Tietojenkäsittelysopimus

TARKOITUS JA TÄRKEYSJÄRJESTYS

Tämä Tietojenkäsittelysopimus ja sen liitteet sekä kaikki Asiakirjat, joihin nimenomaisesti viitataan ristiin (”**TKS**”), katsotaan osaksi Iron Mountainin ja Asiakkaan välistä Palvelusopimusta (”**Sopimus**”). Sopimusehtoja sovelletaan osapuolten tämän TKS:n mukaisiin oikeuksiin ja velvollisuuksiin.

Jos jotkin tämän TKS:n sisältämät ehdot ovat ristiriidassa Sopimuksessa esitettyjen ehtojen kanssa, tässä TKS:ssa esitetyt ehdot ovat hallitsevia ehtoja tämän TKS:n aiheen osalta. Tämä TKS syrjäyttää ja korvaa kaikki edeltävät tietojenkäsittelysopimukset ja osapuolten väliset yksityisyys- ja Tietosuojalausekkeet, jotka liittyvät Sopimuksen nojalla tarjottuihin Palveluihin.

YLEISET EHDOT

1. MÄÄRITELMÄT

Ellei tässä Asiakirjassa ole nimenomaisesti määritelty, kaikilla termeillä, joilla on iso alkukirjain, on samat merkitykset kuin mitkä on annettu niille Sopimuksessa.

”**Rekisterinpitäjä**” tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä muiden kanssa päättää Henkilötietojen Käsittelyn tarkoituksista ja keinoista.

”**Asiakkaan henkilötiedot**” tarkoittavat Henkilötietoja, jotka kuuluvat Asiakkaalle tai sen Yleinen tietosuoja-asetus tai joita Käsitellään osana Palveluja.

”**Rekisteröity**” tarkoittaa tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä.

"Tietosuojalainsäädäntö" tarkoittaa kaikkia Henkilötietojen Käsittelyyn liittyviä lakeja ja asetuksia, jotka voivat olla voimassa asiaankuuluvilla lainkäyttöalueilla, mukaan lukien rajoittumatta, EU:n Yleinen tietosuoja-asetus (Asetus (EU) 2016/679), Yhdistyneen kuningaskunnan Yleinen tietosuoja-asetus (GDPR sellaisena kuin se soveltuu osana Yhdistyneen kuningaskunnan sisäistä lainsäädäntöä vuoden 2018 European Union (Withdrawal) Act 2018 -lain (Euroopan unionista vetäytymistä koskeva laki) 3 pykälän nojalla ja sellaisena kuin se on muutettu Tietosuojaa, Yksityisyyden suojaa ja Sähköistä viestintää koskevalla lailla (muutokset jne.) (EU Exit) Regulations 2019 (muutoksineen)), Data Protection Act 2018, FADP (Swiss Federal Act on Data Protection, Sveitsin liittovaltion Tietosuojalaki), Yhdysvaltojen osavaltioiden Tietosuojalait, LGPD (Brasilian yleinen Tietosuojalaki, Brazilian General Data Protection Law), PIPL (Personal Information Protection Law of the People's Republic of China, Kiinan kansantasavallan henkilötietojen suojaa koskeva laki) ja kaikki niiden täytäntöönpanemiseksi tai niiden nojalla annetut lait ja/tai asetukset, tai lait ja/tai asetukset joilla muutetaan, korvataan, saatetaan uudelleen voimaan tai konsolidoidaan/yhdistetään mitä tahansa niistä (edellä mainituista), mukaan lukien soveltuvin osin valvontaviranomaisten antamat ohjeistukset sekä menettelysäännöt ja -käytännöt;

”**Henkilötiedot**” tarkoittavat mitä tahansa Rekisteröityä koskevia tietoja.

”**Henkilötietojen käsittelijä**” tarkoittaa luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka Käsittelee Henkilötietoja Rekisterinpitäjän puolesta.

”**Käsittely**” tarkoittaa mitä tahansa toimintoa tai toimintosarjaa, joka suoritetaan Henkilötiedoille tai Henkilötietojoukoille joko automaattisesti tai muutoin, kuten keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakemista, kyselyä, käyttöä, luovuttamista siirtämällä, levittämällä tai asettamalla muutoin saataville, yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

”**Tietoturvaloukkaus**” tarkoittaa mitä tahansa sellaisten Asiakkaan henkilötietojen tahatonta tai laitonta vahingoittumista, tuhoutumista, häviämistä, muuttamista tai luvatonta luovuttamista tai pääsyä niihin, joita Iron Mountain, sen henkilökunta tai alihankkijat käsittelevät Palvelujen tarjoamisen yhteydessä.

”**Palvelut**” tarkoittavat mitä tahansa Palveluja, joita Iron Mountain tai sen tytäryhtiöt tai kumppanit tarjoavat Asiakkaalle tai sen tytäryhtiöille tai kumppaneille Sopimuksen nojalla.

”**Yhdysvaltain osavaltioiden Tietosuojalait**” tarkoittavat kaikkia Yhdysvaltain osavaltioiden Tietosuojalakeja, joita sovelletaan Sopimuksen mukaiseen Henkilötietojen Käsittelyyn, mukaan lukien rajoittumatta ja siinä muodossa johon niitä saatetaan muuttaa, tai jolla ne saatetaan korvata ajoittain: (1) Kalifornian kuluttajien Tietosuojalaki (California Consumer Privacy Act), siihen Kalifornian Tietosuojaoikeuslailla (California Privacy Rights Act) tehtyjen muutosten mukaisesti ja kaikki niihin liittyvät täytäntöönpanosäädökset (yhdessä ”**CCPA** ”); (2) Coloradon Tietosuojalaki (”**CPA**”, Colorado Privacy Act), (3) Virginian kuluttajien Tietosuojalaki (Virginia Consumer Data Protection Act) (”**CDPA**”) (4) Utahin kuluttajien Tietosuojalaki (Utah Consumer Privacy Act, ”**UCPA**”); ja (5) Connecticutin Tietosuojalaki (Connecticut Data Privacy Act, ”**CTDPA**”).

2. TIETOJEN KÄSITTELYN LAAJUUS JA YKSITYISKOHTAISTA TIETOA TIETOJEN KÄSITTELYSTÄ

2.1 Tätä TKS:ää sovelletaan Asiakkaan henkilötietoihin, joita Iron Mountain Käsittelee Henkilötietojen käsittelijänä toimittaessaan Palveluja Sopimuksen mukaisesti Asiakkaan puolesta.

2.2 Iron Mountain voi Rekisterinpitäjänä kerätä ja käsitellä Asiakkaan ja sen konsernin työntekijöiden Henkilötietoja laillisiin liiketoimintatarkoituksiin, kuten Sopimusten ja asiakassuhteiden hallintaan sekä noudattaen Tietosuojalainsäädäntöä ja Iron Mountainin Tietosuojailmoitusta, joka on saatavilla Iron Mountainin verkkosivustoilla, ja muita soveltuvia Tietosuojakäytäntöjä. Tässä TKS:ssä määritellyt Iron Mountainin velvollisuudet eivät koske edellä mainitun kaltaisten Henkilötietojen Käsittelyä.

2.3 Henkilötietojen Käsittelyn aiheena ja tarkoituksena on Palvelujen suorittaminen. Asiakkaan ja Iron Mountainin oikeudet ja velvollisuudet on määritelty tässä TKS:ssä. Tämän TKS:n liitteessä 1 määritellään Käsittelyn luonne, kesto ja tarkoitus, minkä tyyppisiä Asiakkaan henkilötietoja Iron Mountain Käsittelee ja Rekisteröityjen kategoriat, joiden Henkilötietoja käsitellään.

2.4 Kun Iron Mountain Käsittelee Asiakkaan henkilötietoja Palvelujen tarjoamisen yhteydessä, Iron Mountain:

2.4.1 Käsittele Asiakkaan henkilötietoja vain Asiakkaan dokumentoitujen ohjeiden mukaisesti. Jos Iron Mountainin on käsiteltävä Asiakkaan henkilötietoja mihin tahansa muuhun tarkoitukseen sellaisen lainsäädännön mukaisesti, jonka alainen Iron Mountain on, Iron Mountain ilmoittaa Asiakkaalle tästä vaatimuksesta ensin, ellei kyseinen laki (lait) kiellä tätä tärkeästä yleisen edun mukaisesta syystä; ja

2.4.2 Noudata aina soveltuvaa Tietosuojalainsäädäntöä ja ilmoita Asiakkaalle välittömästi, jos Iron Mountainin mielestä Asiakkaan antama Asiakkaan henkilötietojen Käsittelyä koskeva ohjeistus tai määräys rikkoo soveltuvaa Tietosuojalainsäädäntöä.

2.5 Asiakkaan ohjeistus tai määräys sitoo Iron Mountainia, ellei ohjeiden täyttäminen edellytä Sopimuksen mukaisen Palvelun tarjoamista, ja Asiakas ei suostu maksamaan palvelumaksuja kyseisistä Palveluista.

2.6 Iron Mountain varmistaa, että henkilöstö, joka tarvitsee pääsyn Asiakkaan henkilötietoihin, on näiden Asiakkaan henkilötietojen osalta sitovan luottamuksellisuutta edellyttävän velvollisuuden alainen, ja ryhtyy kohtuullisiin toimenpiteisiin varmistaakseen niiden Iron Mountainin henkilöstön jäsenten luotettavuuden ja pätevyyden, joilla on pääsy Asiakkaan henkilötietoihin.

3. ASIAKASPALVELUN TARJOAMINEN

3.1 Iron Mountainin tulee auttaa asiakasta aina ottaen myös huomioon Käsittelyn luonteen:

3.1.1 asianmukaisin teknisin ja organisatorisin toimenpitein ja mahdollisuuksien mukaan täyttämällä Asiakkaan velvoitteet vastata oikeuksiaan käyttävien Rekisteröityjen pyyntöihin

3.1.2 Asiakkaan velvoitteiden noudattamisen varmistaminen (kuten Käsittelyn turvallisuus, Henkilötietojen Tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle, Henkilötietojen Tietoturvaloukkauksesta ilmoittaminen Rekisteröidylle, Tietosuojaa koskeva vaikutusten arviointi ja valvontaviranomaisten ennakkokuuleminen, jos Käsittely aiheuttaisi suuren riskin, jos Rekisterinpitäjä ei olisi ryhtynyt toimenpiteisiin vähentääkseen riskiä) ottaen huomioon Iron Mountainin saatavilla olevat tiedot.

3.1.3 asettamalla Asiakkaan saataville kaikki tiedot, joita Asiakas kohtuudella pyytää, jotta Asiakas voisi osoittaa, että sen Iron Mountainin valintaan ja nimittämiseen liittyvät velvollisuudet on täytetty.

4. TURVALLISUUSTOIMENPITEET

4.1 Ottaen huomioon tavanomaiset operatiiviset menettelyt, toimeenpanokustannukset sekä Käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset Iron Mountain toteuttaa asianmukaiset ja kohtuulliset tekniset ja organisatoriset toimenpiteet, joiden tarkoituksena on suojata Asiakkaan henkilötietojen luottamuksellisuutta, eheyttä ja saatavuutta sekä suojata Asiakkaan henkilötietoja luvattomalta tai lainvastaiselta Käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta, vahingoittumiselta, muuttumiselta, luovuttamiselta tai paljastamiselta. Iron Mountainin turvallisuusstandardit on esitetty tämän TKS:n liitteessä 2.

4.2 Asiakas vastaa yksin siitä, täyttävätkö nämä tekniset ja organisatoriset toimenpiteet Asiakkaan vaatimukset.

5. LAKIEN NOUDATTAMINEN

Asiakas ja sen konsernin jäsenet: (i) käsittelevät Asiakkaan henkilötietoja Tietosuojalainsäädännön mukaisesti; (ii) on valtuutettu antamaan Iron Mountainille kirjallisia ohjeita ja ohjeistusta Asiakkaan henkilötietojen Käsittelystä Palvelujen yhteydessä (mukaan lukien Asiakkaan henkilötietojen Rekisterinpitäjänä toimivan minkä tahansa kolmannen osapuolen tahon puolesta); ja (iii) säilyttävät aina Asiakkaan henkilötietojen Käsittelyn hallinnan ja toimivallan.

6. ALIKÄSITTELY

6.1 6.1 Asiakas tiedostaa ja hyväksyy sen, että Iron Mountain voi käyttää emoyhtiönsä, sen tytäryhtiöitä ja muita kolmannen osapuolen Alikäsittelijöitä (mukaan lukien Iron Mountainin tytäryhtiöiden tai emoyhtiön käyttämät kolmannen osapuolen Alikäsittelijät) Asiakkaan henkilötietojen käsittelyä varten. tämän tietosuojasopimuksen mukaisesti jäljempänä olevan Lausekkeen 6.2 alaisena.

6.2 Luettelo Asiakkaan tämän TKS:n päivämääränä hyväksymistä Alikäsittelijöistä on saatavilla tästä[1] . Iron Mountain voi milloin tahansa vaihtaa tai nimittää uuden Alikäsittelijän edellyttäen, että Asiakkaalle annetaan kirjallinen ilmoitus viisitoista (15) päivää etukäteen, ja että Asiakas ei vastusta tällaisia muutoksia todistettavasti Tietosuojaan liittyvin perustein kyseisellä 15 päivän aikavälillä. Saadakseen näitä sähköposti-ilmoituksia Asiakkaan on tilattava ja hallinnoitava olemassa olevaa Iron Mountainin ilmoituspalvelun tilausta tämän verkkosivun kautta. [2]

6.3 Jos asiakas ei tilaa tätä ilmoituspalvelua, Iron Mountain ei ole vastuussa Alikäsittelijäilmoituksen puuttumisesta, ja kaikki tällaiset Alikäsittelijän tehtävään asettamiset katsotaan Asiakkaan valtuuttamiksi**.** Jos Asiakas vastustaa kirjallisesti todistettavin Tietosuojaan liittyvin perustein korvaavan tai uuden Alikäsittelijän nimittämistä viidentoista (15) päivän kuluessa kirjallisesta ilmoituksesta, tällöin Iron Mountain pyrkii kohtuullisin keinoin saamaan Asiakkaan saataville Palvelujen muutoksen tai suosittelee muutosta Asiakkaan Palvelujen kokoonpanoon/konfiguraatioon tai käyttöön, kussakin tapauksessa estääkseen sen, että Alikäsittelijä, jota on vastustettu, käsittelisi Asiakkaan henkilötietoja Asiakkaan harkintaa ja hyväksyntää varten. Jos Asiakas ei hyväksy tällaisia Iron Mountainin ehdottamia muutoksia viidentoista (15) päivän kuluessa, Iron Mountain voi kirjallisen ilmoituksen Asiakkaalle annettuaan irtisanoa välittömästi Palvelun tai Palvelun osan, jota Iron Mountain ei voi tarjota ilman vastalauseen kohteena olevan toimivan Alikäsittelijän käyttöä. Tällainen irtisanominen ei vaikuta osapuolten kertyneisiin oikeuksiin tai vastuisiin, edellyttäen, että Iron Mountainin tai Iron Mountainin tytäryhtiöt eivät maksa irtisanomisen yhteydessä irtisanomismaksuja, -kuluja tai muita korvauksia, ja Asiakas ottaa viipymättä haltuunsa Iron Mountainille osana irtisanottuja Palveluja toimittamansa resurssit Sopimusehtojen mukaisesti ja Asiakkaan omalla kustannuksella.

6.4 Iron Mountain varmistaa, että kaikki tämän TKS:n Alikäsittelijöiden kanssa tehdyt Sopimukset sisältävät määräykset, jotka ovat olennaisilta osiltaan samat kuin tässä TKS:ssä, ja jotka ovat soveltuvan Tietosuojalainsäädännön mukaiset. Jos Iron Mountainin Alikäsittelijä aiheuttaa sen, että Iron Mountain rikkoo tämän TKS:n tai minkä tahansa soveltuvan Tietosuojalainsäädännön mukaisia velvoitteitaan, Iron Mountain on edelleen täysin vastuussa Asiakkaalle näiden ehtojen mukaisten Iron Mountainin velvoitteiden täyttämisestä.

7. TURVALLISUUSRIKKOMUKSET

7.1 Epäillyn Tietoturvaloukkauksen sattuessa Iron Mountain:

7.1.1 toimii viipymättä epäillyn Tietoturvaloukkauksen tutkimiseksi ja epäillyn Tietoturvaloukkauksen vaikutusten tunnistamiseksi, estämiseksi ja lieventämiseksi sekä Tietoturvaloukkauksen korjaamiseksi

7.1.2 ilmoittaa Asiakkaalle ilman aiheetonta viivytystä, kun se on kohtuullisen varma siitä, että on tapahtunut jokin Tietoturvaloukkaus, ja antaa Asiakkaalle yksityiskohtaisen kuvauksen kyseessä olevasta Tietoturvaloukkauksesta, mukaan lukien tiedot, jotka ovat kohtuudella tarpeen, jotta Asiakas voi täyttää Tietosuojalainsäädännön mukaiset raportointivelvoitteensa.

7.2 Asiakas hyväksyy, että Iron Mountain voi antaa Lausekkeen 7.1.2 mukaiset tiedot vaiheittain. Tällaisissa tapauksissa, joissa Iron Mountainilla ei ole pääsyä määrättyihin Lausekkeessa 7.1.2 lueteltuihin tietoihin tai se ei pysty toimittamaan niitä Asiakkaalle, Iron Mountain ilmoittaa asiasta Asiakkaalle, eikä Iron Mountain ole vastuussa tällaisten tietojen toimittamatta jättämisestä.

---

[1] https://www.ironmountain.com/-/media/files/Utility/Legal/GLOBAL-Personal-Data-Subprocessors-List.xlsx?la=en

[2] https://urldefense.proofpoint.com/v2/url?u=https-3A__reach.ironmountain.com_LegalSubprocessorSubscription&d=DwMFaQ&c=jxhwBfk-KSV6FFIot0PGng&r=JTlzF2zjl-gYEq5GmWmZcbgd--hgyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

8. TARKASTUKSET

Iron Mountain sallii Asiakkaan ja kyseisten tarkastajien tai valtuutettujen edustajien, kun asiasta on ilmoitettu Iron Mountainille vähintään kymmenen (10) arkipäivää etukäteen, suorittaa tarkastuksia Sopimuskaudella sillä edellytyksellä, että Iron Mountainia ei vaadita antamaan tai sallimaan pääsyä tietoihin, jotka koskevat seuraavia asioita: (i) muut Iron Mountainin Asiakkaat (ii) Iron Mountainin ei-julkiset ulkoiset raportit ja (iii) Iron Mountainin sisäisen tarkastus- tai vaatimustenmukaisuusosaston laatimat sisäiset raportit. Tämän Lausekkeen mukaisen tarkastuksen tarkoitus on rajoitettu sen varmistamiseen, että Iron Mountain Käsittelee Asiakkaan henkilötietoja tämän TKS:n mukaisten velvoitteidensa mukaisesti. Ellei ole tapahtunut Tietoturvaloukkaus, enintään yksi tällainen tarkastus suoritetaan kahdentoista (12) kuukauden aikana.

9. KANSAINVÄLISET TIEDONSIIRROT (RAJOITETUT SIIRROT)

9.1 Soveltuvassa laajuudessa Asiakas hyväksyy ja valtuuttaa asiakaskohtaisten Henkilötietojen kansainväliset siirrot tahoille, Kohdassa 6.2 esitetyllä tavalla ja Liitteen 3 mukaisesti Palvelujen toimittamiseksi, ja Asiakas ja Iron Mountain sopivat:

9.1.1 noudattavansa tällaisiin siirtoihin liittyen soveltuvaa Tietosuojalainsäädäntöä

9.1.2 että heillä on, ottaen huomioon rajoittumatta, i) Asiakkaan henkilötietojen luokat, ii) maat, joiden kansalliset lait eivät välttämättä tarjoa Henkilötiedoille EU/UK:n lakiin verrattavaa suojauksen tasoa ("**Kolmas maa**") laajuudeltaan, iii) Kohdassa 7 määritellyt asiaankuuluvat tekniset ja organisatoriset toimenpiteet ja iv) kyseiset osapuolet, jotka osallistuvat tällaisten Asiakkaan henkilötietojen käsittelyyn, suorittivat arvioinnin hyväksytyn asiaankuuluvan siirtomekanismin asianmukaisuudesta jäljempänä, jos laki sitä edellyttää, ja ovat päättäneet, että tällainen siirtomekanismi on suunniteltu asianmukaisesti varmistamaan, että tämän tietosuojalain mukaisesti siirretyt Henkilötiedot saavat kohdemaassa suojan, joka vastaa olennaisesti Tietosuojalainsäädännössä taattua suojaustasoa.

10. VASTUU JA VAHINGONKORVAUS

10.1 Vaikka Sopimuksessa ei ole toisin mainittu, jos Tietoturvaloukkaus johtuu suoraan siitä, että Iron Mountain rikkoo tämän TKS:n mukaisia velvollisuuksiaan, Iron Mountain korvaa Asiakkaalle soveltuvan lain sallimissa rajoissa suorat, todennettavissa olevat, välttämättömät ja kohtuudella Asiakkaalle aiheutuneet kolmannen osapuolen kulut, jotka ovat aiheutuneet kyseisen Tietoturvaloukkauksen (a) tutkinnasta (b) Tietosuojalainsäädännön mukaisten ilmoitusten laatimisesta ja lähettämisestä kyseisille Rekisteröidyille ja sääntelyviranomaisille (c) luotonvalvontapalvelujen tarjoamisesta kyseisille henkilöille lain edellyttämällä tavalla enintään kahdentoista (12) kuukauden ajan ja (d) niiden sääntelyllisten sakkojen, rangaistuksien, tai valvontaviranomaisen määräämien seuraamuksien osien maksamisesta, joista valvontaviranomainen ilmoittaa Iron Mountain olevan suoraan vastuussa.

10.2 Mikäli Rekisteröity nostaa kanteen jompaakumpaa tai molempia osapuolia vastaan väitetystä Tietosuojalainsäädännön rikkomisesta (”**Rekisteröidyn vaateet”)** tilanteessa, jossa se on sallittu, kukin osapuoli hallitsee mitä tahansa tällaista vaadetta vastaan puolustautumistaan (tai omaa osuuttaan puolustautumisesta) ja on yksin vastuussa omista kustannuksistaan, puolustamiseen tai tapaukseen liittyvistä kuluista, korvausvelvollisuuksista ja veloista, mukaan lukien oikeudenkäyntikulut tai kaikki tuomioistuimen osapuolta vastaan määräämistä tai sovittelussa sovituista summista, edellyttäen kuitenkin, että jos kumpikin osapuoli on vastuussa osasta tai kumpi tahansa osapuoli on vastuussa samasta tapauksesta tai tapahtumasarjasta Rekisteröidylle aiheutuneiden vahinkojen koko summasta ja Rekisteröity on saanut täyden korvauksen vain yhdeltä osapuolelta (”**korvausosapuoli**”), silloin korvauksen maksavalla osapuolella on oikeus vaatia toiselta osapuolelta korvausta, joka vastaa tällaisen toisen osapuolen aiheuttamaa vahinkoa. Korvaava osapuoli voi esittää vaatimuksensa toiselle osapuolelle vain 12 kuukauden sisällä tapahtuman jälkeen soveltuvan lain sallimissa rajoissa.

10.3 Soveltuvan lainsäädännön sallimissa rajoissa tässä Sopimuksessa asetettuja vastuun rajoituksia ja vahingonkorvausten poissulkemisia sovelletaan kokonaisvastuuseen kaikista Asiakkaan Iron Mountainia vastaan esittämistä vaateista ja vaatimuksista, jotka johtuvat tästä TKS:stä ja/tai Sopimuksesta tai liittyvät niihin. Nämä vastuunrajoitukset ja vahingonkorvausten poissulkemiset koskevat kaikkia vaateita ja vaatimuksia, riippumatta siitä, johtuvatko ne Sopimuksesta, oikeudenloukkauksesta tai mistä tahansa muusta vahingonkorvausoikeudellisesta perusteesta, ja viittaus Iron Mountainin vastuuseen tarkoittaa Iron Mountainin ja kaikkien Iron Mountainin tytäryhtiöiden yhteenlaskettua (korvaus)vastuuta Asiakkaan ja kaikkien muiden Asiakkaan tytäryhtiöiden vaateista ja vaatimuksista. Soveltuvien lakien edellyttämässä laajuudessa tämän kohdan tarkoituksena ei ole (i) muokata tai rajoittaa osapuolten vastuuta Rekisteröidyn vaateiden suhteen, jotka on tehty osapuolta vastaan, kun kyseessä on yhteinen tai useita vastuita, tai (ii) rajoittaa kummankaan osapuolen velvollisuutta maksaa sääntelyviranomaisen määräämiä rangaistussakkoja (tai muita rangaistuksia) kyseiselle osapuolelle.

10.4 Lausekkeissa 10.1–10.3 mainitaan kummankin osapuolen ainoa ja yksinomainen oikeussuojakeino ja kummankin osapuolen yksinomainen vastuu kaikista tähän TKS:ään liittyvistä menetyksistä, vahingoista, kuluista tai korvausvastuista.

11. VIRANOMAISTEN PYYNNÖT

11.1 Jäljempänä olevien kohtien 11.2–11.5 mukaisesti Iron Mountain sitoutuu ilmoittamaan Asiakkaalle, jos se

11.1.1 saa kohdemaan viranomaiselta, mukaan lukien oikeusviranomaiset, lakien mukaisen oikeudellisesti sitovan pyynnön, jossa pyydetään Sopimuksen nojalla siirrettyjen Asiakkaan henkilötietojen luovuttamista; tai

11.1.2 tulee tietoiseksi viranomaisten suorasta pääsystä Asiakkaan henkilötietoihin, jotka on siirretty Sopimuksen nojalla ja kohdemaan lakien mukaisesti i.

11.2 jos Iron Mountain ei saa kohdemaan lakien mukaan ilmoittaa Asiakkaalle, Iron Mountain suostuu parhaansa mukaan hankkimaan vapautuksen kiellosta tiedottaakseen asiasta mahdollisimman paljon tietoja mahdollisimman pian.

11.3 suostuu tarkistamaan tietojen luovutuspyynnön laillisuuden ja erityisesti sen, onko pyyntö sen esittäneelle viranomaiselle myönnettyjen valtuuksien rajoissa, ja kyseenalaistamaan pyynnön, jos Iron Mountain tulee siihen tulokseen, että on perustellusti syytä katsoa, että pyyntö on kohdemaan lakien mukaan laiton. Iron Mountain ei luovuta pyytämiäsi Asiakkaan henkilötietoja, ennen kuin se on välttämätöntä soveltuvien menettelysääntöjen mukaisesti.

11.4 Iron Mountain sopii, että Vastatessaan luovutuspyyntöön, se antaa niin vähän tietoja kuin on sallittu luovutuspyyntöön vastattaessa, perustuen pyynnön kohtuulliseen tulkintaan.

11.5 Iron Mountain sitoutuu säilyttämään tämän Lausekkeen mukaiset tiedot Sopimuskaudella ja toimittamaan ne pyynnöstä toimivaltaisen valvontaviranomaisen saataville.

12. SEKALAISTA

12.1 Iron Mountainin tarjoamien Palvelujen luonteen mukaisesti Sopimuksen päättyessä Asiakkaan erityisohjeiden mukaisesti ja Sopimusehtojen mukaisesti, Iron Mountain joko poistaa/tuhoaa tai palauttaa Asiakkaalle tai Asiakkaan nimeämälle kolmannelle osapuolelle kaikki Asiakkaan henkilötiedot. Kaikki Asiakkaan tietoihin Asiakkaan puolesta tallennetut Asiakkaan henkilötiedot, joita Iron Mountain säilyttää Asiakkaan puolesta, palautetaan Asiakkaalle sovitun poistumis- tai siirtymissuunnitelman mukaisesti ja sovituin kustannuksin Sopimuksessa tai muussa soveltuvassa Sopimusasiakirjassa kuvatulla tavalla. Kaikissa muissa tapauksissa, jos Sopimus ei koske Asiakkaan henkilötietojen poistamista/hävittämistä tai palauttamista, ja jos Asiakas ei anna Asiakkaan henkilötietojen poistamista/hävittämistä tai palauttamista koskevia ohjeita viidentoista (15) päivän kuluessa Sopimuksen irtisanomisesta tai päättymisestä, Iron Mountain lähettää Asiakkaalle kirjallisen ilmoituksen, jossa se pyytää 15 (viidentoista) päivän kuluessa yksityiskohtaisia ohjeita siitä, poistetaanko/hävitetäänkö vai palautetaanko Asiakkaan henkilötiedot, ja ilmoittaa Asiakkaalle kaikista soveltuvista turvallisen hävittämisen maksuista tai muista maksuista, jotka Asiakas on velvollinen maksamaan. Jos asiakas ei toimita kirjallisia ohjeita tällaisen viidentoista (15) päivän kuluessa ja maksa soveltuvia maksuja tämän saman ajanjakson aikana, asiakas valtuuttaa täten Iron Mountainin käsittelemään, poistamaan ja tuhoamaan kaikki Asiakkaan henkilötiedot Sopimuksen päättymisen jälkeen Iron Mountainin valinnan mukaan ja Asiakkaan kustannuksella.

12.2 Lausekkeesta 12.1 huolimatta Iron Mountain ei riko velvoitteitaan, jotka koskevat varmuuskopionauhoilla säilytettyjen Asiakkaan henkilötietojen poistamista, kunhan tällaiset varmuuskopionauhat (ja siten poistetut Asiakkaan henkilötiedot) ohitetaan normaalin liiketoiminnan yhteydessä.

12.3 Poikkeuksena tämän TKS:n liitteessä 3 määritellyt Mallisopimuslausekkeet (tämän TKS:n liitteessä 3), tämä TKS ja kaikki tästä TKS:stä tai sen rikkomuksesta, irtisanomisesta tai pätevyydestä johtuvat tai siihen liittyvät riidat, vaateet, vaatimukset tai erimielisyydet ovat Sopimuksen lainvalintaa koskevan määräyksen alaisia, ja kaikki tästä TKS:stä johtuvat tai siihen liittyvät riidat, kiistat, vaateet ja vaatimukset pyritään ensisijaisesti ratkaisemaan Sopimukseen sisältyvän määritellyn riidanratkaisuprosessin kautta.

12.4 Kumpikin osapuoli voi ajoittain ilmoittaa toiselle osapuolelle kirjallisesti tähän Tietosuojasopimukseen tehdyistä muutoksista, joita osapuoli kohtuudella pitää tarpeellisina Tietosuojalainsäädännön vaatimusten tai valvontaviranomaisen tai toimivaltaisen tuomioistuimen päätöksen täyttämiseksi. Kaikki tällaiset muutokset tulevat voimaan vain, jos ja siinä määrin kuin on esitetty kummankin osapuolen yhdessä sovitussa tämän TKS:n muutoksessa, paitsi jos toinen osapuoli ilmoittaa toiselle osapuolelle mistä tahansa uusista lakisääteisistä vaatimuksista ja lähettää tällaisen (uusien vaatimusten mukaisen) muutoksen, joka sisältää vain tarvittavat muutokset, ja joka voidaan hyväksyä ilman muodollista sopimista, ts. siten, että vastalausetta ei esitetä tietyssä määräajassa, katsotaan yhteisesti sovituksi muutokseksi tähän TKS:ään.

LIITE 1

Tietoja Käsittelystä ja Tiedonsiirrosta (jos soveltuu)

A. LUETTELO OSAPUOLISTA:

Tämän TKS:n osapuolet ja tietojen viejän ja tietojen tuojan roolit on asetettu Sopimuksessa ja liitteessä 3 (Kansainväliset Tiedonsiirrot), jos niitä sovelletaan.

B. KÄSITTELYN/SIIRRON KUVAUS (jos soveltuu):

Rekisteröityjen ryhmät, joiden Henkilötietoja käsitellään/siirretään:

Iron Mountainin Palvelujen luonteesta ja Asiakkaan liiketoiminnasta riippuen Asiakas voi toimittaa Iron Mountainille Henkilötietoja, jotka kuuluvat eri Rekisteröityjen ryhmiin/kategorioihin, ja joiden laajuutta Asiakas oman harkintansa mukaan hallitsee. Rekisteröityjen ryhmiä voivat olla: entiset ja nykyiset työntekijät, entiset ja nykyiset urakoitsijat tai konsultit, välitystoimiston toimittamat urakoitsijat tai konsultit ja ulkoiset toimeksisaajat, työnhakijat ja ehdokkaat, opiskelijat ja vapaaehtoiset, työntekijöiden tunnistamat yksilöt tai eläkkeelle jääneet henkilöt edunsaajina, puoliso, asuin-/avokumppani/rekisteröidyn parisuhteen kumppani, huollettavat ja hätäyhteyshenkilöt, eläkkeelle jääneet entiset ja nykyiset johtajat ja päälliköt, osakkeenomistajat, joukkovelkakirjan haltijat, tilinhaltijat, loppukäyttäjät/kuluttajat (aikuiset ja lapset); potilaat (aikuiset ja lapset); ohikulkijat (valvontakamerat); ja verkkosivuston käyttäjät.

Käsiteltävien/siirrettävien Henkilötietojen luokat:

Iron Mountainin Palvelujen luonteesta ja Asiakkaan liiketoiminnasta riippuen Asiakas voi toimittaa Iron Mountainille Henkilötietoja, jotka kuuluvat eri Henkilötietojen ryhmiin/kategorioihin, ja joiden laajuutta Asiakas oman harkintansa mukaan hallitsee. Näin ollen ryhmiin voi kuulua henkilökohtaisia tietoja, jotka liittyvät Asiakkaaseen ja/tai Asiakkaan omiin Asiakkaisiin, työntekijöihin jne.

Siirretyt arkaluontoiset tiedot (jos soveltuu):

Iron Mountainin Palvelujen luonteesta ja Asiakkaan liiketoiminnasta riippuen Asiakas voi toimittaa Iron Mountainille arkaluontoisia tietoja, joiden laajuutta Asiakas oman harkintansa mukaan hallitsee.

Tarvittaessa siirtojen tiheys (esim. siirretäänkö tietoja kertaluontoisesti vai jatkuvasti):

Siirtoja tapahtuu jatkuvasti.

Käsittelyn luonne:

Kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, mukauttaminen tai muuttaminen, hakeminen, konsultointi, käyttö, luovuttaminen siirtämällä, levittämällä tai muutoin asettamalla saataville, kohdistaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

Tietojen käsittelyn/siirron (jos soveltuu) tarkoitus (tarkoitukset) ja jatkokäsittely:

Palvelujen tarjoaminen Sopimuksessa kuvatulla tavalla.

Tietojen säilyttäminen:

Iron Mountain säilyttää Henkilötietoja Asiakkaalle tarjottavien Palvelujen ajan ja siihen asti, kunnes Henkilötiedot palautetaan tai tuhotaan tämän TKS:n Lausekkeen 12.1 mukaisesti määritetyllä tavalla.

(Ali)käsittelijöille tehtävissä siirroissa on myös tarvittaessa määriteltävä Käsittelyn aihe, luonne ja kesto:

Asiakkaan kanssa solmitun Sopimuksen keston ajan alihankkijana toimivat käsittelijät tarjoavat muun muassa tietotekniikka- (IT) ja konsultointipalveluita, mukaan lukien maailmanlaajuista IT-tukea, tapahtumaraportointia ja hallintapalveluita.

C. TOIMIVALTAINEN VALVONTAVIRANOMAINEN

Kuten liitteessä 3 (Kansainväliset Tiedonsiirrot) on tarvittaessa määritetty.

LIITE 2

TEKNISET JA ORGANISATORISET TOIMENPITEET (”TURVATOIMENPITEET”)

1. TIETOTURVAOHJELMA JA -KÄYTÄNTÖ

Iron Mountainin on ylläpidettävä tietoturvaohjelmaa, jossa on asianmukaiset fyysiset, tekniset ja hallinnolliset suojakeinot, jotka on suunniteltu täyttämään alan standardit. Tietoturvaohjelman tulee sisältää:

1.1 Iron Mountainin tietoturvakäytäntöjen, -standardien ja -menettelyjen dokumentointi, sisäinen julkaisu ja viestintä.

1.2. Dokumentoitu ja selvä tietoturvaohjelman perustamisen ja ylläpidon vastuiden ja valtuuksien määrääminen;

1.3 Tietoturvaohjelman tärkeimpien valvontamekanismien, järjestelmien ja menettelyjen säännöllinen testaus

1.4 Hallinnolliset, tekniset ja operatiiviset toimenpiteet, joiden tarkoituksena on suojata kaikkia Asiakkaan henkilötietoja käyttäen tässä turvallisuusliitteessä kuvattuja käytäntöjä, menettelyjä ja prosesseja siinä määrin kuin ne ovat olennaisia ja soveltuvat siinä muodossa, jossa Asiakkaan henkilötietoja ylläpidetään/säilytetään.

2. RISKIN ARVIOINTI

Iron Mountainin on ylläpidettävä tietoturvariskien arviointiohjelmaa, joka on suunniteltu tunnistamaan ja arvioimaan kohtuullisesti ennakoitavia sisäisiä ja ulkoisia riskejä ja haavoittuvuuksia, jotka voivat vaikuttaa Asiakkaan henkilötietojen turvallisuuteen, luottamuksellisuuteen ja/tai eheyteen. Iron Mountain arvioi ja päivittää, tarvittaessa kohtuullista ja asianmukaista, nykyisen tietoturvaohjelman tehokkuutta tällaisten riskien rajoittamiseksi vuosittain tai aina, kun Asiakkaan henkilötietoihin kohdistuvassa riskissä tai haavoittuvuuksissa tapahtuu olennainen muutos.

3. TIEDONKÄSITTELYRESURSSIEN JA -VÄLINEIDEN SEKÄ FYYSISEN MEDIAN HALLINTA

3.1 Tietojenkäsittelyresurssien ja -välineiden hallinta. Iron Mountain ylläpitää tietojenkäsittelyresurssien ja -välineiden varastonhallintaohjelmaa hallitakseen Iron Mountainin tietojenkäsittelyresursseja ja -välineitä (kuten tietokoneita, palvelimia, tallennuslaitteita, viestintäverkkoja, henkilökohtaisia tietokoneita, kannettavia tietokoneita ja oheislaitteita) koskevia fyysisiä, teknisiä ja hallinnollisia tarkastuksia.
Tietojenkäsittelyresurssien ja -välineiden varastonhallintaohjelma sisältää seuraavaa:

- 3.1.1 Dokumentoitu resurssien ja välineiden omistajuuden määrääminen Iron Mountainin henkilöstölle tietojen asianmukaisen luokittelun, pääsyrajoituksista päättämisen ja pääsynvalvonnan tarkastamisen varmistamiseksi.
- 3.1.2 Resurssien ja välineiden sisällön/sisältämien tietojen poistaminen ennen niiden hävittämistä NIST 800-88:n mukaisesti.
- 3.1.3 Johdolta saatavan luvan vaatimus, ennen kuin poistetaan Iron Mountainin tiloista sellaisia laitteita tai ohjelmistoja, joita ei ole osoitettu/nimetty jollekulle tietylle henkilölle.

3.2 Hallinta- ja valvontakeinot. Iron Mountainilla on muun muassa seuraavat hallinta- ja valvontakeinot:

- 3.2.1 Toimintamenetelmät ja tekniset tarkastukset, jotka on suunniteltu suojaamaan Asiakirjoja, tietokonemediaa, syöttö-, tuotos- ja varmuuskopiointitietoja ja järjestelmän Asiakirjoja luvattomalta luovuttamiselta, paljastamiselta, muokkaamiselta ja tuhoamiselta.
- 3.2.2 Asiakkaan henkilötietoja sisältävien sähköisten tai fyysisten tallennusvälineiden turvalliset hävittämismenetelmät.
- 3.2.3 3.2.3Vakiintunut prosessi, jolla seurataan kaikkia Asiakkaan fyysisiä tieto- ja tallennusvälineitä Iron Mountainin alkuperäisestä säilytyksestä aina pysyvään poistamiseen tai tuhoamiseen asti.

4. TYÖNTEKIJÖIDEN TURVATOIMET

4.1 Luottamuksellisuus. Iron Mountain edellyttää kohtuudella, että kaikki Iron Mountainin työntekijät, mukaan lukien tilapäiset ja sopimustyöntekijät, suostuvat pitämään Asiakkaan henkilötiedot luottamuksellisina ja noudattamaan Iron Mountainin sisäisiä tietoturvaa ja hyväksyttävää käyttöä koskevia vaatimuksia.

4.2 Taustatutkimuskäytäntö. Iron Mountainilla on työntekijöilleen voimassa oleva taustatutkimus- ja huumetestauskäytäntö (vain Yhdysvalloissa). Iron Mountain jatkaa tällaisten käytäntöjen ylläpitämistä Sopimuskaudella. Käytäntöön liittyviä vaatimuksia ovat rajoittumatta huumeseulonta (vain Yhdysvallat), henkilöstön henkilöllisyyden todennus, rikosrekisterihaut, työsuhdetarkastukset, valtioiden/terroristien tarkkailuluettelohaut sekä määrättyjen työntekijöiden koulutuksen tarkastukset sekä tulevien (työrooliin ehdolla olevien) kuljettajien ja nykyisten kuljettajien ajokorttien ja rikkomushistorian tarkastukset. Kun taustatarkastuksessa tunnistetaan henkilön huonoon valoon asettavia tietoja, Iron Mountain suorittaa yksilöllisen arvioinnin soveltuvien työlakien ja parhaiden käytäntöjen mukaisesti.

4.3 Työskentely Alihankkijoiden kanssa. Iron Mountain edellyttää, että kaikki Sopimuksen mukaisia Palveluja suorittavat alihankkijat noudattavat samanlaisia rajoituksia kuin tässä Kohdassa esitetyt, jotka koskevat kaikkia alihankkijoiden työntekijöitä, jotka suorittavat Sopimuksen mukaisia Palveluja, joihin liittyy Asiakkaan henkilötietojen Käsittelyä.

4.4 Turvallisuustietoisuuskoulutus. Iron Mountainin on järjestettävä vähintään vuosittain yleinen turvallisuustietoisuuskoulutus ja erityinen roolikohtainen turvallisuuskoulutus kaikille Iron Mountainin työntekijöille, joilla on pääsy Asiakkaan henkilötietoihin. Iron Mountainin täytyy ylläpitää tietokantaa, josta käy ilmi koulutuksissa paikalla olevien Iron Mountainin työntekijöiden nimet ja kunkin turvallisuustietoisuuskoulutuksen päivämäärä. Iron Mountain tarkistaa ja päivittää turvallisuustietoisuuskoulutusohjelmansa säännöllisesti.

4.5 Iron Mountainin henkilöstön poistaminen. Iron Mountain ylläpitää kurinpidollista prosessia, jota sovelletaan Iron Mountainin työntekijöihin, jotka rikkovat tässä Asiakirjassa esitettyjä turvavaatimuksia.

4.6 Käyttöoikeuden lopettaminen irtisanomisen/toiseen rooliin siirtämisen yhteydessä. Kun työntekijä irtisanotaan tai siirretään rooliin, joka ei edellytä pääsyä Asiakkaan henkilötietoihin, Iron Mountainin työntekijän pääsy Asiakkaan henkilötietoihin lopetetaan viipymättä.

5. FYYSINEN JA YMPÄRISTÖN TURVALLISUUS

5.1 Fyysiset turvatoimet. Iron Mountainin tiloissa käytetään fyysisiä hallinta- ja valvontakeinoja, jotka rajoittavat kohtuullisesti pääsyä Asiakkaan henkilötietoihin, sisältäen Iron Mountainin asianmukaiseksi katsomalla tavalla, kuten kulunvalvontaprotokollat, fyysiset esteet kuten lukitut tilat ja alueet, työntekijöiden kulkuluvat, vierailijalokit, vierailijoiden kulkukortit, kortinlukijat, videovalvontakamerat ja tunkeutumisen havaitsemisen hälytykset. Kaikkien vierailijoiden on kirjauduttava sisään ja oltava aina saattajan kanssa.

5.2 Tukevat apuohjelmat. Iron Mountainin on käytettävä menetelmiä, jotka on suunniteltu suojaamaan Asiakkaan henkilötietoja ja järjestelmiä sisältäviä tiloja sähkö-, tietoliikenne-, vesi-, jätevesi-, lämmitys-, ilmanvaihto- ja ilmastointijärjestelmien vioilta soveltuvin osin.

5.3 Lähetysjärjestelmän turvallisuus. Iron Mountainin on käytettävä toimenpiteitä, jotka on suunniteltu suojaamaan sen verkkoinfrastruktuurin ja tietoliikennejärjestelmien fyysistä turvallisuutta Tiedonsiirron sieppaamiselta ja sen vahingoilta.

5.4 Toimipaikan ulkopuoliset laitteet. Siinä tapauksessa, että Iron Mountain ulkoistaa toimintoja, jotka edellyttävät toimipaikan ulkopuolisten laitteiden käyttöä Palvelujen tukena, kaikki Asiakkaan henkilötietoja tallentavat toimipaikan ulkopuoliset laitteet suojataan tietoturvakeinoilla, jotka vastaavat samaan tarkoitukseen käytettävien toimipaikan laitteiden tietoturvan tasoa.

5.5 Fyysinen pääsy tiedonkäsittelyresursseihin ja -välineisiin. Iron Mountain pitää kirjaa Iron Mountainin työntekijöistä, joilla on oikeus saada fyysinen pääsy Iron Mountainin hallinnoimaan tietokoneympäristöön (ympäristöihin), jota Iron Mountain käyttää Palvelujen tarjoamiseen yhden vuoden ajan, Asiakkaan Tietoturvaloukkaukseen liittyvän pyynnön tapauksessa ja Iron Mountainin turvakäytäntöjen mukaisesti, antaa Asiakkaalle pääsyn, jotta Asiakas voisi tarkastella tällaisten Iron Mountainin työntekijöiden tarkastettavia tietoja.

5.6 Rajoitettu fyysinen käyttö. Iron Mountain rajoittaa fyysistä pääsyä Iron Mountainin hallinnoimiin tiloihin, joissa käsitellään Asiakkaan henkilötietoja, ainoastaan niihin Iron Mountainin työntekijöihin ja valtuutettuihin yksilöihin, joilla on liiketoiminnallinen tarve tällaiseen pääsyyn. Iron Mountainilla on oltava hyväksyntäprosessi, jolla hyväksytään ja seurataan pyyntöjä saada fyysinen pääsy kyseisiin tiloihin.

5.7 Korjaukset ja muutokset. Iron Mountain pitää kirjaa kaikista fyysisiin komponentteihin tehtävistä turvallisuuteen liittyvät korjauksista ja muutoksista mukaan lukien turvavalvottujen alueiden laitteistot, seinät, ovet ja lukot tiloissa, joissa Asiakkaan henkilötietoja säilytetään.

5.8 Kirjan pitäminen. Pidä kirjaa laitteiston ja sähköisen median siirroista ja kaikista vastuuhenkilöistä.

6. VIESTINNÄN JA TIEDONKÄSITTELYTOIMINTOJEN HALLINTA

6.1 Laitteen konfiguronnin standardit. Iron Mountainin on luotava, otettava käyttöön ja ylläpidettävä järjestelmän hallintamenetelmiä, jotka täyttävät alan standardit, mukaan lukien rajoittumatta järjestelmän kovettaminen, järjestelmän ja laitteen päivitykset (käyttöjärjestelmä ja sovellukset) sekä asianmukainen virustorjuntaohjelman asennus ja päivitykset.

6.2 Tietojenkäsittelyjärjestelmien muutoksenhallinta. Iron Mountainilla on oltava käytössä sisäinen virallinen muutoksenhallintapyynnön prosessi tiedonkäsittely- ja viestintäverkkojärjestelmiä varten, ja Iron Mountainin muutospyynnöt on dokumentoitava, testattava ja hyväksyttävä ennen uusien tiedonkäsittely- tai verkkoviestintäominaisuuksien, järjestelmäkorjausten tai nykyisten järjestelmien muutosten käyttöönottoa.

6.3 Vastuiden ja tehtävien erottelu. Iron Mountain erottelee vastuut, tehtävät ja vastuualueet siten, ettei yksikään henkilö ole ainoa, joka voisi muokata Asiakkaan henkilötietoja käyttäviä tiedonkäsittelyjärjestelmiä.

6.4 Kehitys- ja tuotantoympäristöjen erottaminen. Iron Mountainin tiedonkäsittelyjärjestelmien kehitys-, testaus- ja tuotantoympäristöt on erotettava loogisesti tai fyysisesti toisistaan.

6.5 Tekninen arkkitehtuurin hallinta. Iron Mountain luo konfiguraation hallintaprosessin määritelläkseen ja hallitakseen tietojenkäsittelyjärjestelmän komponentteja, joita käytetään Palvelujen tarjoamiseen, sekä hallitakseen näiden komponenttien teknistä infrastruktuuria.

6.6 Hyökkäysten havaitseminen. Iron Mountain valvoo jatkuvasti tietokonejärjestelmiä ja -prosesseja Tietoturvaloukkausten tai -rikkomusten varalta ja ilmoittaa Asiakkaalle kaikesta luvattomasta pääsystä Asiakkaan henkilötietoihin.

6.7 Verkon turvallisuus. Iron Mountainin on varmistettava, että seuraavat asiat ovat kunnossa:

6.7.1 Kun kyseessä on Iron Mountainin isännöimä ympäristö, jota käytetään Palvelujen tarjoamiseen, verkkotunkeutumisen tunnistusjärjestelmä (IDS) ja tunkeutumisen estoanturit

(IPS), lokiin kirjatut hälytystapahtumat ja päivittäiset raportit, jotka annetaan tarkastettavaksi (yhdessä ”IDS/IPS”)

6.7.2 Iron Mountainin isännöimän Palvelujen tarjoamiseen käytettävän ympäristön (ympäristöjen) osalta IDS/IPS-järjestelmät, joita päivitetään ainakin viikoittain, mutta kohtuudella mahdollisimman pian päivitysten vastaanoton jälkeen, ja uusimpien threat signature -koodien (uhat toimintamallien kautta tunnistava koodi) tai sääntöjen nopea suorittaminen

6.7.3 Ulkoisesti asennettavien järjestelmien korkean riskin portteihin ei pääse internetistä.

6.7.4 Iron Mountainin verkkoyhteydet kirjataan ja tallennetaan lokitiedostoihin.

6.7.5 Palomuurin (palomuurien) käyttöönotto, joka on suunniteltu suojaamaan ja tarkistamaan kaikki saapuvat ja lähtevät verkkopalvelut määriteltyjen verkkopisteiden välillä;

6.7.6 Saapuvien ja lähtevien verkkoporttien tai palveluliikenteen koventamiskäytännöt kaikille Iron Mountainin omistamille tai hallinnoimille järjestelmille, jotka on dokumentoitu ja valtuutettu tietoturvaohjelmassa

6.7.7 Verkko- ja diagnostiikkaportit, jotka on kiinnitetty asianmukaisesti; ja

6.7.8 Käytännöt, menettelyt ja tekniset tarkastukset, jotka on suunniteltu estämään, havaitsemaan ja poistamaan haitallinen koodi tai tunnetut hyökkäykset Iron Mountainin tietojärjestelmiä vastaan.

6.8 Salatun todennuksen tunnukset. Iron Mountain varmistaa, että todennustiedot salataan Iron Mountainin verkkolaitteiden kautta lähettämisen aikana.

6.9 Turvallinen verkon hallinta. Iron Mountainin verkkoja on hallittava ja valvottava kohtuullisesti tunnettujen uhkien varalta ja turvallisuutta ylläpidettävä kaikkien Iron Mountainin hallinnoimien verkossa olevien tai verkon kautta siirrettävien sovellusten ja tietojen osalta. Teknisiä valvontatoimia ja turvallisia viestintäprotokollia on käytettävä estämään epäluotettaviin verkkoihin tai julkisesti käytettävissä oleviin palvelimiin tapahtuvat rajoittamattomat yhteydet.

6.10 Suojaus viruksia vastaan. Iron Mountainin on otettava käyttöön ja ylläpidettävä virustorjuntaohjelmaa, joka sisältää haittaohjelmasuojauksen, ajantasaiset allekirjoitustiedostot tai vaihtoehtoisen suojauksen uusia uhkia, korjaustiedostoja ja virusmääritelmiä vastaan, Iron Mountainin hallinnoimia palvelimia ja työasemia varten, joita käytetään säilyttämään Asiakkaan henkilötietoja tai niihin pääsyyn.

6.11 Verkkosivusto – Asiakkaan salaus. Iron Mountain varmistaa, että kullakin verkkosivustolla on käytössä Secure Sockets Layering (SSL) sekä voimassa oleva SSL-sertifikaatin, joka edellyttää luottamuksellisuutta, todennusta tai lupien hallintaa.

6.12 Tietojen varmuuskopiointi. Iron Mountainin on luotava asianmukaiset varmuuskopiot järjestelmätiedostoista. Lisäksi Iron Mountain kehittää ja ylläpitää menettelyjä katastrofista palautumiseksi. Katso lisätietoja jäljempänä olevasta kohdasta ”katastrofeista palautuminen”.

6.13 Siirrettävät sähköiset tiedot. Iron Mountainin on käytettävä salausta alan standardialgoritmilla, jonka avainpituus on vähintään 128 bittiä, suojaamaan julkisissa verkoissa lähetettäviä Asiakkaan henkilötietoja, kun ne ovat peräisin Iron Mountainin isännöimästä infrastruktuurista.

6.14 Kryptografiset hallinta- ja valvontakeinot. Iron Mountain noudattaa dokumentoitua käytäntöä kryptografisten hallintakeinojen (salauskontrollien) osalta. Iron Mountainin kryptografisten hallinta- ja valvontakeinojen täytyy:

6.14.1 olla suunniteltu suojaamaan kohtuullisesti Iron Mountainin käsittelemien, siirtämien tai tallentamien Asiakkaan henkilötietojen luottamuksellisuutta ja eheyttä missä tahansa jaetussa verkkoympäristössä Sopimusehtojen mukaisesti.

6.14.2 Iron Mountainin kryptografisia hallinta- ja valvontakeinoja on sovellettava Palvelujen tarjoamiseen käytetyssä Iron Mountainin isännöimässä ympäristössä (ympäristöissä) Asiakkaan henkilötietoihin, joita siirretään ”epäluotettaviin” verkkoihin tai niiden kautta (ts. verkot, joita Iron Mountain ei lain mukaan hallitse), mukaan lukien verkot, joita käytetään tietojen lähettämiseen Asiakkaan yritysverkkoon Iron Mountainin verkosta, edellyttäen kussakin tapauksessa yhteistyötä Asiakkaan kanssa hallittaessa Asiakkaan saamien siirtojen salauksen purkamiseen tarvittavia salausavaimia; ja

6.14.3 sisältää salaustekniikan turvallisuuden tueksi keskeisiä dokumentoituja salauksenhallintakäytäntöjä.

6.14.4 sisältää kaiken Asiakkaan henkilötietojen salauksen kannettavissa tietokoneissa tai kannettavissa laitteissa.

6.15 Kirjausvaatimukset. Iron Mountain on varmistettava seuraavat asiat:

6.15.1 Merkittävät turvallisuus- ja järjestelmätapahtumat kirjataan ja tarkastetaan.

6.15.2 Tarkastuslokeja säilytetään vähintään vuoden ajan järjestelmissä, jotka sijaitsevat Iron Mountainin isännöimässä ympäristössä (ympäristöissä), jota Iron Mountain käyttää Palvelujen tarjoamiseen;

6.15.3 Järjestelmän tarkastuslokit tarkistetaan poikkeamien varalta; ja

6.15.4 Lokien tilat ja järjestelmätiedot suojataan kohtuullisesti peukaloinnilta ja luvattomalta käytöltä.

6.16 Verkon ajan synkronointi. Iron Mountain synkronoi kaikkien tiedonkäsittelyjärjestelmien järjestelmäkellot käyttäen yhteistä virallista aikalähdettä.

6.17 Verkkojen erottelu. Iron Mountain on erotettava asianmukaisesti asiaankuuluvat tietopalvelut, käyttäjät ja verkkojen tietojärjestelmät.

7. PÄÄSYN HALLINTA

7.1 Pääsynhallinnan käytäntö. Iron Mountain ylläpitää pääsynhallinnan käytäntöjä sellaisten tiedonkäsittelyresurssien suhteen, jotka Iron Mountain virallisesti hyväksyy, julkaisee ja ottaa käyttöön.

7.2 Loogisen pääsyn hyväksyntä. Iron Mountainilla on oltava hyväksyntäprosessi, joka koskee loogisen pääsyn pyyntöjä Asiakkaan henkilötietoihin sekä pyyntöjä päästä Palveluja varten tarkoitettuihin Iron Mountainin järjestelmiin.

7.3 Pääsynhallinta ja -valvonta. Iron Mountain myöntää pääsyn Asiakkaan henkilötietoihin vain aktiivisille Iron Mountainin työntekijöille, mukaan lukien tilapäiset ja sopimustyöntekijät, ja aktiivisille käyttäjätileille, jotka tarvitsevat tällaista pääsyä suoriutuakseen työtehtävistään. Kaikki etuoikeutettu pääsy ja käyttö on tarkastettava ja vahvistettava olevan tämänhetkisen työtehtävän mukaista ja dokumentoitava vähintään neljännesvuosittain.

7.4 Kolmannen osapuolen pääsyn hallinta. Ennen pääsyn myöntämistä ulkopuolisille tahoille Iron Mountainin tietojärjestelmiin, jotka käyttävät Asiakkaan henkilötietoja, Iron Mountainin on varmistettava, että asianmukaiset valvontakeinot ovat käytössä.

7.5 Järjestelmän kulunvalvonta. Iron Mountain hallitsee pääsyä käyttöjärjestelmiin (sekä ohjelmisto- että laitteistopohjaisiin käyttöjärjestelmiin) vaatimalla turvallisen kirjautumisprosessin, jossa tunnistetaan käyttöjärjestelmää käyttävä henkilö.

7.6 Mobiilitietokonelaitteet. Iron Mountain -yhtiöllä on käytäntö tai menettely, joka on suunniteltu suojaamaan Iron Mountain -yhtiön mobiililaitteita luvattomalta käytöltä. Tällaisten käytäntöjen tai menettelytapojen täytyy käsitellä fyysistä suojausta, kulunvalvontaa ja turvavalvontaa, kuten salausta, virustorjuntaa ja laitteiden varmuuskopiointia.

7.7 Asiakasjärjestelmien eristäminen. Iron Mountainin täytyy, Palvelujen tarjoamiseen käyttämissään ja isännöimissään ympäristöissä, erottaa loogisesti Asiakkaan henkilötiedot kaikesta muusta tiedosta.

7.8 Tilit. Iron Mountainin täytyy suorittaa seuraavat asiat tilien osalta:

7.8.1 Vaatia henkilöllisyyden todentamista kultakin Iron Mountainin työntekijältä, joka yrittää saada pääsyn Asiakkaan henkilötietoja käsitteleviin Iron Mountainin järjestelmiin ja kieltää käyttämästä jaettuja käyttäjätilejä tai yleisillä kirjautumistunnuksilla (esim. ID:t) varustettuja käyttäjätilejä ja pääsemästä käsiksi Asiakkaan henkilötietoihin tai järjestelmiin.

7.8.2 Edellyttää, että kaikki käyttäjätilien tunnukset, mukaan lukien etuoikeutetut tilit, on sidottu suoraan henkilöön (ei asemaan työpaikalla).

7.8.3 Jos järjestelmänvalvojan oletustilejä ei poisteta käytöstä tai poisteta, järjestelmänvalvojan oletustilin käyttö edellyttää väliaikaisten salasanojen, poistumistunnuksien tai vastaavien valvontatoimien käyttöä.

7.8.4 Edellyttää, että passiiviset tavalliset tilit lukitaan tai poistetaan käytöstä 90 päivän käyttämättömyyden jälkeen.

7.8.5 Kieltää pääsy tilille useiden epäonnistuneiden pääsy-yritysten jälkeen.

7.8.6 Vaatia yksilöllisiä tunnisteita ja vahvoja salasanoja, jotka täyttävät vähintään seuraavat vaatimukset: vähintään 8 merkkiä; salasana vaihdettava 90 päivän välein; ja salasanalle on oltava vaatimuksia monimutkaisuudesta.

7.8.7 Kieltää työntekijöitä jakamasta salasanoja tai kirjoittamasta niitä muistiin.

7.9 Valvomattomien järjestelmien hallinta- ja valvontakeinot. Iron Mountainin on käytettävä salasanalla suojattua näytönsäästäjää kaikissa järjestelmissä, jotka on jätetty ilman valvontaa ja joita ei ole käytetty 30 minuuttiin.

8. TIETOJÄRJESTELMIEN HANKINNAN KEHITYS JA YLLÄPITO

8.1 Järjestelmän kehityksen turvallisuus. Iron Mountainin täytyy varmistaa, että turvallisuus on osa kaikkea tietojärjestelmien kehittämistä ja toimintaa, ja sen on julkaistava ja noudatettava sisäisiä suojattuja koodausmenetelmiä, jotka perustuvat sovelluskehityksen turvastandardeihin.

8.2 Ohjelmiston turvallisuuden hallinta. Iron Mountainin tietojärjestelmät (mukaan lukien käyttöjärjestelmät, infrastruktuuri, liiketoiminnan sovellukset, palvelut ja käyttäjien kehittämät sovellukset) on suunniteltava tietoturvastandardien mukaisiksi.

8.3 Verkkokaaviot. Iron Mountainin on kehitettävä, dokumentoitava ja ylläpidettävä verkkolaitteiden ja liikenteen fyysisiä ja loogisia kaavioita.

8.4 Haavoittuvuusarvioinnit / Riskianalyysit / Eettinen hakkerointi Iron Mountain suorittaa vähintään vuosittain haavoittuvuusarviointeja sovelluksille, joita käytetään Asiakkaan henkilötietoja käsittelevien Palvelujen tarjoamiseen Iron Mountainin isännöimässä ympäristöissä. Yksityiskohtaiset tulokset ovat Iron Mountainin luottamuksellisia ja omistusoikeudellisia tietoja, eikä niitä saa antaa kenellekään.

8.5 Muutosten testaus ja arviointi. Iron Mountain arvioi, tarkistaa ja testaa sovellusten ja käyttöjärjestelmien muutokset ennen käyttöönottoa varmistaakseen, ettei niillä ole haitallisia vaikutuksia Asiakkaan henkilötietoihin tai järjestelmiin.

9. Katastrofeista palautuminen

Iron Mountainin on ylläpidettävä suunnitelmaa katastrofeista palautumista varten, mukaan lukien varmuuskopiointi tukemaan Palveluja järjestelmien ja sähköisen tiedon varmuuskopiointikeskukseen. Järjestelmien ja sähköisten tietojen varmuuskopiointi ei sisällä Asiakkaan henkilötietoja, joita säilytetään fyysisesti Iron Mountainin toimitiloissa. Iron Mountain ylläpitää liiketoiminnan jatkuvuussuunnitelmaa voidakseen palauttaa kriittiset liiketoiminnan toiminnot. Iron Mountain suorittaa katastrofista palautumisen testauksen vähintään kahdentoista (12) kuukauden välein.

10. ULKOISET TARKASTUKSET JA ARVIOINNIT

Iron Mountainin turvallisuusprotokollat on suunniteltu vastaamaan alan standardeja. Iron Mountain toimittaa Asiakkaalle kaikki kolmannen osapuolen riippumattomat tarkastusraportit, jotka se on tilannut (esim. PCI, ISO27001, SOC2 jne.), ja jotka ovat merkityksellisiä alueella, jolla kyseiset Palvelut tarjotaan (”Tarkastusraportti”). Iron Mountain toimittaa kaikki tällaiset tilatut raportit tarkoituksenaan olla asiakaslähtöinen raportin tuloksista riippumatta. Iron Mountainin ei tarvitse antaa sisäisiä tarkastustuloksia tai tuloksia muista riippumattomista arvioinneista, jotka on tarkoitettu vain Iron Mountainille ja joita pidetään luottamuksellisina. Asiakkaalle ja sen ulkoisille tarkastajille toimitetaan pyynnöstä kopiot tarkastusraportista. Kaikki tämän osion vaatimilla testeillä tai tarkastuksilla luodut Tarkastusraportit tai muut tulokset katsotaan Iron Mountainin Luottamuksellisiksi tiedoiksi. Asiakkaalla on oikeus toimittaa kopio tällaisesta Tarkastusraportista mille tahansa soveltuvalle Asiakkaan asiakkaalle tai sääntelyviranomaiselle, tässä Asiakirjassa esitettyjen luottamuksellisten ehtojen mukaisesti. Asiakkaan pyynnöstä Iron Mountain vahvistaa kirjallisesti, että kyseisissa käytännöissä, menettelytavoissa ja sisäisissä valvontamekanismeissa ei ole tapahtunut muutoksia tällaisen Tarkastusraportin valmistumisen jälkeen, eikä vahvistuksen antaminen saa kestää yli kolmea kuukautta Tarkastusraportin raportointijakson jälkeen.

LIITE 3

Kansainväliset tiedonsiirrot

1. MÄÄRITELMÄT

”**Vuoden 2021 EU:n Mallisopimuslausekkeet** ” tarkoittavat Mallisopimuslausekkeita, jotka koskevat Henkilötietojen siirtämistä kolmansiin maihin GDPR:n mukaisesti, ja jotka Euroopan komissio on hyväksynyt Komission täytäntöönpanopäätöksen (EU) 2021/914 mukaisesti, ja jotka ovat saatavilla tästä[3] .

”**Vuoden 2022 Yhdistyneen kuningaskunnan liite**” tarkoittaa Yhdistyneen kuningaskunnan Tietosuojavaltuutetun toimiston julkaisemaa ja parlamentissa 2. helmikuuta 2018 annetun Tietosuojalain s119A:n mukaisesti laadittua liitettä B.1.0, jota voidaan muuttaa Kohdan 18 mukaisesti, joka on saatavilla tästä[4] .

”**EU:n Asiakkaiden henkilötiedot**” tarkoittavat sellaisten Asiakkaiden henkilötietojen Käsittelyä, joihin Euroopan unionin tai Euroopan unionin tai Euroopan talousalueen jäsenvaltion Tietosuojalakeja oli sovellettu, ennen kuin Iron Mountain käsitteli niitä.

”**Suojattu alue**” tarkoittaa:

i. EU:n Asiakkaiden henkilötietojen osalta: Euroopan unionin ja Euroopan talousalueen jäsenvaltioita sekä maita, alueita, toimialoja tai kansainvälisiä järjestöjä, joiden Tietosuojan riittävyyden osalta on voimassa päätös GDPR-asetuksen 45. Artiklan nojalla.

ii. Yhdistyneen kuningaskunnan Asiakkaiden henkilötietojen osalta: Yhdistynyttä kuningaskuntaa ja mitä tahansa maata, aluetta, alaa tai kansainvälistä järjestöä, jonka osalta on voimassa Yhdistyneen kuningaskunnan riittävyyttä koskevien määräysten mukaista riittävyyttä koskeva päätöstä,

iii. Sveitsin Asiakkaiden henkilötietojen osalta: mitä tahansa maata, aluetta, sektoria tai kansainvälistä järjestöä, joka on Sveitsin lainsäädännön mukaan riittävä;

iv. Kun kyseessä ovat muut Asiakkaan henkilötiedot, jotka on siirretty sellaiselta lainkäyttöalueelta, joka tarjoaa samanlaisen suojan kuin EU, Yhdistynyt kuningaskunta tai Sveitsi, mitä tahansa maata, aluetta, sektoria tai kansainvälistä järjestöä, joka on tunnustettu riittäväksi tällaisen lainkäyttöalueen lakien mukaan;

”**Mallisopimuslausekkeilla**” (Standard Contractual Clauses) tarkoitetaan yhdessä sekä vuoden 2021 EU:n Mallisopimuslausekkeita, että vuoden 2022 Yhdistynyttä kuningaskuntaa koskevaa Liitettä (2022 UK Addendum).

”Sveitsin Asiakkaan henkilötiedot” (Swiss Customer Personal Data) tarkoittaa sellaisten Asiakkaan henkilötietojen Käsittelyä, joihin oli sovellettu Sveitsin Tietosuojalakeja, ennen kuin Iron Mountain käsitteli niitä.

”**Yhdistyneen kuningaskunnan Asiakkaan henkilötiedot**” tarkoittavat sellaisten Asiakkaan henkilötietojen Käsittelyä, joihin sovellettiin Yhdistyneen kuningaskunnan Tietosuojalakeja, ennen kuin Iron Mountain käsitteli niitä.

2. SEKALAISTA

2.1 Tämä liite 3 sisältää seuraavat osat: (i) osa A – EU:n Asiakkaiden henkilötietojen siirrot; (ii) osa B – Sveitsin Asiakkaiden henkilötietojen siirrot; (iii) osa C – Yhdistyneen kuningaskunnan Asiakkaiden henkilötietojen siirrot, joita sovelletaan asiaankuuluvina Iron Mountainin Palveluihin liittyvissä Asiakkaan henkilötietojen siirrossa.

2.2 Mallisopimuslausekkeet koskevat Iron Mountainia ja sen tytäryhtiöitä ”tietojen tuojina” ja Asiakasta ja sen tytäryhtiöitä ”tietojen viejinä”.

2.3 Sopimuksen allekirjoitus ja päiväys muodostavat kaikki Mallisopimuslausekkeiden edellyttämät allekirjoitukset ja päivämäärät.

2.4 Jos osapuolet siirtävät EU:n, Yhdistyneen kuningaskunnan tai Sveitsin Asiakkaiden henkilötietoja suojatun alueen ulkopuolella ja asiaankuuluva Euroopan komission päätös tai muu voimassa oleva riittävyysmenetelmä soveltuvan Tietosuojalainsäädännön mukaisesti, johon Iron Mountain on nojautunut tietojen siirrossa, on katsottu olevan pätemätön, tai jos valvontaviranomainen edellyttää tällaisen päätöksen nojalla tehtävien Henkilötietojen siirtojen keskeyttämistä, osapuolet ovat yhteistyössä ja mahdollistavat vaihtoehtoisen siirtomekanismin käytön. Osapuolet sopivat myös, että tämän Liitteen 3 kansainvälisten siirtojen helpottamiseksi käytetyt asianmukaiset suojatoimet eivät ole poissulkevia, ja että osapuolet voivat käyttää muita siirtomekanismeja, kuten EU:n ja Yhdysvaltojen välistä Tietosuojakehystä (EU-U.S. Data Privacy Framework).

OSA A – EU:N ASIAKKAIDEN HENKILÖTIETOJEN SIIRROT

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

Jos ja siltä osin kuin Asiakas tai sen konserni- tai kumppanuus yhtiöt siirtävät EU:n Asiakkaan henkilötietoja suojatun alueen ulkopuolelle Iron Mountainille tai sen tytäryhtiöille Sopimuksen mukaisten Iron Mountainin Palvelujen yhteydessä, sovelletaan tätä Liitteen 3 osaa A ja Osapuolet sopivat seuraavasti:

1. **Mallisopimuslausekkeiden valinnat.** Vuoden 2021 EU:n Mallisopimuslausekkeiden MODUULIN KAKSI tekstiä sovelletaan, kun Asiakas tai jokin sen tytäryhtiöistä on Rekisterinpitäjä ja Iron Mountain tai jokin sen tytäryhtiöistä on Henkilötietojen käsittelijä; vuoden 2021 EU:n Mallisopimuslausekkeiden MODUULIN KOLME tekstiä sovelletaan, kun Asiakas tai jokin sen tytäryhtiöistä on Henkilötietojen käsittelijä, ja Iron Mountain tai jokin sen tytäryhtiöistä on Alikäsittelijä. Vuoden 2021 EU:n Mallisopimuslausekkeiden sisältämät asiaankuuluvat määräykset sisällytetään viittauksella tähän Tietosuojasopimukseen, ja ne ovat olennainen osa tätä Tietosuojasopimusta. Muita EU:n Mallisopimuslausekkeissa valinnaisiksi merkittyjä moduuleja tai Lausekkeita ei sovelleta. Vuoden 2021 EU:n Mallisopimuslausekkeiden liitteiden tarkoituksia varten tarvittavat tiedot on esitetty TKS:n liitteessä 1 (Luettelo alihankkijoina toimivista käsittelijöistä), liitteessä 2 (Käsittelyn/siirron kuvaus) sekä Lausekkeessa 6.2 (Tekniset ja organisatoriset toimenpiteet).

2. **Alikäsittelijöiden käyttö.**Vuoden 2021 EU:n Mallisopimuslausekkeiden 9 Lausekkeessa sovelletaan Alikäsittelijöiden käyttöön liittyvää vaihtoehtoa 2 (Yleinen kirjallinen lupa) Palvelujen suorittamisen osalta. Asiakas tiedostaa ja hyväksyy sen, että Iron Mountain voi palkata uusia Alikäsittelijöinä toimivia käsittelijöitä tämän TKS:n Lausekkeessa 6 sovitun mekanismin kautta, ja että alikäsittelijöinä toimiville käsittelijöille lähetettyjen muutospyyntöjen toimittamisen määräaika on viisitoista (15) päivää.

3. **Soveltuva laki ja oikeuspaikan valinta.** Vuoden 2021 EU:n Mallisopimuslausekkeiden 17 Lausekkeen (Soveltuva laki) soveltamisen osalta sovelletaan vaihtoehtoa 2, ja näihin Lausekkeisiin sovelletaan sen EU:n jäsenvaltion lakia, johon tietojen viejä sijaitsee, siinä määrin kuin se sallii oikeuksia kolmannen osapuolen edunsaajalle. Vuoden 2021 EU:n Mallisopimuslausekkeiden 18 Lausekkeen (Oikeuspaikan ja Lainkäyttöalueen valinta) soveltamisen osalta nämä ovat sen EU:n jäsenvaltion tuomioistuimet, joissa tietojen viejä sijaitsee.

4. **Todistus poistamisesta.** Vuoden 2021 EU:n Mallisopimuslausekkeiden Lausekkeiden 8.5 ja 16(d) soveltamisen osalta Iron Mountain toimittaa Asiakkaalle todistuksen Henkilötietojen poistamisesta vain Asiakkaan kirjallisesta pyynnöstä.

5. **Henkilötietojen Tietoturvaloukkaukset.** Vuoden 2021 EU:n Mallisopimuslausekkeiden Lausekkeessa 8.6(c) Henkilötietojen Tietoturvaloukkauksia käsitellään Tietosuojasopimuksen Lausekkeessa 7 sovitun mekanismin mukaisesti.

6. **Tarkastukset.** Vuoden 2021 EU:n Mallisopimuslausekkeiden Lausekkeessa 8.9 mainitut tarkastukset suoritetaan Sopimuksessa sovitun tarkastusmekanismin mukaisesti.

7. **Valitukset.** Vuoden 2021 EU:n Mallisopimuslausekkeiden 11 Lausekkeen soveltamiseksi Iron Mountain ilmoittaa Asiakkaalle, jos se vastaanottaa Rekisteröidyltä EU:n Asiakkaan henkilötietoja koskevan valituksen, ja ilmoittaa valituksesta Asiakkaalle Sopimuksessa sovitun mekanismin mukaisesti.

8. **Valvontaviranomainen.** Vuoden 2022 EU:n Mallisopimuslausekkeiden osalta toimivaltainen valvontaviranomainen määrätään EU:n Mallisopimuslausekkeiden Lausekkeen 13 mukaisesti.

OSA B – SVEITSIN ASIAKKAIDEN HENKILÖTIETOJEN SIIRROT

Jos ja siltä osin kuin Asiakas tai sen konserni- tai kumppanuus yhtiöt siirtävät Sveitsin Asiakkaan henkilötietoja suojatun alueen ulkopuolelle Iron Mountainille tai sen tytäryhtiöille Sopimuksen mukaisten Iron Mountainin Palvelujen yhteydessä, sovelletaan tätä Liitteen 3 osaa B ja Osapuolet sopivat seuraavasti:

1. **Mallisopimuslausekkeiden valinnat.** Vuoden 2021 EU:n Mallisopimuslausekkeita ja osan A mukaisia asiaankuuluvia määräyksiä sovelletaan, kun Asiakas tai sen Tytäryhtiö on Rekisterinpitäjä, ja Iron Mountain tai sen Kumppanuustyhtiö on Henkilötietojen käsittelijä ja/tai Asiakas tai sen Tytäryhtiö on Henkilötietojen käsittelijä, ja Iron Mountain tai sen Kumppanuustyhtiö on Alikäsittelijä, paitsi että:

   a. EU:n Mallisopimuslausekkeiden 13 Lausekkeen mukainen toimivaltainen valvontaviranomainen on Sveitsin liittovaltion Tietosuoja- ja tietokomissio (Swiss Federal Data Protection and Information Commission).

   b. vuoden 2021 EU:n Mallisopimuslausekkeiden Lausekkeen 17 mukaista Sopimusvaadetta koskeva soveltuva laki on Sveitsin laki ja Lausekkeen 18 kohdan (b) mukaisten osapuolten välisten toimien toimivaltainen paikka on Sveitsin tuomioistuimissa.

2. Viittaukset EU:n GDPR:ään vuoden 2021 EU:n Mallisopimuslausekkeissa tulkitaan viittauksina FADP:hen.

3. Vuoden 2021 EU:n Mallisopimuslausekkeiden termiä ”jäsenvaltio” ei tulkita siten, että Sveitsissä olevat Rekisteröidyt eivät voisi haastaa oikeuteen asuinpaikassaan (Sveitsi) vuoden 2021 EU:n Mallisopimuslausekkeiden kohdan 18 (c) mukaisesti.

OSA C – YHDISTYNEEN KUNINGASKUNNAN ASIAKKAIDEN HENKILÖTIETOJEN SIIRROT

Jos ja siltä osin kuin Asiakas tai sen konserni- tai kumppanuus yhtiöt siirtävät Yhdistyneen kuningaskunnan Asiakkaan henkilötietoja suojatun alueen ulkopuolelle Iron Mountainille tai sen Tytäryhtiöille Sopimuksen mukaisten Iron Mountainin Palvelujen yhteydessä, sovelletaan tätä Liitteen 3 osaa C ja Osapuolet sopivat seuraavasti:

1. **Mallisopimuslausekkeiden valinnat.** Vuoden 2021 EU:n Mallisopimuslausekkeita, osan A mukaisia asiaankuuluvia määräyksiä ja vuoden 2022 Yhdistyneen kuningaskunnan liitettä sovelletaan, kun Asiakas tai sen Kumppanuustyhtiö on Rekisterinpitäjä, ja Iron Mountain tai sen Kumppanuustyhtiö on Henkilötietojen käsittelijä ja/tai Asiakas tai sen Kumppanuustyhtiö on Henkilötietojen käsittelijä, ja Iron Mountain tai sen Kumppanuustyhtiö on Alikäsittelijä.

2. **Osa 1: Vuoden 2022 Yhdistyneen kansakunnan lisäyksen taulukot 1–3:**Osapuolia koskevat tiedot - Taulukko 1; Valitut Mallisopimuslausekkeet, Moduulit ja Valitut Lausekkeet sekä Liitteen tiedot, mukaan lukien Liite 1A: Osapuolten luettelo, Liite 1B: Siirron kuvaus ja Liite 1C: Tekniset ja organisatoriset toimenpiteet tietojen turvallisuuden varmistamiseksi – Taulukko 3, katsotaan suoritetuiksi viittauksella tähän liitteeseen 3, mukaan lukien Yhdistyneen kuningaskunnan Liitteen osan A Taulukko 4: Asiakas ja Iron Mountain tiedostavat, kuittaavat ja hyväksyvät, että kumpikin osapuoli voi irtisanoa Yhdistyneen kuningaskunnan Liitteen.

3. **Osa 2:** Yhdistyneen kuningaskunnan Liitteen Pakolliset lausekkeet: Asiakas ja Iron Mountain tiedostavat, kuittaavat ja hyväksyvät Yhdistyneen kuningaskunnan lisäyksen Pakolliset lausekkeet.

4. **Valvontaviranomainen.** Toimivaltaisena valvontaviranomaisena toimii Yhdistyneen kuningaskunnan Tietosuojavaltuutetun toimisto.

OSA D – MUIDEN ASIAKKAIDEN HENKILÖTIETOJEN SIIRROT

Jos ja siltä osin kuin asiakas tai sen tytäryhtiöt siirtävät Asiakkaan henkilötietoja, joita ei ole käsitelty OSISSA A-C, Iron Mountainille tai sen tytäryhtiöille Sopimuksen mukaisten Iron Mountainin Palvelujen yhteydessä, Liitteen 3 osaa A sovelletaan soveltuvan Tietosuojalainsäädännön mukaisessa laajuudessa. Muussa tapauksessa, mikäli Tietosuojalainsäädännön mukaisia korvaavia tai ylimääräisiä asianmukaisia suojatoimia tai siirtomekanismeja vaaditaan Asiakkaan henkilötietojen siirtämiseksi maahan, joka ei tarjoa riittävää Henkilötietojen suojaustasoa tietojen viejän näkökulmasta, osapuolet sitoutuvat ottamaan ne käyttöön niin pian kuin käytännössä on mahdollista ja dokumentoimaan tällaiset vaatimukset ja asettamaan ne liitteeksi tähän Tietosuojasopimukseen.

LIITE 4

HIPAA – Liikekumppanin Sopimus (”LKS”)(Business Associate Agreement)

Tämä LKS täydentää ja muuttaa kaikkia nykyisiä ja tulevia Iron Mountainin ja sen tytäryhtiöiden ja Asiakkaan ja sen tytäryhtiöiden välisiä Sopimuksia, joiden alaisuudessa Iron Mountain tai sen tytäryhtiöt tarjoavat tiettyjä Palveluja Asiakkaalle tai sen tytäryhtiöille, ja jotka Palvelut edellyttävät Liikekumppanin Käyttävän ja/tai Luovuttavan suojattuja terveystietoja Soveltamisalan tahon (Covered Entity) puolesta. Lukuun ottamatta tässä BAA-sopimuksessa esitettyjä muutoksia, kaikki Sopimuksessa esitetyt ehdot pysyvät täysin voimassa ja koskevat Iron Mountainin Asiakkaalle tarjoamia Palveluja.

Iron Mountain ja Asiakas solmivat tämän BAA-sopimuksen, jotta molemmat osapuolet voivat täyttää velvollisuutensa, jotka tulevat voimaan ja sitovat osapuolia HIPAA:n Tietosuojaa, tietoturvaa ja Tietoturvaloukkauksista ilmoittamista koskevien sääntöjen sekä mahdollisten täytäntöönpanosäännösten mukaisesti, mukaan lukien ne, jotka on pantu täytäntöön osana Omnibus-sääntöä (jäljempänä yhdessä "HIPAA-säännöt"), jonka mukaan Asiakas ja sen tytäryhtiöt ovat "soveltamisalaan kuuluvia tahoja" (Covered Entity) tai "Liikekumppaneita" ja Iron Mountain ja sen tytäryhtiöt Asiakkaan "Liikekumppaneita". Tässä Sopimuksessa kaikki jäljempänä olevat liikekumppaniin liittyvät viittaukset katsotaan viittauksiksi Iron Mountainiin tai sen soveltuvaan tytäryhtiöön.

1. MÄÄRITELMÄT

Tässä LKS:ssä käytetyillä isoilla ja pienillä alkukirjaimilla kirjoitetuilla termeillä, joita ei ole muutoin määritelty tässä LKS:ssä, on sama merkitys kuin HIPAA-säännöissä tai Sopimuksessa, soveltuvin osin.

”**Rikkomusilmoitussääntö**” tarkoittaa CFR-säädöksen 45 §164 Alakohdan D mukaista sääntöä Suojaamattomien suojattujen terveystietojen rikkomusilmoituksesta (Breach Notification for Unsecured Protected Health Information).

”**Liikekumppani**” tarkoittaa edellä mainittua Liikekumppania siltä osin kuin se vastaanottaa, ylläpitää tai lähettää Suojattuja terveystietoja toimittaessaan Palveluja Asiakkaille.

”**HIPAA**” tarkoittaa vuoden 1996 Sairasvakuutuksen siirtämistä ja vastuuta koskevaa lakia (Health Insurance Portability and Accountability Act).

”**HITECH**” tarkoittaa Taloudellista ja kliinistä terveyttä varten käytettävää terveystietoteknologiaa koskevan lain (Health Information Technology for Economic and Clinical Health Act) soveltuvia säännöksiä, jotka on sisällytetty Yhdysvaltain palautumis- ja uudelleensijoituslakiin (American Recovery and Reinvestment Act) vuonna 2009, mukaan lukien kaikki täytäntöönpanosäännökset.

”**Tietosuojasääntö**” tarkoittaa CFR-säädöksen 45 §160- ja §164 -kohtien A- ja E-alakohtien yksilötunnistetietojen Tietosuojastandardeja.

Termillä ”**Suojatut terveystiedot**” eli ”**STT**” on sama merkitys kuin termillä ”Protected Health Information” (suojatut terveystiedot) laissa CFR-säädöksen 45 §160.103, ja ne rajoittuvat liikekumppanin Asiakkaan puolesta luomaan tai Asiakkaalta tai Asiakkaan puolesta Sopimuksen mukaisesti saatuihin suojattuihin terveystietoihin.

”**Turvallisuussääntö**” tarkoittaa säädöksen CFR-säädöksen 45 §160 ja §164 A ja C Alakohtien mukaisia turvallisuusstandardeja, jotka koskevat sähköisten suojattujen terveystietojen suojaamista.

2. LIIKEKUMPPANIN VELVOLLISUUDET JA TOIMINTA

2.1. Liikekumppani sitoutuu olemaan käyttämättä tai luovuttamatta suojattuja terveystietoja muuten kuin tämän LKS:n sallimalla tai vaatimalla tavalla tai lain vaatimalla tavalla.

2.2. Liiketoiminnan yhteistyökumppani sitoutuu käyttämään asianmukaisia suojatoimia ja noudattamaan soveltuvin osin CFR-säädöksen 45 § 164 C alaluvun säännöksiä sähköisten suojattujen terveystietojen osalta estääkseen suojattujen terveystietojen käytön tai luovuttamisen muulla tavoin kuin tässä BAA-sopimuksessa tai Sopimuksessa edellytetyllä tavalla. Osapuolet kuitenkin tunnustavat ja sopivat, että on Asiakkaan eikä Liikekumppanin vastuulla noudattaa CFR-säädöksen 45 §164.312:n vaatimuksia, jotka koskevat sähköisten suojattujen terveystietojen Asiakkaan liikekumppanin luona fyysisillä tietovälineillä (esimerkiksi nauhoilla) säilyttämien salaus- tai purkumekanismien käyttöönottoa.

2.3. Liikekumppani sitoutuu raportoimaan Asiakkaalle viipymättä kaikista turvallisuusongelmista, Tietoturvaloukkauksista tai muusta suojattujen terveystietojen käytöstä-, paljastamisesta tai luovuttamisesta, josta se saa tietää, ja jota tämä LKS tai Sopimus ei salli tai vaadi. Rikkomuksen sattuessa ilmoitus on tehtävä HIPAA-sääntöjen mukaisesti ja liikekumppanin vaatimusten mukaisesti, mukaan lukien rajoittumatta CFR-säädöksen 45 §164.410 mukaisesti, mutta ei missään tapauksessa yli kolme (3) arkipäivää sen jälkeen, kun liikekumppani on suorittanut sisäisen tutkintansa ja vahvistanut rikkomuksen tapahtuneen. Liikekumppani avustaa ja tekee kohtuullista yhteistyötä tällaisen Rikkomuksen tutkinnassa ja dokumentoi vaarantuneet nimenomaiset Tallenteet, kaikkien sellaisten luvattomien kolmansien osapuolten henkilöllisyyden, jotka ovat saattaneet käyttää tai vastaanottaa

Suojattuja terveystietoja, jos tiedossa, sekä kaikki toimenpiteet, joihin Liikekumppani on ryhtynyt tällaisen rikkomuksen vaikutusten lieventämiseksi.

2.4. Liikekumppanin on soveltuvin osin varmistettava CFR-säädöksen 45 §164.502(e)(1)(ii)- ja §164.308(b)(2) -säädösten mukaisesti, että liikekumppani, joka luo, vastaanottaa, ylläpitää tai lähettää Suojattuja terveystietoja Liikekumppanin puolesta avustaakseen Palvelujen tarjoamisessa Sopimuksen mukaisesti, hyväksyy samat rajoitukset, ehdot ja vaatimukset, joita sovelletaan Liikekumppaniin kyseisten Suojattuihin terveystietojen kanssa tämän LKS:n kautta.

2.5. Jos liikekumppani on säilyttänyt joidenkin henkilöiden Suojattuja terveystietoja Nimetyssä tietojoukossa, ja jos Asiakas niin pyytää, Liikekumppani suostuu antamaan pääsyn kyseisiin Suojattuihin terveystietoihin Asiakkaalle noutamalla ja toimittamalla kyseiset Suojatut terveystiedot Sopimusehtojen mukaisesti, jotta Asiakas voisi vastata henkilölle täyttääkseen CFR-säädöksen 45 §164.524 -vaatimukset.

2.6. Liikekumppani suostuu siihen, että jos Liikekumppanin hallussa olevassa Nimetyssä tietojoukossa on tehtävä muutos Suojattuihin terveystietoihin, ja jos Asiakas ohjeistaa Liikekumppania noutamaan kyseiset suojatut terveystiedot Sopimuksen mukaisesti, Liikekumppani suorittaa kyseisen Palvelun, jotta Asiakas voisi tehdä minkä tahansa muutoksen sellaisiin Suojattuihin terveystietoihin, joita joko Asiakas tai Henkilö voi vaatia CFR-säädöksen 45 §164.526 mukaisesti.

2.7. Liikekumppani sitoutuu dokumentoimaan ja asettamaan Asiakkaan saataville tiedot, joita vaaditaan Suojattujen terveystietojen paljastamista ja luovuttamista koskevan kirjanpidon laatimiseen, edellyttäen, että Asiakas on antanut Liikekumppanille riittävästi tietoja, jotta Liikekumppani voisi päättää, mitkä Liikekumppanin Asiakkaalta tai sen puolesta vastaanottamat Asiakirjat tai tiedot sisältävät Suojattuja terveystietoja. Tietojen luovuttamista koskevien Asiakirjojen tulee sisältää sellaisia tietoja, joita vaaditaan, jotta Asiakas voisi vastata yksityishenkilön pyyntöön, joka koskee Suojattujen terveystietojen paljastamista tai luovuttamista CFR-säädöksen 45 §164.528:n tai muiden HIPAA-sääntöjen määräysten mukaisesti.

2.8. Ellei Sopimuksessa nimenomaisesti toisin sovita, Liikekumppanin on viipymättä ilmoitettava Asiakkaalle kaikista yksityishenkilöiden esittämistä Suojattuihin terveystietoihin pääsyä tai niiden tuntemista tai korjaamista koskevista pyynnöistä vastaamatta tällaisiin pyyntöihin, ja Asiakas on vastuussa tällaisten Henkilöiden pyyntöjen vastaanottamisesta ja niihin vastaamisesta.

2.9. Siltä osin kuin liikekumppanin on täytettävä yksi tai useampi Asiakkaan CFR-säädöksen 45 §164 Alakohdan E mukainen velvoite (velvoitteet), liikekumppani noudattaa Alakohdan E vaatimuksia, jotka koskevat asiakasta kyseisen velvoitteen (velvoitteiden) suorittamisen osalta.

2.10. Liikekumppani sitoutuu antamaan sisäiset käytäntönsä, kirjanpitonsa ja tietueensa sihteerin (Secretary) saataville. jotta tämä ottaisi selvää HIPAA-sääntöjen noudattamisesta.

3. LIIKEKUMPPANIN SALLITTU KÄYTTÖ JA LUOVUTTAMINEN

3.1. Liikekumppani voi Käyttää tai Luovuttaa suojattuja terveystietoja tarpeen mukaan Sopimuksessa esitettyjen Palvelujen suorittamiseksi.

3.2. Liikekumppani voi käyttää tai Luovuttaa suojattuja terveystietoja lain vaatimalla tavalla.

3.3. Liiketoimintayhteistyökumppani sitoutuu tekemään kohtuullisia ponnisteluja rajoittaakseen Suojattujen terveystietojen Käytön, Luovuttamisen tai pyynnön aiotun tarkoituksen saavuttamisen vaatimaan välttämättömään vähimmäismäärään.

3.4. Liikekumppani ei saa Käyttää tai Luovuttaa Suojattuja terveystietoja tavalla, joka rikkoisi CFR-säädöksen 45 §164 Alakohtaa E, jos asiakas tekee niin.

3.5. Liikekumppani voi luovuttaa Suojattuja terveystietoja Liiketoimintakumppanin asianmukaista johtamista ja hallintoa varten tai Liikekumppaniin lakisääteisten velvollisuuksien täyttämiseksi edellyttäen, että laki edellyttää tietojen luovuttamista tai että Liikekumppani saa kohtuulliset takeet henkilöltä, jolle tiedot luovutetaan, siitä, että tiedot pysyvät luottamuksellisina ja että niitä käytetään tai luovutetaan edelleen vain lain edellyttämällä tavalla tai niihin tarkoituksiin, joita varten ne luovutettiin henkilölle, ja että henkilö ilmoittaa Liikekumppanille tietoonsa tulleista tapauksista, joissa tietojen luottamuksellisuutta on rikottu.

4. ASIAKKAAN VELVOLLISUUDET

4.1. Asiakas ei saa määrätä liikekumppania toimimaan tavalla, joka ei olisi HIPAA-sääntöjen mukaista.

4.2. Asiakkaan on ilmoitettava Liikekumppanille kaikista rajoituksista ilmoituksessaan Asiakkaan Tietosuojakäytännöistä CFR-säädöksen 45 §164.520:n mukaisesti siltä osin kuin kyseinen rajoitus voi vaikuttaa Liikekumppanin suorittamaan Suojattujen terveystietojen Käyttöön tai Luovuttamiseen.

4.3. Asiakkaan on ilmoitettava Liikekumppanille kaikista muutoksista, jotka koskevat tai kumoavat Henkilön luvan Käyttää tai Luovuttaa Suojattuja terveystietojaan, siinä määrin kuin kyseiset muutokset voivat vaikuttaa Liikekumppanin suorittamaan Suojattujen terveystietojen käyttöön tai julkistamiseen.

4.4. Asiakkaan on ilmoitettava Liikekumppanille kirjallisesti kaikista Suojattujen terveystietojen käyttöä tai julkistamista koskevista rajoituksista, jotka Asiakas on hyväksynyt CFR-säädöksen 45 §164.522:n mukaisesti, siinä määrin kuin kyseinen rajoitus voi vaikuttaa Liikekumppanin Suojattujen terveystietojen Käyttöön tai Luovuttamiseen.

5. VOIMASSAOLOAIKA JA IRTISANOMINEN

5.1. Tämän LKS-sopimuksen voimassaoloaika alkaa voimaantulopäivästä ja päättyy automaattisesti, kun (i) Sopimus päättyy tai (ii) kaikki Asiakkaan Liikekumppanille toimittamat Suojatut terveystiedot hävitetään tai palautetaan Asiakkaalle.

5.2. Kun toinen osapuoli tietää, että toinen osapuoli on olennaisesti rikkonut LKS:ää, rikkomaton osapuoli antaa rikkomuksen tehneelle osapuolelle mahdollisuuden korjata rikkomuksen. Jos rikkova osapuoli ei korjaa rikkomusta kolmenkymmenen (30) päivän kuluessa siitä, kun rikkova osapuoli on saanut kirjallisen ilmoituksen rikkomattomalta osapuolelta, jossa ilmoitetaan kyseisen olennaisen rikkomuksen yksityiskohdat, rikkomattomalla osapuolella on oikeus irtisanoa tämä LKS ja Sopimus Sopimusehtojen mukaisesti, tai jos irtisanominen ei ole mahdollista, ilmoittaa ongelmasta Sihteerille tai muulle toimivaltaiselle viranomaiselle.

5.3. Irtisanomisen vaikutus:

5.3.1.1. Ellei jäljempänä kohdassa 5.3.2 toisin mainita, kun tämä LKS mistä tahansa syystä irtisanotaan, Liikekumppani palauttaa tai tuhoaa kaikki Asiakkaalta Sopimuksen mukaisesti saadut Suojatut terveystiedot. Tämä ehto koskee Suojattuja terveystietoja, jotka ovat Liikekumppanin Alihankkijoiden tai edustajien hallussa. Liikekumppani ei saa säilyttää mitään kopioita Suojatuista terveystiedoista (STT).

5.3.1.2. Jos Liikekumppani päättää, että suojattujen terveystietojen palauttaminen tai tuhoaminen ei ole mahdollista, Liikekumppani ilmoittaa Asiakkaalle ehdoista, jotka tekevät palauttamisesta tai tuhoamisesta mahdottoman. Ilmoitettuaan asiasta Asiakkaalle Liikekumppani laajentaa tämän LKS:n suojaa kyseisiin Suojattuihin terveystietoihin ja rajoittaa kyseisten Suojattujen terveystietojen Käytön ja Luovuttamisen niihin tarkoituksiin, jotka tekevät palauttamisen tai tuhoamisen mahdottomaksi, niin kauan kuin Liikekumppani ylläpitää/säilyttää kyseisiä Suojattuja terveystietoja Sopimusehtojen mukaisesti.

6. SEKALAISTA

6.1. Korvaukset. Liikekumppani sitoutuu korvaamaan Asiakkaalle kaikki sakot tai rangaistukset, jotka johtuvat Sihteerin aloittamasta täytäntöönpanomenettelystä tai osavaltion Syyttäjän nostamasta siviilikanteesta Asiakasta vastaan, ja jotka ovat suoraan ja yksinomaan seurausta Liikekumppanin toiminnasta tai laiminlyönnistä, joka on joko HIPAA-sääntöjen vastaista tai rikkoo merkittävästi tätä LKS:ää (”Vaade”). Liikekumppani ei ole velvollinen korvaamaan Asiakkaalle mitään osaa tällaisista sakoista tai rangaistuksista, jotka johtuvat (i) Asiakkaan HIPAA-sääntöjen tai tämän LKS:n rikkomisesta tai (ii) Asiakkaan huolimattomuudesta tai tahallisista toimista tai laiminlyönneistä. Edellä mainittu korvausvelvollisuus riippuu nimenomaisesti siitä, että Asiakas myöntää Liikekumppanille oikeuden Liikekumppanin valinnan ja kustannuksen perusteella ja oman valintansa perusteella asiamiehen/asniajajan kanssa valvoa tai osallistua tällaisen Vaateen puolustamiseen, kuitenkin sillä edellytyksellä, että sikäli kuin kyseinen Vaade on osa laajempaa menettelyä tai kannetta, Liikekumppanin oikeus hallita tai osallistua rajoittuu vain Vaateeseen eikä tällaista oikeutta ole kyseisen Vaateen laajempaan prosessiin tai kanteeseen. Siinä tapauksessa, että liikekumppani käyttää oikeuttaan puolustuksen hallintaan, (i) Liikekumppani ei sovittele mitään Vaadetta, joka edellyttää Asiakkaan taholta tapahtuneen virheen myöntämistä ilman sen etukäteen antamaa kirjallista suostumusta, (ii) Asiakkaalla on oikeus omalla kustannuksellaan osallistua Vaateeseen tai kanteeseen ja (iii) Asiakas tekee yhteistyötä liikekumppanin kohtuudella esitettyjen pyyntöjen myötä. Edellä mainittu on Asiakkaan ainoa ja yksinomainen oikeussuojakeino ja Liikekumppanin yksinomainen (korvaus)vastuu kaikista Asiakkaan menetyksistä, vahingoista, kuluista tai (korvaus)vastuista, jotka aiheutuvat tähän BAA-sopimukseen liittyvistä vaateista ja vaatimuksista.

6.2. Kieltomääräys. Liikekumppani tiedostaa, että Liikekumppanin suorittama Suojattujen terveystietojen luvaton Läyttö tai Luovuttaminen voi aiheuttaa Asiakkaalle korjaamatonta vahinkoa, johon Asiakkaalla on oikeus, jos se niin valitsee, hakea kieltomääräystä tai muuta oikeussuojakeinoa.

6.3. Sääntelyä koskevat viitteet. Tässä LKS:ssa oleva viittaus johonkin HIPAA-sääntöjen osioon tarkoittaa sitä, että sitä HIPAA:n kohta, Tietosuojasääntöä, Turvasääntöä, HITECH ACTia tai lopullisia Omnibus-sääntöjä sellaisina kuin ne ovat muutettuina ja voimassa, sovelletaan, ja että niiden noudattamista edellytetään.

6.4. Muutos. Osapuolet suostuvat neuvottelemaan hyvässä uskossa kaikista tähän LKS:ään tehdyistä muutoksista, joita saatetaan vaatia ajoittain, jotta Asiakas tai liikekumppani voisi noudattaa HIPAA-sääntöjen vaatimuksia. Jos osapuolet eivät pääse yhteisymmärrykseen tällaisen muutoksen ehdoista kuudenkymmenen (60) päivän kuluessa Asiakkaan esittämästä ja liikekumppanin vastaanottamasta kirjallisesta pyynnöstä, kummallakin osapuolella on oikeus irtisanoa tämä LKS ja Sopimus toimittamalla kirjallinen ilmoitus toiselle osapuolelle vähintään kolmekymmentä (30) päivää ennen varsinaista irtisanomista (30 päivän irtisanomisaika).

6.5. Ei kolmannen osapuolen edunsaajia. Minkään tässä LKS:ssä ilmaistun tai oletetun ei ole tarkoitus antaa kenellekään muulle henkilölle kuin Asiakkaalle, Liikekumppanille tai heidän seuraajilleen tai oikeudenhaltijoilleen mitään oikeuksia, oikeussuojakeinoja, velvoitteita tai vastuita.

6.6. Itsenäinen urakoitsija. Liikekumppani, mukaan lukien sen johtajat, toimihenkilöt, työntekijät ja edustajat, on itsenäinen urakoitsija eikä Asiakkaan tai sen työntekijän edustaja (Liittovaltion yleisen lain mukaisesti). Rajoittamatta edellä mainitun yleisluontoisuutta, Asiakkaalla ei ole oikeutta hallita, ohjata tai muuten vaikuttaa Liikekumppanin toimintaan Palvelujen suorittamisen yhteydessä muutoin kuin tämän LKS:n tai Sopimuksen täytäntöönpanon tai niihin tehtävän yhtäläisen muutoksen kautta.

6.7. Etusijajärjestys; koko Sopimus. Kaikki tämän LKS:n epäselvyydet ratkaistaan selvitetään siten, että osapuolet voivat noudattaa HIPAA-sääntöjä. Tämä LKS muodostaa osapuolten välisen Sopimuksen kokonaisuudessaan sen aiheeseen liittyen ja korvaa kaikki edelliset HIPAA-sääntöihin liittyvän viestinnän, esitykset, sopimukset ja yhteisymmärryksen, mukaan lukien kaikki aikaisemmat osapuolten väliset liikekumppanisopimukset.