Duomenų tvarkymo sutartis

PASKIRTIS IR EILIŠKUMO TVARKA

Ši Duomenų tvarkymo sutartis kartu su jos priedais ir visais dokumentais, į kuriuos yra aiškios kryžminės-nuorodos (toliau –**DTS**), laikoma „Iron Mountain“ ir Kliento paslaugų sutarties (toliau – **Sutartis**) dalimi. Sutarties sąlygos taikomos ir jos reglamentuoja šios DTS šalių teises ir pareigas.

Jei kurios nors šioje DTS nustatytos sąlygos prieštarauja Sutartyje nustatytoms sąlygoms, DTS dalyko atžvilgiu pirmenybė teikiama šioje DTS nustatytoms sąlygoms. Ši DTS pakeičia ir pakeičia visus ankstesnius šalių susitarimus dėl duomenų tvarkymo arba duomenų apsaugos ar privatumo sąlygas, susijusias su pagal Sutartį teikiamomis paslaugomis.

BENDROSIOS SĄLYGOS

1. APIBRĖŽTYS

Jei šiame dokumente nėra konkrečiai apibrėžta, visos didžiosiomis raidėmis rašomos sąvokos turi tą pačią reikšmę, kaip ir Sutartyje.

Duomenų valdytojas – fizinis ar juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri viena ar kartu su kitais nustato asmens duomenų tvarkymo tikslus ir priemones;

Kliento asmens duomenys – asmens duomenys, priklausantys Klientui ar jo filialams arba surinkti Kliento ar jo susijusių įmonių, tvarkomi teikiant Paslaugas;

Duomenų subjektas – fizinis asmuo, kurio tapatybė nustatyta, arba gali būti nustatyta;

Duomenų apsaugos teisės aktai – visi taikytini įstatymai ir kiti teisės aktai, susiję su asmens duomenų tvarkymu, kurie gali būti taikomi atitinkamose jurisdikcijose, įskaitant, bet neapsiribojant, ES BDAR (Reglamentas (ES) 2016/679), JK BDAR (BDAR, taikomas kaip JK vidaus teisės dalis pagal 2018 m. Europos Sąjungos (išstojimo) įstatymo 3 skirsnį ir su pakeitimais, padarytais Duomenų apsaugos, privatumo ir elektroninių ryšių (pakeitimai ir kt.) (išstojimas iš ES) 2019 m. reglamentai (su pakeitimais)), 2018 m. Duomenų apsaugos įstatymas, FADP (Šveicarijos federalinis duomenų apsaugos įstatymas), JAV valstijų privatumo įstatymai, LGPD (Brazilijos bendrasis duomenų apsaugos įstatymas), PIPL (Kinijos Liaudies Respublikos asmens duomenų apsaugos įstatymas) ir visi teisės aktai ir (arba) reglamentai, kuriais jie įgyvendinami arba priimami pagal juos, arba kurie iš dalies keičia, pakeičia, iš naujo priima ar konsoliduoja bet kurį iš jų, įskaitant, kai taikoma, priežiūros institucijų paskelbtas gaires ir praktikos kodeksus;

Asmens duomenys – bet kokie su duomenų subjektu susiję duomenys;

Duomenų tvarkytojas – fizinis ar juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri tvarko asmens duomenis duomenų valdytojo vardu;

Duomenų tvarkymas – bet kokia operacija ar operacijų rinkinys, atliekamas su asmens duomenimis ar asmens duomenų rinkiniais automatizuotomis arba neautomatizuotomis priemonėmis, pavyzdžiui, rinkimas, įrašymas, organizavimas, struktūrizavimas, saugojimas, adaptavimas ar keitimas, paieška, susipažinimas, naudojimas, atskleidimas perduodant, platinant ar kitaip padarant juos prieinamus, lyginimas ar derinimas, apribojimas, ištrynimas ar sunaikinimas;

Duomenų saugumo pažeidimas – bet koks atsitiktinis ar neteisėtas Kliento asmens duomenų, kuriuos „Iron Mountain“, jos darbuotojai ar subrangovai tvarko teikdami paslaugas, sugadinimas, sunaikinimas, praradimas, praradimas, pakeitimas, neteisėtas atskleidimas ar prieiga prie jų;

Paslaugos – bet kokios „Iron Mountain“ ar jos susijusių įmonių klientui pagal Sutartį teikiamos paslaugos;

JAV valstijų privatumo įstatymai – visi JAV valstijos privatumo ir duomenų apsaugos įstatymai, kurie taikomi tvarkant asmens duomenis pagal šią Sutartį, be kita ko, toliau nurodytieji, ir kurie kartais gali būti iš dalies pakeisti, papildyti ar pakeisti: 1) Kalifornijos vartotojų privatumo įstatymas su pakeitimais, padarytais Kalifornijos privatumo teisių įstatymu, ir visi su juo susiję įgyvendinimo reglamentai (toliau kartu –– **CCPA**); 2) Kolorado

privatumo įstatymas (toliau – **CPA**); 3) Virdžinijos vartotojų duomenų apsaugos įstatymas (toliau –– **CDPA**); 4) Jutos vartotojų privatumo įstatymas (toliau –– **UCPA**); ir 5) Konektikuto duomenų privatumo įstatymas (toliau –– **CTDPA**).

2. DUOMENŲ TVARKYMO APIMTIS IR IŠSAMESNĖ INFORMACIJA

2.1 Ši BDAR taikoma kliento asmens duomenims, kuriuos tvarko „Iron Mountain“, kaip duomenų tvarkytojas, teikdamas paslaugas pagal Sutartį kliento vardu.

2.2 „Iron Mountain“ gali rinkti ir tvarkyti kliento ir jos susijusių įmonių darbuotojų asmens duomenis kaip valdytojas teisėtais verslo tikslais, pavyzdžiui, sutarčių ir santykių su klientais valdymo tikslais, vadovaudamasi duomenų apsaugos teisės aktais ir „Iron Mountain“ privatumo pranešimu, kurį galima rasti „Iron Mountain“ interneto svetainėse, bei kitomis taikomomis privatumo taisyklėmis. Šioje DTS nustatyti „Iron Mountain“ įsipareigojimai tokiam asmens duomenų tvarkymui netaikomi.

2.3 Asmens duomenys tvarkomi siekiant teikti paslaugas. Šioje DTS apibrėžtos kliento ir „Iron Mountain“ teisės ir pareigos. Šios DTS 1 priede pateikiamas tvarkymo pobūdis, trukmė ir tikslas, klientų asmens duomenų tipai, kuriuos tvarko „Iron Mountain“, ir duomenų subjektų, kurių asmens duomenys tvarkomi, kategorijos.

2.4 Kai teikdama paslaugas „Iron Mountain“ tvarko kliento asmens duomenis, „Iron Mountain“:

2.4.1 tvarko kliento asmens duomenis tik pagal dokumentais patvirtintus kliento nurodymus; Jei pagal taikomus teisės aktus, „Iron Mountain“ privalo tvarkyti kliento asmens duomenis bet kokiu kitu tikslu, „Iron Mountain“ pirmiausia informuos klientą apie šį reikalavimą, išskyrus atvejus, kai tokie teisės aktai draudžia tai daryti dėl svarbių viešojo intereso priežasčių; ir

2.4.2 visada laikosi galiojančių duomenų apsaugos teisės aktų ir nedelsiant praneša klientui, jei, „Iron Mountain“ nuomone, kliento pateiktas jo asmens duomenų tvarkymo nurodymas pažeidžia galiojančius duomenų apsaugos teisės aktus.

2.5 Kliento nurodymai bus privalomi bendrovei „Iron Mountain“, išskyrus atvejus, kai nurodymams įvykdyti reikia suteikti paslaugą pagal Sutartį, o klientas nesutinka mokėti paslaugų mokesčių už tokias paslaugas.

2.6 Bendrovė „Iron Mountain“ užtikrina, kad darbuotojai, turintys prieigą prie kliento asmens duomenų, būtų saistomi konfidencialumo pareigos tokių kliento asmens duomenų atžvilgiu, ir imasi pagrįstų priemonių, kad užtikrintų bendrovės „Iron Mountain“ darbuotojų, turinčių prieigą prie kliento asmens duomenų, patikimumą ir kompetenciją.

3. PAGALBOS TEIKIMAS KLIENTAMS

3.1 „Iron Mountain“ teikia pagalbą klientui, visada atsižvelgdama į duomenų tvarkymo pobūdį:

3.1.1 tinkamomis techninėmis ir organizacinėmis priemonėmis ir kiek tai įmanoma, vykdant kliento įsipareigojimus atsakyti į duomenų subjektų, besinaudojančių savo teisėmis, prašymus;

3.1.2 užtikrindama kliento prievolių laikymąsi (pavyzdžiui, duomenų tvarkymo saugumas, pranešimas priežiūros institucijai apie asmens duomenų saugumo pažeidimą, pranešimas duomenų subjektui apie asmens duomenų saugumo pažeidimą, poveikio duomenų apsaugai vertinimas ir išankstinės konsultacijos su priežiūros institucijomis, jei dėl duomenų tvarkymo kiltų didelis pavojus, jei duomenų valdytojas nesiimtų priemonių rizikai sumažinti), atsižvelgiant į „Iron Mountain“ turimą informaciją; ir

3.1.3 pateikdama klientui visą informaciją, kurios klientas pagrįstai prašo, kad Klientas galėtų įrodyti, jog jo įsipareigojimai pasirenkant ir paskiriant „Iron Mountain“ buvo įvykdyti.

4. SAUGUMO PRIEMONĖS

4.1. Atsižvelgdama į įprastas veiklos procedūras, įgyvendinimo sąnaudas ir tvarkymo pobūdį, apimtį, kontekstą bei tikslus, „Iron Mountain“ įgyvendina tinkamas ir pagrįstas technines ir organizacines priemones, skirtas apsaugoti kliento asmens duomenų konfidencialumą, vientisumą ir prieinamumą bei apsaugoti kliento asmens duomenis nuo neleistino ar neteisėto tvarkymo ir nuo atsitiktinio praradimo, sunaikinimo, sugadinimo, pakeitimo ar atskleidimo. „Iron Mountain“ saugumo standartai yra išdėstyti šios DTS 2 priede.

4.2. Ar šios techninės ir organizacinės priemonės atitinka Kliento reikalavimus privalo vertinti tik klientas.

5. ATITIKTIS TEISĖS AKTAMS

Klientas ir jo susijusios įmonės: i) tvarko kliento asmens duomenis laikydamiesi duomenų apsaugos teisės aktų; ii) yra įgalioti duoti raštiškus nurodymus bendrovei „Iron Mountain“ dėl kliento asmens duomenų tvarkymo, susijusio su paslaugomis (įskaitant bet kurio trečiosios šalies subjekto, kuris yra

kliento asmens duomenų valdytojas, vardu); ir iii) duomenis tvarkydami visada išlaiko kliento asmens duomenų kontrolę ir įgaliojimus.

6. PAGALBINIS DUOMENŲ TVARKYMAS

6.1. Klientas pripažįsta ir sutinka, kad „Iron Mountain“ gali pasitelkti savo patronuojančiąją bendrovę, jos susijusias įmones ir kitus trečiųjų šalių subtiekėjus (įskaitant trečiųjų šalių subtiekėjus, kuriuos pasitelkia „Iron Mountain“ susijusioji įmonė arba patronuojančioji bendrovė), kad šie tvarkytų kliento asmens duomenis pagal šią DTS, atsižvelgiant į toliau esantį 6.2. punktą.

6.2. Užsakovo patvirtintų pagalbinių duomenų tvarkytojų sąrašas, galiojantis nuo šios DTS sudarymo dienos, pateikiamas čia[1]. „Iron Mountain“ gali bet kuriuo metu pakeisti arba paskirti naują pagalbinį duomenų tvarkytoją su sąlyga, kad klientas bus įspėtas raštu prieš penkiolika (15) dienų ir per tą laiką klientas neprieštaraus tokiems pakeitimams dėl akivaizdžių priežasčių, susijusių su duomenų apsauga.. Norėdamas gauti šiuos pranešimus el. paštu, klientas užsiprenumeruoja ir tvarko bet kokią esamą „Iron Mountain“ pranešimų paslaugos prenumeratą per šią svetainę[2].

6.3. Jei klientas neprisijungia prie šios pranešimo paslaugos, „Iron Mountain“ neatsako už tai, kad apie pagalbinį tvarkytoją nebuvo pranešta, ir visi tokie paskyrimai laikomi kliento patvirtintais**.** Jei klientas per penkiolika (15) dienų iki rašytinio pranešimo raštu pateikia prieštaravimą dėl įrodomų priežasčių, susijusių su duomenų apsauga, dėl pakaitinio ar naujo pagalbinio duomenų tvarkytojo paskyrimo, tuomet „Iron Mountain“ deda protingas pastangas pakeisti klientui teikiamas paslaugas arba rekomenduoti klientui apsvarstyti galimybę konfigūruoti paslaugas arba pakeisti naudojimosi jomis tvarką, kiekvienu atveju užtikrindama, kad kliento asmens duomenys nebūtų tvarkomi pagalbinio tvarkytojo, dėl kurio klientas yra pareiškęs prieštaravimą. Jei klientas per penkiolika (15) dienų nepritaria bet kokiems tokiems „Iron Mountain“ pasiūlytiems pakeitimams, bendrovė „Iron Mountain“, raštu pranešusi klientui, gali nedelsdama nutraukti paslaugos arba paslaugos dalies, kurios bendrovė „Iron Mountain“ negali teikti nenaudodama pagalbinio duomenų tvarkytojo, dėl kurio klientas buvo pareiškęs prieštaravimą, teikimą. Toks paslaugų nutraukimas neturi įtakos jokioms įgytoms šalių teisėms ir įsipareigojimams, su sąlyga, kad „Iron Mountain“ ar „Iron Mountain“ filialai susijusios įmonės dėl tokio nutraukimo nemokės jokių nutraukimo mokesčių, išlaidų ar kitų kompensacijų, o klientas nedelsdamas perims turtą, kurį jis suteikė „Iron Mountain“ nutraukdamas paslaugų teikimą, laikydamasis Sutarties sąlygų ir savo sąskaita bei lėšomis.

6.4. „Iron Mountain“ užtikrina, kad bet kurioje sutartyje su pagalbiniais duomenų tvarkytojais, kuriems taikoma ši DTS, būtų nuostatos, kurios visais esminiais atžvilgiais yra tokios pačios kaip šioje DTS ir atitinka galiojančių duomenų apsaugos teisės aktų reikalavimus. Jei naudojant pagalbinį duomenų tvarkytoją „Iron Mountain“ pažeidžia savo įsipareigojimus pagal šią DTS arba bet kuriuos taikomus duomenų apsaugos teisės aktus, „Iron Mountain“ lieka visiškai atsakinga klientui už „Iron Mountain“ įsipareigojimų pagal šias sąlygas vykdymą.

7. SAUGUMO PAŽEIDIMAI

7.1. Įtarusi saugumo pažeidimą „Iron Mountain“:

7.1.1. nedelsdama imasi veiksmų įtariamam saugumo pažeidimui ištirti, įtariamam saugumo pažeidimui nustatyti, užkirsti jam kelią, sušvelninti jo poveikį ir ištaisyti saugumo pažeidimą;

7.1.2. nedelsdama informuoja klientą, pakankamai įsitikinęs, kad saugos pažeidimas įvyko, ir pateikti klientui išsamų saugos pažeidimo aprašymą, įskaitant informaciją, kuri pagrįstai reikalinga, kad klientas įvykdytų pranešimo įsipareigojimus pagal duomenų apsaugos teisės aktus.

7.2. Klientas sutinka, kad „Iron Mountain“ gali pateikti 7.1.2 punkte nurodytą informaciją etapais. Jeigu „Iron Mountain“ neturi prieigos prie tam tikros 7.1.2 punkte nurodytos informacijos arba negali jos pateikti Klientui, „Iron Mountain“ apie tai informuoja klientą ir neprisiima atsakomybės už tokios informacijos nepateikimą.

8. AUDITAI

„Iron Mountain“ leis klientui ir jo atitinkamiems auditoriams arba įgaliotiesiems atstovams, įspėjus „Iron Mountain“ ne mažiau kaip prieš dešimt (10) darbo dienų, atlikti auditą arba patikrinimus sutarties galiojimo metu, su sąlyga, kad „Iron Mountain“ nebus reikalaujama suteikti arba leisti prieigą prie informacijos apie: i) kitus „Iron Mountain“ klientus; ii) bet kokias neviešas „Iron Mountain“ išorės ataskaitas; ir iii) bet kokias vidines ataskaitas, parengtas „Iron Mountain“ vidaus audito arba atitikties tarnybos. Auditas ar patikrinimas pagal šį punktą atliekamas tik siekiant patikrinti, ar bendrovė „Iron Mountain“ tvarko kliento asmens duomenis laikydamasi savo įsipareigojimų pagal šią DTS. Nebent

[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=

įvyktų duomenų saugumo pažeidimas, per bet kurį dvylikos (12) mėnesių laikotarpį atliekamas ne daugiau kaip vienas toks auditas.

9. TARPTAUTINIS DUOMENŲ PERDAVIMAS (RIBOTI PERDAVIMAI)

9.1. Tiek, kiek taikytina, klientas sutinka ir leidžia tarptautiniu mastu perduoti kliento asmens duomenis subjektams, kaip nurodyta 6.2 skirsnyje ir pagal 3 priedą dėl paslaugų teikimo, o Klientas ir „Iron Mountain“ susitaria:

9.1.1. laikytis galiojančių duomenų apsaugos teisės aktų, susijusių su tokiu perdavimu;

9.1.2. kad jie, be apribojimų, atsižvelgdami į: i) kliento asmens duomenų kategorijas, ii) šalis, kurių nacionaliniai įstatymai gali nesuteikti tokio asmens duomenų apsaugos lygio, kuris būtų panašus į ES/JK teisės aktų lygį (toliau – **Trečioji šalis**), iii) atitinkamas technines ir organizacines priemones, nurodytas 7 skirsnyje, ir iv) atitinkamas šalis, dalyvaujančias tvarkant tokius kliento asmens duomenis, atliko atitinkamo perdavimo mechanizmo, priimto pagal šį reglamentą, tinkamumo vertinimą, kai reikalaujama pagal įstatymą ir nustatė, kad toks perdavimo mechanizmas yra tinkamai sukurtas siekiant užtikrinti, kad pagal šį DTS perduodamiems asmens duomenims paskirties šalyje būtų suteiktas toks apsaugos lygis, iš esmės lygiavertis garantuojamam pagal duomenų apsaugos teisės aktus.

10. ATSAKOMYBĖ IR ŽALOS ATLYGINIMAS

10.1. Nepaisant Sutartyje numatytų priešingų nuostatų, jeigu „Iron Mountain“ pažeidus įsipareigojimus pagal šią DTS pažeidžiamas duomenų saugumas, „Iron Mountain“ kompensuoja klientui tiek, kiek leidžia galiojantys įstatymai už tiesiogines, patikrinamas, būtinas kliento dėl trečiosios šalies patirtas išlaidas: a) tiriant saugumo pažeidimą; b) rengiant ir siunčiant pranešimus tokiems duomenų subjektams ir reguliavimo institucijoms, kaip reikalaujama pagal Duomenų apsaugos teisės aktus, c) teikiant kredito stebėjimo paslaugas tokiems asmenims, kaip reikalaujama pagal įstatymą ne ilgesniam kaip dvylikos (12) mėnesių laikotarpiui, ir d) mokant priežiūros institucijos nustatytą baudų, nuobaudų ar sankcijų dalį, už kurią priežiūros institucijos nurodymu yra tiesiogiai atsakinga „Iron Mountain“.

10.2. Jei duomenų subjektas pareiškia ieškinį vienai arba abiem šalims dėl tariamo duomenų apsaugos teisės aktų pažeidimo (toliau – **Duomenų subjekto pretenzijos**), kai tai leidžiama, kiekviena šalis turi kontroliuoti savo gynybą dėl bet kokio tokio reikalavimo (ar jo dalies), ir lieka visiškai atsakinga už savo sąnaudas, išlaidas ir su tuo susijusius įsipareigojimus, įskaitant teisinius mokesčius arba bet kokias sumas, kurias jai priteisė teismas arba sumokėjo taikos sutartimi, tačiau jei kiekviena šalis yra atsakinga už dalį arba bet kuri šalis yra atsakinga už visą žalą, kurią duomenų subjektas patyrė dėl to paties incidento ar kelių tokių incidentų, o duomenų subjektas išieškojo visą kompensaciją tik iš vienos šalies (toliau – **kompensuojanti šali**s), tada kompensuojanti šalis turi teisę reikalauti iš kitos šalies kompensacijos dalį, atitinkančią tos kitos šalies padarytą žalą. Kompensuojančioji šalis savo reikalavimą kitai šaliai gali pareikšti tik per 12 mėnesių nuo incidento, kiek tai leidžiama pagal taikytiną teisę.

10.3. Didžiausia galiojančių įstatymų leidžiama apimtimi, įsipareigojimų apribojimai ir bet kokios šioje sutartyje nustatytos pažeidimų išimtys reglamentuoja bendrą atsakomybę dėl visų kliento pretenzijų, kylančių dėl šios DTS ir (arba) „Iron Mountain“ sutarties arba su ja susijusias. Šie atsakomybės apribojimai ir išimtys dėl žalos atlyginimo taikomi visiems reikalavimams, kylantiems pagal sutartį, deliktą ar bet kokią kitą atsakomybės teoriją, o bet kokia nuoroda į „Iron Mountain“ atsakomybę reiškia bendrą „Iron Mountain“ ir visų „Iron Mountain“ susijusių įmonių atsakomybę už kliento ir visų kitų kliento susijusių įmonių reikalavimus. Tiek, kiek to reikalauja galiojantys įstatymai, šiuo skirsniu nesiekiama i) pakeisti ar apriboti šalių atsakomybės už duomenų subjekto pretenzijas, pareikštas šaliai, kai atsakomybė yra solidari, arba ii) apriboti bet kurios iš šalių atsakomybės sumokėti baudas, kurias tokiai šaliai skiria reguliavimo institucija.

10.4. 10.1–10.3 punktuose nurodyta vienintelė ir išimtinė kiekvienos šalies teisių gynimo priemonė ir vienintelė kiekvienos šalies atsakomybė už bet kokius su šia DTS susijusius nuostolius, žalą, išlaidas ar atsakomybę.

11. VALDŽIOS INSTITUCIJŲ PRAŠYMAI

11.1. Jeigu leidžiama pagal teisės aktus ir atsižvelgiant į toliau esančius 11.2–11.5 punktus „Iron Mountain“ sutinka pranešti klientui, jeigu „Iron Mountain“:

11.1.1. gauna teisiškai privalomą valdžios institucijos, įskaitant teismų įstaigas, prašymą pagal paskirties šalies įstatymus atskleisti pagal Sutartį perduotus kliento asmens duomenis; arba

11.1.2. sužino apie bet kokią tiesioginę valdžios institucijų prieigą prie kliento asmens duomenų, perduotų pagal Sutartį, pagal paskirties šalies įstatymus..

11.2. Jei pagal paskirties šalies įstatymus „Iron Mountain“ draudžiama pranešti klientui, „Iron Mountain“ sutinka dėti visas pastangas, kad toks draudimas jai nebūtų taikomas, siekdama kuo greičiau perduoti kuo daugiau informacijos.

11.3. „Iron Mountain“ sutinka peržiūrėti prašymo atskleisti informaciją teisėtumą, ypač tai, ar jis atitinka prašančiajai valdžios institucijai suteiktus įgaliojimus, ir užginčyti prašymą, jei nuspręs, kad yra pagrįstų priežasčių manyti, jog pagal paskirties šalies įstatymus toks prašymas yra neteisėtas. „Iron Mountain“ atskleidžia prašomus kliento asmens duomenis tik jeigu reikalaujama pagal galiojančias procedūrines taisykles.

11.4. „Iron Mountain“ sutinka pateikti mažiausią leistiną informacijos kiekį, atsakydama į prašymą atskleisti informaciją, remdamasi pagrįstu prašymo aiškinimu.

11.5. „Iron Mountain“ sutinka saugoti šiame punkte nurodytą informaciją visą Sutarties galiojimo laikotarpį ir, gavusi prašymą, pateikti ją kompetentingai priežiūros institucijai.

12. ĮVAIRIOS NUOSTATOS

12.1. Atsižvelgiant į „Iron Mountain“ teikiamų Paslaugų pobūdį, nutraukus Sutartį ir (arba) jai pasibaigus, remdamasi konkrečiais kliento nurodymais ir laikydamasi Sutarties sąlygų, „Iron Mountain“ ištrina ir (arba) sunaikina arba grąžina klientui arba kliento nurodytai trečiajai šaliai visus Kliento asmens duomenis. Visi kliento asmens duomenys, esantys kliento turte, kurį „Iron Mountain’ saugo Kliento vardu, bus grąžinti Klientui pagal sutartą pasitraukimo arba perėjimo planą, už šalių susitarimu nustatytą- mokestį, kaip nurodyta Sutartyje arba kitame taikomame sutartiniame dokumente. Visais kitais atvejais, jei Sutartyje nieko nepasakyta apie kliento asmens duomenų ištrynimą (sunaikinimą) ar grąžinimą, o klientas per 15 (penkiolika) dienų nuo Sutarties nutraukimo (galiojimo pabaigos) nepateikia jokių nurodymų dėl jo asmens duomenų ištrynimo (sunaikinimo) ar grąžinimo, „Iron Mountain“ išsiunčia klientui rašytinį pranešimą, prašydama per 15 (penkiolika) dienų gauti konkrečius nurodymus dėl Kliento asmens duomenų ištrynimo (sunaikinimo) ar grąžinimo ir informuodama klientą apie visus taikomus saugaus sunaikinimo ar kitus kliento mokėtinus mokesčius. Jei Klientas per tokį penkiolikos (15) dienų laikotarpį nepateikia raštiškų nurodymų ir per tą patį laikotarpį nesumoka taikomų mokesčių, Klientas įgalioja „Iron Mountain“ toliau tvarkyti, ištrinti ir sunaikinti visus Kliento asmens duomenis po Sutarties nutraukimo „Iron Mountain“ pasirinkimu ir Kliento sąskaita.

12.2. Nepaisant 12.1punkto nuostatų, „Iron Mountain“ nepažeidžia savo įsipareigojimų dėl atsarginėse juostose saugomų kliento asmens duomenų ištrynimo tol, kol tokios atsarginės juostos pakeičiamos (ir taip ištrinami kliento asmens duomenys) vykdant įprastą veiklą.

12.3. Išskyrus standartines sutarties sąlygas (kaip apibrėžta šios DTS 3 priede), šiai DTS ir bet kokiam ginčui, pretenzijai ar nesutarimui, kylančiam dėl šios DTS, jos pažeidimo, nutraukimo ar galiojimo, taikoma Sutarties nuostata dėl teisės pasirinkimo; bet kokį ginčą, nesutarimą ar pretenziją, kylančią dėl šios DTS ar su ja susijusią, visų pirma bus siekiama išspręsti taikant bet kurį Sutartyje nustatytą ginčų sprendimo procesą.

12.4. Kiekviena šalis kartkartėmis gali raštu pranešti kitai šaliai apie bet kokius šios DTS pakeitimus, kurie, šalies nuomone, yra būtini siekiant laikytis duomenų apsaugos teisės aktų reikalavimų arba priežiūros institucijos ar kompetentingo teismo sprendimo. Bet kokie tokie pakeitimai įsigalioja tik tuo atveju ir tokia apimtimi, kaip nustatyta abiejų šalių pasirašytame abipusiškai suderintame šios DTS pakeitime, išskyrus atvejus, kai viena šalis informuoja kitą šalį apie bet kokį naują teisinį reikalavimą ir išsiunčia tokį pakeitimą, į kurį įtraukiami tik būtini pakeitimai ir kuris gali būti priimtas be oficialaus sutikimo, t. y. per tam tikrą terminą nepateikus jokių prieštaravimų, laikomas abipusiškai suderintu šios DTS pakeitimu.

1 PRIEDAS

Informacija apie duomenų tvarkymą ir perdavimą (jeigu taikoma)

A. ŠALIŲ SĄRAŠAS:

Šios DTS šalys ir duomenų eksportuotojo bei duomenų importuotojo vaidmenys nurodyti Sutartyje ir 3 priede (Tarptautinis duomenų perdavimas), jei taikoma.

B. DUOMENŲ TVARKYMO IR PERDAVIMO APRAŠAS (jeigu taikoma):

Duomenų subjektų, kurių duomenys tvarkomi, arba kuriems jie perduodami, kategorijos:

Priklausomai nuo „Iron Mountain“ paslaugų pobūdžio ir kliento verslo, klientas gali pateikti „Iron Mountain“ įvairioms duomenų subjektų kategorijoms priklausančius asmens duomenis, kurių apimtį savo nuožiūra nustato ir kontroliuoja klientas. Todėl duomenų subjektų kategorijos gali būti šios: buvę ir esami darbuotojai; buvę ir esami rangovai ar konsultantai; agentūrų samdomi rangovai ar konsultantai ir išorės komandiruotieji darbuotojai; kandidatai ir pretendentai į darbą; studentai ir savanoriai; asmenys, kuriuos darbuotojai ar pensininkai nurodė kaip naudos gavėjus, sutuoktinius, šeimos ir (arba) civilinius partnerius, išlaikytinius ir skubios pagalbos kontaktus; pensininkai; buvę ir esami direktoriai ir pareigūnai; akcininkai; obligacijų turėtojai; sąskaitų turėtojai; galutiniai naudotojai ir (arba) vartotojai (suaugusieji, vaikai); pacientai (suaugusieji, vaikai); praeiviai (vaizdo stebėjimo kameros); ir svetainių naudotojai.

Tvarkomų / perduodamų asmens duomenų kategorijos:

Priklausomai nuo „Iron Mountain“ paslaugų pobūdžio ir kliento verslo, klientas gali pateikti „Iron Mountain“ asmens duomenis, priklausančius įvairioms asmens duomenų kategorijoms, kurių apimtį savo nuožiūra nustato ir kontroliuoja klientas. Todėl tai gali būti asmens duomenys, susiję su klientu ir (arba) kliento klientais, darbuotojais ir kt.

Perduodami neskelbtini duomenys (jeigu taikoma):

Priklausomai nuo „Iron Mountain“ paslaugų pobūdžio ir kliento verslo, klientas gali pateikti „Iron Mountain“ neskelbtinus duomenis, kurių apimtį savo nuožiūra nustato ir kontroliuoja klientas.

Jei taikoma, duomenų perdavimo dažnumas (pvz., ar duomenys perduodami vieną kartą, ar nuolat):

Duomenys perduodami nuolat.

Duomenų tvarkymo pobūdis:

Rinkimas, įrašymas, organizavimas, struktūrizavimas, saugojimas, adaptavimas ar keitimas, paieška, konsultavimas, naudojimas, atskleidimas perduodant, platinant ar kitaip padarant prieinamą, lyginimas ar derinimas, apribojimas, ištrynimas ar sunaikinimas.

Duomenų tvarkymo (perdavimo) tikslas (jeigu taikoma) ir tolesnis tvarkymas:

Paslaugų teikimas, kaip apibrėžta Sutartyje:

Duomenų saugojimas:

Asmens duomenis „Iron Mountain“ saugos klientui siūlomų paslaugų teikimo laikotarpiu ir tol, kol asmens duomenys bus grąžinti arba sunaikinti, kaip nustatyta pagal šios DTS 12.1 punktą.

Jei taikoma, perduodant duomenis (pagalbiniams) duomenų tvarkytojams, taip pat nurodykite duomenų tvarkymo dalyką, pobūdį ir trukmę:

Sutarties su klientu galiojimo laikotarpiu pagalbiniai duomenų tvarkytojai, be kita ko, teikia informacinių technologijų (IT) ir konsultavimo paslaugas, įskaitant bendrą IT pagalbą, įvykių ataskaitų teikimo ir valdymo paslaugas.

C. KOMPETENTINGA PRIEŽIŪROS INSTITUCIJA

Kaip nurodyta 3 priede (Tarptautinis duomenų perdavimas), jeigu taikoma.

2 PRIEDAS

TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS (TOLIAU – SAUGUMO PRIEMONĖS)

1. INFORMACIJOS SAUGUMO PROGRAMA IR POLITIKA

Bendrovė „Iron Mountain“ vykdo informacijos saugumo programą su atitinkamomis fizinėmis, techninėmis ir administracinėmis kontrolės priemonėmis, atitinkančiomis pramonės standartus. Informacijos saugumo programą sudaro:

1.1. „Iron Mountain“ informacijos saugumo politikos, standartų ir procedūrų dokumentavimas, vidinis skelbimas ir komunikavimas;

1.2. dokumentuotas, aiškus atsakomybės ir įgaliojimų už informacijos saugumo programos sukūrimą ir palaikymą paskyrimas;

1.3. reguliarus pagrindinių informacijos saugumo programos kontrolės priemonių, sistemų ir procedūrų testavimas;

1.4. administracinės, techninės ir operacinės priemonės, skirtos visiems kliento asmens duomenims apsaugoti, naudojant šiame Saugumo priede aprašytą praktiką, procedūras ir procesus tiek, kiek jie yra svarbūs ir taikytini formatui, kuriuo saugomi Kliento asmens duomenys.

2. RIZIKOS VERTINIMAS

„Iron Mountain“ vykdo informacijos saugumo rizikos vertinimo programą, skirtą nustatyti ir įvertinti pagrįstai numatomą vidinę ir išorinę riziką bei pažeidžiamumą, kurie gali turėti įtakos kliento asmens duomenų saugumui, konfidencialumui ir (arba) vientisumui. „Iron Mountain“ įvertina ir, jei reikia, pagrįstai ir tinkamai, atnaujina dabartinės informacijos saugumo programos veiksmingumą siekiant apriboti tokią riziką kasmet arba kai iš esmės pasikeičia rizika ar kliento asmens duomenų pažeidžiamumas.

3. DUOMENŲ TVARKYMO TURTO IR FIZINIŲ LAIKMENŲ VALDYMAS

3.1. Duomenų tvarkymo priemonių valdymas. „Iron Mountain“ vykdo turto valdymo programą, skirtą fizinei, techninei ir administracinei kontrolei, susijusiai su „Iron Mountain“ duomenų tvarkymo turtu (pavyzdžiui, kompiuteriais, serveriais, saugojimo įrenginiais, ryšių tinklais, asmeniniais kompiuteriais, nešiojamaisiais kompiuteriais ir periferiniais įrenginiais).
Turto valdymo programą sudaro:

3.1.1. dokumentuotas turto nuosavybės teisių priskyrimas „Iron Mountain“ darbuotojams, siekiant užtikrinti tinkamą informacijos klasifikavimą, prieigos apribojimų nustatymą ir prieigos kontrolės priemonių peržiūrą;

3.1.2. turto dezinfekavimas prieš jį sunaikinant pagal NIST 800-88;

3.1.3. reikalavimas gauti vadovybės leidimą prieš išvežant iš "Iron Mountain" patalpų įrangą ar programinę įrangą, kuri nėra priskirta konkrečiam asmeniui.

3.2. Kontrolės priemonės. „Iron Mountain“ taiko tokias kontrolės priemones:

3.2.1. veiklos procedūros ir techninės kontrolės priemonės, skirtos apsaugoti dokumentus, kompiuterines laikmenas, įvesties / išvesties / atsarginės kopijos duomenis ir sistemos dokumentaciją nuo neteisėto atskleidimo, pakeitimo ir sunaikinimo;

3.2.2. saugaus elektroninių ar fizinių laikmenų, kuriose yra kliento asmens duomenų, sunaikinimo procedūros;

3.2.3. nustatytas procesas, skirtas sekti visas kliento fizines laikmenas nuo pirminio „Iron Mountain“ saugojimo iki visiško pašalinimo ar sunaikinimo.

4. DARBUOTOJAMS TAIKOMOS SAUGUMO PRIEMONĖS

4.1. Konfidencialumas. „Iron Mountain“ pagrįstai reikalauja, kad visi „Iron Mountain“ darbuotojai, įskaitant laikinuosius ir sutartinius darbuotojus, sutiktų išlaikyti kliento asmens duomenų konfidencialumą ir laikytis „Iron Mountain“ vidaus informacijos saugumo ir priimtino naudojimo reikalavimų.

4.2. Asmens patikrinimo politika. „Iron Mountain“ savo darbuotojams taiko praeities tyrimų ir narkotikų testavimo politiką (tik JAV). Bendrovė „Iron Mountain“ ir toliau laikysis tokios politikos Sutarties galiojimo laikotarpiu. Pagal politikos reikalavimus numatyta, be kita ko, narkotinių medžiagų patikra (tik JAV), personalo tapatybės patikrinimas, teistumo informacijos paieškas, įdarbinimo patikrinimas, paieška vyriausybės ir (arba) teroristų stebėjimo sąrašuose, taip pat tam tikrų darbuotojų išsilavinimo patikrinimas, kandidatų į vairuotojus ir esamų vairuotojų vairuotojo pažymėjimai ir pažeidimų istorija. Kai patikrinimo metu nustatoma įžeidžianti informacija, „Iron Mountain“ atlieka individualų vertinimą, vadovaudamasi galiojančiais darbo įstatymais ir geriausia praktika.

4.3. Darbas su subrangovais. „Iron Mountain“ reikalauja, kad bet kuris subrangovas, teikiantis paslaugas pagal Sutartį, laikytųsi panašių į šiame skirsnyje nustatytus apribojimus, taikomus bet kuriam subrangovo personalui, kuris teiks paslaugas pagal Sutartį, susijusias su kliento asmens duomenų tvarkymu

4.4. Mokymas saugumo klausimais. Ne rečiau kaip kartą per metus „Iron Mountain“ visiems „Iron Mountain“ darbuotojams, turintiems prieigą prie kliento asmens duomenų, rengia bendruosius saugumo informuotumo mokymus ir konkrečių vaidmenų saugumo mokymus. „Iron Mountain“ saugo įrašus,

kuriuose nurodomi tokių „Iron Mountain“ darbuotojų, dalyvavusių šiuose mokymuose, vardai ir pavardės bei kiekvieno saugumo informuotumo mokymų data. Tokią saugumo informuotumo mokymų programą „Iron Mountain“ reguliariai peržiūri ir atnaujina.

4.5. „Iron Mountain“ darbuotojų nušalinimas. „Iron Mountain“ taiko drausminę procedūrą, kuri taikoma „Iron Mountain“ darbuotojams, pažeidusiems čia nurodytus saugumo reikalavimus.

4.6. Prieigos nutraukimas nutraukus darbo sutartį / perkėlus į kitas pareigas. Nutraukus darbo sutartį arba perėjus į pareigas, kurioms nereikia prieigos prie kliento asmens duomenų, „Iron Mountain“ darbuotojo prieiga prie kliento asmens duomenų turi būti nedelsiant panaikinta.

5. FIZINIS IR APLINKOSAUGINIS SAUGUMAS

5.1. Fizinės saugumo kontrolės priemonės. „Iron Mountain" patalpose naudojamos fizinės kontrolės priemonės, kuriomis pagrįstai ribojama prieiga prie kliento asmens duomenų, įskaitant, „Iron Mountain“ nuomone, prieigos kontrolės protokolus, fizinius barjerus, pavyzdžiui, užrakintas patalpas ir zonas, darbuotojų prieigos ženklelius, lankytojų žurnalus, lankytojų prieigos ženklelius, kortelių skaitytuvus, vaizdo stebėjimo kameras ir įsilaužimo aptikimo signalizaciją. Visi lankytojai registruojami ir palydimi įmonės darbuotojo.

5.2. Pagalbinės paslaugos. „Iron Mountain“ taiko priemones, skirtas apsaugoti savo patalpas, kuriose saugomi kliento asmens duomenys, ir sistemas nuo elektros energijos, telekomunikacijų, vandens tiekimo, kanalizacijos, šildymo, vėdinimo ir oro kondicionavimo sutrikimų.

5.3. Perdavimo sistemos saugumas. „Iron Mountain“ taiko priemones, skirtas tinklo infrastruktūros ir telekomunikacijų sistemų fiziniam saugumui apsaugoti nuo perdavimo perėmimo ir sugadinimo.

5.4. Įranga už įmonės ribų. Jei „Iron Mountain perduoda funkcijas, kurioms atlikti reikia naudoti ne vietoje esančią įrangą, bet kokia ne vietoje esanti įranga, kurioje saugomi Kliento asmens duomenys, turi būti apsaugota saugumu, lygiaverčiu tam, kuris naudojamas tam pačiam tikslui vietoje esančiai įrangai.

5.5. Fizinė prieiga prie duomenų tvarkymo priemonių. „Iron Mountain“ vienerius metus saugo įrašus apie „Iron Mountain“ darbuotojus, kuriems suteikta fizinė prieiga prie „Iron Mountain" kontroliuojamos (-ų) kompiuterinės (-ių) aplinkos (-ų), kurią (-ias) "Iron Mountain" naudoja paslaugoms teikti, ir kliento prašymu, susijusiu su Saugumo pažeidimu, laikydamasi „Iron Mountain" saugumo politikos, suteikia klientui prieigą prie tokių „Iron Mountain“ darbuotojų įrašų, kuriuos galima patikrinti.

5.6. Apribota fizinė prieiga. „Iron Mountain“ apriboja fizinę prieigą prie „Iron Mountain“ kontroliuojamų patalpų, kuriose tvarkomi kliento asmens duomenys, tik tiems „Iron Mountain“ darbuotojams ir įgaliotiems asmenims, kuriems tokia prieiga reikalinga verslo tikslais. „Iron Mountain“ turi būti nustačiusi patvirtinimo procesą, skirtą prašymams suteikti fizinę prieigą prie tokių įrenginių tvirtinti ir stebėti.

5.7. Taisymas ir keitimas. „Iron Mountain“ registruoja visus su saugumu susijusius bet kokių fizinių komponentų, įskaitant įrangą, sienas, duris ir užraktus saugiose patalpose, kuriose saugomi kliento asmens duomenys, remontus ir pakeitimus.

5.8. Registro žurnalai. Registruoja techninės įrangos ir elektroninių laikmenų judėjimą ir už tai atsakingus asmenis.

6. RYŠIŲ IR INFORMACIJOS APDOROJIMO OPERACIJŲ VALDYMAS

6.1. Įrenginių konfigūravimo standartai. „Iron Mountain“ sukuria, įgyvendina ir palaiko pramonės standartus atitinkančias sistemos administravimo procedūras, įskaitant, bet neapsiribojant, sistemos sustiprinimą, sistemos ir įrenginio pataisymus (operacinės sistemos ir taikomųjų programų) bei tinkamą antivirusinių programų diegimą ir atnaujinimus.

6.2. Duomenų tvarkymo sistemos pakeitimų kontrolė. „Iron Mountain“ turi būti įdiegusi vidinį oficialų informacijos apdorojimo ir ryšių tinklo sistemų pakeitimų valdymo procesą, o „Iron Mountain“ pakeitimų prašymai turi būti dokumentuojami, išbandomi ir patvirtinami prieš įgyvendinant bet kokias naujas informacijos apdorojimo ar ryšių tinklo galimybes, sistemos pataisas ar esamų sistemų pakeitimus.

6.3. Pareigų atskyrimas. „Iron Mountain“ atskiria pareigas ir atsakomybės sritis taip, kad nė vienas asmuo neturėtų išimtinių galimybių keisti informacijos apdorojimo sistemas, kurios turi prieigą prie kliento asmens duomenų.

6.4. Kūrimo ir gamybos aplinkų atskyrimas. „Iron Mountain“ informacijos apdorojimo sistemų kūrimo, bandymų ir gamybos aplinkos turi būti logiškai arba fiziškai atskirtos.

6.5. Techninės architektūros valdymas. „Iron Mountain“ nustato konfigūracijos valdymo procesą, kad apibrėžtų, valdytų ir kontroliuotų informacijos apdorojimo sistemos komponentus, naudojamus paslaugoms teikti, ir tokių komponentų techninę infrastruktūrą.

6.6. Įsilaužimo aptikimas. „Iron Mountain“ nuolat stebi kompiuterių sistemas ir procesus, ar nėra bandymų ar faktinių įsilaužimų ar saugumo pažeidimų, ir praneša klientui apie bet kokią neteisėtą prieigą prie kliento asmens duomenų.

6.7. Tinklo saugumas. „Iron Mountain“ užtikrina, kad būtų priimtos ir taikomos tokios priemonės:

6.7.1. Paslaugoms teikti naudojamoje (-ose) „Iron Mountain" prieglobos aplinkoje (-ose), tinklo įsilaužimo aptikimo sistemoje (toliau – IDS) ir įsilaužimo prevencijos jutikliuose (toliau -– IPS) registruojami įspėjamieji įvykiai, o kasdien pateikiamos ataskaitos, kurias galima peržiūrėti (bendrai vadinamos IDS/IPS);

6.7.2. „Iron Mountain“ prieglobos aplinkoje (-ose), kuri (-ios) naudojama (-os) Paslaugoms teikti, IDS ir (arba) IPS, kuri (-ios) atnaujinama (-os) ne rečiau kaip kartą per savaitę, bet kuo greičiau po to, kai gaunami atnaujinimai, ir nedelsiant paleidžiamos naujausios grėsmių signatūros arba taisyklės;

6.7.3. į išorę nukreiptų sistemų didelės rizikos prievadai nepasiekiami iš interneto;
6.7.4. prisijungimai prie „Iron Mountain“ tinklo registruojami ir įrašomi į žurnalo failus;
6.7.5. įdiegtos ugniasienės (-ių), skirtos apsaugoti ir tikrinti visą įeinantį ir išeinantį tinklo paslaugų srautą tarp nustatytų tinklo taškų;
6.7.6. visų "Iron Mountain" priklausančių ar valdomų sistemų įeinančių ir išeinančių tinklo prievadų ar paslaugų srauto nustatymo griežtinimo politika, kuri yra dokumentuota ir patvirtinta pagal informacijos saugumo programą;
6.7.7. tinklo ir diagnostikos prievadai, kurie yra tinkamai apsaugoti; ir
6.7.8. politikos, procedūros ir techninės kontrolės priemonės, skirtos užkirsti kelią kenkėjiškam kodui ar žinomoms "Iron Mountain" informacinių sistemų atakoms, aptikti ir pašalinti.

6.8 Užšifruoti autentikavimo duomenys. „Iron Mountain“ užtikrina, kad „Iron Mountain“ tinklo įrenginiais perduodami autentifikavimo duomenys būtų šifruojami.

6.9. Saugus tinklo administravimas. „Iron Mountain“ tinklai turi būti pagrįstai valdomi ir kontroliuojami, siekiant apsisaugoti nuo žinomų grėsmių ir užtikrinti visų „Iron Mountain“ valdomų taikomųjų programų ir duomenų, esančių tinkle arba perduodamų tinklu, saugumą. Turi būti įdiegtos techninės kontrolės priemonės ir saugaus ryšio protokolai, kad būtų uždrausti neriboti ryšiai su nepatikimais tinklais ar viešai prieinamais serveriais.

6.10. Apsauga nuo virusų. „Iron Mountain“ įdiegia ir prižiūri „Iron Mountain“ valdomų serverių ir darbo vietų, naudojamų kliento asmens duomenims saugoti arba prieigai prie jų, antivirusinę valdymo programą, įskaitant apsaugą nuo kenkėjiškų programų, atnaujinamus parašų failus arba alternatyvią apsaugą nuo naujų grėsmių, pataisas ir virusų apibrėžimus

6.11. Svetainė – kliento šifravimas. „Iron Mountain“ užtikrina, kad kiekvienoje jos interneto svetainėje būtų įjungtas saugiųjų lizdų sluoksniavimas (SSL) ir joje būtų galiojantis SSL sertifikatas, reikalaujantis konfidencialumo, autentiškumo arba autorizavimo kontrolės.

6.12. Informacijos atsarginės kopijos. „Iron Mountain" sukuria atitinkamas atsargines sistemos failų kopijas. Be to, „Iron Mountain“ parengia ir palaiko atkūrimo po avarijos procedūras, žr. toliau esantį skyrių „Atkūrimas po avarijos“, kuriame pateikiama daugiau informacijos.

6.13. Perduodama elektroninė informacija. „Iron Mountain“ naudoja pramoninio standarto algoritmą su mažiausiai 128 bitų ilgio raktu, kad apsaugotų viešaisiais tinklais perduodamus kliento asmens duomenis, kai jie gaunami iš „Iron Mountain“ prieglobos infrastruktūros.

6.14. Kriptografinės kontrolės priemonės. „Iron Mountain“ laikosi dokumentuotos kriptografinių kontrolės priemonių naudojimo politikos. „Iron Mountain“ kriptografinės kontrolės priemonės:
6.14.1. suprojektuotos taip, kad būtų pagrįstai apsaugotas „Iron Mountain“ tvarkomų, perduodamų ar saugomų kliento asmens duomenų konfidencialumas ir vientisumas bet kurioje bendro naudojimo tinklo aplinkoje pagal Sutarties sąlygas;
6.14.2. „Iron Mountain“ prieglobos aplinkoje (-ose), naudojamoje (-ose) paslaugoms teikti, taikomos kliento asmens duomenims, perduodamiems per „nepatikimus“ tinklus (t. y. tinklus, kurių „Iron Mountain" teisiškai nekontroliuoja), įskaitant tinklus, naudojamus duomenims iš „Iron Mountain" tinklo siųsti į kliento įmonės tinklą, visais atvejais klientui bendradarbiaujant valdant šifravimo raktus, reikalingus kliento gautiems perdavimams iššifruoti; ir
6.14.3. numato dokumentais pagrįstą šifravimo raktų valdymo praktiką, kad užtikrintumėte kriptografinių technologijų saugumą.
6.14.4. numato visų nešiojamuosiuose kompiuteriuose ar kituose nešiojamuosiuose įrenginiuose esančių kliento asmeninių duomenų šifravimą.

6.15. Prisijungimo reikalavimai. „Iron Mountain“ taiko reikalavimus, pagal kuriuos:
6.15.1. svarbūs saugumo ir sistemų įvykiai registruojami ir peržiūrimi;
6.15.2. audito žurnalai saugomi ne trumpiau kaip vienerius metus „Iron Mountain“ paslaugų teikimui naudojamose sistemose, esančiose „Iron Mountain“ prieglobos aplinkoje (-ose);
6.15.3. sistemos audito žurnalai peržiūrimi dėl nukrypimų; ir
6.15.4. žurnalų saugojimo įrenginiai ir sistemų informacija yra tinkamai apsaugoti nuo klastojimo ir neteisėtos prieigos.

6.16. Tinklo laiko sinchronizavimas. „Iron Mountain“ sinchronizuoja visų informacijos apdorojimo sistemų laikrodžius, naudodama bendrą autoritetingą laiko šaltinį.

6.17. Atskyrimas tinkluose. „Iron Mountain“ tinkluose tinkamai atskiria susijusias informacinių paslaugų, naudotojų ir informacinių sistemų grupes.

7. PRIEIGOS KONTROLĖ

7.1. Prieigos kontrolės taisyklės. „Iron Mountain“ taiko prieigos prie informacijos apdorojimo išteklių kontrolės politiką, kurią „Iron Mountain“ oficialiai patvirtina, paskelbia ir įgyvendina.

7.2. Loginės prieigos autorizavimas. „Iron Mountain“ taiko loginės prieigos prie kliento asmens duomenų ir prieigos prie „Iron Mountain“ sistemų, skirtų naudoti paslaugose, prašymų patvirtinimo procesą.

7.3. Prieigos kontrolė ir peržiūra. „Iron Mountain" prieigą prie kliento asmens duomenų suteikia tik aktyviems „Iron Mountain" darbuotojams, įskaitant laikinuosius ir sutartinius darbuotojus, ir aktyvių naudotojų paskyroms, kuriems tokia prieiga reikalinga jų darbo funkcijoms atlikti. Visos privilegijuotos prieigos teisės turi būti peržiūrimos, patvirtinama, kad jos atitinka einamas pareigas, ir bent kartą per ketvirtį dokumentuojamos.

7.4. Trečiųjų šalių prieigos kontrolė. Prieš suteikdama prieigą išorės šalims prie „Iron Mountain“ informacinių sistemų, turinčių prieigą prie kliento asmens duomenų, „Iron Mountain“ užtikrina, kad būtų įdiegtos tinkamos kontrolės priemonės.

7.5. Prieigos prie operacinių sistemų kontrolė. „Iron Mountain“ kontroliuoja prieigą prie operacinių sistemų (tiek programinės, tiek aparatinės įrangos pagrindu veikiančių operacinių sistemų), reikalaudama saugaus prisijungimo proceso, kuris unikaliai identifikuoja asmenį, kuris jungiasi prie operacinės sistemos.

7.6. Mobilioji kompiuterinė įranga. „Iron Mountain" turi politiką arba procedūrą, skirtą apsaugoti „Iron Mountain“ mobiliuosius kompiuterinius įrenginius nuo neteisėtos prieigos. Tokioje politikoje ar procedūrose aptariama fizinė apsauga, prieigos kontrolė ir saugumo kontrolės priemonės, pavyzdžiui, šifravimas, apsauga nuo virusų ir atsarginių kopijų darymas.

7.7. Klientų sistemų atskyrimas. „Iron Mountain“ savo prieglobos aplinkoje(-ose), naudojamoje (-ose) Paslaugoms teikti, logiškai atskiria ir atskiria kliento asmens duomenis nuo visos kitos informacijos.

7.8. Paskyros. „Iron Mountain“ paskyrų atžvilgiu taiko tokias priemones:

7.8.1. reikalauja, kad kiekvieno „Iron Mountain“ darbuotojo, siekiančio gauti prieigą prie „Iron Mountain“ sistemų, kuriose tvarkomi kliento asmens duomenys, tapatybė būtų patvirtinta, ir uždrausti naudotis bendromis naudotojo paskyromis arba naudotojo paskyromis su bendrais įgaliojimais (t. y. ID), kad būtų galima gauti prieigą prie kliento asmens duomenų arba sistemų;

7.8.2. reikalauja, kad visi naudotojo paskyros ID, įskaitant privilegijuotas paskyras, būtų tiesiogiai susieti su asmeniu (o ne su pareigomis);

7.8.3. jei numatytoji administravimo paskyra nėra išjungta arba pašalinta, reikalauja, kad numatytosios administravimo paskyros prieigai būtų naudojami laikinieji slaptažodžiai, tikrinimo ID arba panašios kontrolės priemonės;

7.8.4. reikalauja, kad neaktyvios įprastos paskyros būtų užrakinamos arba išjungiamos po 90 dienų neaktyvumo;

7.8.5. uždraudžia prieigą prie paskyros po kelių nesėkmingų bandymų prisijungti;

7.8.6. reikalauja unikalių identifikatorių ir patikimų slaptažodžių, kuriuos sudaro bent šie elementai: ne mažiau kaip 8 simboliai; turi būti keičiami kas 90 dienų; taiko sudėtingumo reikalavimus;

7.8.7. draudžia darbuotojams dalytis slaptažodžiais arba juos užsirašyti;

7.9. Neprižiūrimų sistemų kontrolė. „Iron Mountain“ turi naudoti slaptažodžiu apsaugotą ekrano užsklandą visose sistemose, kurios paliktos be priežiūros ir kuriose 30 minučių nebuvo atliekami jokie veiksmai.

8. INFORMACINIŲ SISTEMŲ ĮSIGIJIMAS, KŪRIMAS IR PRIEŽIŪRA

8.1. Sistemų kūrimo saugumas. „Iron Mountain“ užtikrina, kad saugumas būtų visų informacinių sistemų kūrimo ir operacijų dalis, skelbia ir laikosi vidinių saugaus kodavimo metodikų, pagrįstų taikomųjų programų kūrimo saugumo standartais.

8.2. Programinės įrangos saugumo valdymas. „Iron Mountain“ informacinės sistemos (įskaitant operacines sistemas, infrastruktūrą, verslo taikomąsias programas, paslaugas ir naudotojų sukurtas taikomąsias programas) turi būti suprojektuotos taip, kad atitiktų informacijos saugumo standartus.

8.3. Tinklo diagramos. „Iron Mountain“ sukuria, dokumentuoja ir tvarko fizines ir logines tinklo įrenginių ir srauto diagramas.

8.4. Taikomųjų programų pažeidžiamumo vertinimai / etiškas įsilaužimas. „Iron Mountain“ bent kartą per metus atlieka prieglobos aplinkoje (-ose) esančių taikomųjų programų, naudojamų paslaugoms, kuriomis tvarkomi kliento asmens duomenys, teikti, pažeidžiamumo vertinimą. Išsamūs rezultatai yra konfidenciali ir nuosavybės teise priklausanti „Iron Mountain“ informacija, kuri nebus teikiama.

8.5. Pakeitimų testavimas ir peržiūra. „Iron Mountain“ peržiūri ir išbando taikomųjų programų ir operacinių sistemų pakeitimus prieš diegimą, kad užtikrintų, jog jie neturės neigiamo poveikio kliento asmens duomenims ar sistemoms.

9. VEIKLOS ATKŪRIMAS PO AVARIJOS

„Iron Mountain“ turi turėti atkūrimo po avarijos planą, įskaitant Paslaugoms palaikyti naudojamų sistemų ir elektroninių duomenų kopijavimą į atsarginį duomenų centrą. Sistemų ir elektroninių duomenų kopijavimas netaikomas klientų asmens duomenims, kurie fiziškai saugomi „Iron Mountain“ patalpose. „Iron Mountain“ prižiūri verslo tęstinumo planą, skirtą svarbiausioms verslo funkcijoms atkurti. „Iron Mountain“ ne rečiau kaip kartą per dvylika (12) mėnesių atlieka atkūrimo po avarijos bandymus.

10. NEPRIKLAUSOMI AUDITAI IR VERTINIMAI

„Iron Mountain" saugumo protokolai sukurti taip, kad atitiktų pramonės standartus. „Iron Mountain“ pateiks klientui visas trečiosios šalies užsakytas nepriklausomo audito ataskaitas (pvz., PCI, ISO27001, SOC2 ir kt.), susijusias su paslaugomis tame regione, kuriame teikiamos tokios paslaugos (toliau – Audito ataskaita). „Iron Mountain“ pateiks visas tokias ataskaitas, kurios buvo užsakytos siekiant jas pateikti klientams, neatsižvelgiant į ataskaitos rezultatus. Bendrovė „Iron Mountain“ neprivalo pateikti vidaus audito rezultatų ar kitų nepriklausomų vertinimų rezultatų, kurie buvo užsakyti siekiant juos laikyti konfidencialiais bendrovei „Iron Mountain". Klientui ir jo išorės auditoriams paprašius bus pateiktos audito ataskaitos kopijos. Bet kokia audito ataskaita ar kiti rezultatai, gauti atlikus šiame skyriuje reikalaujamus bandymus ar auditą, bus laikomi „Iron Mountain“ konfidencialia informacija. Klientas turi teisę pateikti tokios audito ataskaitos kopiją bet kuriam taikomam klientui ar reguliavimo institucijoms, laikydamasis konfidencialumo nuostatų, kurios yra tokios pat griežtos, kaip ir šiame dokumente. Kliento prašymu „Iron Mountain" raštu patvirtina, kad atitinkama politika, procedūros ir vidaus kontrolė nuo bet kurios tokios audito

ataskaitos užbaigimo nepasikeitė, ne ilgiau kaip per tris mėnesius nuo audito ataskaitos ataskaitinio laikotarpio pabaigos.

3 PRIEDAS

Tarptautinis duomenų perdavimas

1. APIBRĖŽTYS

2021 m. ES standartinės sutarčių sąlygos – standartinės sutarčių sąlygos dėl asmens duomenų perdavimo į trečiąsias šalis pagal BDAR, kurias Europos Komisija priėmė Komisijos įgyvendinimo sprendimu (ES) 2021/914 ir kurias galima rasti čia[3].

2022 m. JK papildymas – šabloninis papildymas B.1.0, kurį 2022 m. vasario 2 d. išleido Jungtinės Karalystės informacijos komisaro biuras ir pateikė Parlamentui pagal 2018 m. Duomenų apsaugos įstatymo 119A straipsnį, kuris gali būti peržiūrėtas pagal šio įstatymo 18 straipsnį, paskelbtas čia[4].

ES Kliento asmens duomenys – tai kliento asmens duomenų tvarkymas, kuriam buvo taikomi Europos Sąjungos arba Europos Sąjungos valstybės narės ar Europos ekonominės erdvės duomenų apsaugos įstatymai prieš „Iron Mountain“ pradedant juos tvarkyti;

Apsaugota teritorija yra:

i. ES klientų asmens duomenų atveju – Europos Sąjungos ir Europos ekonominės erdvės valstybės narės ir bet kuri šalis, teritorija, sektorius ar tarptautinė organizacija, kurios atžvilgiu galioja sprendimas dėl tinkamumo pagal BDAR 45 straipsnį;

ii. Jungtinės Karalystės klientų asmens duomenų atveju – Jungtinė Karalystė ir bet kuri šalis, teritorija, sektorius ar tarptautinė organizacija, kurios atžvilgiu galioja sprendimas dėl tinkamumo pagal Jungtinės Karalystės tinkamumo taisykles;

iii. Šveicarijos klientų asmens duomenų atveju – bet kuri šalis, teritorija, sektorius ar tarptautinė organizacija, pripažinta tinkama pagal Šveicarijos įstatymus;

iv. bet kokių kitų kliento asmens duomenų, perduodamų iš jurisdikcijos, kurioje užtikrinama panaši apsauga kaip ir ES, JK ar Šveicarijos kliento asmens duomenų atveju – bet kuri šalis, teritorija, sektorius ar tarptautinė organizacija, kuri pagal tokios jurisdikcijos įstatymus pripažįstama tinkama;

Standartinės sutarties sąlygos – tai kartu 2021 m. ES standartinės sutarties sąlygos ir 2022 m. JK priedas.

Šveicarijos Kliento asmens duomenys – tai kliento asmens duomenų, kuriems buvo taikomi Šveicarijos duomenų apsaugos įstatymai prieš „Iron Mountain" pradedant juos tvarkyti, tvarkymas;

JK Kliento asmens duomenys – tai kliento asmens duomenų tvarkymas, kuriam buvo taikomi Jungtinės Karalystės duomenų apsaugos įstatymai prieš „Iron Mountain“ pradedant juos tvarkyti;

2. ĮVAIRIOS NUOSTATOS

2.1. Šį 3 priedą sudaro šios dalys: i) A dalis – ES Kliento asmens duomenų perdavimas; ii) B dalis – Šveicarijos kliento asmens duomenų perdavimas; iii) C dalis – Jungtinės Karalystės kliento asmens duomenų perdavimas, kuri taikoma „Iron Mountain“ perduodant kliento asmens duomenis, susijusius su jos Paslaugomis.

2.2. Standartinės sutarčių sąlygos taikomos „Iron Mountain“ ir su ja susijusioms įmonėms kaip „duomenų importuotojams“ ir klientui ir su juo susijusioms įmonėms kaip „duomenų eksportuotojus“.

2.3. Pasirašant Sutartį ir nurodant jos datą, nurodomi ir visi reikalaujami standartinių sutarties sąlygų parašai ir datos.

2.4. Jei šalys perduoda ES, JK ar Šveicarijos kliento asmens duomenis už Saugomos teritorijos ribų ir atitinkamas Europos Komisijos sprendimas ar kitas galiojantis tinkamumo metodas pagal taikomus duomenų apsaugos teisės aktus, kuriuo „Iron Mountain“ rėmėsi perduodama duomenis, pripažįstamas negaliojančiu arba bet kuri priežiūros institucija reikalauja sustabdyti pagal tokį sprendimą atliekamą asmens duomenų perdavimą, šalys bendradarbiauja ir padeda naudoti alternatyvų perdavimo mechanizmą. Šalys taip pat susitaria, kad šiame 3 priede nurodytos tinkamos apsaugos priemonės, naudojamos tarptautiniam duomenų perdavimui palengvinti, nėra išimtinės ir kad šalys gali taikyti papildomus duomenų perdavimo mechanizmus, pavyzdžiui, ES ir JAV duomenų privatumo sistemą.

A DALIS – ES KLIENTO ASMENS DUOMENŲ PERDAVIMAS

[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

Jei klientas arba su juo susijusios įmonės perduoda ES Kliento asmens duomenis už apsaugotos teritorijos ribų bendrovei „Iron Mountain" arba su ja susijusioms įmonėms dėl „Iron Mountain" paslaugų teikimo pagal Sutartį, taikoma ši 3 priedo A dalis ir Šalys susitaria taip:

1. **Standartinių sutarčių sąlygų pasirinkimas.** 2021 m. ES standartinių sutarčių sąlygų ANTROJO MODULIO tekstas taikomas, kai klientas arba bet kuris iš jo filialų yra valdytojas, o „Iron Mountain" arba bet kuris iš jo filialų yra tvarkytojas; 2021 m. ES standartinių sutarčių sąlygų TREČIOJO MODULIO tekstas taikomas, kai klientas arba bet kuris iš jo filialų yra tvarkytojas, o „Iron Mountain" arba bet kuris iš jo filialų yra pagalbinis tvarkytojas. Atitinkamos 2021 m. ES standartinių sutarčių sąlygų nuostatos yra įtrauktos į šią DTS kaip nuoroda ir yra neatskiriama šios DTS dalis. Jokie kiti moduliai ar 2021 m. ES standartinėse sutarčių sąlygose kaip neprivalomi pažymėti punktai netaikomi. 2021 m. ES standartinių sutarčių sąlygų priedų tikslais reikalaujama informacija pateikta 1 priede „Tvarkymo / perdavimo aprašas“, 2 priede „Techninės ir organizacinės priemonės’ ir DTS 6.2 punkte „Pagalbinių duomenų tvarkytojų sąrašas“.

2. **Naudojimasis pagalbinių tvarkytojų paslaugomis.** Taikant 2021 m. ES standartinių sutarčių sąlygų 9 punktą, Paslaugoms teikti taikomas 2 variantas (Bendrasis rašytinis leidimas) dėl subtiekėjų pasitelkimo. Klientas pripažįsta ir sutinka, kad „Iron Mountain“ gali pasitelkti naujus pagalbinius duomenų tvarkytojus pagal šios DTS 6 punkte sutartą mechanizmą ir kad prašymų pakeisti pagalbinius duomenų tvarkytojus pateikimo laikotarpis yra penkiolika (15) dienų.

3. **Reglamentuojanti teisė ir teismo vieta.** Taikant 2021 m. ES standartinių sutarčių sąlygų 17 punktą (Reglamentuojanti teisė), taikomas 2 taikytinos teisės variantas, o šioms sąlygoms taikoma ES valstybės narės, kurioje yra įsisteigęs duomenų eksportuotojas, teisė tiek, kiek ji leidžia taikyti trečiosios šalies naudos gavėjo teises. Taikant 2021 m. ES standartinių sutarčių sąlygų 18 punktą (Teismo vietos pasirinkimas ir jurisdikcija), tai yra ES valstybės narės, kurioje yra įsisteigęs duomenų eksportuotojas, teismai.

4. **Ištrynimo patvirtinimas.** 2021 m. ES standartinių sutarčių sąlygų 8.5 punkto ir 16 punkto d papunkčio tikslais „Iron Mountain“ patvirtinimą apie asmens duomenų ištrynimą klientui pateikia tik kliento rašytiniu prašymu.

5. **Asmens duomenų saugumo pažeidimas.** Taikant 2021 m. ES standartinių sutarčių sąlygų 8.6 punkto c papunktį, asmens duomenų saugumo pažeidimai sprendžiami pagal mechanizmą, dėl kurio susitarta DTS 7 punkte.

6. **Auditai.** Taikant 2021 m. ES standartinių sutarčių sąlygų 8.9 punktą, šių sąlygų auditas atliekamas pagal Susitarime sutartą audito mechanizmą.

7. **Skundai.** Taikant 2021 m. ES standartinių sutarčių sąlygų 11 punktą, „Iron Mountain" informuoja klientą, jei gauna duomenų subjekto skundą dėl ES kliento asmens duomenų, ir perduoda skundą klientui pagal Sutartyje sutartą mechanizmą.

8. **Priežiūros institucija.** Taikant 2022 m. ES standartines sutarčių sąlygas atitinkama kompetentinga priežiūros institucija nustatoma pagal ES standartinių sutarčių sąlygų 13 punktą.

D DALIS – ŠVEICARIJOS KLIENTŲ ASMENS DUOMENŲ PERDAVIMAS

Jei klientas ar jo filialai perduoda Šveicarijos Kliento asmens duomenis už apsaugotos teritorijos ribų bendrovei „Iron Mountain" ar jos filialams, susijusiems su „Iron Mountain" paslaugomis pagal Sutartį, taikoma ši 3 priedo B dalis ir Šalys susitaria taip:

1. **Standartinių sutarčių sąlygų pasirinkimas.** 2021 m. ES standartinės sutarčių sąlygos ir atitinkamos A dalies nuostatos taikomos tais atvejais, kai klientas arba bet kuris iš jo filialų yra Valdytojas, o „Iron Mountain“ arba bet kuris iš jo filialų yra tvarkytojas, ir (arba) klientas arba bet kuris iš jo filialų yra tvarkytojas, o „Iron Mountain" arba bet kuris iš jo filialų yra pagalbinis tvarkytojas, išskyrus:

   a. kompetentinga priežiūros institucija pagal 2021 m. ES standartinių sutarčių sąlygų 13 punktą yra Šveicarijos federalinė duomenų apsaugos ir informacijos komisija;

   b. sutartiniams reikalavimams pagal 2021 m. ES standartinių sutarčių sąlygų 17 punktą taikytina teisė yra Šveicarijos teisė, o jurisdikcijos vieta ieškiniams tarp šalių pagal 18 punkto b papunktį yra Šveicarijos teismai.

2. Nuorodos į ES BDAR 2021 m. ES standartinėse sutarčių sąlygose turi būti suprantamos kaip nuorodos į FADP.

3. 2021 m. ES standartinių sutarčių sąlygų sąvoka „valstybė narė“ neturi būti aiškinama taip, kad Šveicarijoje esantiems duomenų subjektams būtų atimta galimybė pareikšti ieškinį dėl savo teisių savo nuolatinėje gyvenamojoje vietoje (Šveicarijoje) pagal 2021 m. ES standartinių sutarčių sąlygų 18 punkto c papunktį.

C DALIS – JK KLIENTO ASMENS DUOMENŲ PERDAVIMAS

Jei klientas arba su juo susijusios įmonės perduoda JK asmens duomenis už Saugomos teritorijos ribų bendrovei „Iron Mountain“ arba su ja susijusioms įmonėms dėl „Iron Mountain“ paslaugų teikimo pagal Sutartį, taikoma ši 3 priedo C dalis ir Šalys susitaria taip:

1. **Standartinių sutarčių sąlygų pasirinkimas.** 2021 m. ES standartinės sutarčių sąlygos, atitinkamos A dalies nuostatos ir 2022 m. JK papildymas taikomi, kai klientas arba bet kuris iš jo susijusių įmonių yra duomenų valdytojas, o „Iron Mountain“ arba bet kuris iš jo susijusių įmonių – duomenų tvarkytojas, ir (arba) Klientas arba bet kuris iš jo susijusių įmonių yra duomenų tvarkytojas, o „Iron Mountain“ arba bet kuris iš jo filialų – pagalbinis duomenų tvarkytojas.

2. **1 dalis: 1 lentelė – trys 2022 m. JK papildymai.** Informacija apie šalis – 1 lentelė, atrinktos SSS, moduliai ir atrinkti straipsniai, priedėlio informacija, įskaitant 1A priedą: Šalių sąrašas, 1B priedas: Perdavimo aprašas ir 1C priedas: Techninės ir organizacinės priemonės, skirtos duomenų saugumui užtikrinti – 3 lentelė, laikomos užpildytomis pagal šį 3 priedą, įskaitant Jungtinės Karalystės papildymo A dalies 4 lentelę: Klientas ir „Iron Mountain“ pripažįsta ir sutinka, kad JK priedą gali nutraukti bet kuri Šalis.

3. **2 dalis:** Privalomos JK papildymo sąlygos: Klientas ir „Iron Mountain“ pripažįsta ir sutinka su JK priedo privalomomis nuostatomis.

4. **Priežiūros institucija.** Jungtinės Karalystės Informacijos komisaro biuras veikia kaip kompetentinga priežiūros institucija.

D DALIS – KITŲ KLIENTŲ ASMENS DUOMENŲ PERDAVIMAS

Jei klientas ar jo filialai perduoda „Iron Mountain" ar jos filialams kliento asmens duomenis, kuriems netaikoma A-C dalis, ir tiek, kiek tai susiję su „Iron Mountain" paslaugomis pagal Sutartį, 3 priedo A dalis taikoma tiek, kiek tai aktualu ir taikytina pagal taikomus duomenų apsaugos teisės aktus. Priešingu atveju, jei norint perduoti kliento asmens duomenis į šalį, kuri duomenų eksportuotojo požiūriu neužtikrina tinkamo asmens duomenų apsaugos lygio, pagal duomenų apsaugos teisės aktus reikia taikyti kokias nors pakaitines ar papildomas tinkamas apsaugos priemones ar perdavimo mechanizmus, šalys susitaria juos įgyvendinti kuo greičiau ir tokius įgyvendinimo reikalavimus dokumentuoti šios DTS priede.

4 PRIEDAS

HIPAA (Sveikatos draudimo mobilumo ir atskaitomybės aktas) – Verslo partnerio sutartis (VPS)

Ši VPS papildo ir iš dalies keičia visas esamas ar būsimas sutartis, sudarytas tarp „Iron Mountain“ ir jos filialų bei kliento ir jo filialų, pagal kurias „Iron Mountain" ar jos filialai teikia tam tikras paslaugas klientui ar jo susijusioms įmonėms ir pagal kurias paslaugos reikalauja, kad verslo partneris naudotų ir (arba) atskleistų saugomą informaciją apie sveikatą (toliau – PHI) atitinkamos įmonės vardu. Visos Sutartyje nustatytos sąlygos ir terminai lieka galioti ir taikomi „Iron Mountain“ klientui teikiamoms paslaugoms, išskyrus tuos atvejus, kai jie keičiami šioje VPS.

„Iron Mountain“ ir Klientas sudaro šią VPS kad abi šalys įvykdytų savo atitinkamus įsipareigojimus, kai jie įsigalios ir taps privalomi šalims pagal HIPAA privatumo, saugumo ir pranešimo apie pažeidimus taisykles kartu su visais įgyvendinimo teisės aktais, įskaitant tuos, kurie įgyvendinami kaip „Omnibus“ taisyklės dalis (toliau kartu vadinamos „HIPAA taisyklėmis“), pagal kurias klientas ir jo filialai yra "Apdraustasis subjektas" arba "Verslo partneris", o „Iron Mountain“ ir jos susijusios įmonės yra kliento „verslo partneris“. Šioje Sutartyje visos nuorodos į Verslo partnerį toliau laikomos nuorodomis į „Iron Mountain“ arba jos atitinkamą susijusią įmonę.

1. APIBRĖŽTYS

Didžiąja raide rašomos sąvokos, vartojamos, bet kitaip neapibrėžtos šioje VPS, turi tokią pačią reikšmę, kokia šioms sąvokoms priskiriama atitinkamai HIPAA taisyklėse arba Sutartyje.

Pranešimo apie pažeidimus taisyklė – tai 45 CFR §164 D poskyryje nustatyta pranešimo apie nesaugomos saugomos sveikatos informacijos pažeidimus taisyklė.

Verslo partneris – pirmiau nurodytas Verslo partneris, kuris gauna, saugo arba perduoda saugomą sveikatos informaciją teikdamas paslaugas klientams.

HIPAA – 1996 m. priimtas sveikatos draudimo mobilumo ir atskaitomybės aktas.

HITECH aktas – taikytinos Sveikatos informacijos technologijų ekonominei ir klinikinei sveikatai akto nuostatos, įtrauktos į 2009 m. Amerikos ekonomikos atgaivinimo ir reinvestavimo aktą, įskaitant visas įgyvendinimo taisykles.

Privatumo taisyklė – asmeniškai identifikuojamos sveikatos informacijos privatumo standartai, nurodyti 45 CFR §160 ir §164, A ir E dalyse.

Saugoma sveikatos informacija arba PHI turi tą pačią reikšmę, kaip ir 45 CFR §160.103 vartojama sąvoka "saugoma sveikatos informacija", ir apsiriboja PHI, kurią verslo partneris sukūrė kliento vardu arba gavo iš kliento ar jo vardu pagal Sutartį.

Saugumo taisyklė – 45 CFR §160 ir §164 A ir C dalyse nustatyti Saugumo standartai elektroninės saugomos sveikatos informacijos apsaugai.

2. VERSLO PARTNERIO PAREIGOS IR VEIKLA

2.1. Verslo partneris sutinka nenaudoti ir toliau neatskleisti PHI kitaip, nei leidžiama ar reikalaujama pagal šią VPS arba kaip to reikalauja įstatymai.

2.2. Verslo partnerio įmonė sutinka naudoti tinkamas apsaugos priemones ir, jei taikytina, laikytis 45 CFR §164 C poskyrio nuostatų dėl elektroninės PHI, kad būtų užkirstas kelias PHI naudojimui ar atskleidimui kitaip, nei numatyta šioje VPS ar Sutartyje; tačiau šalys pripažįsta ir susitaria, kad klientas, o ne verslo partnerio įmonė yra atsakinga už 45 CFR §164.312 reikalavimų dėl elektroninės PHI, saugomos fizinėse laikmenose (pvz., juostose), kurias klientas saugo pas verslo partnerio įmonę, šifravimo ar dešifravimo mechanizmų įdiegimo.

2.3. Verslo partneris sutinka nedelsdamas pranešti klientui apie bet kokį saugumo incidentą, pažeidimą ar kitokį jam žinomą PHI naudojimą ar atskleidimą, kuris nėra leidžiamas ar privalomas pagal šią VPS ar Sutartį. Pažeidimo atveju toks pranešimas pateikiamas pagal HIPAA taisykles, įskaitant, bet neapsiribojant, pagal 45 CFR 164.410 straipsnį, tačiau jokiu būdu ne vėliau kaip per tris (3) darbo dienas po to, kai verslo partneris baigia vidaus tyrimą ir patvirtina, kad įvyko pažeidimas. Verslo partneris suteikia pagrįstą pagalbą ir bendradarbiavimą tiriant bet kokį tokį pažeidimą ir dokumentuose nurodo konkrečias sąlygas, kurios buvo pažeistos, bet kokios neįgaliotos trečiosios šalies, kuri galėjo pasiekti arba gauti PHI, tapatybę, jei ji žinoma, ir bet kokius veiksmus, kurių ėmėsi Verslo partneris, kad sušvelnintų tokio pažeidimo poveikį.

2.4. Pagal 45 CFR 164.502(e)(1)(ii) ir 164.308(b)(2), kaip taikytina, verslo partneris užtikrina, kad bet kuris verslo partneris, kuris yra subrangovas, verslo partnerio vardu kuriantis, gaunantis, saugantis arba perduodantis PHI, kad padėtų teikti paslaugas pagal Sutartį, sutiktų su tais pačiais apribojimais, sąlygomis ir reikalavimais, kurie taikomi verslo partneriui tokių PHI atžvilgiu pagal šią VPS.

2.5. Jei verslo partnerio įmonė saugo paskirtojo įrašų rinkinio PHI, susijusią su asmenimis, ir jei klientas to prašo, verslo partnerio įmonė sutinka suteikti klientui prieigą prie tokios PHI, išreikalaudama ir pristatydama tokią PHI pagal Sutarties sąlygas, kad klientas galėtų atsakyti asmeniui, kad būtų laikomasi 45 CFR § 164.524 reikalavimų.

2.6. Verslo partneris sutinka, kad, jei reikia iš dalies pakeisti PHI, esančią verslo partnerio įmonės saugomame paskirtųjų įrašų rinkinyje, ir jei klientas paveda verslo partnerio įmonei gauti tokią PHI pagal Sutartį, verslo partnerio įmonė atliks tokią paslaugą, kad klientas galėtų atlikti bet kokius tokios PHI pakeitimus, kurių gali reikalauti klientas arba fizinis asmuo pagal 45 CFR §164.526.

2.7. Verslo partneris sutinka dokumentuoti ir pateikti klientui informaciją, reikalingą PHI atskleidimo apskaitai pateikti, su sąlyga, kad klientas pateikė verslo partneriui informaciją, kurios pakanka, kad verslo partneris galėtų nustatyti, kuriuose įrašuose ar duomenyse, kuriuos verslo partneris gavo iš kliento ar jo vardu, yra PHI. Informacijos atskleidimo dokumentuose turi būti tokia informacija, kurios reikia, kad klientas galėtų atsakyti į asmens prašymą pateikti PHI atskleidimo apskaitą pagal 45 CFR § 164.528 arba kitas HIPAA taisyklių nuostatas.

2.8. Sutartyje aiškiai nesusitarta kitaip, verslo partneris nedelsdamas praneša klientui apie bet kokius asmenų prašymus suteikti prieigą prie PHI, susipažinti su ja arba ją ištaisyti, neatsakydamas į tokius prašymus, o klientas yra atsakingas už tokių asmenų prašymų priėmimą ir atsakymą į juos.

2.9. Tiek, kiek verslo partneris turi vykdyti vieną ar daugiau kliento įsipareigojimų pagal 45 CFR § 164 E poskyrį, verslo partneris, vykdydamas tokį (-ius) įsipareigojimą (-us), laikosi klientui taikomų E poskyrio reikalavimų.

2.10. Verslo partnerio įmonė sutinka leisti Sekretoriui susipažinti su savo vidaus praktika, buhalterinėmis knygomis ir įrašais, kad būtų galima nustatyti atitiktį HIPAA taisyklėmis.

3. VERSLO PARTNERIUI LEIDŽIAMI NAUDOJIMO BŪDAI IR ATSKLEIDIMAS

3.1. Verslo partneris gali naudoti arba atskleisti PHI, jei tai būtina Sutartyje nustatytoms paslaugoms teikti.

3.2. Verslo partneris gali naudoti arba atskleisti PHI, jei taip reikalaujama pagal įstatymus.

3.3. Verslo partneris sutinka dėti pagrįstas pastangas, kad PHI būtų apribota iki minimumo, būtino numatytam naudojimo, atskleidimo ar prašymo tikslui pasiekti.

3.4. Verslo partneris negali naudoti ar atskleisti PHI tokiu būdu, kuris pažeistų 45 CFR § 164 E poskyrį, jei tai padarytų klientas.

3.5. Verslo partnerio įmonė gali atskleisti PHI dėl tinkamo verslo partnerio įmonės valdymo ir administravimo arba verslo partnerio įmonės teisiniams įsipareigojimams vykdyti, jei atskleisti informaciją reikalaujama pagal įstatymus arba jei verslo parterio įmonė iš asmens, kuriam atskleidžiama informacija, gauna pagrįstas garantijas, kad informacija išliks konfidenciali ir bus naudojama ar toliau atskleidžiama tik pagal įstatymus arba tais tikslais, dėl kurių ji buvo atskleista asmeniui, o asmuo informuos verslo partnerio įmonę apie visus jam žinomus atvejus, kai buvo pažeistas informacijos konfidencialumas.

4. KLIENTO ĮSIPAREIGOJIMAI

4.1. Klientas negali nurodyti verslo partneriui veikti taip, kad jis neatitiktų HIPAA taisyklių.

4.2. Klientas informuoja verslo partnerį apie bet kokį (-ius) apribojimą (-us) savo pranešime apie kliento privatumo praktiką pagal 45 CFR § 164.520 tiek, kiek toks apribojimas gali turėti įtakos verslo partnerio vykdomam PHI naudojimui ar atskleidimui.

4.3. Klientas informuoja verslo partnerį apie bet kokius fizinio asmens leidimo naudoti ar atskleisti jo PHI pasikeitimus ar atšaukimą, jei tokie pasikeitimai gali turėti įtakos verslo partnerio vykdomam PHI naudojimui ar atskleidimui.

4.4. Klientas raštu informuoja verslo partnerį apie bet kokį PHI naudojimo ar atskleidimo apribojimą, su kuriuo klientas sutiko pagal 45 CFR § 164.522, jei toks apribojimas gali turėti įtakos verslo partnerio vykdomam PHI naudojimui ar atskleidimui.

5. SUTARTIES GALIOJIMO TERMINAS IR NUTRAUKIMAS

5.1. Ši VPS įsigalioja jos Įsigaliojimo datą ir automatiškai baigiasi, kai įvyksta vėlesnė iš šių datų: i) pasibaigia Sutarties galiojimas; arba ii) kai visa kliento verslo partneriui pateikta PHI sunaikinama arba grąžinama klientui.

5.2. Šalis, sužinojusi apie kitos šalies padarytą esminį VPS pažeidimą, pažeidimo nepadariusiai šaliai suteikia galimybę pažeidimą padariusiai šaliai ištaisyti pažeidimą. Jei pažeidimą padariusi šalis nepašalina pažeidimo per trisdešimt (30) dienų nuo tada, kai pažeidimą padariusi šalis gauna raštišką pažeidimo nepadariusios šalies pranešimą, kuriame pateikiama išsami informacija apie tokį esminį pažeidimą, pažeidimo nepadariusi šalis turi teisę nutraukti šią VPS ir Sutartį pagal Sutarties sąlygas arba, jei nutraukimas neįmanomas, apie problemą praneša sekretoriui arba bet kuriai kitai kompetentingai institucijai.

5.3. <u>Nutraukimo pasekmės:</u>

5.3.1.1. Išskyrus 5.3.2 punkte numatytą atvejį, nutraukus šią VPS dėl bet kokios priežasties, verslo partneris grąžina arba sunaikina visą iš kliento gautą PHI pagal Sutartį. Ši nuostata taikoma PHI, kurią turi verslo partnerio subrangovai ar atstovai. Verslo partneris negali saugoti jokių PHI kopijų.

5.3.1.2. Jei verslo partneris nusprendžia, kad PHI grąžinti ar sunaikinti neįmanoma, verslo partneris pateikia klientui pranešimą apie sąlygas, dėl kurių grąžinti ar sunaikinti PHI neįmanoma. Pranešusi klientui, verslo partnerio įmonė tokiems PHI taiko šio VPS apsaugą ir apriboja tolesnį tokių PHI naudojimą ir atskleidimą tik tais tikslais, dėl kurių jų grąžinimas ar sunaikinimas yra neįmanomas, kol verslo partnerio įmonė saugo tokius PHI pagal Sutarties sąlygas.

6. ĮVAIRIOS NUOSTATOS

6.1. Žalos atlyginimas. Verslo partneris sutinka atlyginti klientui nuostolius nuo bet kokių baudų ar nuobaudų, skirtų klientui dėl bet kokios sekretoriaus pradėtos vykdymo užtikrinimo procedūros arba bet kokio valstijos generalinio prokuroro prieš klientą iškelto civilinio ieškinio, kuris tiesiogiai ir išimtinai kyla dėl bet kokio verslo partnerio veiksmo ar neveikimo, kuriuo pažeidžiamos HIPAA taisyklės arba padaromas esminis šios VPS pažeidimas (toliau – Reikalavimas). Verslo partneris neprivalo atlyginti klientui jokios tokių baudų ar nuobaudų dalies, susidariusios dėl i) kliento padaryto HIPAA taisyklių ar šios VPS pažeidimo; arba ii) kliento aplaidžių ar tyčinių veiksmų ar neveikimo. Pirmiau nurodytas įsipareigojimas atlyginti žalą yra aiškiai susietas su sąlyga, kad klientas suteikia verslo partnerio įmonei teisę verslo partnerio įmonei savo pasirinkimu ir sąskaita bei pasitelkdamas savo pasirinktą advokatą kontroliuoti arba dalyvauti ginant bet kokį tokį Reikalavimą, tačiau su sąlyga, kad tiek, kiek toks Reikalavimas yra didesnės bylos ar ieškinio dalis, verslo partnerio įmonė gali kontroliuoti arba dalyvauti tik su Reikalavimu susijusiuose svarstymuose. Jei verslo partnerio įmonė pasinaudoja galimybe kontroliuoti gynybą, tuomet i) Verslo partnerio įmonė be išankstinio raštiško kliento sutikimo nesprendžia jokių pretenzijų, reikalaujančių pripažinti kliento kaltę, ii) klientas turi teisę savo sąskaita dalyvauti pretenzijoje ar ieškinyje; ir iii) klientas bendradarbiauja su verslo partnerio įmone, kaip pagrįstai reikalaujama. Tai, kas išdėstyta pirmiau, yra vienintelė ir išimtinė kliento teisių gynimo priemonė ir vienintelė verslo partnerio atsakomybė už bet kokius kliento nuostolius, žalą, išlaidas ar atsakomybę dėl bet kokių su šia VPS susijusių reikalavimų.

6.2. Draudimo priemonių taikymas. Verslo partneris pripažįsta, kad bet koks neleistinas verslo partnerio atliekamas PHI naudojimas ar atskleidimas gali sukelti nepataisomą žalą klientui, dėl kurios klientas turi teisę, jei to pageidauja, kreiptis į teismą dėl uždraudimo ar kitų teisingų priemonių.

6.3. Reglamentavimo nuorodos. Šioje VPS nuoroda į HIPAA taisyklių skyrių reiškia tą HIPAA skyrių, privatumo taisyklę, saugumo taisyklę, HITECH ACT arba galutines „Omnibus“ taisykles su pakeitimais ir galiojančiomis nuostatomis, kurių reikalaujama laikytis.

6.4. Pakeitimas. Šalys susitaria geranoriškai derėtis dėl bet kokių šios VPS pakeitimų, kurių kartais gali prireikti, kad klientas arba verslo partneris atitiktų HIPAA taisyklių reikalavimus. Jei per šešiasdešimt (60) dienų nuo kliento rašytinio prašymo verslo partneriui gavimo dienos šalys negali pasiekti abipusio susitarimo dėl bet kokio tokio pakeitimo sąlygų, bet kuri šalis turi teisę nutraukti šią VPS ir Sutartį, apie tai raštu pranešusi kitai šaliai ne vėliau kaip prieš trisdešimt (30) dienų.

6.5. Nėra trečiųjų šalių naudos gavėjų. Jokia šioje VPS išreikšta ar numanoma nuostata nesiekiama suteikti ir nesuteikia jokių teisių, teisių gynimo priemonių, pareigų ar įsipareigojimų jokiam kitam asmeniui, išskyrus klientą, verslo partnerį ir jų atitinkamus teisių perėmėjus ar perleidėjus.

6.6. Nepriklausomas rangovas. Verslo partneris, įskaitant jo direktorius, pareigūnus, darbuotojus ir atstovus, yra nepriklausomas rangovas, o ne kliento ar jo darbuotojų atstovas (kaip apibrėžta pagal bendrąją federalinę atstovavimo teisę. Neapribojant bendro pirmiau esančių nuostatų pobūdžio, klientas neturi teisės kontroliuoti, vadovauti ar kitaip daryti įtaką Verslo asocijuotojo elgesiui teikiant paslaugas, išskyrus šios VPS ar Sutarties vykdymą arba abipusius jų pakeitimus.

6.7. Pirmenybė; visa Sutartis. Bet kokie šios VPS neaiškumai ar dviprasmybės sprendžiami taip, kad šalys galėtų laikytis HIPAA taisyklių. Ši VPS yra visas šalių susitarimas dėl jos dalyko ir pakeičia visus ankstesnius pranešimus, pareiškimus, susitarimus ir susitarimus, susijusius su HIPAA taisyklėmis, įskaitant visus ankstesnius šalių verslo partnerių susitarimus.