**RSM Finland Oy**
**RSM Finland Recovery Oy**

Ratamestarinkatu 7 b
00520 Helsinki
Finland

T+358 29 3700 788
F +358 9 7289 0041

www.rsm.fi

# SOPIMUS HENKILÖTIETOJEN KÄSITTELYSTÄ

**ALUKSI**
RSM ja toimeksiannon tilaaja ovat tehneet toimeksiantosopimuksen, jolla toimeksiannon tilaaja hankkii toimeksiantosopimuksessa kuvatut palvelut RSM:ltä. RSM:llä viitataan tässä henkilötietojen käsittelyä koskevassa sopimuksessa RSM Finland Oy:ön sekä kaikkiin muihin RSM-konserniyhtiöihin.

Toimeksiannon kohteena voi olla myös muu oikeushenkilö kuin toimeksiannon tilaaja. Tällaisessa tilanteessa sopimus henkilötietojen käsittelystä tehdään rekisterinpitäjänä toimivan toimeksiannon kohteen kanssa.

RSM käsittelee henkilötietoja palvelujen yhteydessä ja tässä sopimuksessa henkilötietojen käsittelystä sovitaan ehdoista, joiden mukaisesti RSM käsittelee rekisterinpitäjän henkilötietoja. RSM Finland Oy -konsernin yleiseksi määritellyt käsittelytoimet kuvataan liitteessä 1A, jota osapuolet tarvittaessa päivittävät tai täydentävät erillisellä asiakaskohtaisella liitteellä sopimuksen voimassaoloaikana.

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

”Henkilötietojen käsittelyllä” tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Käsiteltäessä henkilötietoja toimeksiantosopimuksessa yksilöidyn toimeksiannon suorittamista varten, rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, ja RSM on käsittelijä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Sopijapuolet ymmärtävät, että viranomaiset voivat antaa määräyksiä ja ohjeita Tietosuoja-asetuksen soveltamisalalla tämän henkilötietojen käsittelyä koskevan sopimuksen allekirjoittamisen jälkeen. Sopijapuolet sitoutuvat täydentämään tätä sopimusta henkilötietojen käsittelystä tarvittaessa kyseisten määräysten ja ohjeiden perusteella.

Tämä sopimus sisältää seuraavat liitteet, joita sovelletaan seuraavassa järjestyksessä:

1A Seloste käsittelytoimista
1B Henkilötietojen tietoturva RSM:llä
1C Rekisterinpitäjän antama ohjeistus henkilötietojen käsittelystä

**YLEISET OIKEUDET JA VELVOLLISUUDET**
**Rekisterinpitäjän yleiset oikeudet ja velvollisuudet**
Rekisterinpitäjä
a) vastaa henkilötietojen keräämisestä;
b) käsittelee henkilötietoja laillisesti, huolellisesti ja hyvää tietojenkäsittelytapaa noudattaen sekä toimii muutoinkin niin, ettei rekisteröityjen yksityiselämän suojaa ja muita yksityisyyden suojan

turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta;

c) määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot sekä antaa RSM:lle kirjalliset ohjeet henkilötietojen käsittelystä. Henkilötietojen käsittelyn tarkoituksesta tulee ilmetä, minkälaisissa tehtävissä (mm. palkkatietojen tarkastus) henkilötietoja käsitellään;
d) vastaa siitä, että rekisteröidyille toimitetaan kaikki lainsäädännön edellyttämät henkilötietojen käsittelyä koskevat ilmoitukset ja tiedot;
e) vastaa rekisteröityjen oikeuksien toteutumisesta;
f) varmistaa, että henkilötietojen siirtäminen RSM:lle sekä henkilötietojen käsittely tämän sopimuksen mukaisesti on lainmukaista koko sopimuksen voimassaolon ajan;
g) vakuuttaa, että jos se edustaa tässä sopimuksessa konserniyhtiöitään tai kolmansia osapuolia, sillä on oikeus sitoutua tähän sopimukseen ja antaa RSM:lle oikeus käsitellä henkilötietoja tämän sopimuksen ja toimeksiantosopimuksen mukaisesti;
h) vahvistaa ja vastaa siitä, että tämän sopimuksen mukainen henkilötietojen käsittely on lainsäädännössä asetettujen vaatimusten mukaista, mukaan lukien tietoturvavaatimukset;
i) vahvistaa, että se on antanut RSM:lle kaikki tarvittavat tiedot, jotta RSM voi täyttää tässä sopimuksessa ja toimeksiantosopimuksessa sille asetetut velvoitteet tietosuojalainsäädännön vaatimusten mukaisesti;
j) tai sen valtuuttama ulkopuolinen tarkastaja voi auditoida RSM:n tai RSM:n alihankkijoiden tämän sopimuksen alaista toimintaa;
k) vastaa siitä, että korjaukset, poistot ja muutokset henkilötietoihin toimitetaan viivytyksettä RSM:lle; ja
l) pidättää itsellään kaikki omistusoikeudet, immateriaalioikeudet ja muut oikeudet henkilötietoihin.

Jos osapuolet ovat sopineet, että RSM avustaa rekisterinpitäjää tämän lainmukaisten selosteiden laatimisessa, rekisterinpitäjän tulee antaa RSM:lle tämän sitä varten tarvitsemat tiedot. RSM toimittaa selosteet vain rekisterinpitäjälle.

**RSM:n yleiset oikeudet ja velvollisuudet käsittelijänä**

RSM

a) käsittelee henkilötietoja ainoastaan toimeksiantosopimuksessa ja tässä henkilötietojen käsittelyä koskevassa sopimuksessa määriteltyihin tarkoituksiin, vain siinä laajuudessa kuin on tarpeen toimeksiannosta tapahtuvaa palvelua varten, ja ainoastaan tämän sopimuksen voimassaoloajan, ellei pakottavasta lainsäädännöstä muuta johdu. RSM:llä ei ole oikeutta käyttää toimeksiantosuhteessa saamiaan henkilötietoja omassa toiminnassaan, luovuttaa niitä, käsitellä niitä, eikä yhdistää tietoja muuhun hallussaan olevaan aineistoon muutoin kuin toimeksiantosopimuksen tarkoittamassa laajuudessa ja sen mukaista tehtävää hoitaessaan;
b) käsittelee henkilötietoja laillisesti, huolellisesti ja hyvää tietojenkäsittelytapaa noudattaen sekä toimii muutoinkin niin, ettei rekisteröityjen yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta;
c) käsittelee ja varmistaa alaisuudessaan toimivan henkilön, jolla on pääsy henkilötietoihin, käsittelevän henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen, lainmukaisten ja kohtuullisten ohjeiden mukaisesti, paitsi jos sovellettavassa laissa toisin vaaditaan. Siinä tilanteessa RSM informoi rekisterinpitäjää välittömästi tästä oikeudellisesta vaatimuksesta, edellyttäen, ettei sovellettava lainsäädäntö kiellä sellaista informointia;
d) varmistaa, että henkilötietoja käsittelevät vain ne henkilöt, joiden työtehtävien hoitaminen sitä edellyttää ja, että kyseiset henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä sitoo asianmukainen lakisääteinen salassapitovelvollisuus;
e) toteuttaa kaikki lainsäädännön henkilötietojen käsittelijöiltä edellyttämät turvallisuustoimenpiteet siten kuin tässä sopimuksessa on tarkemmin sovittu;
f) avustaa rekisterinpitäjää mahdollisuuksien mukaan ja käsittelyn luonteen huomioon ottaen asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröityjen oikeuksien käyttämistä;
g) avustaa käsittelyn luonteen ja RSM:n saatavilla olevat tiedot huomioon ottaen rekisterinpitäjää varmistamaan, että rekisterinpitäjälle laissa asetettuja velvollisuuksia, kuten turvatoimia, vaikutusten arviointia ja ennakkokuulemista, noudatetaan. RSM on velvollinen avustamaan rekisterinpitäjää vain sovellettavan lainsäädännön RSM:lle käsittelijänä asettamien velvoitteiden mukaisessa laajuudessa;
h) huomioi rekisterinpitäjän toimittamat tietojen korjaukset, poistot ja muutokset ilman aiheetonta viivytystä henkilötietojen käsittelyssä;
i) tämän sopimuksen aikana tai sen päätyttyä joko tuhoaa tai palauttaa rekisterinpitäjälle rekisterinpitäjän valinnan ja ohjeiden mukaisesti kaikki henkilötiedot ja poistaa olemassa olevat jäljennökset, ellei pakottavasta lainsäädännöstä muuta johdu. Tuhoamista ja palauttamista rajoittaa tilintarkastuslain nojalla tehtävissä toimeksiannoissa tilintarkastuslain 7 luvun 3 §:n 3 momentissa mainittu kantelua koskeva kuuden vuoden määräaika. Tämä sopimus henkilötietojen käsittelystä katsotaan päättyneeksi kuuden vuoden

jälkeen sen vuoden lopusta, kun toimeksiantoon liittyvät jatkotoimenpiteet kuten oikeudenkäynnit on suoritettu kaikilta osin loppuun. Koska myös muissa toimeksiannoissa tiimiin voi kuulua auktorisoitu tilintarkastaja, RSM noudattaa tätä tuhoamista ja palauttamista koskevaa periaatetta myös kaikissa muissa toimeksiannoissa. Tuhoamista ja palauttamista koskevista käytännöistä voidaan sopia tarkemmin erikseen osapuolten kesken;

j) ylläpitää tarvittavia selosteita/kirjanpitoa käsittelytoimista ja saattaa rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka osoittavat, että RSM noudattaa sille tässä sopimuksessa ja sovellettavassa lainsäädännössä säädettyjä velvollisuuksia;
k) sallii rekisterinpitäjän tai rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit ja osallistuu niihin siten kuin tässä sopimuksessa on tarkemmin sovittu;
l) ilmoittaa rekisterinpitäjälle, jos RSM katsoo, että rekisterinpitäjän antama ohjeistus rikkoo sovellettavaa lainsäädäntöä;
m) ilmoittaa rekisterinpitäjälle, jos RSM katsoo, että rekisterinpitäjän toimintatavoissa on puutteita, ja avustaa tarvittaessa rekisterinpitäjää toimintatapojen korjaamisessa.

RSM:llä on oikeus laskuttaa yllä kuvatuista avustamis-, korjaus- ja pyyntöihin vastaamistoimista, auditoinnin tuesta sekä rekisterinpitäjän ohjeistuksen muutoksista johtuvista toimista ja kustannuksistaan erikseen.

**TIETOTURVA**

RSM toteuttaa ja ylläpitää asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan henkilötietojen käsittelyn riittävä turvallisuustaso ja joilla suojellaan henkilötietoja luvattomalta ja laittomalta käsittelyltä sekä tahattomalta menettämiseltä, tuhoamiselta, vahingolta, muutokselta tai luovuttamiselta, ottaen huomioon erityisesti uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

RSM:n tämän sopimuksen johdosta toteuttamat käsittelyn tietoturvaperiaatteet on kuvattu tarkemmin tämän sopimuksen liitteessä 1B.

Rekisterinpitäjä on velvollinen varmistamaan, että RSM:ää informoidaan kaikista niistä rekisterinpitäjän toimittamiin henkilötietoihin liittyvistä seikoista (kuten riskiarvioinneista sekä erityisten henkilötietoryhmien käsittelystä), jotka vaikuttavat tämän sopimuksen mukaisiin teknisiin ja organisatorisiin toimenpiteisiin.

Tietoturvajärjestelyjä arvioidaan, tarkistetaan ja päivitetään säännöllisesti.

**ALIHANKKIJAT**

RSM saa käyttää alihankkijoita henkilötietojen käsittelyssä tämän sopimuksen perusteella. ”Alihankkijalla” tarkoitetaan käsittelijää, joka käsittelee henkilötietoja tämän sopimuksen mukaisesti, kokonaan tai osittain, käsittelijän lukuun ja tämän toimeksiannosta. Käsittelyssä käytettävät alihankkijat sopimuksen alkaessa ilmoitetaan rekisterinpitäjän pyynnöstä. RSM tiedottaa rekisterinpitäjälle ennalta suunnitelluista muutoksista, joilla alihankkijoita lisätään tai vaihdetaan. Mikäli rekisterinpitäjä ei hyväksy suunniteltua muutosta, rekisterinpitäjällä ja RSM:llä on oikeus kolmenkymmenen (30) päivän ajan muutoksen tiedottamisesta irtisanoa toimeksiantosopimus päättymään kyseisen kolmenkymmenen (30) päivän jakson päättyessä sen palvelun osalta, jonka tuottamiseen alihankkijan muutos vaikuttaa ja jossa henkilötietoja käsitellään. Mikäli alihankkijavaihdos, jota rekisterinpitäjä ei hyväksy ja johon RSM ei voi vaikuttaa, estää tai olennaisesti vaikeuttaa palveluntuottamista, RSM:llä ei ole velvollisuutta tuottaa sellaista palvelua.

RSM solmii kirjallisen käsittelysopimuksen alihankkijan kanssa ja edellyttää kaikkien alihankkijoiden noudattavan RSM:lle tässä sopimuksessa asetettuja tietosuojavelvoitteita tai vastaavan tietosuojan tason takaavia velvoitteita. Alihankkija käsittelee henkilötietoja vain kirjallisen sopimuksen mukaisesti. RSM vastaa käyttämiensä alihankkijoiden toimista kuin omistaan.

**HENKILÖTIETOJEN SIIRTO**

RSM voi siirtää henkilötietoja Euroopan unionin, Euroopan talousalueen tai muiden maiden, joiden Euroopan komissio on todennut takaavan riittävän tietosuojan tason, ulkopuolelle ainoastaan rekisterinpitäjän etukäteisellä kirjallisella suostumuksella. Mikäli siirretään tietoja edellä mainittujen alueiden ulkopuolelle, RSM solmii sovellettavan lain edellytysten mukaisen sopimuksen henkilötietojen siirrosta tarvittavien osapuolten kanssa. Sopimus henkilötietojen siirrosta laaditaan Euroopan komission hyväksymien mallisopimuslausekkeiden mukaisesti. Vaihtoehtona mallisopimuslausekkeiden käytölle siirto voi tapahtua muita soveltuvan lainsäädännön hyväksymiä siirtoperusteita käyttäen/hyödyntäen.

Mikäli mallisopimuslausekkeiden tai minkä tahansa muun lainmukaisen siirtoperusteen ja tämän sopimuksen välillä on ristiriita, mallisopimuslausekkeet ja vaihtoehtoiset siirtoperusteet saavat soveltamisjärjestyksessä aina etusijan suhteessa toimeksiantosopimukseen ja tähän sopimukseen.

**HENKILÖTIETOJEN TIETOTURVALOUKKAUKSISTA ILMOITTAMINEN**

”Henkilötietojen tietoturvaloukkauksella” tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

RSM:n on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä siitä, kun RSM tai sen käyttämä alihankkija on saanut loukkauksen tietoonsa. Elleivät osapuolet ole toisin sopineet, ilmoitus tulee tehdä rekisterinpitäjän ilmoittamalle yhteyshenkilölle.

RSM:n on ilman aiheetonta viivytystä toimitettava rekisterinpitäjälle tieto henkilötietojen tietoturvaloukkaukseen johtaneista olosuhteista sekä muista siihen liittyvistä RSM:n saatavilla olevista seikoista rekisterinpitäjän kohtuullisten pyyntöjen mukaisesti.

Siltä osin kuin kyseinen tieto on RSM:n saatavilla, on rekisterinpitäjälle tehtävässä ilmoituksessa kuvattava ainakin:

a) kuvaus henkilötietojen tietoturvaloukkauksesta, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;
b) sen henkilön nimi ja yhteystiedot, joka vastaa käsittelijän tietosuoja-asioista;
c) kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; sekä
d) kuvaus niistä toimenpiteistä, jotka RSM ehdottaa toteutettaviksi ja/tai on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, mukaan lukien tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Jos ja siltä osin kuin edellä listattuja tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

**AUDITOINTI**

Rekisterinpitäjällä on oikeus auditoida käsittelijän tämän sopimuksen alainen tietojenkäsittelytoiminta. Rekisterinpitäjä on velvollinen käyttämään auditoinnissa vain sellaisia ulkopuolisia tarkastajia, jotka eivät ole RSM:n kilpailijoita. Osapuolet sopivat auditoinnin ajankohdasta ja muista yksityiskohdista hyvissä ajoin ennen sen suorittamista. Auditointi tulee suorittaa tavalla, joka ei haittaa RSM:n sitoumuksia kolmansiin osapuoliin nähden. Kaikkien rekisterinpitäjän edustajien ja auditointiin osallistuvien ulkopuolisten tarkastajien tulee allekirjoittaa tavanomainen salassapitositoumus RSM:n hyväksi.

Rekisterinpitäjä vastaa kaikista auditoinnista aiheutuvista kustannuksista. RSM:llä on myös oikeus laskuttaa avustamisesta auditoinnissa ja muusta auditoinnista johtuvasta lisätyöstä.

**SALASSAPITO**

RSM sitoutuu

a) pitämään luottamuksellisena kaikki rekisterinpitäjältä vastaanottamansa henkilötiedot,
b) varmistamaan, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta, sekä
c) varmistamaan, että henkilötietoja ei siirretä/luovuteta kolmansille osapuolille ilman rekisterinpitäjän etukäteistä kirjallista suostumusta, ellei käsittelijä ole velvollinen ilmaisemaan tietoja pakottavan lainsäädännön tai viranomaisen määräyksen perusteella.

Selvyyden vuoksi todetaan, että salassapitovelvollisuus ei koske toimeksiantosopimuksen mukaisen toimeksiannon tuloksena syntyvän, henkilötietoja sisältävän raportin tai muun materiaalin luovuttamista toimeksiannon tilaajalle tilanteessa, jossa toimeksiannon tilaaja ja rekisterinpitäjä ovat eri tahoja. Mikäli rekisteröity tai viranomainen tekee henkilötietoja koskevan pyynnön, RSM:n tulee, niin pian kuin on kohtuullisesti mahdollista, ilmoittaa rekisterinpitäjälle tällaisesta pyynnöstä ennen pyyntöön vastaamista tai muiden henkilötietoja koskevien toimenpiteiden suorittamista. Mikäli toimivaltainen viranomainen vaatii välitöntä vastausta, ilmoittaa RSM rekisterinpitäjälle pyynnöstä niin pian kuin on mahdollista pyyntöön vastaamisen jälkeen, ellei pakottavasta laista muuta johdu.

**VASTUUNRAJOITUS**

Toimeksiantosopimuksen mukaisia vastuunrajoituksia sovelletaan myös tähän sopimukseen. Jos vastuunrajoituksista ei ole toimeksiantosopimuksessa sovittu, noudatetaan seuraavaa:

RSM vastaa vain huolimattomuudestaan johtuvista välittömistä vahingoista.

RSM ei vastaa välillisistä vahingoista, kuten tulon, liikevaihdon tai markkinoiden menetyksestä, tuotannon tai palvelun keskeytymisestä, saamatta jääneestä voitosta taikka muusta niihin verrattavasta vahingosta.

Jos kolmas osapuoli tekee osapuolelle henkilötietojenkäsittelyn perusteella korvausvaatimuksen, siitä on ilmoitettava toiselle osapuolelle viipymättä. Jos RSM joutuu maksamaan kolmannelle osapuolelle vahingonkorvausta, rekisterinpitäjän on hyvitettävä RSM:lle tästä aiheutunut menetys sikäli kuin se ei johdu RSM:n virheestä tai laiminlyönnistä sopimusehtojen noudattamisessa.

RSM:n vastuun enimmäismäärä on kuitenkin aina enintään toimeksiantosopimuksen ehtojen mukaan yhteensä RSM:lle toimeksiannosta maksetun palkkion määrä tai muu toimeksiantosopimuksessa mainittu vahingonkorvauksen enimmäismäärä, jos sellaisesta on erikseen sovittu. Sopimusrikkomus, virhe tai laiminlyönti eivät aiheuta RSM:lle muuta seuraamusta kuin mitä edellä on todettu.

Henkilötietojen käsittelyyn perustuvat vaatimukset RSM:lle on tehtävä kirjallisesti viipymättä. Jos virhe tai puute havaitaan tai on havaittavissa välittömästi, huomautus on tehtävä heti ja viimeistään neljäntoista (14) päivän kuluessa. Jos eriteltyä henkilötietojen käsittelyyn perustuvaa vaatimusta ei ole tehty RSM:lle kuuden (6) kuukauden kuluessa vahingon toteamisesta, ei korvausta makseta. Korvausta ei myöskään makseta, jos vaatimus tehdään, kun on kulunut yli kolme (3) vuotta kyseisestä käsittelytapahtumasta.

Kaikissa tapauksissa kumpikin osapuoli vastaa itse valvontaviranomaisen tai toimivaltaisen tuomioistuimen sille määräämistä hallinnollisista sanktioista, jotka ovat ko. valvontaviranomaisen tai tuomioistuimen päätöksen mukaisesti seurausta siitä, että kyseinen osapuoli ei ole noudattanut sille tietosuojalainsäädännössä asetettuja vaatimuksia tai velvoitteita.

**VOIMASSAOLO**

Tämä sopimus henkilötietojen käsittelystä katsotaan päättyneeksi kuuden vuoden jälkeen sen vuoden lopusta, kun toimeksiantoon liittyvät jatkotoimenpiteet kuten oikeudenkäynnit on suoritettu kaikilta osin loppuun. Koska myös muissa toimeksiannoissa tiimiin voi kuulua auktorisoitu tilintarkastaja, RSM noudattaa tätä tuhoamista ja palauttamista koskevaa periaatetta myös kaikissa muissa toimeksiannoissa.

Mikäli rekisterinpitäjä rikkoo tätä sopimusta, RSM:llä on oikeus purkaa toimeksiantosopimus ja tämä sopimus, mikäli rekisterinpitäjä ei seitsemän (7) päivän kuluessa RSM:n lähettämästä kehotuksesta ole korjannut menettelyään ja huolehtinut kaikkiin toimiin ryhtymisestä rikkomuksesta johtuvien seurausten välttämiseksi, korjaamiseksi ja korvaamiseksi.

Velvoitteet, joiden on niiden luonteen vuoksi tarkoitus säilyä voimassa tämän sopimuksen voimassaolon päättymisestä riippumatta, jäävät voimaan tämän sopimuksen päättymisestä riippumatta.

Tästä sopimuksesta on tehty kaksi (2) samanlaista kappaletta, yksi kullekin allekirjoittajalle.

## SELOSTE KÄSITTELYTOIMISTA

**Liite nro 1A**

Palveluntarjoajan (RSM) seloste henkilötietojen käsittelytoimista

**Alihankkijat**
Rekisterinpitäjä on antanut yleisen suostumuksen alihankkijoiden käyttöön. RSM toimittaa pyydettäessä luettelon alihankkijoista

**Rekisteröityjen ryhmät sekä henkilötietojen käsittelyn tarkoitus ja luonne**
Tuottaakseen annetun tarjouksen tai toimeksiantosopimuksen mukaisesti sovitut palvelut, RSM käsittelee palveluiden toteuttamista varten tarpeellisia rekisteröityjen tietoja seuraaviin tarkoituksiin, ellei liitteessä 1C ole toisin määritetty:

- Rekisterinpitäjän palkan- ja palkkionsaajat palkka- ja henkilöstöhallintoa koskevien tarkastustoimenpiteiden suorittamiseksi ja raportoimiseksi;
- Rekisterinpitäjän avainhenkilöitä koskevat tiedot palkitsemisjärjestelmien tarkastamiseksi, raportoimiseksi ja kehittämiseksi;
- Rekisterinpitäjän kirjanpidossa ja toimeksiannon suorittamista varten saaduissa talousraporteissa olevien palkka- ja muiden henkilöstölle maksettujen kulujen oikeellisuuden varmistamiseksi ja raportoimiseksi;
- Rekisterinpitäjän henkilöasiakkaat ja toimittajat saatavien ja velkojen seuraamista varten;
- Osakasrekisteri osakeyhtiölain edellyttämällä tavalla ja jäsenrekisteri yhdistyslain edellyttämällä tavalla;
- Muut ryhmät, joiden käsittely on välttämätöntä toimeksiantojen suorittamiseksi.

**Käsittelyiden kohde ja ryhmät sekä henkilötietojen tyyppi**
Edellä kuvattuja, toimeksiantosopimuksessa määriteltyjä palveluja tuottaessaan RSM käsittelee seuraavia henkilötietoryhmiä:

- Nimi ja yhteystiedot;
- Henkilötunnus;
- Henkilön perustiedot kuten syntymäaika, sukupuoli ja koulutustiedot;
- Palkanlaskennassa tarvittavat tiedot kuten ennakonpidätystiedot, sairauspoissaoloja koskevat tiedot;
- Palkanlaskennan perusteella syntyneet palkka-, eläke-, ja verotustiedot sekä muut vastaavat tiedot;
- Laskutusta ja perintää varten tarvittavat laskutus- ja perintätiedot, sekä
- Osakeyhtiön tai asunto-osakeyhtiön hallinnointia varten tarvittavat osakas- ja osakkuustiedot.

**RSM käsittelee lisäksi erityisiä henkilötietoryhmiä:**
Palkanlaskentaan liittyvissä toimeksiannoissa (esim. palkkaturvassa avustaminen) tarvittavat tietosuoja-asetuksen tarkoittamat erityiset henkilötietoryhmät sairauspoissaolot/terveystiedot ja ammattiyhdistysjäsenyystiedot, mikäli tästä on erikseen sovittu toimeksiantosopimuksessa. Tällöin rekisterinpitäjä vastaa siitä, että käsittelyn kohteena olevien henkilötietojen osalta on tarvittavat suostumukset.

**Henkilötietojen käsittelyn kesto**
Elleivät osapuolet ole toisin sopineet, henkilötietoja käsitellään niin pitkään kuin palveluita toimitetaan toimeksiantosopimuksen mukaisesti tai lainsäädäntö edellyttää tietojen säilyttämistä.

**Henkilötietojen maantieteellinen sijainti**
Ellei rekisterinpitäjän kanssa ole erikseen muuta sovittu, henkilötietoja käsitellään seuraavissa maissa / seuraavilla alueilla: Suomi ja muut ETA-maat.

**Tietosuojasta vastaava**
RSM Finland Oy -konsernissa tietosuojasta vastaa sopimuksen tekohetkellä konsernin COO Tytti Saarinen, e-mail tytti.saarinen@rsm.fi, puh. +358 50 544 6127.

# HENKILÖTIETOJEN TIETOTURVA RSM:LLÄ

**Liite nro 1B**

Tietoturvaa ja henkilötietojen lainmukaista käsittelyä varmentavat toimet.

| Palveluntarjoaja | Laatija, päivittäjä | Päiväys, muutospäiväys |
|---|---|---|
| RSM Finland Oy -konserni | Tytti Saarinen | 21.5.2018 |

**Hallinto**
Tietoturva sekä henkilötietojen lainmukainen käsittely ovat keskeinen osa RSM:n toimintaperiaatteita. Tietoturvaan ja henkilötietojen käsittelyyn liittyvät roolit ja vastuut on nimetty henkilötasolla. Tietoturvapolitiikka ja siihen liittyvät käytännöt on määritelty. Tietoturvapolitiikka ja tietoturvakäytännöt on auditoitu ulkopuolisen asiantuntijan toimesta ja katselmoidaan säännöllisesti.

**Henkilöstö**
Henkilöstön roolit, työtehtävät ja vastuut on määritetty selkeästi. Työntekijöiden kanssa on laadittu sopimus liike- ja ammattisalaisuuksien salassapidosta. Työsuhteiden päättymisen varalle on luotu toimintamalli, jossa on huomioitu käyttöoikeuksien poistaminen ja työntekijän hallussa mahdollisesti olevien aineistojen palauttaminen. Henkilöstö on perehdytetty tietoturvapolitiikkaan ja -käytäntöihin ja perehdytys kuuluu osana uusien työntekijöiden koulutusohjelmaan. Olennaisten tietoturvaan liittyvien vaaratilanteiden raportointiin ja käsittelyyn on toimintamalli.

**Toimintamallit**
Suojattavan tiedon käsittely erilaisissa viestintäjärjestelmissä, kuten sähköpostissa tai pikaviestimissä on määritelty ja internetin ja sosiaalisen median käytölle RSM:n tietoverkossa luotu hyväksyttävän käytön pelisäännöt. Ulkopuolisten pilvitallennuspalveluiden käyttö tapahtuu ainoastaan yrityksen johdon määrittämissä tilanteissa ja hyväksymillä palveluntarjoajilla. Etätyöskentelylle on luotu tietoturvaan liittyvät ohjeet.

**Toimitilaturvallisuus**
RSM:n tiloissa on turvalukitus. RSM:n tiloissa on sähköinen kulunvalvonta. RSM:llä on ajantasainen rekisteri toimitilojen ja muiden suojattavien kohteiden avaimista sekä kulkutunnisteista. Asiakkaiden ja kolmansien osapuolten pääsy työpisteisiin sekä suojattaviin kohteisiin ja tietoihin on estetty.

**Asiakkaan tunnistaminen ja aineistojen luovutukset**
Asiakkaiden edustajat tunnistetaan ennen asiakassuhteen alkamista ja tunnistetiedot tallennetaan rahanpesulain edellyttämällä tavalla. Asiakkaan aineistojen luovutustilanteessa noudatetaan asiakkaan kanssa sovittuja tunnistus- ja luovutuskuittauskäytäntöjä.

Jos RSM hallinnoi sopimuksen mukaan rekisterinpitäjän puolesta rekisterinpitäjän käyttäjien pääsyä tietojärjestelmiin, käyttäjähallinnointi tapahtuu rekisterinpitäjän nimettyjen henkilöiden kanssa, sovittuja tunnustamistapoja hyödyntäen sekä huolehtien tunnusten ja salasanojen tietoturvallisista toimitustavoista.

**Käyttövaltuushallinta ja salasanapolitiikka**
Tietojärjestelmissä käytetään vain yksilöityjä nimetyille henkilöille osoitettuja käyttäjätunnus/salasanapareja. Poikkeuksena ovat tilanteet, joissa RSM:n johto on arvioinut riskin epäolennaiseksi.

Työntekijöiden käyttöoikeuksien tarpeellisuutta tarkastellaan työtehtävien olennaisesti muuttuessa. Salasanat, PIN-koodit ja käyttäjähallintaan tarkoitetut koodit säilytetään tarkoitukseen soveltuvassa turvallisessa tietojärjestelmässä/tiedostossa. Kaikissa luottamuksellista tietoa sisältävissä tietojärjestelmissä on käytössä salasanaan tai vastaavaan menettelyyn perustuva pääsynhallinta. Tietojärjestelmien pääkäyttäjätunnusten oletussalasanat on vaihdettu ja tietojärjestelmien salasanat vaihdetaan säännöllisesti.

**Ulkopuoliset toimijat**
Ulkopuolisia toimijoita ovat esimerkiksi siivousliikkeet, vartiointiliikkeet, kiinteistönhoitoyritykset, isännöintiliikkeet ja muut yhteistyökumppanit, joilla on pääsy organisaation toimitiloihin tai suojattaviin tietoihin.

RSM:n yhteistyökumppaneiden kanssa on laadittu kirjallinen sopimus luottamuksellisen tiedon salassapidosta ja yhteistyökumppanit ovat tietoisia RSM:n tietoturvakäytännöistä ja suojattavista kohteista sekä tietosuoja-asetuksen vaatimuksista.

Toimitiloissa säännöllisesti työskentelevät ulkopuolisten toimijoiden työntekijät perehdytetään tarvittavissa määrin RSM:n tietoturvakäytäntöihin.

**Ulkoistetut ICT-palvelut**
Ulkoistetuilla ICT-palveluilla tarkoitetaan tässä kohdassa RSM:n ulkopuolisia yrityksiä, jotka tuottavat

RSM:lle esimerkiksi palvelimien ja työasemien ylläpitopalvelua, tallennus- sekä varmistuspalveluita, tietoturvan ylläpitopalvelua tai tietoliikenneyhteyksien ylläpitopalvelua.

Ulkopuolisista ICT-palveluista on laadittu kirjalliset palvelusopimukset sekä kirjallinen sopimus luottamuksellisen tiedon salassapidosta.

RSM:n ja palveluntarjoajan välinen vastuunjako on dokumentoitu kirjallisesti ja palveluntarjoaja on tietoinen RSM:n tietoturvakäytännöistä ja suojattavista kohteista.

RSM:n ja ulkoistettujen ICT-palveluiden toiminnan ylläpidosta ja kehittämisestä keskustellaan määräajoin palveluntarjoajan kanssa.

**Suojattavien kohteiden ja tiedon hallinta**
Suojattavia kohteita ovat esimerkiksi työasemat, kannettavat tietokoneet, palvelimet ja mobiililaitteet. Suojattaville kohteille on määritelty hyväksyttävän käytön pelisäännöt. Toimeksiantoa varten saaduille rekisterinpitäjän kirjanpitoaineistolle, henkilötiedoille ja muille tiedoille on laadittu käsittelyohjeet.

Sekä digitaalisen tiedon, että tulosteiden tuhoamiselle on laadittu tietoturvallisen tuhoamisen menettelyohjeet. Käytössä on asianmukaiset tietosuojaroskasäiliöt tai asiakirjasilppuri luokitellun tiedon tuhoamista varten.

**Tietokoneiden ja mobiililaitteiden tietoturva**
RSM:n käytössä olevat työasemat, kannettavat tietokoneet, mobiililaitteet ja muut päätelaitteet on rekisteröity ja dokumentoitu asianmukaisesti.

Koneiden säännöllisistä tietoturvapäivityksistä on huolehdittu asianmukaisesti ja päivityksiä valvotaan. Työntekijöiden oikeutta asentaa ohjelmistoja työasemille on rajattu ja asennuksia valvotaan.

Asianmukainen virus- ja haittaohjelmien torjuntaohjelmisto on käytössä. Tietoverkko ja tietokoneet on suojattu palomuurilla.

Työntekijöiden henkilökohtaisten tietokoneiden ja mobiililaitteiden käyttö henkilötietojen käsittelyyn on kielletty.

**Siirrettävät tietovälineet**
Siirrettäviä tietovälineitä ovat esimerkiksi USB-muistitikut, USB-massamuistit, CD/DVD-levyt ja muut vastaavat muistilla tai tallennustilalla varustetut laitteet, jotka voidaan kytkeä tietokoneeseen.

RSM:llä ei käytetä siirrettäviä tietovälineitä työtehtävien hoitamiseen tai suojattavan tiedon käsittelyyn lukuun ottamatta erikseen sovittuja tilanteita kuten aineiston luovutus tilintarkastajalle tai aineiston luovutus tai vastaanotto rekisterinpitäjän nimetyn yhteyshenkilön kanssa tai aineiston luovutus rekisterinpitäjän suostumuksella nimetylle kolmannelle taholle.

Käytettäessä siirrettäviä tietovälineitä edellä mainittuihin tarkoituksiin on niiden sisältö suojattu salasanalla.

**Palvelin- ja tietoliikenneturvallisuus**
Toimitilojen palvelintilat ja tietoliikenneyhteyksien edellyttämät tilat pidetään lukittuina. Langattomien verkkojen tietoliikenne on salattu. Vierasverkot on eriytetty RSM:n sisäisestä tietoverkosta luotettavalla menetelmällä. Palvelinkäyttöjärjestelmät päivitetään säännöllisesti. Palvelinjärjestelmä on rakennettu vikasietoiseksi tai kahdennetuksi siten, että tietojärjestelmien toiminta ei keskeydy yksittäisestä laiterikosta.

# REKISTERINPITÄJÄN ANTAMA OHJEISTUS HENKILÖTIETOJEN KÄSITTELYSTÄ

**Liite nro 1C**