet		x
C. uskonnollinen tai filosofinen vakaumus		x
D. ammattiliiton jäsenyys		x
E. geneettisiä tietoja tai biometrisiä tietoja luonnollisen henkilön yksiselitteistä tunnistamista varten		x
F. terveyttä tai henkilön seksuaalista käyttäytymistä tai seksuaalista suuntautumista koskevia tietoja	x	
G. taikka rikostuomioihin ja rikoksiin liittyviä tietoja		x
H. Mitä erityisiä rajoituksia ja/tai täydentäviä suojatoimia sovelletut rajoitukset tai suojatoimet, joissa otetaan täysimääräisesti huomioon tietojen luonne ja niihin liittyvät riskit, kuten tiukat käyttötarkoituksen rajoitukset, pääsyräjoitukset (mukaan lukien pääsy vain erikoiskoulutusta saan henkilöstölle), tietojen saantia koskevan rekisterin pitäminen, tietojen edelleen siirtämisen rajoitukset tai lisäturvatoimenpiteet.		
[H. Rekisterinpitäjän kuvaus rajoituksista ja suojatoimista]		

## 14 LIITE 1.2: KÄSITTELIJÄN TEKNISET JA ORGANISATORISET TOIMENPITEET

### 2.1 Henkilötietojen käsittelijän tekniset ja organisatoriset toimenpiteet, mukaan lukien tekniset ja organisatoriset toimenpiteet tietoturvan varmistamiseksi.

Kuvaus **henkilötietojen käsittelijän/käsittelijöiden** toteuttamista teknisistä ja organisatorisista turvatoimenpiteistä (mukaan lukien asiaankuuluvat sertifiointit) asianmukaisen turvallisuustason varmistamiseksi ja ottaen huomioon käsittelyn luonne, soveltamisala, asiayhteys ja tarkoitus sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit.

#### **Esimerkkejä mahdollisista toimenpiteistä:**

1. Henkilötietojen pseudonymisointi ja salaus
2. Henkilötietojen käsittelyjärjestelmien ja palveluiden jatkuvan luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden varmistaminen
3. Henkilötietojen saatavuuden ja henkilötietoihin pääsyn nopean palauttamisen varmistaminen fyysisen tai teknisen vian sattuessa
4. Teknisten ja organisatoristen toimenpiteiden tehokkuuden säännöllisen testauksen, tutkinnan ja arvioinnin prosessit, joilla varmistetaan tietojen käsittelyn turvallisuus
5. Käyttäjän tunnistaminen ja luvan myöntäminen
6. Tietojen suojaaminen siirron aikana
7. Tietojen suojaaminen siirron aikana
8. Henkilötietojen käsittelypaikkojen fyysisen turvallisuuden varmistaminen
9. Tapahtumien kirjaamisen varmistaminen
10. Järjestelmän konfiguraation varmistaminen (ml. oletuskokoonpano)
11. Sisäistä tietotekniikka- ja tietoturvahallintoa ja koskevat toimenpiteet
12. Prosessien ja tuotteiden sertifiointi/varmistus
13. Prosessien ja tuotteiden sertifiointi/varmistus
14. Tietojen laadun varmistaminen
15. Tietojen rajoitetun säilyttämisen varmistaminen
16. Vastuuvollisuuden varmistaminen
17. Tietojen siirrettävyyden mahdollistaminen ja niiden poistamisen varmistaminen.
18. Jos kyseessä on siirto henkilötietojen (ali)käsittelijöille, kuvaile myös teknisiä ja organisatorisia toimenpiteitä, jotka (ali)käsittelijän on toteutettava voidakseen avustaa rekisterinpitäjää
19. toteutettava voidakseen avustaa rekisterinpitäjää
20. Kuvaus teknisistä ja organisatorisista toimenpiteistä, jotka henkilötietojen käsittelijän on toteutettava voidakseen avustaa rekisterinpitäjää.

### 2.2 Henkilötietojen käsittelijä kuvaus konkreettisista toimenpiteistään:

Tekniset ja organisatoriset toimenpiteet on kuvattava konkreettisesti eikä yleisellä tasolla.

[Henkilötietojen käsittelijä kuvaa tähän tekniset ja organisatoriset toimenpiteesi]

## 15 LIITE 1.3: HENKILÖTIETOJEN ALIKÄSITTELIJÖIDEN LUETTELO

<p><b>VAIHTOEHTO 1: ERILLINEN ENNAKKOLUPA:</b> Henkilötietojen käsittelijä ei saa antaa mitään rekisterinpitäjän puolesta DPA-sopimuksen nojalla suorittamistaan käsittelytoimista alihankintana henkilötietojen alikäsittelijälle ilman rekisterinpitäjän erillistä kirjallista ennakkolupaa.</p> <p>Henkilötietojen käsittelijän on toimitettava erillistä lupaa koskeva pyyntö vähintään [<b>MÄÄRITÄ AJANJAKSO</b>] ennen asianomaisen henkilötietojen alikäsittelijän palkkaamista sekä tarvittavat tiedot, jotta rekisterinpitäjä voi päättää luvasta.</p> <p>Luettelo rekisterinpitäjän valtuuttamista henkilötietojen alikäsittelijöistä on alla, jota Osapuolten on pidettävä ajan tasalla.</p>	
<p><b>1.ERILLINEN ENNAKKOLUPA: Henkilötietojen alikäsittelijöiden luettelo</b> Tämä kohta on täytettävä, jos henkilötietojen alikäsittelijälle on myönnetty erillinen lupa.</p>	
<p>Rekisterinpitäjä on antanut luvan seuraavien henkilötietojen alikäsittelijöiden käyttöön:</p>	
<p><u>1.Nimi ja osoite</u></p>	<p>[täytettävä]</p>
<p><u>Yhteyshenkilö:</u> nimi, asema ja yhteystiedot</p>	<p>[täytettävä]</p>
<p><u>Kuvaus henkilötietojen käsittelystä</u> (mukaan lukien selkeä vastuunjako, jos lupa on myönnetty useammalle henkilötietojen alikäsittelijälle)</p>	<p>[täytettävä]</p>
<p><u>2.Nimi ja osoite</u> (jatka em. luetteloa)</p>	<p>[täytettävä]</p>
<p><u>Yhteyshenkilö:</u> nimi, asema ja yhteystiedot</p>	<p>[täytettävä]</p>
<p><u>Kuvaus henkilötietojen käsittelystä</u> (mukaan lukien selkeä vastuunjako, jos lupa on myönnetty useammalle henkilötietojen alikäsittelijälle)</p>	<p>[täytettävä]</p>
<p><u>3.Nimi ja osoite</u> (jatka em. luetteloa)</p>	<p>[täytettävä]</p>

## 16 LIITE 1.4 KESKEISIÄ TIETOSUOJASÄÄNTELYN MÄÄRITELMIÄ

<b>EU:n yleinen tietosuoja-asetus tai Tietosuoja-asetus (TSA tai GDPR)</b>	EU:n yleinen tietosuoja-asetus (EU 2016/679), annettu 27.04.2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. Velvoittaa rekisterinpitäjää huolehtimaan tietoturvasuudesta koko henkilötietojen elinkaaren ajan. Henkilötietojen elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon. Voimassa 25.5.2018 alkaen.
<b>Tietosuoja laki (TiSL)</b>	Tietosuoja laki (1050/2018) on EU:n yleistä tietosuoja-asetusta täydentävää lainsäädäntöä, jolla kumottiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta.
<b>Tietosujalainsäädäntö</b>	Tietosuoja-asetus, tietosuoja laki ja muut tietosujasääntely yhdessä.
<b>Henkilötieto</b>	Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (jäljempänä ”rekisteröity”) liittyvät tiedot.  Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, osoitteen, henkilötunnuksen, kuvan, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, biometrisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.
<b>Arkaluonteiset henkilötiedot</b>	Jos käsittelyyn liittyy henkilötietoja, joista käy ilmi rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja tai biometrisiä tietoja luonnollisen henkilön yksiselitteistä tunnistamista varten, terveyttä tai henkilön seksuaalista käyttäytymistä tai seksuaalista suuntautumista koskevia tietoja taikka rikostuomioihin ja rikoksiin liittyviä tietoja, jäljempänä ’arkaluonteiset tiedot’, henkilötietojen käsittelijän on sovellettava erityisiä rajoituksia ja/tai täydentäviä suojatoimia.
<b>Rekisterinpitäjä</b>	<ul style="list-style-type: none"> <li>• on se, joka on saanut suostumuksen Rekisteröidyltä henkilötietojensa käsittelyyn ja määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.</li> <li>• vastaa tietosuoja-asetuksen mukaan siitä, että rekisterinpitäjän käyttämät henkilötiedon käsittelijät noudattavat soveltuvaan lainsäädäntöä.</li> </ul>
<b>Henkilötietojen käsittelijä (”Käsittelijä”)</b>	Luonnollinen tai oikeushenkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun DPA-sopimuksen ja rekisterinpitäjän antamien ohjeiden perusteella. (Esimerkiksi tilitoimisto, sovellustoimittaja jne.)
<b>Rekisteröity</b>	Henkilö, jonka Henkilötietoja käsitellään ja joka on antanut Rekisterinpitäjälle suostumuksensa Henkilötietojensa käsittelyyn.
<b>Henkilötietojen käsittely</b>	Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

<b>Henkilötietojen tietoturvaloukkaus</b>	Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.
<b>Tietosuojaja</b>	<b>Yksityisyyden suojaaminen</b> henkilötietoja käsiteltäessä.
<b>Tietosuojaperiaatteet</b>	<p>Tietosuojajaperiaatteissa säädetään <b>henkilötietojen käsittelyä koskevista periaatteista</b>, jotka tulee ottaa huomioon henkilötietojen käsittelyssä. Tietosuojaperiaatteilla on tärkeä merkitys myös käytännössä, kun on arvioitava mikä on sallittua.</p> <p>Tietosuojajaperiaatteita ovat:</p> <ul style="list-style-type: none"><li>• käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys</li><li>• käyttötarkoitussidonnaisuus</li><li>• tietojen minimointi</li><li>• tietojen täsmällisyys</li><li>• tietojen säilytyksen rajoittaminen</li><li>• tietojen eheys ja luottamuksellisuus</li><li>• rekisterinpitäjän osoitusvelvollisuus.</li></ul>
<b>Anonymisointi</b>	Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista.
<b>Tietosuojavaltuutetun toimisto</b>	Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista.  <a href="https://tietosuojafi">https://tietosuojafi</a>