

***Tämä asiakirja on suomenkielinen käännös englanninkielisestä sopimuksellisesti sitovista ehdoista ja määräyksistä**

Muutoshistoria

VERSIO

- **2.0** Tarkistus ja vakiomuotoisen tietojenkäsittelysopimuksen luominen.
- **3.0** Tarvittava tarkistus, ei olennaisia muutoksia.

TIETOJENKÄSITTELYSOPIMUS

Vakiosopimuslausekkeet – GDPR-asetuksen (2016/679) 28 artiklan 3 kohdan mukaisesti

osapuolten välillä

Yritys, joka tekee palvelu- ja/tai tuotteen hankintasopimuksen Avonova Solutionsin kanssa erillisellä sopimuksella

(rekisterinpitäjä)

ja

Avonova Solutions AS

Y-tunnus: 925160601

Avonova Solutions AB

Y-tunnus: 556680-5981

Avonova Solutions OY

Y-tunnus: 3406862-8

(tietojenkäsittelijä)

Jokainen erikseen ”osapuoli”; yhdessä ”osapuolet”.

Osapuolet ovat sopineet allekirjoittamalla hankintasopimuksen myös seuraavista sopimuslausekkeista (”lausekkeet”) täyttääkseen GDPR:n vaatimukset ja varmistaakseen rekisteröidyn oikeuksien suojelun.

Sisällysluettelo

1. Sisällysluettelo
2. Esipuhe
3. Rekisterinpitäjän oikeudet ja velvollisuudet
4. Henkilötietojen käsittelijä toimii ohjeiden mukaisesti
5. Luottamuksellisuus
6. Käsittelyn turvallisuus
7. Alihankkijoiden käyttö
8. Tietojen siirto kolmansiin maihin tai kansainvälisiin organisaatioihin
9. Rekisterinpitäjän avustaminen
10. Henkilötietojen tietoturvaloukkauksen ilmoittaminen
11. Tietojen poistaminen ja palauttaminen
12. Auditointi ja tarkastus
13. Osapuolten sopimus muista ehdoista
14. Sopimuksen voimaantulo ja päätyminen
15. Rekisterinpitäjän ja henkilötietojen käsittelijän yhteystiedot/yhteyspisteet
 - Liite A Käsittelyä koskevat tiedot
 - Liite B Hyväksytyt alihankkijat
 - Liite C Ohjeet henkilötietojen käsittelyyn
 - Liite D Osapuolten sopimusehdot muihin aiheisiin liittyen

2. Esipuhe

1. Nämä sopimuslausekkeet (jäljempänä "Lausekkeet") määrittelevät rekisterinpitäjän ja henkilötietojen käsittelijän oikeudet ja velvollisuudet, kun henkilötietoja käsitellään rekisterinpitäjän lukuun. Tämä henkilötietojen käsittelysopimus hyväksytään osapuolten välillä Avonova Assist -palvelun toimitusta koskevan sopimuksen solmimisen yhteydessä.
2. Lausekkeet on laadittu varmistamaan osapuolten noudattaminen Euroopan parlamentin ja neuvoston 27. huhtikuuta 2016 antaman asetuksen (EU) 2016/679 (luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, jäljempänä yleinen tietosuoja-asetus) 28 artiklan 3 kohdan mukaisesti.
3. Avonova Digital -palvelun tarjoamisen yhteydessä henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun Lausekkeiden mukaisesti.
4. Lausekkeet ovat ensisijaisia muihin osapuolten välisten sopimusten vastaaviin määräyksiin nähden.
5. Lausekkeisiin on liitetty neljä liitettä, jotka muodostavat erottamattoman osan Lausekkeista.
6. Liitteessä A esitetään yksityiskohtaiset tiedot henkilötietojen käsittelystä, mukaan lukien käsittelyn tarkoitus ja luonne, henkilötietojen tyypit, rekisteröityjen ryhmät ja käsittelyn kesto.
7. Liitteessä B määritellään rekisterinpitäjän asettamat ehdot henkilötietojen käsittelijän alihankkijoiden käytölle sekä luettelo rekisterinpitäjän hyväksymistä alihankkijoista.
8. Liitteessä C annetaan rekisterinpitäjän ohjeet henkilötietojen käsittelyyn, vähimmäisturvatoimenpiteet, jotka henkilötietojen käsittelijän on toteutettava, sekä auditointien suorittamiseen liittyvät ohjeet käsittelijälle ja mahdollisille alihankkijoille.
9. Liitteessä D esitetään määräykset muista toimista, joita Lausekkeet eivät kata.
10. Lausekkeet ja niiden liitteet on säilytettävä kirjallisesti, myös sähköisesti, kummankin osapuolen toimesta.
11. Lausekkeet eivät vapauta henkilötietojen käsittelijää niistä velvoitteista, joita yleinen tietosuoja-asetus (GDPR) tai muu lainsäädäntö asettavat henkilötietojen käsittelijälle.

3. Rekisterinpitäjän oikeudet ja velvollisuudet

1. Rekisterinpitäjä vastaa siitä, että henkilötietojen käsittely tapahtuu GDPR:n (katso GDPR:n 24 artikla), sovellettavan EU:n tai jäsenvaltion tietosuojalainsäädännön ja näiden Lausekkeiden mukaisesti.
2. Rekisterinpitäjällä on oikeus ja velvollisuus päättää henkilötietojen käsittelyn tarkoituksista ja keinoista.
3. Rekisterinpitäjä vastaa muun muassa siitä, että henkilötietojen käsittelyllä, jota käsittelijältä pyydetään, on lainmukainen peruste.

4. Henkilötietojen käsittelijä toimii annettujen ohjeiden mukaisesti

1. Henkilötietojen käsittelijä saa käsitellä henkilötietoja vain rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti, ellei käsittelijää velvoita tähän EU:n tai jäsenvaltion lainsäädäntö. Tällaiset ohjeet määritellään liitteissä A ja C. Rekisterinpitäjä voi antaa lisäohjeita koko henkilötietojen käsittelyn ajan, mutta ohjeet on aina dokumentoitava ja säilytettävä kirjallisessa muodossa, myös sähköisesti, osana näitä Lausekkeitä.
2. Henkilötietojen käsittelijän on viipymättä ilmoitettava rekisterinpitäjälle, jos tämän antamat ohjeet käsittelijän näkemyksen mukaan ovat ristiriidassa GDPR:n tai sovellettavan EU:n tai jäsenvaltion tietosuojalainsäädännön kanssa.

5. Luottamuksellisuus

1. Henkilötietojen käsittelijä sallii pääsyn rekisterinpitäjän lukuun käsiteltäviin henkilötietoihin vain sellaisille käsittelijän toimivallan alaisille henkilöille, jotka ovat sitoutuneet luottamuksellisuuteen tai joita sitoo asianmukainen lakisääteinen salassapitovelvollisuus, ja ainoastaan, jos pääsy on tarpeen. Pääsyä saaneiden henkilöiden luetteloa tarkastellaan säännöllisesti. Tämän tarkastelun perusteella pääsy henkilötietoihin voidaan poistaa, jos sitä ei enää tarvita, eikä henkilötietojen tule olla enää tällöin näiden henkilöiden saatavilla.
2. Henkilötietojen käsittelijän on rekisterinpitäjän pyynnöstä osoitettava, että käsittelijän toimivallan alaiset henkilöt ovat edellä mainitun luottamuksellisuuden alaisia.

6. Käsittelyn turvallisuus

1. GDPR:n 32 artiklan mukaan, ottaen huomioon tekniikan tason, toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja

tarkoitukset sekä oikeuksien ja vapauksien suojaamiseen kohdistuvan riskin todennäköisyys ja vakavuus, rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan riskin mukainen tietoturvan taso.

Rekisterinpitäjän on arvioitava käsittelyyn liittyvät riskit luonnollisten henkilöiden oikeuksille ja vapauksille sekä toteutettava toimenpiteitä näiden riskien lieventämiseksi. Toimenpiteet voivat niiden merkityksellisyyden mukaan sisältää esimerkiksi:

- a. Henkilötietojen pseudonymisointi ja sala
 - b. kyky varmistaa käsittelyjärjestelmien ja -palveluiden jatkuva luottamuksellisuus, eheys, saatavuus ja kestävyys;
 - c. kyky palauttaa henkilökohtaisiin tietoihin pääsy ja saatavuus ajallaan fyysisen tai teknisen häiriön sattuessa;
 - d. prosessi, jonka avulla testataan, arvioidaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta käsittelyn turvallisuuden varmistamiseksi.
2. GDPR:n 32 artiklan mukaan tietojenkäsittelijän on myös – riippumatta rekisterinpitäjästä – arvioitava luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvät riskit, jotka ovat syntyneet käsittelytoimista, ja toteutettava toimenpiteet näiden riskien lieventämiseksi. Tätä varten rekisterinpitäjän on annettava tietojenkäsittelijälle kaikki tiedot, jotka ovat tarpeen tällaisten riskien tunnistamiseksi ja arvioimiseksi.
 3. Lisäksi tietojenkäsittelijän on avustettava rekisterinpitäjää varmistamaan rekisterinpitäjän velvoitteiden täyttämisen 32 artiklan mukaisesti, muun muassa antamalla rekisterinpitäjälle tietoa niistä teknisistä ja organisatorisista toimenpiteistä, jotka tietojenkäsittelijä on jo toteuttanut 32 artiklan mukaisesti, sekä muista tiedoista, jotka ovat tarpeen rekisterinpitäjän velvoitteiden täyttämiseksi 32 artiklan mukaisesti.

Jos myöhemmin rekisterinpitäjän arvioinnin mukaan riskien lieventämiseksi tarvitaan lisätoimenpiteitä, joita tietojenkäsittelijä ei ole vielä toteuttanut 32 artiklan mukaisesti, rekisterinpitäjän on määriteltävä nämä lisätoimenpiteet liitteessä C.

7. Alikäsittelijöiden käyttö

1. Tietojenkäsittelijän on täytettävä 28 artiklan 2 ja 4 kohtien vaatimukset voidakseen käyttää toista käsittelijää (alikäsitelijää).

1. Lausekkeissa tehtävät viittaukset "jäsenvaltioihin" on ymmärrettävä viittauksiksi "ETA:n jäsenvaltioihin".

2. Tietojenkäsittelijä ei saa siten käyttää toista käsittelijää (alikäsitteijää) lausekkeiden täyttämiseksi ilman rekisterinpitäjän etukäteistä kirjallista hyväksyntää.
3. Tietojenkäsittelijällä on rekisterinpitäjän yleinen hyväksyntä alikäsitteijöiden käyttämiseen. Tietojenkäsittelijän on ilmoitettava rekisterinpitäjälle kirjallisesti kaikista suunnitelluista muutoksista, jotka koskevat alikäsitteijöiden lisäämistä tai korvaamista, vähintään 1 kuukausi etukäteen, jolloin rekisterinpitäjällä on mahdollisuus vastustaa tällaisia muutoksia ennen kyseisen alikäsitteijän käyttöön ottamista. Erityisten alikäsitteilypalveluiden osalta voidaan liitteessä B määrätä pidemmistä etukäteisilmoitusaikaväleistä. Lista rekisterinpitäjän jo hyväksymistä alikäsitteijöistä löytyy liitteestä B.
4. Jos tietojenkäsittelijä käyttää alikäsitteijää suorittamaan tiettyjä käsittelytoimia rekisterinpitäjän puolesta, samat tietosuojavelvoitteet, jotka on määritelty lausekkeissa, on asetettava alikäsitteijälle EU:n tai jäsenvaltion lain mukaisella sopimuksella tai muulla oikeustoimella, erityisesti tarjoten riittävät takeet toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet siten, että käsittely täyttää lausekkeiden ja GDPR:n vaatimukset.

Tietojenkäsittelijän on siis varmistettava, että alikäsitteijä noudattaa vähintään niitä velvoitteita, joihin tietojenkäsittelijä on velvollinen lausekkeiden ja GDPR:n mukaan.

5. Kopio tällaisesta alikäsitteijäsopimuksesta ja myöhemmistä muutoksista on – rekisterinpitäjän pyynnöstä – toimitettava rekisterinpitäjälle, jolloin rekisterinpitäjällä on mahdollisuus varmistaa, että samat tietosuojavelvoitteet, jotka on määritelty lausekkeissa, on asetettu alikäsitteijälle. Liiketoimintaan liittyvät lausekkeet, jotka eivät vaikuta alikäsitteijäsopimuksen oikeudelliseen tietosuojasisältöön, eivät vaadi toimitusta rekisterinpitäjälle.
6. Tietojenkäsittelijän on sovittava kolmannen osapuolen edunsaajalausunnosta alikäsitteijän kanssa, jossa – jos tietojenkäsittelijä menee konkurssiin – rekisterinpitäjä on alikäsitteijäsopimuksen kolmas osapuoli ja sillä on oikeus panna sopimus täytäntöön tietojenkäsittelijän käyttämää alikäsitteijää vastaan, esimerkiksi mahdollistamalla rekisterinpitäjälle ohjeistaa alikäsitteijää poistamaan tai palauttamaan henkilökohtaiset tiedot.
7. Jos alikäsitteijä ei täytä tietosuojavelvoitteitaan, tietojenkäsittelijä vastaa täysimääräisesti rekisterinpitäjälle alikäsitteijän velvoitteiden täyttämisestä. Tämä ei vaikuta rekisteröityjen oikeuksiin GDPR:n mukaan – erityisesti niihin, jotka on ennakoitu artikloissa 79 ja 82 GDPR – rekisterinpitäjää ja tietojenkäsittelijää vastaan, mukaan lukien alikäsitteijä.

8. Henkilötietojen siirto kolmansille maille tai kansainvälisiin järjestöihin

1. Tietojenkäsittelijän suorittama henkilötietojen siirto kolmansille maille tai kansainvälisiin järjestöihin tapahtuu vain rekisterinpitäjän dokumentoitujen ohjeiden perusteella ja aina GDPR:n V luvun mukaisesti.
2. Mikäli kolmansille maille tai kansainvälisiin järjestöihin suoritettavat siirrot, joita tietojenkäsittelijä ei ole saanut suorittaa rekisterinpitäjän ohjeiden mukaan, ovat tarpeen EU:n tai jäsenvaltion lain mukaan, johon tietojenkäsittelijä on alistettu, tietojenkäsittelijän on ilmoitettava rekisterinpitäjälle tästä laillisesta vaatimuksesta ennen käsittelyn aloittamista, ellei laki estä tällaisen tiedon antamista tärkeän julkisen edun vuoksi.
3. Ilman rekisterinpitäjän dokumentoituja ohjeita tietojenkäsittelijä ei siis voi lausekkeiden puitteissa:
 - a. siirtää henkilötietoja rekisterinpitäjälle tai tietojenkäsittelijälle kolmanteen maahan tai kansainväliseen järjestöön,
 - b. siirtää henkilötietojen käsittelyä alikäsittelijälle kolmanteen maahan.
 - c. antaa henkilötiedot käsiteltäväksi tietojenkäsittelijän toimesta kolmannessa maassa
4. Rekisterinpitäjän ohjeet, jotka koskevat henkilötietojen siirtoa kolmanteen maahan, mukaan lukien tarvittaessa siirtotyökalu, joka perustuu GDPR:n V lukuun, asetetaan liitteessä C.6.
5. Lausekkeita ei tule sekoittaa GDPR:n artiklan 46(2)(c) ja (d) mukaisiin vakiotietosuojalausekkeisiin, eikä lausekkeita voida käyttää osapuolten siirtotyökaluna GDPR:n V luvun mukaan.

9. Rekisterinpitäjän avustaminen

1. Ottaen huomioon käsittelyn luonteen, tietojenkäsittelijän on avustettava rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, siltä osin kuin se on mahdollista, rekisterinpitäjän velvoitteiden täyttämiseksi vastata rekisteröidyn oikeuksia koskeviin pyyntöihin, jotka on säädetty GDPR:n III luvussa. Tämä tarkoittaa, että tietojenkäsittelijän on, siltä osin kuin se on mahdollista, avustettava rekisterinpitäjää seuraavissa asioissa:
 - a. oikeus saada tieto, kun henkilötiedot kerätään rekisteröidyltä,
 - b. oikeus saada tieto, kun henkilötietoja ei ole saatu rekisteröidyltä,
 - c. rekisteröidyn oikeus saada pääsy tietoihin,
 - d. oikeus oikaisuun,
 - e. oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi"),
 - f. oikeus rajoittaa käsittelyä,
 - g. ilmoitusvelvollisuus tietojen oikaisemisesta tai poistamisesta tai käsittelyn

rajoittamisesta,

h. oikeus siirtää tiedot,

i. oikeus vastustaa käsittelyä,

j. oikeus olla joutumatta päätökseen, joka perustuu pelkästään automatisoituun käsittelyyn, mukaan lukien profilointi.

2. Lisäksi tietojenkäsittelijän velvollisuus avustaa rekisterinpitäjää lausekkeen 6.3 mukaisesti, tietojenkäsittelijän on lisäksi, ottaen huomioon käsittelyn luonteen ja saatavilla olevat tiedot, avustettava rekisterinpitäjää seuraavissa:

a. Rekisterinpitäjän velvollisuus ilmoittaa ilman aiheetonta viivytystä ja jos mahdollista, mutta kuitenkin viimeistään 72 tunnin kuluessa tiedon saamisesta, henkilötietojen tietoturvaloukkauksesta asianmukaiselle valvontaviranomaiselle, Norjan tietosuojaviranomaiselle (Datatilsynet) ja/tai Ruotsin yksityisyyden suojan viranomaiselle (IMY) ja/tai Suomen tietosuojavaltuutetun toimistolle, ellei tietoturvaloukkaus ole epätodennäköinen ja se ei aiheuta riskiä luonnollisten henkilöiden oikeuksille ja vapauksille;

b. Rekisterinpitäjän velvollisuus ilman aiheetonta viivytystä tiedottaa rekisteröidylle henkilötietojen tietoturvaloukkauksesta, kun loukkaus todennäköisesti aiheuttaa suuren riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

c. rekisterinpitäjän velvollisuus suorittaa arviointi ennakoituista käsittelytoimista henkilötietojen suojan osalta (tietosuojavaikutusten arviointi);

d. rekisterinpitäjän velvollisuus neuvotella asianomaisen valvontaviranomaisen, Norjan tietosuojaviranomaisen (Datatilsynet) ja/tai Ruotsin yksityisyyden suojan viranomaisen (IMY) ja/tai Suomen tietosuojavaltuutetun toimiston kanssa ennen käsittelyn aloittamista, jos tietosuojavaikutusten arviointi osoittaa, että käsittely aiheuttaisi suuren riskin, ellei rekisterinpitäjä ole ryhtynyt toimiin riskin lieventämiseksi.

3. Osapuolet määrittelevät liitteessä C asianmukaiset tekniset ja organisatoriset toimenpiteet, joiden avulla tietojenkäsittelijän on avustettava rekisterinpitäjää sekä avun laajuuden että vaadittavan avun laajuuden. Tämä koskee lausekkeessa 9.1. ja 9.2. ennakoituja velvoitteita.

10. Henkilötietojen tietoturvaloukkauksen ilmoittaminen

1. Henkilötietojen tietoturvaloukkauksen yhteydessä tietojenkäsittelijän on ilmoitettava rekisterinpitäjälle ilman aiheetonta viivytystä sen jälkeen, kun se on saanut tiedon loukkauksesta.

2. Tietojenkäsittelijän ilmoitus rekisterinpitäjälle tulee, jos mahdollista, tapahtua 72 tunnin kuluessa siitä, kun tietojenkäsittelijä on saanut tiedon tietoturvaloukkauksesta, jotta rekisterinpitäjä voi täyttää velvollisuutensa ilmoittaa tietoturvaloukkauksesta asianomaiselle valvontaviranomaiselle, ks. artikla 33 GDPR.
3. Lausekkeen 9(2)(a) mukaisesti tietojenkäsittelijän on avustettava rekisterinpitäjää ilmoittamaan tietoturvaloukkaus asianomaiselle valvontaviranomaiselle, mikä tarkoittaa, että tietojenkäsittelijän on avustettava seuraavien tietojen hankkimisessa, jotka rekisterinpitäjän on ilmoitettava valvontaviranomaiselle artiklan 33(3) mukaisesti:
 - a. Henkilötietojen luonne, mukaan lukien, jos mahdollista, asianomaisille rekisteröidyille kuuluvat kategoriat ja arvioitu määrä sekä henkilötietojen tietueiden kategoriat ja arvioitu määrä;
 - b. tietoturvaloukkauksen todennäköiset seuraukset;
 - c. toimenpiteet, joita rekisterinpitäjä on toteuttanut tai aikoo toteuttaa henkilötietojen tietoturvaloukkauksen käsittelemiseksi, mukaan lukien tarvittaessa toimenpiteet mahdollisten haitallisten vaikutusten lieventämiseksi.
4. Osapuolet määrittelevät liitteessä C kaikki ne elementit, jotka tietojenkäsittelijän on toimitettava avustaessaan rekisterinpitäjää tietoturvaloukkauksen ilmoittamisessa asianomaiselle valvontaviranomaiselle.

11. Tietojen poistaminen ja palauttaminen

1. Kun henkilötietojen käsittelypalvelun toimittaminen päättyy, tietojenkäsittelijällä on velvollisuus poistaa kaikki rekisterinpitäjän puolesta käsitellyt henkilötiedot, ellei unionin tai jäsenvaltion lainsäädäntö vaadi henkilötietojen säilyttämistä.

Tietojenkäsittelijä sitoutuu käsittelemään henkilötiedot yksinomaan tämän lain mukaisiin tarkoituksiin ja sen määrittämään keston sekä tiukasti sovellettavien ehtojen alaisena.

12. Auditointi ja tarkastukset

1. Tietojenkäsittelijän on annettava rekisterinpitäjälle kaikki tarvittavat tiedot, jotka osoittavat noudattamisen artiklan 28 ja lausekkeiden mukaisista velvoitteista, ja sen on mahdollistettava ja osallistuttava tarkastuksiin, mukaan lukien tarkastukset, jotka rekisterinpitäjä tai muu rekisterinpitäjän valtuuttama tarkastaja suorittaa.
2. Rekisterinpitäjän tietojenkäsittelijän ja alikäsittelijöiden tarkastuksiin, mukaan lukien tarkastukset, sovellettavat menettelyt on määritelty liitteissä C.7. ja C.8.
3. Tietojenkäsittelijän on annettava valvontaviranomaisille, jotka voimassa olevan lainsäädännön mukaan voivat päästä rekisterinpitäjän ja tietojenkäsittelijän tiloihin, tai edustajille, jotka toimivat näiden valvontaviranomaisten puolesta, pääsy tietojenkäsittelijän fyysisiin tiloihin esittämällä asianmukaiset tunnistautumistiedot.

13. Osapuolten sopimus muista ehdoista

1. Osapuolet voivat sopia muista lausekkeista, jotka koskevat henkilötietojen käsittelypalvelun tarjoamista, kuten esimerkiksi vastuukysymyksistä, kunhan ne eivät suoraan tai epäsuorasti ole ristiriidassa Lausekkeiden kanssa tai vaaranna rekisteröidyn perusoikeuksia ja -vapauksia sekä GDPR:n tarjoamaa suojaa.

14. Voimaantulo ja päättyminen

1. Lausekkeet tulevat voimaan, kun ostopalvelusopimus Avonovan kanssa on hyväksytty, johon tämä sopimus liittyy.
2. Molemmilla osapuolilla on oikeus vaatia Lausekkeiden uudelleenneuvottelua, jos lainsäädännössä tapahtuu muutoksia tai jos Lausekkeet eivät ole enää tarkoituksenmukaisia.
3. Lausekkeet ovat voimassa niin kauan kuin henkilötietojen käsittelypalveluja tarjotaan. Henkilötietojen käsittelypalvelujen tarjoamisen aikana Lausekkeitä ei voida irtisanoa, ellei osapuolten välillä ole sovittu muista Lausekkeista, jotka säätelevät henkilötietojen käsittelypalveluja.
4. Jos henkilötietojen käsittelypalvelujen tarjoaminen lopetetaan ja henkilötiedot poistetaan tai palautetaan rekisterinpitäjälle Lausekkeen 11.1. ja Liitteen C.4. mukaisesti, Lausekkeet voivat päättyä kirjallisella ilmoituksella kummaltakin osapuolelta.

15. Rekisterinpitäjän ja henkilötietojen käsittelijän yhteystiedot/yhteyspisteet

1. Osapuolet voivat olla yhteydessä toisiinsa seuraavien yhteystietojen/yhteyspisteiden kautta:
2. Osapuolten on jatkuvasti informoitava toisiaan yhteystietojen/yhteyspisteiden muutoksista.

Rekisterinpitäjän yhteystiedot ovat samat kuin ostopalvelusopimuksessa.

Henkilötietojen käsittelijän yhteystiedot:

Nimi: Julie Hem

Asema: DPO

Sähköposti: gdpr@avonova.com

Liite A: Tiedot käsittelystä

Alla kuvataan tietojen käsittelijän suorittaman henkilötietojen käsittelyn tarkoitus, luonne ja tyyppi rekisterinpitäjän puolesta:

Tarkoitus	Henkilötiedot	Oikeusperusta	Säilytysaika
Asiakassuhteiden hallinta	Tilaustiedot, Laskutustiedot, Identiteettitiedot, Viestintä, Yhteystiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään asiakassuhteen hallinnoimiseksi. Sopimuksen täyttäminen, GDPR art. 6(1)(b). Jos sopimus on tehty toiminimen kanssa.	Henkilötietoja säilytetään niin kauan kuin suhde on aktiivinen ja kymmenen (10) vuotta sen jälkeen oikeutetun etumme turvaamiseksi juridisiin vaatimuksiin vastaamisessa.
Tilausten käsittely	Tilaustiedot, Laskutustiedot, Identiteettitiedot, Viestintä, Yhteystiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään tilausten käsittelemiseksi. Sopimuksen täyttäminen, GDPR art. 6(1)(b). Jos sopimus on tehty toiminimen kanssa.	Henkilötietoja säilytetään niin kauan kuin on tarpeen tilauksen käsittelyyn ja kymmenen (10) vuotta sen jälkeen oikeutetun etumme turvaamiseksi juridisiin vaatimuksiin vastaamisessa.
Asiakassuhteiden seuranta ja arviointi	Tilaustiedot, Laskutuksen peruste, Identiteettitiedot, Viestintä, Yhteystiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään asiakassuhteiden seuraamiseksi.	Henkilötietoja säilytetään 27 kuukautta keräyshetkestä. Yleisraportit ja tilastot, jotka eivät sisällä henkilötietoja, säilytetään toistaiseksi tai kunnes ne poistetaan.
Kysymyksiin vastaaminen ja asiakaspalvelu	Tilaustiedot, Laskutustiedot, Identiteettitiedot, Viestintä,	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään asiakaskyselyihin vastaamiseksi ja	Henkilötietoja säilytetään kuusi (6) kuukautta tapauksen päättymisestä.

	Yhteystiedot, Profiilitiedot	asiakaspalvelun tarjoamiseksi.	
Uutiskirjeen lähettäminen	Identiteettitiedot, Yhteystiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään uutiskirjeen lähettämiseksi sen tilanneille.	Henkilötietoja säilytetään toistaiseksi ja siihen asti, kunnes peruutat uutiskirjeen tilauksen.
Liiketoiminnan seuranta ja arviointi	Identiteettitiedot, Tilaustiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään liiketoiminnan arvioimiseksi ja seuraamiseksi.	Henkilötietoja säilytetään 27 kuukautta keräyshetkestä. Yleisraportit ja tilastot, jotka eivät sisällä henkilötietoja, säilytetään toistaiseksi tai kunnes ne poistetaan.
Toiminnan kehittäminen ja parantaminen	Identiteettitiedot, Tilaustiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään toiminnan kehittämiseksi ja parantamiseksi.	Henkilötietoja säilytetään 27 kuukautta keräyshetkestä. Yleisraportit ja tilastot, jotka eivät sisällä henkilötietoja, säilytetään toistaiseksi tai kunnes ne poistetaan.
Toiminnan dokumentointi	Kuvamateriaali ja äänitallenteet, Identiteettitiedot, Viestintä, Yhteystiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään toiminnan dokumentoimiseksi.	Henkilötietoja säilytetään pääsääntöisesti toistaiseksi.
Kyselyjen suorittaminen	Identiteettitiedot, Viestintä, Yhteystiedot, Profiilitiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään liiketoiminnan ja palvelujen arvioimiseksi.	Henkilötietoja säilytetään kyselyn keston ajan ja kolme (3) kuukautta sen jälkeen vastausten raportointia varten. Yleisraportit ja tilastot säilytetään toistaiseksi tai

			kunnes ne poistetaan.
Tekninen toimivuus ja turvallisuus	Kaikki henkilötietokategoriat	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään järjestelmien teknisen toimivuuden ja turvallisuuden takaamiseksi.	Säilytysajat määräytyvät kunkin käsittelytarkoituksen mukaisesti. Lokitiedot säilytetään 13 kuukautta. Varmuuskopiot säilytetään 13 kuukautta.
Juridisiin vaatimuksiin vastaaminen	Tapauskohtaisesti tarvittavat henkilötiedot	Oikeutettu etu, GDPR art. 6(1)(f). Tiedot käsitellään juridisiin vaatimuksiin vastaamiseksi.	Henkilötietoja säilytetään, kunnes juridinen vaatimus on käsitelty.
Lakivelvoitteiden noudattaminen	Tapauskohtaisesti tarvittavat henkilötiedot	Lakisääteinen velvoite, GDPR art. 6(1)(c). Tiedot käsitellään lakisääteisten velvoitteiden noudattamiseksi.	Henkilötietoja säilytetään niin kauan kuin on tarpeen lakisääteisten velvoitteiden täyttämiseksi.

A.5. Tietojen käsittelijän suorittama henkilötietojen käsittely rekisterinpitäjän puolesta voidaan aloittaa, kun sopimus tulee voimaan. Käsittelyn kesto on seuraava:

Kunnes Avonova Digital -sopimus tai tämä tietojen käsittelysopimus päättyy.

Liite B Valtuutetut alikäsittelijät

B.1. Hyväksytyt alikäsittelijät

Kun lausekkeet tulevat voimaan, rekisterinpitäjä valtuuttaa seuraavien alikäsittelijöiden käytön:

Nimi	CRV	Osoite	Käsittelyn kuvaus
Amazon Web Services	-	Ruotsi	Isännöinti
Entirebody	927 988 399	Norja	Yksilöllinen valmennus työntekijöille
Eyr	915 487 467	Norja, Ruotsi	Videolääkäri ja psykologi työntekijöille
Metodika	-	Norja	Yritysjärjestelmä työterveyspalveluille
J4	-	Ruotsi	Yritysjärjestelmä työterveyspalveluille
Safe2Use	-	Norja, Saksa	Aineiden ja tuotteiden rekisterin tarjoaja
Norsk Førstehjelp	-	Norja	Defibrillaattorien tarjoaja

Rekisterinpitäjä valtuuttaa edellä mainittujen alikäsittelijöiden käytön kyseessä olevan osapuolen suorittamaa kuvattua käsittelyä varten lausekkeiden voimaantulon yhteydessä. Tietojen käsittelijällä ei ole oikeutta – ilman rekisterinpitäjän nimenomaista kirjallista lupaa – ottaa käyttöön alikäsittelijää "eri" käsittelyyn kuin mikä on sovittu, tai käyttää muuta alikäsittelijää suorittamaan sovittu käsittely.

Liite C Ohjeet henkilötietojen käsittelyyn

C.1. Käsittelyn kohde/ohjeistus

Tietojen käsittelijän suorittama rekisterinpitäjän puolesta tehtävä henkilötietojen käsittely sisältää seuraavat toimenpiteet:

Käsittelijän tulee suorittaa jatkuvia tietoturvatarkastuksia. Käsittelijä ei saa:

- käsitellä henkilötietoja muihin tarkoituksiin, laajemmin tai muulla tavalla kuin mitä tässä sopimuksessa, palvelu-/tehtäväsopimuksessa tai muissa osapuolten välisissä myöhemmissä kirjallisissa sopimuksissa on sovittu;
- käsitellä henkilötietoja enempää kuin mitä on tarpeen käsittelijän kulloinkin voimassa olevien sopimusvelvoitteiden täyttämiseksi; tai
- luovuttaa, uskoa tai siirtää henkilötietoja kolmannelle osapuolelle tai vastaanottaa henkilötietoja kolmannelta osapuolelta omasta aloitteestaan, ellei kyseessä ole lakisääteinen velvoite tai asiaa ole etukäteen sovittu rekisterinpitäjän kanssa tai rekisterinpitäjä ole antanut tähän kirjallista suostumusta. Tämä rajoitus ei kuitenkaan estä siirtoja tai vastaanottoja liitteessä 2 mainituille alihankkijoille eikä uusille alihankkijoille, jotka käsittelijä nimittää.

Käsittelijän tulee:

- ylläpitää jatkuvaa kontrollia kaikista rekisterinpitäjän puolesta suoritetuista käsittelytoimenpiteistä, ks. liite 1;
- antaa rekisterinpitäjälle pääsy henkilötietoihin, joita käsittelijä käsittelee rekisterinpitäjän puolesta;
- ryhtyä kaikkiin kohtuullisiin toimenpiteisiin auttaakseen rekisterinpitäjää varmistamaan, että henkilötiedot ovat aina oikeita ja ajan tasalla;
- varmistaa, että kaikilla henkilöillä, joilla on pääsy rekisterinpitäjän puolesta käsiteltäviin henkilötietoihin, on salassapitovelvollisuus;
- tarjota rekisterinpitäjälle tarvittava apu, jotta rekisterinpitäjä voi täyttää velvoitteensa rekisteröidyille, mukaan lukien vastata rekisteröityjen oikeuksien käyttöön liittyviin pyyntöihin, kuten GDPR:n III luvussa esitetään;
- ilmoittaa viipymättä rekisterinpitäjälle, jos käsittelijä katsoo, että jokin ohjeistus rikkoo GDPR:ää tai muita henkilötietojen suojaa koskevia määräyksiä;
- tarvittaessa avustaa rekisterinpitäjää varmistamaan GDPR:n artiklojen 35–36 mukaisten velvoitteiden täyttäminen, jotka liittyvät henkilötietojen suojaa koskeviin vaikutustenarviointeihin ja ennakoneuvotteluihin Norjan tietosuojaviranomaisen kanssa; ja

- ilmoittaa välittömästi rekisterinpitäjälle, jos käsittelijä saa viranomaiselta pyynnön luovuttaa tässä tietojenkäsittelijäsopimuksessa käsiteltyjä henkilötietoja. Käsittelijä ei saa noudattaa tällaista pyyntöä ilman rekisterinpitäjän etukäteen antamaa kirjallista suostumusta, ellei luovutus ole lain mukaan pakollista.

C.2. Käsittelyn turvallisuus

Turvallisuuden tasossa tulee ottaa huomioon:

- Käsittelyssä on mukana suuri määrä henkilötietoja, joihin sovelletaan GDPR:n artiklaa 9 koskien "erityisiä henkilötietoryhmiä", minkä vuoksi on perusteltua määrittää "korkea" turvallisuustaso.

Tietojenkäsittelijällä on oikeus ja velvollisuus tehdä päätöksiä tarvittavista teknisistä ja organisatorisista turvatoimista, joilla saavutetaan sovittu tietoturvan taso.

Tietojenkäsittelijän tulee kuitenkin aina vähintään toteuttaa seuraavat rekisterinpitäjän kanssa sovitut toimenpiteet:

- **Fyysinen pääsy:**
 - Henkilötietoja ei käsitellä tai tallenneta säännöllisesti fyysisille tallennusvälineille, kuten paperille.
 - Vain valtuutetuilla henkilöillä on fyysinen pääsy palveluntarjoajan palvelimille.
- **Järjestelmäpääsy:**
 - Vain valtuutetuilla henkilöillä on pääsy järjestelmiin, jotka ovat tarpeen palvelun tuottamiseksi.
- **Henkilötietojen pääsy:**
 - Vain valtuutetuilla henkilöillä on pääsy henkilötietoihin.
 - Pääsy määräytyy tehtäväroolin mukaan työtehtävien perusteella.
- **Henkilötietojen siirto:**
 - Henkilötietoja ei siirretä kolmansiin maihin.
- **Pääsynhallinta:**
 - Käyttöoikeuksia hallinnoidaan käyttäjäroolien perusteella IT-järjestelmissä, joissa henkilötietoja käsitellään.
- **Tietojen salaaminen:**

- Kaikki mobiilit työasemat (kuten matkapuhelimet ja kannettavat tietokoneet) ovat salattuja.
- Kaikki tuotantojärjestelmissä olevat tiedot, mukaan lukien varmuuskopiot ja lokitiedostot, tallennetaan salatuille levyille.
- Tiedostoihin pääsee vain salattujen kanavien kautta (VPN, jossa on kaksivaiheinen tunnistautuminen, ja SSH), jotka ovat käytettävissä vain sisäisille teknisille ylläpitohenkilöille.
- **Turvallinen tunnistautuminen:**
 - Ohjelmistoihin ja järjestelmiin, joissa henkilötietoja käsitellään, pääsee vain asiakasverkon kautta.
 - Pääsy fyysisestä sisäisestä verkosta on mahdollista vain VPN:n tai yksityisavaimilla toimivan SSH:n kautta, joiden käyttöoikeudet uusitaan säännöllisesti.
 - Pääsy rekisterinpitäjän tilille tapahtuu valtuutettuna toimenpiteenä.
- **Tallennusvälineiden hallinta:**
 - Alitoimittaja vastaa tallennusvälineiden käsittelystä.
- **Kapasiteetin ja jatkuvuuden suunnittelu:**
 - Palvelimet, mukaan lukien käyttöliittymä- ja taustatietokantapalvelimet, mitoitetaan käyttäjämäärien ja kuormituksen perusteella.
 - Kaikkia palvelimia seurataan jatkuvasti.

C.2. Varmuuskopiointi ja tietoturvamenetelmät

- **Varmuuskopiointi:**
 - Varmuuskopiointi suoritetaan järjestelmällisesti. Kaikkia varmuuskopioita tarkistetaan, ja onnistuneista/epäonnistuneista toimenpiteistä pidetään lokitiedostoja.
 - Palautustestit suoritetaan säännöllisesti järjestelmällisen aikataulun mukaisesti.
- **Tietojen erottelu (looginen/fyysinen):**
 - Looginen tietojen erottelu toteutetaan järjestelmän käyttöoikeusjärjestelmän avulla ja palvelimien välillä palomuurisäännöillä.
- **Lokitiedostot:**
 - Palvelintoimintoja valvotaan lokittamalla käyttöä ja liikennettä.

- Järjestelmissä, jotka käsittelevät henkilötietoja, käyttäjätoiminnot, kuten kirjautuminen, lukeminen ja muutokset, kirjataan järjestelmäkohtaisesti.
- **Teknisten haavoittuvuuksien hallinta:**
 - Palvelimet suojataan palomureilla.
 - Tietoturvapäivitykset käsitellään manuaalisesti ja niitä valvotaan säännöllisesti.
- **Redundanssi:**
 - Palvelimet ovat redundantteja. Mahdollisessa käyttökatkoksessa viallinen palvelin poistetaan kuormituksesta, ja jäljellä olevat palvelimet tasapainottavat kuormituksen.
 - Tietokantapalvelimet hyödyntävät synkronointia ja failover-mekanismeja klusterointiratkaisun kautta, mikä varmistaa redundanssin.
- **Dokumentoidut toimintarutiinit:**
 - IT-osastolla on dokumentoidut toimintarutiinit palvelimille ja muille IT-toiminnoille.

C.3. Rekisterinpitäjän avustaminen

Tietojenkäsittelijä avustaa rekisterinpitäjää mahdollisuuksien mukaan alla mainittujen teknisten ja organisatoristen toimien puitteissa ja laajuudessa Sääntöjen 9.1. ja 9.2. mukaisesti:

- Toimenpiteet henkilötietojen suojaamiseksi lainsäädännön mukaisesti.
- Pääsy järjestelmään, jossa tiedot säilytetään.
- Tallennettujen tietojen salaus.
- Sisäiset menettelytavat tietojenkäsittelijän henkilötietojen käsittelylle.

C.4. Säilytysaika ja poistomenettelyt

- **Säilytysaika:**
Henkilötietoja säilytetään 12 kuukautta, minkä jälkeen ne poistetaan automaattisesti tietojenkäsittelijän toimesta.
- **Poistomenettelyt palvelujen päättyessä:**
Henkilötiedot poistetaan palvelujen päättyttyä Sääntöjen 11.1. mukaisesti, ellei rekisterinpitäjä ole muuttanut alkuperäistä valintaansa sopimuksen allekirjoittamisen

jälkeen. Muutokset on dokumentoitava ja säilytettävä kirjallisesti, myös sähköisessä muodossa, Sääntöihin liittyen.

C.5. Käsittelypaikka

Henkilötietojen käsittely Sääntöjen mukaisesti ei saa tapahtua muissa paikoissa kuin seuraavissa ilman rekisterinpitäjän etukäteen antamaa kirjallista lupaa:

- Tietojenkäsittelijän käsittelemät tiedot sijaitsevat EU:n sisällä. Kaikkien alihankkijoiden osalta käsittely tapahtuu EU:n/ETA:n alueen puitteissa.

C.6. Ohjeet henkilötietojen siirtoon kolmansiin maihin

Mikäli sovellettavissa, tietojenkäsittelijä käyttää EU:n vakiosopimuslausekkeita.

Ellei rekisterinpitäjä ole Sääntöjen mukaisesti tai myöhemmin toimittanut dokumentoituja ohjeita henkilötietojen siirtämisestä kolmanteen maahan, tietojenkäsittelijällä ei ole oikeutta suorittaa tällaista siirtoa Sääntöjen puitteissa.

C.7. Menettelytavat rekisterinpitäjän suorittamille tarkastuksille, mukaan lukien henkilötietojen käsittelyn tarkastukset tietojenkäsittelijän toimesta

- **Tarkastusraportti:**

Tietojenkäsittelijän tulee rekisterinpitäjän määräyksestä ja kustannuksella hankkia riippumattoman kolmannen osapuolen laatima tarkastusraportti, jossa arvioidaan tietojenkäsittelijän noudattamista GDPR:n, sovellettavan EU:n tai jäsenvaltion tietosuojasäädösten sekä Sääntöjen osalta.

- Tarkastusraportti on toimitettava viipymättä rekisterinpitäjälle tiedoksi.
- Rekisterinpitäjä voi kyseenalaistaa raportin laajuuden ja/tai menetelmät, ja tällöin rekisterinpitäjä voi pyytää uuden tarkastuksen/tarkastelun eri laajuuden ja/tai menetelmien perusteella. Näistä aiheutuvat kustannukset kuuluvat rekisterinpitäjälle.

- **Lisätoimenpiteet:**

Tarkastuksen tulosten perusteella rekisterinpitäjä voi vaatia lisätoimenpiteitä varmistaakseen GDPR:n, sovellettavan EU:n tai jäsenvaltion tietosuojasäädösten sekä Sääntöjen noudattamisen.

- **Fyysiset tarkastukset:**

Rekisterinpitäjällä tai tämän edustajalla on lisäksi oikeus tarkastaa, mukaan lukien

fyysinen tarkastus, paikat, joissa tietojenkäsittelijä käsittelee henkilötietoja. Tämä sisältää fyysiset tilat sekä järjestelmät, joita käytetään tai jotka liittyvät käsittelyyn.

- Tällainen tarkastus suoritetaan, kun rekisterinpitäjä katsoo sen olevan tarpeen.

Liite D Osapuolten sopimusehdot muista aiheista

(Tähän lisätään osapuolten mahdollisesti sopimat erityisehdot, joita ei ole käsitelty aiemmissa kohdissa.)