Andmetöötlusleping

EESMÄRK JA ÜLIMUSLIKKUSE JÄRJEKORD

See Andmetöötlusleping, koos kõigi selle lisade ning igasuguste dokumentidega, millele on selles viidatud (ühiselt „**Andmetöötlusleping**“), on osa Iron Mountaini ja Kliendi vahelisest teenuselepingust („**Teenuseleping**“). Teenuselepingu sätted ja tingimused reguleerivad õigusi ja kohustusi, mis on pooltel vastavalt sellele Andmetöötluslepingule.

Kui mõni selle Andmetöötluslepingu sätetest ja tingimustest on vastuolus Teenuselepingu sätete ja tingimustega, on selle Andmetöötluslepingu sätted ja tingimused ülimuslikud selle suhtes, mis puudutavad selle Andmetöötluslepingu teemat. See Andmetöötlusleping alistab ja asendab kõik varasemad andmetöötluslepingud või isikuandmete kaitset või eraelu puutumatust käsitlevad lepingupunktid, mis reguleerivad poolte vahelist suhet seoses Teenuselepingu alusel osutatavate Teenustega.

ÜLDTINGIMUSED

1. MÄÄRATLUSED

Kui siin pole toodud just teisiti, on kõigil siin suurtähega mõistetel sama tähendus kui Teenuselepingus.

„**Vastutav töötleja**“ tähendab füüsilist või juriidilist isikut, avaliku sektori asutust, ametit või muud organit, kes üksi või koos teistega määrab kindlaks Isikuandmete Töötlemise eesmärgid ja vahendid.

„**Kliendi Isikuandmed**“ tähendab isikuandmeid, mis kuuluvad Kliendile või tema sidusettevõtetele või on kogutud Kliendi või tema sidusettevõtetele poolt, mida Töödeldakse Teenuste osutamise käigus.

„**Andmesubjekt**“ tähendab tuvastatud või tuvastatavat füüsilist isikut.

„**Isikuandmete kaitset käsitlevad õigusaktid**“ tähendab kõiki kohaldatavaid seadusi ja määrusi, mis on seotud isikuandmete Töötlemisega, mis võivad eksisteerida teatud asjaomastes jurisdiktsioonides, sealhulgas, kuid mitte ainult Euroopa Liidu isikuandmete kaitse üldmäärus (määrus (EL) 2016/679), Ühendkuningriigi isikuandmete kaitse üldmäärus (isikuandmete kaitse üldmäärus, nagu see on rakendatud Ühendkuningriigi kohalikus õiguses 2018. a Euroopa Liidust väljaastumise seaduse 3. artiklis ning nagu seda on muudetud Ühendkuningriigi 2019. a andmekaitse, eraelu puutumatuse ja elektroonilise side (muudatused jne) (Euroopa Liidust väljumise) määrustega (koos nende muudatustega)), Ühendkuningriigi 2018. a andmekaitseseadus, Šveitsi föderaalne andmekaitseseadus, USA osariikide eraelu puutumatuse seadused, Brasiilia üldine andmekaitseseadus, Hiina Rahvavabariigi isikuandmete kaitse seadus ning kõik õigusaktid ja/või määrused, mis eelnevalt nimetatud õigusakte rakendavad või on nende põhjal koostatud või neid muudavad, asendavad, taaskehtestavad või liidavad, sealhulgas, kui on asjakohane, järelevalveasutuste avaldatud suunised ja tegevusjuhised.

„**Isikuandmed**“ tähendab igasugust teavet Andmesubjekti kohta.

„**Volitatud töötleja**“ tähendab füüsilist või juriidilist isikut, avaliku sektori asutust, ametit või muud organit, kes Töötleb Isikuandmeid Vastutava töötleja nimel.

„**Töötlemine**“ tähendab igasugust Isikuandmete või nende kogumitega tehtavat automatiseeritud või automatiseerimata toimingut või toimingute kogumit, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

„**Turvarikkumine**“ tähendab Kliendi Isikuandmete, mida Iron Mountain või tema töötajad või alltöövõtjad Teenuste osutamise käigus Töötlevad, igasugust juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist või loata avalikustamist või neile juurdepääsu saamist.

„**Teenused**“ tähendab igasuguseid Teenuseid, mida osutavad Iron Mountain või temaga seotud sidusettevõtted Kliendile või temaga seotud sidusettevõtetele Teenuselepingu alusel.

„**USA osariikide eraelu puutumatuse õigusaktid**“ tähendab kõiki Ameerika Ühendriikide osariikide eraelu puutumatust ja Isikuandmete kaitset käsitlevaid õigusakte, mis reguleerivad selle Teenuselepingu alusel toimuvat isikuandmete Töötlemist, sealhulgas, kuid mitte ainult (ning kõik selliste õigusaktide muudatused, järglased või neid asendavad õigusaktid): (1) California tarbijate eraelu puutumatuse seadus, mida on täiendatud California eraelu puutumatuse õiguste seadusega, ning kõik seotud rakendavad õigusaktid (ühiselt „**CCPA**“); (2) Colorado eraelu puutumatuse seadus („**CPA**“), (3) Virginia tarbijate andmekaitseseadus („**CDPA**“); (4) Utah’ tarbijate eraelu puutumatuse seadus („**UCPA**“); ja (5) Connecticuti isikuandmete kaitse seadus („**CTDPA**“).

2. ANDMETÖÖTLUSE ULATUS JA ÜKSIKASJAD

2.1 Seda Andmetöötluslepingut kohaldatakse kõigile Kliendi Isikuandmetele, mida Töötleb Iron Mountain Volitatud töötlejana osutades Teenuseid Kliendi nimel vastavalt Teenuselepingule.

2.2 Iron Mountain võib koguda ja Töödelda Kliendi ja temaga seotud sidusettevõtete töötajate isikuandmeid Volitatud töötlejana õigustatud ärilistel eesmärkidel, nagu lepinguliste ja kliendisuhete haldus, kooskõlas Isikuandmete kaitset käsitlevate õigusaktidega ja Iron Mountaini privaatsusavaldusega, mis on saadaval Iron Mountaini veebisaitidel ja teistes kohaldatavates privaatsuspoliitikates. Iron Mountaini kohustused, mis on sätestatud selles Andmetöötluslepingus, ei kehti selliste Isikuandmete Töötlemisele.

2.3 Isikuandmete Töötlemine puudutab Teenuste osutamist. Kliendi ja Iron Mountaini kohustused sätestatakse selles Andmetöötluslepingus. Selle Andmetöötluslepingu Lisas 1 on sätestatud Töötlemise laad, kestus ja eesmärk; Kliendi Isikuandmete liigid, mida Iron Mountain Töötleb; ning Andmesubjektide kategooriad, kelle isikuandmeid Töödeldakse.

2.4 Kui Iron Mountain Töötleb Kliendi Isikuandmeid Teenuste osutamise käigus, siis Iron Mountain:

2.4.1 Töötleb Kliendi Isikuandmeid ainult kooskõlas Kliendilt saadud dokumenteeritud korraldustega. Kui mõni kohaldatav õigusakt kohustab Iron Mountainit töötlema Kliendi Isikuandmeid mis tahes muul eesmärgil, teavitab Iron Mountain Klienti eelnevalt sellisest nõudest, kui selline teatamine ei ole olulise avaliku huvi tõttu kõnealuses õigusaktis keelatud.

2.4.2 tegutseb alati kooskõlas kohaldatavate Isikuandmete kaitset käsitlevate õigusaktidega ning teavitab Klienti viivitamatult, kui Iron Mountaini hinnangul rikub Kliendilt saadud Kliendi Isikuandmete Töötlemise korraldus mõnda kohaldatavat Isikuandmete kaitset käsitlevat õigusakti.

2.5 Kliendilt saadud korraldused on Iron Mountainile siduvad, kui selliste korralduste täitmine ei nõua just teenuse osutamist Teenuselepingu alusel ning Klient ei ole nõus sellise teenuse eest teenustasu maksma.

2.6 Iron Mountain tagab, et töötajad, kellel on juurdepääs Kliendi Isikuandmetele, kehtib selliste Kliendi Isikuandmete suhtes siduv konfidentsiaalsuskohustus, ning Iron Mountain võtab mõistlikud meetmed, et tagada selliste töötajate usaldusväärsus ja pädevus, kellel on juurdepääs Kliendi Isikuandmetele.

3. KLIENDILE TUGITEENUSTE OSUTAMINE

3.1 Iron Mountain osutab Kliendile tugiteenuseid, võttes alati arvesse Töötlemise laadi:

3.1.1 kasutades sobivaid tehnilisi ja korralduslikke meetmeid ning ulatuses, mis on võimalik, seoses selliste Kliendi kohustuste täitmisega, mis on seotud oma õigusi kasutavate Andmesubjektide taotlustele vastamisega;

3.1.2 Kliendi kohustuste täitmisel (nt Töötlemise turvalisus, Isikuandmetega seotud rikkumisest teatamine järelevalveasutusele, andmekaitsealase mõjuhinnangu koostamine ja sellele eelnev konsulteerimine järelevalveasutusega, kui Isikuandmete Töötlemise tulemusena tekiks Vastutava töötleja poolt ohu leevendamiseks võetavate meetmete puudumise korral suur oht), võttes arvesse teavet, mis on Iron Mountainile saadaval; ning

3.1.3 tehes Kliendile kättesaadavaks kõik andmed, mida Klient mõistlikult taotleb, et Klient saaks näidata, et ta on Iron Mountaini teenusepakkujaks valimisega oma kohustused täitnud.

4. TURVAMEETMED

4.1 Võttes arvesse tavapärast töökorda, kasutuselevõtu ja laadiga seotud kulusid ning Töötlemise ulatust, konteksti ja eesmärke, võtab Iron Mountain asjakohased ja mõistlikud tehnilised ja korralduslikud meetmed, mille eesmärk on kaitsta Kliendi Isikuandmete konfidentsiaalsust, terviklust ja kättesaadavust ning kaitsta Kliendi Isikuandmeid volitamata või ebaseadusliku Töötlemise ja juhusliku kaotsimineku, hävitamise, kahjustamise, muutmise või avalikustamise eest. Iron Mountaini turvastandardid on sätestatud käesoleva Andmetöötluslepingu Lisas 2.

4.2 See, kas sellised tehnilised ja korralduslikud meetmed vastavad Kliendi nõuetele, on ainuisikuliselt Kliendi enda hinnata.

5. SEADUSTE JÄRGIMINE

Klient ja tema sidusettevõtted peavad: (i) töötlema Kliendi Isikuandmeid kooskõlas Isikuandmete kaitset käsitlevate õigusaktidega; (ii) olema volitatud andma kirjalikke korraldusi Iron Mountainile Kliendi Isikuandmete Töötlemise kohta seoses Teenuste osutamisega (sh mis tahes kolmandast isikust juriidilise isiku nimel, kes on Kliendi Isikuandmete Vastutav töötleja); ning (iii) alati säilitama kontrolli Kliendi Isikuandmete üle, mis on seotud Töötlemisega.

6. ALAMTÖÖTLUS

6.1 Klient on nõus sellega, et Iron Mountain võib kasutada oma emaettevõtte, oma sidusettevõtete ja kolmandast isikust Alamtöötlejate (sh kolmandast isikust Alamtöötlejaid, kelle on palganud Iron Mountaini sidusettevõtted või emaettevõte) Teenuseid selle Andmetöötluslepingu alusel toimuva Kliendi Isikuandmete Töötlemise eesmärkidel, kui peetakse kinni punktist 6.2.

6.2 Kliendi poolt heakskiidetud Alamtöötlejate loetelu selle Andmetöötluslepingu avaldamiskuupäeva seisuga on kättesaadav siin[1]. Iron Mountain võib igal ajal Alamtöötlejaid välja vahetada või lisada uusi Alamtöötlejaid, kuni Kliendile antakse sellest eelnevalt kirjalikult teada viisteist (15) päeva varem ning Klient ei esita sellise muudatuse osas selle vahemiku jooksul vastuväiteid, mis oleks tõendatava alusega ning seotud andmekaitsega. Selliste meiliteavituste saamiseks peab Klient tellima Iron Mountaini teavitusteenuse sellelt veebilehelt[2] ning haldama mis tahes sellist olemasolevat tellimust.

6.3 Kui Klient sellist teavitusteenust ei telli, Iron Mountain ei vastuta Alamtöötlejate muutmisest mitteteavitamise korral ning kõiki selliseid muudatusi loetakse Kliendi poolt heakskiidetuteks**.** Kui Klient esitab Alamtöötleja asendamise või uue Alamtöötleja lisamise kohta viieteist (15) päeva jooksul alates kirjaliku etteteatamise saamisest kirjaliku vastuväite, millel on tõendatav alus ja mis on seotud andmekaitsega, teeb Iron Mountain mõistlikud pingutused, et Teenuseid Kliendile sobivalt muuta või teha Kliendil kaalumiseks ja heakskiitmiseks ettepanek, kuidas oleks soovitatav Kliendi konfiguratsiooni või Teenuste kasutust muuta, et vältida Kliendi Isikuandmete Töötlemist selle Alamtöötleja poolt, kelle kohta vastuväide esitati. Kui Klient ei kiida mis tahes sellist Iron Mountaini pakutud muudatust heaks viieteist (15) päeva jooksul, võib Iron Mountain lõpetada viivitamatult Teenuse või selle Teenuse osa osutamise, mida Iron Mountain ei saa osutada kasutamata Alamtöötlejat, kelle kohta vastuväide esitati, teavitades sellest Klienti kirjalikult. Selline lõpetamine toimub piiramata poolte mis tahes varasemaid õigusi ja kohustusi tingimusel, et Iron Mountain ega Iron Mountaini sidusettevõtted ei pea sellise lõpetamisega seoses maksma mingisuguseid lõpetamistasusid, kulusid ega muid hüvitisi, ning Klient võtab Kliendi enda kulul viivitamata üle nende varade valduse, mis ta andis Iron Mountainile lõpetatud Teenuste osutamiseks, mida osutati vastavalt Teenuselepingu tingimustele.

6.4 Iron Mountain tagab, et kõik selle Andmetöötluslepingu käsitlusalas olevad Alamtöötlejatega sõlmitud lepingud sisaldavad sätteid, mis kattuvad kõigis olulistes aspektides selle Andmetöötluslepingu omadega ning on kooskõlas kohaldatavate Isikuandmete kaitset käsitlevate õigusaktidega. Kui Iron Mountaini Alamtöötleja põhjustab olukorra, kus Iron Mountain on rikkunud kohustusi, mis on tal tulenevalt sellest Andmetöötluslepingust või mis tahes kohaldatavast Isikuandmete kaitset käsitlevast õigusaktist, jääb Iron Mountain vastutama täies ulatuses Kliendi ees selliste Iron Mountaini kohustuste täitmiste eest, mis on tal tulenevalt neist tingimustest.

7. TURVARIKKUMISED

7.1 Turvarikkumise kahtluse korral Iron Mountain:

7.1.1 alustab viivitamatult kahtlustatava Turvarikkumise uurimist ning kahtlustatava Turvarikkumise mõjude tuvastamist, ärahoidmist ja leevendamist ning Turvarikkumise heastamiseks parandusmeetmete võtmist;

7.1.2 teavitab Klienti põhjendamatu viivituseta, kui ta on piisavalt kindel, et Turvarikkumine on aset leidnud, ning annab Kliendile üksikasjaliku Turvarikkumise kirjelduse, sh teabe, mis on Kliendile mõistlikult vajalik Isikuandmete kaitset käsitlevatest õigusaktidest tulenevate aruandluskohustuste täitmiseks.

7.2 Klient nõustub sellega, et Iron Mountain võib anda punktis 7.1.2 nimetatud teavet järkjärguliselt. Juhtudel, kui Iron Mountainil pole võimalik Kliendile esitada teatud teavet, mis on loetletud punktis 7.1.2, või tal pole sellisele teabele juurdepääsu, annab Iron Mountain sellest Kliendile teada ning Iron Mountainil ei teki sellise teabe mitteesitamisega seoses mingisugust vastutust.

---

[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. AUDITID

Iron Mountain lubab Kliendil ja tema audiitoritel või volitatud esindajatel teha Teenuselepingu perioodil auditeid või kontrolle, tingimusel et sellest antakse Iron Mountainile vähemalt kümme (10) tööpäeva ette teada, ning Iron Mountain ei ole kohustatud andma ega lubama juurdepääsu andmetele, mis puudutavad: (i) Iron Mountaini teisi Kliente; (ii) Iron Mountaini mis tahes muid mitteavalikke aruandeid; ning (iii) mis tahes sisearuandeid, mis on koostanud Iron Mountaini siseauditi või vastavuse tagamise funktsioon. Selles punktis käsitletud auditi või kontrolli ainsaks eesmärgiks on veenduda, et Iron Mountain Töötleb Kliendi Isikuandmeid kooskõlas kohustustega, mis tal on vastavalt käesolevale Andmetöötluslepingule. Kui pole just toimunud Turvarikkumine, ei tohi mis tahes kaheteist (12) kuulise perioodi jooksul toimuda rohkem kui üks selline audit.

9. ANDMETE RAHVUSVAHELINE EDASTAMINE (KEELATUD EDASTAMISED)

9.1 Klient annab käesolevaga nõusoleku ja volituse (asjaomases ulatuses) Kliendi Isikuandmete rahvusvaheliseks edastamiseks punktis 6.2 sätestatud juriidilistele isikutele kooskõlas Lisaga 3, et osutada Teenuseid; ning Klient ja Iron Mountain nõustuvad, et:

9.1.1 nad tegutsevad selliste edastamise korral kooskõlas kohaldatavate Isikuandmete kaitset käsitlevate õigusaktidega;

9.1.2 nad on, võtnud arvesse muu hulgas i) Kliendi Isikuandmete liike, ii) riike, mille kohalikud seadused ei pruugi nõuda samal tasemel isikuandmete kaitset kui Euroopa Liidu / Ühendkuningriigi õigusaktid („**kolmandad riigid**“), iii) asjaomaseid tehnilisi ja korralduslikke meetmeid, mis on sätestatud punktis 7, ning iv) asjaomaseid pooli, kes võtavad osa selliste Kliendi Isikuandmete Töötlemisest, ning hinnanud asjaomase selle lepinguga kasutusele võetud edastusmehhanismi sobivust, kui seda nõuab kohaldatav õigus, ning leidnud, et sellise edastamismehhanismi ülesehitus on piisav, et tagada, et selle Andmetöötluslepinguga kooskõlas edastatavate Isikuandmete kaitse sihtriigis on põhimõtteliselt samal tasemel kui see, mida nõuavad Isikuandmete kaitset käsitlevad õigusaktid.

10. VASTUTUS JA KAHJU HÜVITAMINE

10.1 Piiramata ühtki Teenuselepingu sätet, mis on sellega vastuolus, kui turvarikke on põhjustatud otseselt sellise kohustuse rikkumisest, mis on Iron Mountainil tulenevalt sellest Andmetöötluslepingust, hüvitab Iron Mountain Kliendile kohaldatava seadusega lubatud ulatuses otsesed, kontrollitavad, vajalikud ja mõistlikud kulud, mis on tekkinud Kliendil kolmanda isiku ees seoses (a) sellise Turvarikkumise uurimisega, (b) Andmesubjektide ja reguleerivate asutuste teavitamisega ning selliste teavituste ettevalmistamisega, nagu on nõutud Isikuandmete kaitset käsitlevates õigusaktides, (c) krediidiseireteenuste osutamisega sellistele füüsilistele isikutele, kui seda nõuab seadus, kuni kaheteistkümneks (12) kuuks, ning (d) järelevalveasutuse määratud trahvidest või sanktsioonidest selle osa tasumisega, mille kohta on järelevalveasutus otsustanud, et selle eest vastutab otseselt Iron Mountain.

10.2 Juhul, kui Andmesubjekt esitab nõude ühe või mõlema poole kohta seoses Isikuandmete kaitset käsitlevate õigusaktide rikkumisega („**Andmesubjekti nõuded**“) jurisdiktsioonis, kus see on lubatud, juhib kumbki pool ise enda kaitsmist mis tahes sellise nõude eest (või oma osa kaitsest) ning jääb ainuisikuliselt vastutama oma seotud kulude, kulutuste ja vastutuse eest, sh õiguskulude või kohtu määratud mis tahes valuraha eest, kui aga kumbki pool vastutab ainult osa eest või kumbki pool vastutab Andmesubjekti kannatatud kahju eest täissummas samal intsidendil või intsidentide seerial ning Andmesubjekt on sisse nõudnud hüvitise täissumma ainult ühelt poolelt („**hüvitanud pool**“), on hüvitaval poolel õigus esitada nõue teise poole vastu summas, mis vastab kahjule, mille põhjustas selline teine pool. Hüvitanud pool saab esitada nõude teise poole vastu ainult 12 kuu jooksul pärast intsidenti ning ulatuses, mida lubab kohaldatav õigus.

10.3 Maksimaalses kohaldatavate seadustega lubatud ulatuses, reguleerivad maksimaalset kõigi sellest Andmetöötluslepingust ja/või Teenuselepingust tulenevate Kliendi poolt Iron Mountaini vastu esitatud nõuete kogusummat Teenuselepingus toodud vastutuse piirmäärad ja mis tahes välistatud kahjud. Need vastutuse piirmäärad ja välistatud kahjud kehtivad kõigile nõuetele, olenemata sellest, kas nende aluseks on lepinguõigus, deliktiõigus või mis tahes muu õigusteooria ning kõik viited Iron Mountaini vastutusele tähendavad Iron Mountaini ning kõigi Iron Mountaini sidusettevõtete vastutuse kogusummat kõigi nõuete kohta, mis on esitanud Klient ja kõik Kliendi sidusettevõtted kokku. Kohaldatavate seadustega nõutud ulatuses ei ole selle punkti eesmärgiks (i) muuta või piirata poolte vastutust Andmesubjekti nõuete eest, mis on esitatud poole vastu, kui eksisteerib solidaarne vastutuse, või (ii) piirata ükskõik kumma poole vastutust maksta trahve, mis on määranud sellele poolele reguleeriv asutus.

10.4 Punktides 10.1 kuni 10.3 on kirjeldatud kummagi poole ainsat ja eksklusiivset meedet ning kummagi poole ainsat vastutust mis tahes kaotuse, kahju, kulu või vastutusega, mis on seotud selle Andmetöötluslepinguga.

11. TAOTLUSED AMETIASUTUSTELT

11.1 Kui see on seadusega lubatud ning kooskõlas järgnevate punktidega 11.2 kuni 11.5, nõustub Iron Mountain teavitama Klienti, kui ta:

11.1.1 saab õiguslikult siduva sihtriigi seadustele vastava taotluse ametiasutuselt, sh õigusasutuselt, selliste Kliendi Isikuandmete avalikustamiseks, mis on edastatud vastavalt Teenuselepingule; või

11.1.2 ta saab teada, et ametiasutustel on olnud kooskõlas sihtriigi seadustega mis tahes otsene juurdepääs Kliendi Isikuandmetele, mis on edastatud vastavalt Teenuselepingule.

11.2 Kui sihtriigi seadused keelavad Iron Mountainil Klienti teavitada, nõustub Iron Mountain tegema mõistlikud pingutused, et taotleda sellise keelu osas erandit, ning võtab endale eesmärgiks jagada Kliendiga selle kohta võimalikult palju teavet nii kiiresti kui on võimalik.

11.3 Iron Mountain nõustub kontrollima avalikustamise taotluste õiguspärasust, ennekõike selle osas, kas taotleval ametiasutusel on selleks volitus, ning vaidlustama sellise taotluse, kui tema hinnangul on põhjust arvata, et taotlus pole lubatud sihtriigi seaduste järgi. Ta ei avalikusta taotletud Kliendi Isikuandmeid, kuni see ei ole nõutav kooskõlas kohaldatavate menetlusnormidega.

11.4 Iron Mountain nõustub esitama avalikustamise taotlusele vastates nii vähe andmeid kui on lubatud, tuginedes taotluse mõistlikule tõlgendusele.

11.5 Iron Mountain nõustub säilitama selles punktis käsitletud andmeid Teenuselepingu perioodi jooksul ning teeb need nõudmise korral kättesaadavaks pädevale järelevalveasutusele.

12. MUU

12.1 Olenevalt Iron Mountaini osutatavate Teenuste olemusest, kustutab/hävitab Iron Mountain kõik Kliendi Isikuandmed või tagastab need Kliendile või Kliendi määratud kolmandale isikule Teenuselepingu lõpetamise/aegumise korral, sõltuvalt Kliendilt saadud juhistes ja kooskõlas Teenuselepingu tingimustega. Kõik Kliendi Isikuandmed, mis sisalduvad Kliendi varades, mida säilitab Iron Mountain Kliendi nimel, tagastatakse Kliendile kooskõlas kokkulepitud väljumis- või üleminekukavaga ning kokkulepitud kuludega, nagu on sätestatud Teenuselepingus või muus kohaldatavas lepingus. Kõigil muudel juhtudel, kui Teenuselepingus pole Kliendi Isikuandmete kustutamist/hävitamist või tagastamist reguleeritud, ning Klient ei ole andnud mingisuguseid juhiseid Kliendi Isikuandmete kustutamise/hävitamise või tagastamise kohta viieteist (15) päeva jooksul alates Teenuselepingu lõpetamisest/aegumisest, saadab Iron Mountain Kliendile kirjaliku teatise, milles palub saata viieteist (15) päeva jooksul konkreetseid juhiseid selle kohta, kas Kliendi Isikuandmed kustutada/hävitada või tagastada, ning teavitab Klienti kõigist kohaldatavatest turvalise hüvitamise või muuga seotud teenustasudest, mis Klient peab tasuma. Kui Klient ei anna kirjalikke juhiseid sellise viieteist (15) päevase ajavahemiku jooksul ning ei maksa vastavaid tasusid selle perioodi jooksul, annab Klient käesolevaga Iron Mountainile loa otsustada, kuidas Töödelda, kustutada, hävitada kõik Kliendi Isikuandmed pärast lepingu lõppu Iron Mountaini äranägemisel ja Kliendi kulul.

12.2 Piiramata punktis 12.1 toodut ei loeta Iron Mountainit kohustusi rikkunuks seoses selliste Kliendi Isikuandmete kustutamisega, mis on varunduslintidel, kuni sellised varunduslindid kirjutatakse üle (ja Kliendi Isikuandmed kustutatakse) tavapärase äritegevuse käigus.

12.3 Peale lepingu tüüptingimuste (nagu on mõiste määratletud selle Andmetöötluslepingu Lisas 3), reguleerib seda Andmetöötluslepingut ning kõiki selle Andmetöötluslepinguga seotud vaidlusi, nõudeid või lahkarvamusi või selle rikkumist, lõpetamist kehtivust Teenuselepingu kohaldatava õiguse säte; ja kõik selle Andmetöötluslepinguga seotud vaidlused, lahkarvamused või nõuded lahendatakse esmajärjekorras, kasutades vaidluste lahendamise protsessi, mis on kirjas Teenuselepingus.

12.4 Kumbki pool võib aeg-ajalt teavitada teist poolt kirjalikult selle Andmetöötluslepingu mis tahes muudatustest, mis on sellise poole mõistlikul arvamisel vajalikud Isikuandmete kaitset käsitlevates õigusaktides sisalduvate nõuete või järelevalveasutuse või pädeva kohtu mis tahes otsuste täitmiseks. Mis tahes sellised muudatused jõustuvad ainult juhul ja ulatuses, mis mõlemad pooled selle Andmetöötluslepingu paranduses kokku lepivad, välja arvatud juhul, kui üks pool teavitab teist poolt mis tahes uuest õigusnormist ning saadab sellise paranduse, mis sisaldab ainult vajalikke muudatusi ja millega saab nõustuda ilma eraldi nõusoleku andmiseta, s.o esitamata vastuväidet kindlaks tähtajaks, loetakse selle Andmetöötluslepingu kahepoolselt kokkulepitud paranduseks.

LISA 1

Andmete Töötlemise ja edastamise üksikasjad (kui on asjakohane)

A. POOLTE LOETELU:

Selle Andmetöötluslepingu pooled ning Andmeeksportija ja Andmeimportija rollid on sätestatud Teenuselepingus ja Lisas 3 (Andmete rahvusvaheline edastamine), kui see on asjakohane.

B. TÖÖTLEMISE/EDASTAMISE KIRJELDUS (kui on asjakohane):

Andmesubjektide kategooriad, kelle isikuandmeid töödeldakse/edastatakse:

Olenevalt Iron Mountaini Teenuste ja Kliendi äritegevuse olemusest võib Klient edastada Iron Mountainile erinevatesse kategooriatesse kuuluvate Andmesubjektide isikuandmeid, mille ulatuse määrab ja mida kontrollib omal ainuäranägemisel Klient. Seega võivad Andmesubjektide kategooriad hõlmata järgmist: varasemad ja praegused töötajad; varasemad ja praegused töövõtjad või konsultandid; töövahendusbüroo vahendatud töövõtjad või konsultandid ja ajutiselt üle toodud töötajad; tööle kandideerijad; õpilased ja vabatahtlikud; füüsilised isikud, kelle on töötajad või pensionilejäänud töötajad määranud soodustatud isikuks, abikaasaks, partneriks, ülalpeetavaks ja hädaolukorra kontaktisikuks; pensionilejäänud töötajad; varasemad ja praegused direktorid ja juhid; osanikud/aktsionärid; võlakirjaomanikud; kontoomanikud; lõppkasutajad/tarbijad (täiskasvanud, lapsed); patsiendid (täiskasvanud, lapsed); kõrvalised isikud (valvekaamera videotes); ja veebisaidi kasutajad.

Töödeldatavate/edastatavate isikuandmete liigid:

Olenevalt Iron Mountaini Teenuste ja Kliendi äritegevuse olemusest võib Klient edastada Iron Mountainile erinevat liiki Isikuandmeid, mille ulatuse määrab ja mida kontrollib omal ainuäranägemisel Klient. Seega võivad sellised isikuandmete liigid hõlmata isikuandmeid, mis on seotud Kliendiga ja/või Kliendi enda Klientidega, töötajatega jms.

Edastatavad tundlikud andmed (kui on asjakohane):

Olenevalt Iron Mountaini teenuste ja Kliendi äritegevuse olemusest võib Klient edastada Iron Mountainile tundlikke andmeid, mille ulatuse määrab ja mida kontrollib omal ainuäranägemisel Klient.

Kui see on asjakohane, edastamise sageduse (nt, kas andmeid edastatakse ühekordselt või kestvalt):

Edastamine on kestva loomuga.

Töötlemise laad:

Kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

Andmete töötlemise/edastamise (kui on asjakohane) eesmärgid ja edasine Töötlemine:

Teenuste osutamine, nagu on sätestatud Teenuselepingus.

Andmete säilitamine:

Iron Mountain säilitab Isikuandmeid Kliendile Teenuste osutamise perioodil, misjärel sellised Isikuandmed tagastatakse või hüvitatakse kooskõlas selle Andmetöötluslepingu punktiga 12.1.

Kui see on asjakohane, Alamtöötlejatele edastamisel märkida ka Töötlemise laad, kestus ja eesmärk:

Kliendiga sõlmitud Teenuselepingu perioodil osutavad Alamtöötlejad muu hulgas Infotehnoloogia- (IT) ja konsultatsiooniteenuseid, sealhulgas üleilmset IT tuge, ning intsidentidest teavitamise ja nende juhtimise Teenuseid.

C. PÄDEV JÄRELEVALVEASUTUS

Nagu on sätestatud Lisas 3 (Andmete rahvusvaheline edastamine), kui on asjakohane.

LISA 2

TEHNILISED JA KORRALDUSLIKUD MEETMED („TURVAMEETMED“)

1. INFOTURBEPROGRAMM JA POLIITIKA

Iron Mountainil on infoturbeprogramm koos sobivate füüsiliste, tehniliste ja korralduslike turvameetmetega, mis on loodud vastama valdkonna standarditele. Infoturbeprogramm sisaldab järgmist.

1.1 Iron Mountaini infoturbe poliitikate, standardite ja protseduuride dokumenteerimine, organisatsioonisisene avaldamine ja kommunikatsioon.

1.2. Infoturbeprogrammi loomise ja haldamisega seotud kohustuste ja volituste dokumenteeritud ning selge rollide jaotus.

1.3 Infoturbeprogrammi kõige olulisemate turvameetmete, süsteemide ja protseduuride regulaarne testimine.

1.4 Administratiivsed, tehnilised ja operatiivsed meetmed, mis on loodud kaitsma kõiki Kliendi Isikuandmeid, mis kasutavad tavasid, protseduure ja protsesse, mida on kirjeldatud selles turbelisas, ulatuses, mis on asjaomane ja kohaldatav vormile, milles Kliendi Isikuandmeid hoitakse.

2. RISKIDE HINDAMINE

Iron Mountainil on infoturbe alaste riskide hindamise programm, mis on loodud tuvastama ja hindama mõistlikult ettenähtavaid sisemisi ja väliseid riske ning nõrkusi, mis võiksid mõjutada Kliendi Isikuandmete turvalisus, konfidentsiaalsust ja/või terviklust. Kui see on vajalik, mõistlik ja kohane, hindab ja värskendab Iron Mountain kehtiva infoturbeprogrammi tõhusust kord aastas või mis iganes ajal, kui Kliendi Isikuandmeid mõjutavad riskid või nõrkused on oluliselt muutunud.

3. ANDMETÖÖTLUSEVARADE JA FÜÜSILISTE ANDMEKANDJATE HALDUS

3.1 Andmetöötlusvarade haldus. Iron Mountainil on varahaldusprogramm, mille abil hallata füüsilisi, tehnilisi ja administratiivseid turvameetmeid, mis on seotud Iron Mountaini andmetöötlusvaradega (nt arvutid, serverid, salvestid, sidevõrgud, personaalarvutid, sülearvutid ja välisseadmed).
Varahaldusprogramm hõlmab järgmist.

- 3.1.1 Varade ja Iron Mountaini töötajatest omanike dokumenteerimine, et tagada andmete sobiv liigitamine, juurdepääsupiirangute kindlaksmääramine ja juurdepääsu reguleerimise ülevaatamiseks.
- 3.1.2 Varade saneerimine enne kõrvaldamist kooskõlas standardiga NIST 800-88.
- 3.1.3 Juhatuse heakskiidu nõudmine enne Iron Mountaini territooriumilt selliste seadmete või tarkvara eemaldamist, mis pole määratud kindlale füüsilisele isikule.

3.2 Turvameetmed. Iron Mountaini turvameetmed hõlmavad järgmist.

- 3.2.1 Tööprotseduurid ja tehnilised turvameetmed, mis on loodud dokumentide, arvutite andmekandjate, sisend-/väljund-/varundusandmete ja süsteemi dokumentatsiooni kaitsmiseks volitamata avalikustamise, muutmise ja hävitamise eest.
- 3.2.2 Protseduurid Kliendi Isikuandmeid sisaldavate elektrooniliste või füüsiliste andmekandjate turvaliseks hävitamiseks.
- 3.2.3 Järelevalveahela protseduur kõigi Kliendi füüsiliste andmekandjate jälitamiseks alates Iron Mountaini valdusesse andmisest kuni püsiva eemaldamise või hävitamiseni.

4. TÖÖJÕUGA SEOTUD TURVAMEETMED

4.1 Konfidentsiaalsus. Iron Mountain nõuab, et kõik Iron Mountaini töötajad, sh ajutised ja lepingulised töötajad, nõustuks säilitama Kliendi Isikuandmete konfidentsiaalsust ning järgima Iron Mountaini sisemist infoturbe ja aktsepteeritava kasutuse nõudeid.

4.2 Taustakontrolli poliitika. Iron Mountainil on töötajatele taustakontrolli ja narkotesti (ainult USA-s) poliitikad. Iron Mountain säilitab selliste poliitikate kehtivuse Teenuselepingu perioodil. Muu hulgas on nõutud narkotesti tegemine (ainult USA-s), töötaja isiku tuvastamine, karistusregistri väljavõtte saamine, töökäigu kontrollimine, isiku otsimine valitsuse/terroristide jälgimisnimekirjadest ja hariduskäigu kontrollimine (teatud ametite puhul) ning autojuhi kandidaatide ja olemasolevate autojuhtide juhiloa ja liiklusrikkumiste ajaloo kontrollimine. Kui taustakontrolli käigus leitakse midagi negatiivset, hindab Iron Mountain individuaalset olukorda kooskõlas kohaldatavate tööõiguse seaduste ja parimate tavadega.

4.3 Alltöövõtjate kasutamine. Iron Mountain nõuab kõigil Teenuselepingu alusel Teenuseid osutavatelt alltöövõtjatelt selles lepingu punktis kirjeldatutele sarnaste piirangute täitmist kõigi alltöövõtja töötajate puhul, kes osutavad Teenuselepingu alusel selliseid Teenuseid, mis hõlmavad Kliendi Isikuandmete Töötlemist.

4.4 Turvateadlikkuse koolitus. Iron Mountain korraldab vähemalt kord aastas üldise turvateadlikkuse koolituse ning spetsiifilised rollipõhised turvakoolitused kõigile Iron Mountaini töötajatele, kellel on juurdepääs Kliendi Isikuandmetele. Iron Mountain säilitab dokumente turvateadlikkuse koolitusel osalenud Iron Mountaini töötajate nimede ja kuupäevade kohta. Iron Mountain kontrollib ja värskendab oma turvateadlikkuse koolitusprogrammi regulaarselt.

4.5 Iron Mountaini töötaja eemaldamine. Iron Mountainil on distsiplinaarmenetlus, mida rakendatakse juhul, kui Iron Mountaini töötaja on rikkunud siin toodud turvanõudeid.

4.6 Juurdepääsu katkestamine töösuhte lõpetamise / uuele kohale määramise korral. Kui töösuhe lõpetatakse või töötaja uus roll ei nõua juurdepääsu Kliendi Isikuandmetele, tühistatakse viivitamatult Iron Mountaini töötaja juurdepääs Kliendi Isikuandmetele.

5. FÜÜSILINE JA KESKKONNAGA SEOTUD TURVALISUS

5.1 Füüsilised turvameetmed. Iron Mountaini rajatistes on kasutusel mõistlikud füüsilised turvameetmed, mis võimaldavad piirata juurdepääsu Kliendi Isikuandmetele, seahulgas, kui Iron peab seda sobivaks, juurdepääsu reguleerimise protokollid, füüsilised barjäärid (nt lukustatud rajatised ja alad), töötajate identifitseerimiskaardid, külastajate logiraamatud, külaliste identifitseerimiskaardid, kaardilugejad, videovalve kaamerad ning sissetungimise tuvastamise alarmid. Kõik külalised peavad end registreerima ning neil on lubatud ringi liikuda ainult saatjaga.

5.2 Tugiutiliidid. Iron Mountainil on meetmed, mille eesmärk on kaitsta oma Kliendi Isikuandmeid sisaldavaid rajatisi ja süsteeme elektrikatkestuse, telekommunikatsiooni, veevarustuse, kanalisatsiooni, kütte, ventilatsiooni ja kliimasüsteemi rikete eest, nagu on asjakohane.

5.3 Ülekandesüsteemi turvalisus. Iron Mountain võtab meetmed, mille eesmärk on kaitsta oma võrgutaristut ning telekommunikatsioonisüsteeme ülekannete pealtkuulamise ja kahjustamise eest.

5.4 Mujal asuvad seadmed. Juhul, kui Iron Mountain ostab sisse funktsioone, mis nõuavad mujal asuvate seadmete kasutamist Teenuste toetamiseks, peavad kõik mujal asuvad seadmed, milles talletatakse Kliendi Isikuandmeid, olema kaitstud samal tasemel turvameetmetega kui kohapealsed seadmed, mida kasutatakse samal eesmärgil.

5.5 Füüsiline juurdepääs andmetöötlusvaradele. Iron Mountain säilitab ühe aasta jooksul dokumente Iron Mountain töötajate kohta, kellele on antud luba füüsiliseks juurdepääsuks Iron Mountaini kontrolli all oleva(te)le arvutisüsteemi(de)le, mida Iron Mountain kasutab Teenuste osutamiseks. Kui Klient esitab Turvarikkumisega seotud taotluse ja Iron Mountaini turvapoliitikad seda lubavad, antakse Kliendile juurdepääs selliste Iron Mountaini töötajate auditeeritavate dokumentide vaatamiseks.

5.6 Füüsiline juurdepääsu piiramine. Iron Mountain annab füüsilise juurdepääsu Iron Mountaini kontrolli all olevatele rajatistele, milles Töödeldakse Kliendi Isikuandmeid, ainult neile Iron Mountaini töötajatele ja autoriseeritud füüsilistele isikutele, kes vajavad sellist juurdepääsu oma tööülesannete täitmiseks. Iron Mountainil on heakskiidu saamise menetlus, millega antakse lube füüsiliseks juurdepääsuks sellistele rajatistele ning mille abil selliseid taotlusi jälgida.

5.7 Remontimine ja modifitseerimine. Iron Mountain dokumenteerib kõik mis tahes füüsiliste komponentidega, sh rajatiste, kus Kliendi Isikuandmeid hoitakse, turvaliste alade riistvara, seinte, uste ja lukkude turvalisusega seotud remondi- ja modifitseerimistööd.

5.8 Dokumentatsioon. Säilitatakse dokumente riistvara ja elektrooniliste andmekandjate liikumiste ning kõigi vastutavate inimeste kohta.

6. SIDE JA ANDMETÖÖTLUSE OPERATSIOONIDE HALDUS

6.1 Seadme konfiguratsiooni standardid. Iron Mountain loob, juurutab ja säilitab süsteemihalduse protseduure, mis vastavad valdkonna standarditele, sealhulgas, kuid mitte ainult, süsteemi tugevdamine, süsteemi ja seadmete paikade installimine (operatsioonisüsteem ja rakendused) ning nõuetekohase viirusetõrjetarkvara installimine ja ajakohasena hoidmine.

6.2 Andmetöötlussüsteemide muutmise kontrollimine. Iron Mountainil on sisemine ametlik muutmistaotluste halduse menetlus andmetöötluse ja sidevõrgu süsteemide jaoks ning enne mis tahes uue andmetöötluse või sidevõrgu funktsiooni, süsteemipaiga või olemasoleva süsteemi muudatuse kasutuselevõttu peab Iron Mountaini muutmistaotlus olema dokumenteeritud, testitud ja heakskiidetud.

6.3 Ülesannete lahusus. Iron Mountain lahutab ülesanded ja vastutusalad, et mitte ühelgi inimesel ei oleks võimalik muuta Kliendi Isikuandmetele juurdepääsevad andmetöötlussüsteeme üksinda.

6.4 Arendus- ja kasutuskeskkondade eraldamine. Iron Mountaini andmetöötlussüsteemide arendus-, testimis- ja kasutuskeskkonnad peavad olema loogiliselt või füüsiliselt eraldatud.

6.5 Tehnilise arhitektuuri haldus. Iron Mountain võtab kasutusele konfiguratsioonijuhtimise protsessi, et defineerida, hallata ja kontrollida andmetöötlussüsteemi komponente, mida kasutatakse Teenuste osutamiseks ja selliste komponentide tehnilist taristut.

6.6 Sissetungimise tuvastamine. Iron Mountain jälgib pidevalt arvutissüsteeme ja protsesse sissetungimiste või rikkumiste või nende katsete osas ning teavitab Klienti mis tahes volitamata juurdepääsust Kliendi Isikuandmetele.

6.7 Võrgu turvalisus. Iron Mountain tagab järgmise olemasolu.

6.7.1 Teenuste osutamiseks kasutatavate Iron Mountaini majutatud keskkondade puhul logitakse võrku sissetungimise tuvastamise süsteemi („IDS“) ja sissetungimise tõkestamise andurite („IPS“) sündmusi ning neist koostatakse igapäevaseid ülevaatamiseks igapäevaseid aruandeid (ühiselt „IDS/IPS“).

6.7.2 Teenuste osutamiseks kasutatavate Iron Mountaini majutatud keskkondade puhul värskendatakse IDS-e/IPS-e vähemalt kord nädalas ja esimesel mõistlikul võimalusel pärast värskenduse saamist, et kasutada kiiresti kõige värskemaid ohukäekirju või -reegleid.

6.7.3 Avalikkusele kättesaadavate süsteemide kõrge riskitasemega pordid ei ole interneti kaudu kättesaadavad.

6.7.4 Iron Mountaini võrguühendusi logitakse ja salvestatakse logifailidesse.

6.7.5 Juurutatud on tulemüür(id), mille eesmärk on kaitsta ning kontrollida sisenevat ja väljuvat võrguteenuste liiklust kindlate võrgupunktide vahel.

6.7.6 Tugevdamise poliitikad sisenemise ja väljumise võrguportide või võrguliikluse defineerimiseks kõigi Iron Mountaini omatavates või hallatavates süsteemides, mis on dokumenteeritud ja autoriseeritud infoturbeprogrammis.

6.7.7 Võrgu- ja diagnostikapordid on nõuetekohaselt turvatud.

6.7.8 Olemas on poliitikad, protseduurid ja tehnilised turvameetmed, mille abil Iron Mountaini süsteemides ründekoodi või tuntud rünnakuid tõkestada, tuvastada või eemaldada.

6.8 Krüptitud autentimisandmed. Iron Mountain tagab, et autentimisandmed, mida edastatakse Iron Mountaini võrguseadmete kaudu, on ülekande ajal krüptitud.

6.9 Turvaline võrguhaldus. Iron Mountaini võrgud on mõistlikult hallatud ja kontrollitud, et kaitsta neid tuntud ohtude eest ning säilitada kõigi Iron Mountaini hallatavate rakenduste ja andmete turvalisust võrgus või liikumisel üle võrgu. Kasutusel on tehnilised turvameetmed ja turvalised sideprotokollid, et tõkestada piirangutega ühendusi usaldusetute võrkudega või avalikult kättesaadavate serveritega.

6.10 Viirusetõrje. Iron Mountain võtab kasutusele ja haldab viirusetõrjeprogrammi, mis hõlmab kaitset ründevara eest, ajakohaseid allkirjafaile või alternatiivset kaitset esilekerkivate ohtude eest, paikasid ja viiruste definitsioone Iron Mountaini hallatavates serverites ja tööjaamades, mida kasutatakse Kliendi Isikuandmete säilitamiseks või neile juurdepääsemiseks.

6.11 Veebisait – Kliendi krüpteering. Iron Mountain tagab, et turvasoklite kiht (SSL) on aktiveeritud kõigil tema veebisaitidel ning neil kõigil on SSL-sertifikaat, mis nõuab konfidentsiaalsuse, autentimise või autoriseerimise turvameetmeid.

6.12 Andmete varundamine. Iron Mountain loob süsteemifailidest sobivaid varukoopiaid. Lisaks arendab ja haldab Iron Mountain avariitaaste protseduure; lisateavet vt lõigust „Avariitaaste“ dokumendi hilisemas osas.

6.13 Elektroonilised andmed edastamise ajal. Iron Mountain kasutab vähemalt 128 bit võtmega ja valdkonnas tunnustatud algoritmiga krüptimist, et kaitsta Kliendi Isikuandmeid, mida edastatakse üle avalike võrkude, kui lähtekohaks on Iron Mountain taristu.

6.14 Krüptograafilised turvameetmed. Iron Mountain järgib dokumenteeritud poliitikat krüptograafiliste turvameetmete kasutamise kohta. Iron Mountaini krüptograafilised turvameetmed:

6.14.1 on projekteeritud kaitsma mõistlikul tasemel nende Kliendi Isikuandmete konfidentsiaalsust ja terviklikust, mida töötleb, edastab või säilitab Iron Mountain mis tahes jagatud võrgukeskkondades vastavalt Teenuselepingu tingimustele;

6.14.2 on kasutusel Iron Mountaini majutatud keskkondades, mida kasutatakse teenuste osutamiseks, Kliendi Isikuandmetel, mis on teel üle või „usalduseta“ võrkudesse (s.o võrkudesse, mille üle puudub Iron Mountainil juriidiliselt kontroll), sealhulgas need, mida kasutatakse andmete saatmiseks Kliendi ettevõtte võrku Iron Mountaini võrgust, tingimusel et Klient teeb koostööd Kliendi poolt vastu võetud ülekannete dekrüptimiseks vajalike krüptimisvõtmete halduse osas;

6.14.3 hõlmavad dokumenteeritud krüpteerimisvõtme haldamise tavasid, et toetada krüptograafiliste tehnoloogiate turvalisust; ning

6.14.4 hõlmavad kõigi Kliendi isikuandmete krüptimist sülearvutites või teistes kaasaskantavates seadmetes.

6.15 Logimise nõuded. Iron Mountain tagab järgmise.

6.15.1 Olulisi turva- ja süsteemisündmused logitakse ja need vaadatakse üle.

6.15.2 Auditilogisid säilitatakse vähemalt üks aasta nende süsteemide puhul, mida kasutatakse Iron Mountaini majutatud keskkondades Iron Mountaini poolt Teenuste osutamiseks.

6.15.3 Süsteemi auditilogisid kontrollitakse anomaaliate leidmiseks.

6.15.4 Logiregistrid ja süsteemiteave on mõistlikult kaitstud manipuleerimise ja volitamata juurdepääsu eest.

6.16 Võrguaja sünkroonimine. Iron Mountain sünkroonib andmetöötlussüsteemide kõik süsteemikellad ühise autoriteetse ajaserveri järgi.

6.17 Lahusus võrkudes. Iron Mountain lahutab seotud infoteenused, kasutajad ja infosüsteemid võrkudes sobivalt rühmadesse.

7. PÄÄSUKONTROLL

7.1 Juurdepääsu reguleerimise poliitika. Iron Mountainil on andmetöötlusvarade jaoks juurdepääsu reguleerimise poliitikad, mis Iron Mountain ametlikult heaks kiidab, avaldab ja juurutab.

7.2 Loogiline juurdepääsu autoriseerimine. Iron Mountainil on heakskiidu saamise menetlus loogilise juurdepääsu taotluste jaoks, mis on seotud juurdepääsu saamisega Kliendi Isikuandmetele ning Iron Mountaini süsteemidele, mida kasutatakse Teenuste jaoks.

7.3 Juurdepääsu reguleerimine ja ülevaatus. Iron Mountain annab juurdepääsu Kliendi Isikuandmetele ainult aktiivsetele Iron Mountaini töötajatele, sh ajutistele ja lepingulistele töötajatele, ning aktiivsete kasutajate kontodele, kes vajavad sellist juurdepääsu oma tööülesannete täitmiseks. Kõiki kõrgemate juurdepääsuõiguste puhul tuleb neid vähemalt kord kvartalis kontrollida ning veenduda, et need on kooskõlas praeguste tööülesannetega, ning seejärel uuesti kinnitada ja dokumenteerida.

7.4 Kolmandate isikute juurdepääsu reguleerimine. Enne välistele isikutele juurdepääsu andmist sellistele Iron Mountaini infosüsteemidele, millel on juurdepääs Kliendi Isikuandmetele, tagab Iron Mountain, et on võetud sobivad turvameetmed.

7.5 Operatsioonisüsteemide juurdepääsu reguleerimine. Iron Mountain reguleerib juurdepääsu operatsioonisüsteemidele (nii tarkvara kui ka riistvara põhistele operatsioonisüsteemidele), tehes

kohustuslikuks turvalise sisselogimise protseduuri, mis võimaldab operatsioonisüsteemi kasutava isiku tuvastada.

7.6 Mobiilsed arvutusseadmed. Iron Mountainil on poliitika või protseduur, mille eesmärk on kaitsta Iron Mountaini mobiilseid arvutusseadmeid volitamata juurdepääsu eest. Sellised poliitikad või protseduurid käsitlevad füüsilist kaitset, juurdepääsu reguleerimist ja turvameetmeid nagu krüptimine, viirusetõrje ja seadmete varundamine.

7.7 Kliendi süsteemide isoleerimine. Iron Mountain eraldab ja lahutab enda majutatud keskkondades, mida kasutatakse Teenuste osutamiseks, Kliendi Isikuandmed kõigist muudest andmetest.

7.8 Kontod. Iron Mountain teeb kontode osas järgmist.

7.8.1 Nõuab igalt Iron Mountaini töötajalt identiteedi autentimist, kes soovib juurdepääsu Iron Mountaini süsteemidele, mis Töötlevad Kliendi Isikuandmeid, ning keelab jagatud või üldiste autentimisandmetega kasutajakontode (s.o ID-d) kasutamise Kliendi Isikuandmetele või süsteemidele juurdepääsemisel.

7.8.2 Nõuab, et kõik kasutajakontode ID-d, sh kõrgemate juurdepääsuõigustega kontod, oleks seotud otseselt inimesega (mitte ametikohaga).

7.8.3 Kui administraatoriõigustega vaikekontod pole keelatud või eemaldatud, nõuab ajutiste paroolide kasutamist, ID-de väljaregistreerimist või sarnaseid turvameetmeid administraatoriõigustega vaikekonto juurdepääsu jaoks.

7.8.4 Nõuab mitteaktiivsete tavakontode lukustamist või blokeerimist, kui neid pole 90 päeva kasutatud.

7.8.5 Keelab juurdepääsu kontole pärast mitut ebaõnnestunud juurdepääsukatset.

7.8.6 Nõuab kordumatuid identifikaatoreid ja tugevaid paroole, mis vastavad järgmistele miinimumnõuetele: vähemalt 8 tärki, tuleb muuta iga 90 päeva järel, peab vastama keerulisuse nõuetele.

7.8.7 Keelab töötajatel paroole teistega jagada või neid üles kirjutada.

7.9 Järelevalveta süsteemide turvameetmed. Iron Mountain kasutab parooliga kaitstud ekraanisäästjat kõigis süsteemides, mis on jäetud järelevalveta ja mida pole 30 minutit järjest kasutatud.

8. INFOSÜSTEEMIDE HANKIMINE, ARENDAMINE JA HOOLDAMINE

8.1 Süsteemiarenduse turve. Iron Mountain tagab, et turve on osa kõigist infosüsteemide arendustegevustest ja operatsioonidest ning avaldab ja peab kinni organisatsioonisisestest turvalise kodeerimise meetoditest, mis põhinevad rakenduste arendamise turvastandarditele.

8.2 Tarkvara turvalisuse haldamine. Iron Mountaini infosüsteemid (sh operatsioonisüsteemid, taristu, ärirakendused, teenused ja kasutajate arendatud rakendused) on projekteeritud olema kooskõlas infoturbe standarditega.

8.3 Võrgu skeemid. Iron Mountain arendab, dokumenteerib ning säilitab füüsilisi ja loogilisi skeeme võrguseadmete ja -liikluse kohta.

8.4 Rakenduse haavatavuse hindamine / eetiline häkkimine. Iron Mountain hindab vähemalt kord aastas nende rakenduste haavatavust, mis on tema majutatud keskkondades, mida kasutatakse Kliendi Isikuandmeid Töötlevate teenuste osutamiseks. Üksikasjalikud tulemused on konfidentsiaalsed ja Iron Mountaini siseteave ning neid ei avaldata.

8.5 Muudatuste testimine ja ülevaatus. Iron Mountain kontrollib ja testib rakenduste ja operatsioonisüsteemide muudatusi enne nende juurutamist veendumaks, et neil pole negatiivset mõju Kliendi Isikuandmetele ega süsteemidele.

9. AVARIITAASTE

Iron Mountainil on avariitaaste kava, mis hõlmab Teenuste toetamiseks kasutatavate süsteemide ja elektrooniliste andmete dubleerimist varundamise andmekeskusse. Süsteemide ja elektrooniliste andmete dubleerimine ei hõlma Kliendi Isikuandmeid, mida talletatakse füüsiliselt Iron Mountaini rajatises. Iron Mountainil on talitluspidevuse kava kriitilist ärifunktsioonide taastamiseks. Iron Mountain katsetab avariitaaste kava vähemalt kord iga kaheteist (12) kuu järel.

10. VÄLISED AUDITID JA HINDAMISED

Iron Mountaini turvaprotokollid on loodud olema kooskõlas valdkonna standarditega. Iron Mountain esitab Kliendile kõik sõltumatu kolmanda isiku auditiaruanded, mis ta on tellinud (nt PCI, ISO27001, SOC2 jne), mis puudutavad Teenuseid piirkonnas, kus selliseid Teenuseid osutatakse („Auditiaruanne“). Iron Mountain esitab kõik sellised aruanded, mis on tellitud olema kliendile suunatud, olenemata sellise aruande tulemustest. Iron Mountain ei ole kohustatud esitama siseauditi tulemusi ega muid sõltumatuid hinnanguid, mis olid tellitud olema Iron Mountainile konfidentsiaalsed. Kliendile ja tema välistele audiitoritele esitatakse nõudmisel Auditiaruande koopiad. Kõiki Auditiaruandeid või muid tulemusi, mis on loodud testide või auditite abil, mida nõuab see lepingu punkt, loetakse Iron Mountaini konfidentsiaalseks teabeks. Kliendil on õigus esitada sellise Auditiaruande koopia Kliendi mis tahes asjaomastele klientidele või reguleerivatele asutustele, kui järgitakse konfidentsiaalsussätteid, mis on vähemalt sama ranged kui siin toodud. Kliendi nõudmisel kinnitab Iron Mountain kirjalikult, et asjaomaseid poliitikaid, protseduure ja sisemisi turvameetmeid pole muudetud pärast mis tahes sellise auditiaruande koostamist, mis ei tohi toimuda rohkem kui kolm kuud pärast auditiaruande aruandlusperioodi lõppu.

LISA 3

Andmete rahvusvaheline edastamine

1. MÄÄRATLUSED

„**Euroopa Liidu 2021. a lepingu tüüptingimused**“ tähendab lepingu tüüptingimusi Isikuandmete edastamiseks kolmandatesse riikidesse kooskõlas Euroopa Liidu isikuandmete kaitse üldmäärusega, mis on Euroopa Komisjon tarvitusele võtnud komisjoni rakendusotsusega (EL) 2021/914, mis on saadaval siin[3].

„**Ühendkuningriigi 2022. a addendum**“ tähendab addendumi B.1.0 malli, mille on avaldanud Ühendkuningriigi teabevoliniku büroo ning mis on toodud Parlamendi ette kooskõlas Ühendkuningriigi 2018. a andmekaitseseadusega artikliga 119A 2. veebruaril 2022, mida võidakse kohandada vastavalt andmekaitseseaduse artiklile 18, mis on saadaval siin[4].

„**Euroopa Liidu kliendi isikuandmed**“ tähendab Kliendi Isikuandmete Töötlemist, millele kehtisid Euroopa Liidu või Euroopa Liidu või Euroopa Majanduspiirkonna liikmesriigi andmekaitseseadused enne töötlemist Iron Mountaini poolt.

„**Kaitstud piirkond**“ tähendab:

i. Euroopa Liidu kliendi isikuandmete puhul Euroopa Liidu ja Euroopa Majanduspiirkonna liikmesriike ning kõiki riike, territooriume, sektoreid või rahvusvahelisi organisatsioone, kelle puhul kehtib kaitse piisavuse otsus vastavalt Euroopa Liidu isikuandmete kaitse üldmääruse artiklile 45;

ii. Ühendkuningriigi kliendi isikuandmete puhul Ühendkuningriiki ning kõiki riike, territooriume, sektoreid või rahvusvahelisi organisatsioone, kelle puhul kehtib kaitse piisavuse otsus vastavalt Ühendkuningriigi kaitse piisavuse õigusaktidele;

iii. Šveitsi kliendi isikuandmete puhul kõiki riike, territooriume, sektoreid või rahvusvahelisi organisatsioone, kelle puhul on kaitse piisav Šveitsi seaduste järgi;

iv. mis tahes muu Kliendi Isikuandmete edastamisel välja jurisdiktsioonist, mis pakub Euroopa Liidu, Ühendkuningriigi või Šveitsi kliendi isikuandmetele sarnast kaitset, kõiki riike, territooriume, sektoreid või rahvusvahelisi organisatsioone, kelle puhul on kaitse piisav vastava jurisdiktsiooni seaduste järgi.

„**Lepingu tüüptingimused**“ tähendab ühiselt Euroopa Liidu 2021. a lepingu tüüptingimusi ja Ühendkuningriigi 2022. a addendumit.

„**Šveitsi kliendi isikuandmed**“ tähendab Kliendi Isikuandmete Töötlemist, millele kehtisid Šveitsi andmekaitseseadused enne töötlemist Iron Mountaini poolt.

„**Ühendkuningriigi kliendi isikuandmed**“ tähendab Kliendi Isikuandmete Töötlemist, millele kehtisid Ühendkuningriigi andmekaitseseadused enne töötlemist Iron Mountaini poolt.

2. MUU

2.1 See Lisa 3 koosneb järgmistest osadest: (i) Osa A – Euroopa Liidu kliendi isikuandmete edastamine; (ii) Osa B – Šveitsi kliendi isikuandmete edastamine; (iii) Osa C – Ühendkuningriigi kliendi isikuandmete edastamine, mis kehtivad vastavalt konkreetsele Kliendi Isikuandmete edastamisele Iron Mountaini poolt seoses oma Teenuste osutamisega.

2.2 Lepingu tüüptingimuste mõistes on Iron Mountain ja tema sidusettevõtted „andmeimportijad“ ning Klient ja tema sidusettevõtted „andmeeksportijad“.

2.3 Lepingu allkirjastamist ja dateerimist käsitatakse kõigi lepingu tüüptingimuste järgi nõutud allkirjade ja kuupäevadena.

2.4 Juhul, kui pooled edastavad Euroopa Liidu, Ühendkuningriigi või Šveitsi kliendi isikuandmeid Kaitstud piirkonnast välja ning asjaomane Euroopa Komisjoni otsus või muu kehtiv kaitse piisavuse otsustamise meetod kohaldatavates Isikuandmete kaitset käsitlevates õigusaktides, millele Iron Mountain on tuginenud, leitakse olevat tühine või mis tahes järelevalveasutus nõuab, et sellisele otsusele tuginev Isikuandmete edastamine lõpetataks, teevad pooled koostööd ning leiavad kasutamiseks alternatiivse edastamismehhanismi. Pooled lepivad kokku ka selles, et selles Lisas 3 nimetatud rahvusvaheliste edastamiste jaoks sobivad kaitsemeetmed pole välistavad ning pooltel on õigus kasutada ka teisi edastamismehhanisme nagu Euroopa Liidu ja USA andmekaitseraamistik.

OSA A – EUROOPA LIIDU KLIENDI ISIKUANDMETE EDASTAMINE

Kui Klient või tema Sidusettevõte edastab Euroopa Liidu kliendi isikuandmeid Kaitstud piirkonnast väljapoole Iron Mountainile või tema Sidusettevõtetele seoses Iron Mountaini Teenustega, mida osutatakse Teenuselepingu alusel, kehtib selle osas Lisa 3 see Osa A ning Pooled lepivad kokku järgmises.

[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

1. **Lepingu tüüptingimuste valikud.** Kui Klient või tema mis tahes Sidusettevõte on Vastutav töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on volitatud töötleja, kehtib Euroopa Liidu 2021. a lepingu tüüptingimuste TEISE MOODULI tekst, ja kui Klient või tema mis tahes Sidusettevõte on Volitatud töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on Alamtöötleja, kehtib Euroopa Liidu 2021. a lepingu tüüptingimuste KOLMANDA MOODULI tekst. Euroopa Liidu 2021. a lepingu tüüptingimuste asjaomased sätted on liidetud sellele Andmetöötluslepingule viitamise teel ning on selle Andmetöötluslepingu lahutamatuks osaks. Ei kehti ükski muu moodul ega tingimus, mis on märgitud Euroopa Liidu 2021. a lepingu tüüptingimustes vabatahtlikuks. Teave, mis on nõutud Euroopa Liidu 2021. a lepingu tüüptingimuste liidete jaoks on sätestatud Lisas 1 – Töötlemise/edastamise kirjeldus, Lisas 2 – Tehnilised ja korralduslikud meetmed ning Andmetöötluslepingu punktis 6.2 – Alamtöötlejate loetelu.

2. **Alamtöötlejate kasutamine.** Euroopa Liidu 2021. a lepingu tüüptingimuste 9. tingimuse otstarbel kehtib Teenuste osutamisel Alamtöötlejate kasutamisele 2. variant (Üldine kirjalik luba). Klient on nõus sellega, et Iron Mountain võib palgata uusi Alamtöötlejaid, kasutades mehhanismi, milles on kokku lepitud selle Andmetöötluslepingu punktis 6, ning ajavahemik Alamtöötlejate muutmisega seotud taotluste esitamiseks on viisteist (15) päeva.

3. **Kohaldatav õigus ja vaidluste lahendamise organ.** Euroopa Liidu 2021. a lepingu tüüptingimuste 17. tingimuse (Kohaldatav õigus) otstarbel kehtib kohaldatava õiguse 2. variant, mis tähendab, et nende tingimuste suhtes kohaldatakse selle Euroopa Liidu liikmesriigi õigust, kus andmeeksportija asub, ulatuses, milles see lubab näha ette kolmandast isikust soodustatud isiku õigusi. Euroopa Liidu 2021. a lepingu tüüptingimuste 18. tingimuse (Vaidluste lahendamise organi ja kohtualluvuse valimine) otstarbel on nendeks selle Euroopa Liidu liikmesriigi kohtud, kus andmeeksportija asub.

4. **Kustutamise tõend.** Euroopa Liidu 2021. a lepingu tüüptingimuste punkti 8.5 ja 16. tingimuse punkti d otstarbel esitab Iron Mountain Kliendile Isikuandmete kustutamise tõendi, kui Klient seda kirjalikult taotleb.

5. **Isikuandmetega seonduv rikkumine.** Euroopa Liidu 2021. a lepingu tüüptingimuste punkti 8.6 alapunkti c otstarbel tegeletakse isikuandmetega seonduvate rikkumistega vastavalt mehhanismile, mis on kokku lepitud Andmetöötluslepingu punktis 7.

6. **Auditid.** Euroopa Liidu 2021. a lepingu tüüptingimuste punkti 8.9 otstarbel viiakse nende tingimuste auditid läbi kooskõlas Teenuselepingus kokku lepitud auditimehhanismiga.

7. **Kaebused.** Euroopa Liidu 2021. a lepingu tüüptingimuste 11. tingimuse otstarbel teavitab Iron Mountain Klienti, kui ta saab Andmesubjektilt kaebuse, mis on seotud Euroopa Liidu kliendi isikuandmetega, ning edastab kaebuse Kliendile kooskõlas Teenuselepingus kokku lepitud mehhanismiga.

8. **Järelevalveasutus.** Euroopa Liidu 2022. a lepingu tüüptingimuste puhul määratakse pädev järelevalveasutus vastavalt Euroopa Liidu lepingu tüüptingimuste 13. tingimusega.

OSA B – ŠVEITSI KLIENDI ISIKUANDMETE EDASTAMINE

Kui Klient või tema Sidusettevõte edastab Šveitsi kliendi isikuandmeid Kaitstud piirkonnast väljapoole Iron Mountainile või tema sidusettevõtetele seoses Iron Mountaini Teenustega, mida osutatakse Teenuselepingu alusel, kehtib selle osas Lisa 3 see Osa B ning Pooled lepivad kokku järgmises.

1. **Lepingu tüüptingimuste valikud.** Kui Klient või tema mis tahes Sidusettevõte on Vastutav töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on volitatud töötleja või Klient või tema mis tahes Sidusettevõte on Volitatud töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on Alamtöötleja, kehtivad Euroopa Liidu 2021. a lepingu tüüptingimused ja Osa A asjaomased sätted, järgmiste eranditega:

   a. pädev järelevalveasutus Euroopa Liidu 2021. a lepingu tüüptingimuste 13. tingimuse mõttes on Šveitsi föderaalne andmekaitse ja teabe komisjon;

   b. lepingulistele nõuetele kohaldatav õigus Euroopa Liidu 2021. a lepingu tüüptingimuste 17. tingimuse mõttes on Šveitsi õigus ning poolte vaheliste vaidluste puhul on kohtualluvus 18. tingimuse punkti b mõttes Šveitsi kohtutel.

2. Viiteid Euroopa Liidu isikuandmete kaitse üldmäärusele Euroopa Liidu 2021. a lepingu tüüptingimustes tuleb tõlgendada viidetena Šveitsi föderaalsele andmekaitseseadusele.

3. Mõistet „liikmesriik“ Euroopa Liidu 2021. a lepingu tüüptingimustes ei tohi tõlgendada selliselt, et see välistaks Šveitsis olevatel Andmesubjektidel õiguse pöörduda oma õiguste kaitseks kohtusse oma elukohariigis (Šveitsis) kooskõlas Euroopa Liidu 2021. a lepingu tüüptingimuste 18. tingimuste punktile C.

OSA C – ÜHENDKUNINGRIIGI KLIENDI ISIKUANDMETE EDASTAMINE

Kui Klient või tema Sidusettevõte edastab Ühendkuningriigi kliendi isikuandmeid Kaitstud piirkonnast väljapoole Iron Mountainile või tema Sidusettevõtetele seoses Iron Mountaini Teenustega, mida osutatakse Teenuselepingu alusel, kehtib selle osas Lisa 3 see Osa C ning Pooled lepivad kokku järgmises.

1. **Lepingu tüüptingimuste valikud.** Kui Klient või tema mis tahes Sidusettevõte on Vastutav töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on volitatud töötleja või Klient või tema mis tahes Sidusettevõte on Volitatud töötleja ning Iron Mountain või tema mis tahes Sidusettevõte on Alamtöötleja, kehtivad Euroopa Liidu 2021. a lepingu tüüptingimused, Osa A asjaomased sätted ning Ühendkuningriigi 2022. a addendum, järgmiste eranditega.

2. **Osa 1. Tabelid 1–3 Ühendkuningriigi 2022. a addendumis:** Teave poolte kohta – Tabel 1; Valitud lepingu tüüptingimused moodulid ja Valitud tingimused; ning Lisateavet, sh Lisa 1A: Poolte loetelu, Lisa 1B: Edastamise kirjeldus ning Lisa 1C: Tehnilised ja korralduslikud meetmed andmete turvalisuse tagamiseks – Tabel 3, loetakse lõpetatuks viitamisega sellele Lisale 3, sh Osa A Tabelile 4 Ühendkuningriigi addendumis: Klient ja Iron Mountain lepivad kokku, et ükskõik kumb Pool võib igal ajal Ühendkuningriigi addendumi lõpetada.

3. **Osa 2.**Ühendkuningriigi addendumi kohustuslikud tingimused. Klient ja Iron nõustuvad järgima Ühendkuningriigi addendumi kohustuslikke tingimusi.

4. **Järelevalveasutus.** Pädevaks järelevalveasutuseks on Ühendkuningriigi teabevoliniku büroo.

OSA D – TEISTE KLIENTIDE ISIKUANDMETE EDASTAMINE

Kui Klient või tema Sidusettevõte edastab Kaitstud piirkonnast väljapoole Iron Mountainile või tema Sidusettevõtetele Kliendi Isikuandmeid, mida ei käsitle OSAD A–C, seoses Iron Mountaini Teenustega, mida osutatakse Teenuselepingu alusel, kehtib sellele Lisa 3 Osa A ulatuses, mis on asjaomane ja kohaldatav kooskõlas kohaldatavate Isikuandmete kaitset käsitlevate õigusaktidega. Muul juhul, kui Isikuandmete kaitset käsitlevate õigusaktidega on nõutud mis tahes asendavad või täiendavad sobivad kaitsemeetmed või edastamismehhanismid, et edastada Kliendi Isikuandmeid riiki, kus pole Isikuandmete kaitsetase piisav andmeeksportija seisukohast, nõustuvad pooled rakendama neid samu kohe, kui see on praktiline, ning dokumenteerima selliste nõuete täitmist selle Andmetöötluslepingu lisas.

LISA 4

HIPAA – äripartnerileping („Äripartnerileping“)

See Äripartnerileping täiendab ja muudab kõiki praegu või tulevikus kehtivaid Teenuselepinguid, mis on sõlmitud Iron Mountaini ja tema sidusettevõtete ning Kliendi ja tema sidusettevõtete vahel, mille alusel Iron Mountain või tema sidusettevõtted osutavad teatud Teenuseid Kliendile või tema sidusettevõtetele, kui sellised Teenused nõuavad, et Äripartner Kasutaks ja/või Avalikustaks Kaitstud terviseandmeid Privaatsusreeglile alluva juriidilise isiku nimel. Välja arvatud ulatuses, mida on muudetud käesoleva Äripartnerilepinguga, jäävad kõik Teenuselepingu sätted ja tingimused kehtima täis jõus ning reguleerivad Teenuseid, mida osutab Iron Mountain Kliendile.

Iron Mountain ja Klient sõlmivad selle Äripartnerilepingu selleks, et mõlemad pooled täidaks oma kohustused, kui need muutuvad pooltele siduvaks vastavalt HIPAA eraelu puutumatuse, turvalisuse ja rikkumisest teavitamise reeglitele koos kõigi rakendusaktidega, sealhulgas nendega, mis on osa koondreeglist (ühiselt „HIPAA reeglid“), mille järgi on Klient ja tema sidusettevõtted „Privaatsusreeglile alluvaks juriidiliseks isikuks“ või „Äripartneriks“ ning Iron Mountain ja tema sidusettevõtted on Kliendi „Äripartneriks“. Selles lepingus tähendavad edaspidi kõik viited Äripartnerile Iron Mountainit või tema asjaomast sidusettevõtet.

1. MÄÄRATLUSED

Suurtähega mõistetel, mida pole selles Äripartnerilepingus eraldi määratletud, on sama tähendus kui HIPAA reeglites või Teenuselepingus, nagu on asjakohane.

„**Rikkumisest teavitamise reegel**“ tähendab Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164 alaosas D toodud reeglit, mis käsitleb turvamata kaitstud terviseandmete rikkumisest teavitamist.

„**Äripartner**“ tähendab eespool tuvastatud Äripartnerist juriidilist isikut, mis võtab vastu, haldab või edastab Kaitstud terviseandmeid, kui ta Klientidele Teenuseid osutab.

„**HIPAA**“ tähendab Ameerika Ühendriikide 1996. a tervisekindlustuse ülekantavuse ja vastutuse seadust.

„**HITECH-seadus**“ tähendab Ameerika Ühendriikide majanduslike ja kliinilise tervise terviseinfotehnoloogia seadust, mis on liidetud Ameerika Ühendriikide 2009. a Ameerika majanduse taastamise ja reinvesteerimise seadusesse, ning kõiki rakendavaid õigusakte.

„**Privaatsusreegel**“ tähendab Tuvastatava füüsilise isiku terviseandmete privaatsuse norme, mis on toodud Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 160 ja § 164 alaosades A ja E.

„**Kaitstud terviseandmed**“ on sama tähendus kui „kaitstud terviseandmetele“ Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 160.103 ning see on piiratud Kaitstud terviseandmetele, mis on loonud Äripartner Kliendi nimel või saanud Kliendilt või Kliendi nimel kooskõlas Teenuselepinguga.

„**Turvareegel**“ täiendab elektrooniliste Kaitstud terviseandmete turvanorme, mis on toodud Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 160 ja § 164 alaosades A ja C.

2. ÄRIPARTNERI KOHUSTUSED JA TEGEVUSED

2.1. Äripartner nõustub mitte Kasutama ega Avaldama Kaitstud terviseandmeid viisil, mida ei luba või nõua see Äripartnerileping või seadused.

2.2. Äripartner nõustub kasutama sobivaid ettevaatusabinõusid ning järgima, nagu on asjakohane, Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164 alaosa C seoses elektrooniliste Kaitstud terviseandmetega, et hoida ära Kaitstud terviseandmete Kasutamised või Avalikustamised, mida pole ette nähtud selles Äripartnerilepingus või Teenuselepingus, kuid pooled nõustuvad sellega, et Klient, mitte Äripartner, vastutab selle eest, et oleks täidetud Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164.312 nõuded, mis on seotud füüsilistele andmekandjatele (nt lintidele) salvestatud elektrooniliste Kaitstud terviseandmete krüptimis- ja dekrüptimismehhanismidega, mida Klient hoiab Äripartneri juures.

2.3. Äripartner nõustub teavitama Klienti viivitamatult igasugustest Turvaintsidentidest, rikkumistest või muust Kaitstud terviseandmete Kasutusest või Avalikustamisest, millest ta saab teada ning mis pole lubatud või nõutud selle Äripartnerilepingu või Teenuselepinguga. Rikkumise korral peab selline teavitamine toimuma kooskõlas äripartneritele kehtivate nõuetega HIPAA reeglites, sealhulgas, kuid mitte ainult kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.410, kuid mitte mingil juhul hiljem kui kolme (3) tööpäeva jooksul pärast seda, kui Äripartner on viinud lõpule oma sisejuurdluse ning veendunud selles, et Rikkumine on toimunud. Äripartner osutab mõistlikku abi ja teeb koostööd mis tahes sellise rikkumise juurdlusega ning dokumenteerib kõik konkreetsed Hoiule usaldatud andmed, mis on rikutud, mis tahes volitamata kolmanda isiku identiteedi, kes võis Kaitstud terviseandmetele juurde pääseda või neid vastu võtta, kui see on teada, ning kõik meetmed, mis Äripartner on võtnud sellise Rikkumise mõjude leevendamiseks.

2.4. Äripartner tagab, kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.502(e)(1)(ii) ja §-ga 164.308(b)(2), nagu asjakohane, et kõik alltöövõtjatest äripartnerid, kes on

loonud, vastu võtnud, hooldanud või edastanud Kaitstud terviseandmeid Äripartneri nimel seoses Teenuselepingu alusel osutatavate Teenuste osutamise toetamisega, nõustuvad samade piirangute, tingimuste ja nõuetega, mis kehtivad Äripartnerile selliste Kaitstud terviseandmete osas selle Äripartnerilepingu tõttu.

2.5. Kui Äripartneri valduses on Kaitstud terviseandmete komplekte Füüsiliste isikute kohta ning Klient seda nõuab, nõustub Äripartner andma Kliendile juurdepääsu sellistele Kaitstud terviseandmetele, otsides välja ja toimetades kohale sellised Kaitstud terviseandmed kooskõlas Teenuselepingu tingimustega, et Klient saaks Füüsilisele isikule vastata ning täita Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164.524 nõuded.

2.6. Äripartner nõustub, et kui on vajalik parandada Kaitstud terviseandmeid Äripartneri valduses olevas dokumendikomplektis ning Klient annab Äripartnerile korralduse sellised Kaitstud terviseandmed välja otsida kooskõlas Teenuselepinguga, osutab Äripartner sellist teenust, et Klient saaks teha sellistes Kaitstud terviseandmetes mis tahes parandused, mida võib nõuda Klient või Füüsiline isik kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.526.

2.7. Äripartner nõustub dokumenteerima ja Kliendile kättesaadavaks tegema andmed, mis on vajalikud Kaitstud terviseandmete Avalikustamiste üle arve pidamiseks, eeldusel et Klient on esitanud Äripartnerile piisavalt teavet, et Äripartner saaks kindlaks teha, millised dokumendid või andmed, mis Äripartner on Kliendilt või Kliendi nimel vastu võtnud, võivad sisaldada Kaitstud terviseandmeid. Avalikustamiste dokumentatsioon peab sisaldama sellist teavet, mida vajab Klient, et vastata Füüsilise isiku päringule Kaitstud terviseandmete avalikustamise kohta kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.528 või teiste HIPAA reeglite sätetega.

2.8. Kui Teenuselepingus pole just teisiti kokku lepitud, peab Äripartner teavitama Klienti viivitamatult sellest, kui ta on saanud Füüsiliselt isikult päringu Kaitstud terviseandmetega tutvumise, nende olemasolu kinnitamise või nende parandamise kohta ning jätma sellisele taotlusele vastamata, ning jätma selliste Füüsiliste isikute taotluste vastuvõtmise ja neile vastamise Kliendi vastutada.

2.9. Kui Äripartner peab täitma ühte või mitut Kliendi kohustustest, mis on sätestatud Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164 alaosas E, peab Äripartner pidama kinni selliste kohustuste täitmisel alaosa E nõuetest, mis kehtivad Kliendile.

2.10. Äripartner nõustub tegema oma sisemised tavad, raamatud ja dokumendid kättesaadavaks Ameerika Ühendriikide tervishoiu- ja teenindusministrile, et oleks võimalik kontrollida vastavust HIPAA reeglitele.

3. LUBATUD KASUTUS JA AVALIKUSTAMISED ÄRIPARTNERI POOLT

3.1. Äripartner võib Kasutada või Avalikustada Kaitstud terviseandmeid, kui see on vajalik Teenuselepingus sätestatud Teenuste osutamiseks.

3.2. Äripartner võib Kasutada või Avalikustada Kaitstud terviseandmeid, kui see on nõutud seadusega.

3.3. Äripartner nõustub tegema mõistlikud pingutused, et piirata Kaitstud terviseandmete ulatust miinimumile, mis on vajalik Kasutamise, Avalikustamise või taotlusele vastamise eesmärkide täitmiseks.

3.4. Äripartner ei tohi Kasutada ega Avalikustada Kaitstud terviseandmeid viisil, mis rikuks Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise § 164 alaosa E, kui seda teeks Klient.

3.5. Äripartner võib Avalikustada Kaitstud terviseandmeid Äripartneri tegevuste nõuetekohaseks juhtimiseks või administreerimiseks või Äripartneri õiguskohustuste täitmiseks, eeldusel et Avalikustamised on nõutud seadusega või Äripartner on hankinud mõistlikud kinnitused isikult, kellele andmed avalikustatakse, et andmed jäävad konfidentsiaalseks ning neid kasutatakse või avalikustatakse edasi ainult seadusega nõutud ulatuses või eesmärkidel, milleks neid avalikustati sellele isikule, ning see isik teavitab Äripartnerit igast juhtumist, mille puhul on ta teadlik selliste andmete konfidentsiaalsuse rikkumisest.

4. KLIENDI KOHUSTUSED

4.1. Klient ei tohi anda Äripartnerile korraldust tegutseda viisil, mis ei oleks kooskõlas HIPAA reeglitega.

4.2. Klient teavitab Äripartnerit kõigist piirangutest oma Kliendi privaatsustavade teatises kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.520, kui selline piirang võib mõjutada Kaitstud terviseandmete Kasutamist või Avalikustamist Äripartneri poolt.

4.3. Klient peab teavitama Äripartnerit, kui Füüsiliselt isikult saadud luba tema Kaitstud terviseandmete Kasutamiseks või Avalikustamiseks on muutunud või tagasi võetud, kui selline muudatus võib mõjutada seda, kuidas Äripartner tohib Kaitstud terviseandmeid Kasutada või Avalikustada.

4.4. Klient teavitab Äripartnerit kirjalikult kõigist Kaitstud terviseandmete Kasutamise või Avalikustamisega seotud keeldudest, millega Klient on nõustunud, kooskõlas Ameerika Ühendriikide föderaalõigusaktide koodeksi 45. jaotise §-ga 164.522, kui selline keeld võib mõjutada Kaitstud terviseandmete Kasutamist või Avalikustamist Äripartneri poolt.

5. TÄHTAEG JA LÕPETAMINE

5.1. See Äripartnerileping hakkab kehtima Jõustumise kuupäeval ning lõpetab kehtivuse automaatselt järgmiste hulgast hiliseima toimumisel: (i) Teenuselepingu aegumine või (ii) kui kõik Kliendi poolt Äripartnerile esitatud Kaitstud terviseandmed on hävitatud või Kliendile tagastatud.

5.2. Kui pool saab teada, et teine pool on Äripartnerilepingut oluliselt rikkunud, annab mitterikkunud poole rikkunud poolele võimaluse rikkumine heastada. Kui rikkunud pool ei heasta rikkumist kolmekümne (30) päeva jooksul pärast seda, kui rikkunud pool on saanud mitterikkunud poolelt kirjaliku teate sellise

olulise rikkumise üksikasjade kohta, on mitterikkunud poolel õigus lõpetada see Äripartnerileping ja Teenuseleping kooskõlas Teenuselepingu tingimustega, või juhul, kui lõpetamine pole võimalik, teatada probleemist Ameerika Ühendriikide tervishoiu- ja teenindusministrile või mis tahes muule pädevale asutusele.

5.3. Lõpetamise mõju:

5.3.1.1. Välja arvatud juhul, mida on kirjeldatud järgnevalt punktis 5.3.2, kui see Äripartnerileping mis tahes põhjusel lõpetatakse, peab Äripartner tagastama või hävitama kõik Kliendilt saadud Kaitstud terviseandmed kooskõlas Teenuselepinguga. See säte kehtib ka Kaitstud terviseandmetele, mis on Äripartneri alltöövõtjate või esindajate valduses. Äripartner ei tohi säilitada Kaitstud terviseandmetest ühtki koopiat.

5.3.1.2. Juhul, kui Äripartner teeb kindlaks, et Kaitstud terviseandmete tagastamine või hävitamine pole võimalik, peab Äripartner teatama Kliendile tingimused, mis teevad tagastamise või hävitamise võimatuks. Pärast Kliendi teavitamist peab Äripartner rakendama selles Äripartnerilepingus toodud kaitseid sellistele Kaitstud terviseandmetele ning piirama selliste Kaitstud terviseandmete edasist Kasutamist või Avalikustamist ainult eesmärkidele, mis teevad tagastamise või hävitamise võimatuks, kuni Äripartner säilitab selliseid Kaitstud terviseandmeid kooskõlas Teenuselepingu tingimustega.

6. MUU

6.1. Kahju hüvitamine. Äripartner nõustub hüvitama Kliendile kõik trahvid või karistused, mis on määratud Kliendile mis tahes täitemenetluse raames, mille on algatanud Ameerika Ühendriikide tervishoiu- ja teenindusminister, või mis tahes tsiviilmenetluse raames, mille on algatanud osariigi peaprokurör Kliendi vastu, kui see menetlus või kohtuasi tuleneb otseselt ja täielikult Äripartneri mis tahes tegevusest või tegematajätmisest, mis kujutas HIPAA reeglite rikkumist või selle Äripartnerilepingu olulist rikkumist („Nõue“). Äripartner ei ole kohustatud hüvitama Kliendile mingis osas trahve või karistusi, mis tulenevad (i) HIPAA reeglite või selle Äripartnerilepingu rikkumisest Kliendi poolt või (ii) Kliendi hooletusest või tahtlikest tegudest või tegematajätmistest. Eespool kirjeldatud hüvitamise kohustus on sõnaselgelt tingimuslik ning eeldab seda, et Klient annab Äripartnerile õiguse, Äripartneri kulul ja äranägemisel ning Äripartneri valitud kaitsjaga, juhtida mis tahes sellise Nõude eest kaitsmist või sellest osa võtta, kui aga selline nõue on osa mõnest suuremast menetlusest või kohtuasjast, piirdub Äripartneri õigus juhtida või osaleda ainult Nõudega, mitte suurema menetluse või kohtuasjaga. Juhul, kui Äripartner kasutab oma õigust kaitset juhtida, siis (i) Äripartner ei lähe kokkuleppele ühegi nõudega, mis nõuab Kliendipoolse vea tunnistamist saamata selleks Kliendilt eelnevat kirjalikku luba, (ii) Kliendil on õigus osaleda, omal kulul, nõudes või hagis, ning (iii) Klient peab tegema Äripartneriga mõistlikku koostööd. Eespool toodu on Kliendi üheks ja ainsaks parandusmeetmeks ning Äripartneri ainsaks vastutuseks mis tahes kahjude, kahjustuste, kulude või vastutuse eest, mis kliendil on tekkinud seoses mis tahes Nõudega seoses selle Äripartnerilepinguga.

6.2. Tõkend. Äripartner nõustub sellega, et igasugune Kaitstud terviseandmete volitamata Kasutamine või Avalikustamine Äripartneri poolt võib tekitada Kliendile korvamatut kahju, mille eest on Kliendil õigus, kui ta otsustab seda teha, nõuda tõkendi või muu samaväärse keelu kohaldamist.

6.3. Viited õigusaktidele. Kõik viited selles Äripartnerilepingus HIPAA reeglite kindlale osale tähendavad vastavat HIPAA, privaatsusreegli, turbereegli, HITECH-seaduse või lõpliku koondreegli osa koos kõigi selle parandustega, mis kehtib ja millele vastavust nõutakse.

6.4. Muudatused. Pooled nõustuvad heas usus rääkima läbi kõiki selle Äripartnerilepingu muudatusi, mis võivad olla aeg-ajalt vajalikud, et Klient või Äripartner saaks täita HIPAA reeglite nõudeid. Kui pooled ei jõua mis tahes sellise muudatuse tingimuste osas kokkuleppele kuuekümne (60) päeva jooksul alates mis tahes sellise kirjaliku taotluse esitamist Kliendi poolt Äripartnerile, on mõlemal poolel õigus lõpetada see Äripartnerileping ja Teenuseleping, teatades sellest teisele poolele vähemalt kolmkümmend (30) päeva ette.

6.5. Kolmandast isikust soodustatud isikute puudumine. Mitte miski selles Äripartnerilepingus ei anna otseselt või kaudselt ega pole mõeldud andma otseselt või kaudselt midagi ühelegi isikule peale Kliendi, Äripartneri ja nende vastavate õigusjärglaste, ega loovuta ühtki õigust, parandusmeedet, kohustustust ega vastustust.

6.6. Sõltumatu töövõtja. Äripartner, sealhulgas tema direktorid, juhid, töötajad ja esindajad, on Kliendi või tema personali sõltumatud töövõtjad, mitte esindajad (nagu on defineeritud Ameerika Ühendriikide föderaalses esinduse tavaõiguses). Eeltoodut piiramata, pole Kliendil mingisugust õigust kontrollida, suunata ega muul viisil mõjutada Äripartnerit teenuste osutamise ajal peale selle Äripartnerilepingu või Teenuselepingu või nende kahepoolselt kokku lepitud muudatuste jõustamise.

6.7. Järjestus; terviklik leping. Kui selles Äripartnerilepingus on mis tahes vasturääkivusi, tuleb need lahendada selliselt, et pooled saaks täita HIPAA reegleid. See Äripartnerileping moodustab tervikliku lepingu poolte vahel, mis reguleerib selle teemat, ning alistab kõik varasemad läbirääkitud tingimused, avaldused, kokkulepped ja lepingud, mis on seotud HIPAA reeglitega, sealhulgas kõik varasemad poolte vahel sõlmitud äripartnerilepingud.