Datu Apstrādes Līgums

NOLŪKS UN PRIORITĀTES SECĪBA

Šis Datu Apstrādes Līgums kopā ar tā pielikumiem un jebkuriem dokumentiem, uz kuriem ir skaidras atsauces (turpmāk — "**DAL**"), tiek uzskatīts par daļu no pakalpojumu līguma starp Iron Mountain un Klientu (turpmāk — "**Līgums**"). Līguma noteikumi un nosacījumi attiecas un regulē pušu tiesības un pienākumus saskaņā ar šo DAL.

Ja kādi šajā DAL ietvertie noteikumi un nosacījumi ir pretrunā ar Līgumā izklāstītajiem noteikumiem un nosacījumiem, šajā DAL izklāstītie noteikumi un nosacījumi ir kontrolējošie noteikumi un nosacījumi attiecībā uz šīs DAL priekšmetu. Šis DAL aizstāj visus un jebkurus iepriekšējos datu apstrādes līgumus vai datu aizsardzības vai privātuma klauzulas starp pusēm saistībā ar Pakalpojumiem, kas sniegti saskaņā ar Līgumu.

VISPĀRĒJIE NOTEIKUMI

1. DEFINĪCIJAS

Ja vien šeit nav īpaši definēts, visiem ar lielajiem burtiem rakstītajiem jēdzieniem ir tāda pati nozīme, kāda tiem ir piešķirta Līgumā.

"**Pārzinis**" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai cita struktūra, kas viena pati vai kopā ar citiem nosaka Personas Datu Apstrādes nolūkus un līdzekļus.

"**Klienta Personas Dati**" ir Personas Dati, kas pieder Klientam vai ko vāc Klients vai tā saistītie uzņēmumi, kas tiek Apstrādāti Pakalpojumu ietvaros.

"**Datu Subjekts**" ir identificēta vai identificējama fiziska persona.

"Datu Aizsardzības Tiesību Akti" ir visi piemērojamie tiesības akti un noteikumi, kas attiecas uz Personas Datu Apstrādi, kas var pastāvēt attiecīgajās jurisdikcijās, tostarp, bet ne tikai, ES VDAR (Regula (ES) 2016/679), Apvienotās Karalistes VDAR (VDAR, kas piemērojama kā daļa no Apvienotās Karalistes iekšzemes tiesību aktiem saskaņā ar 2018. gada Eiropas Savienības (Izstāšanās) likuma 3. sadaļu un kas grozīta ar Datu aizsardzību, Privātuma un elektroniskā saziņa (grozījumi utt.) (ES izstāšanās) 2019. gada regulas (ar grozījumiem), 2018. gada datu aizsardzības likums, Šveices federālais datu aizsardzības likums (Federal Act on Data Protection jeb FADP), ASV štata privātuma likumi, LGPD (Brazīlijas Vispārīgais datu aizsardzības likums), ar jebkuriem tiesību aktiem un/vai noteikumiem, ar kuriem tiek īstenoti vai pieņemti saskaņā ar tiem vai kas kādus no tiem groza, aizstāj, ievieš no jauna vai konsolidē, tostarp, ja piemērojams, uzraudzības iestāžu izdotās vadlīnijas un prakses kodeksus.

"**Personas Dati**" ir jebkura informācija, kas attiecas uz Datu Subjektu.

"**Apstrādātājs**" ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai cita struktūra, kas Apstrādā Personas Datus Pārziņa vārdā.

"**Apstrāde**" ir jebkura darbība vai darbību kopums, kas tiek veikts ar Personas Datiem vai Personas Datu kopām, vai nu ar automatizētiem līdzekļiem, piemēram, vākšanu, ierakstīšanu, organizēšanu, strukturēšanu, glabāšanu, pielāgošanu vai pārveidošanu, izguvi, konsultēšanu, izmantošanu, izpaušanu, nosūtot, izplatot vai citādi padarot pieejamu, saskaņošanu vai apvienošanu, ierobežošanu, dzēšanu vai iznīcināšanu.

"**Drošības Pārkāpums**" nozīmē jebkuru nejaušu vai nelikumīgu bojājumu, iznīcināšanu, pazaudēšanu, pārveidošanu vai neatļautu izpaušanu vai piekļuvi Klienta Personas Datiem, ko Iron Mountain, tā darbinieki vai apakšuzņēmēji Apstrādā Pakalpojumu sniegšanas laikā.

"**Pakalpojumi**" nozīmē jebkādus pakalpojumus, ko Iron Mountain vai tā saistītie uzņēmumi sniedz Klientam vai tā saistītajiem uzņēmumiem saskaņā ar Līgumu.

"**ASV Štata Privātuma Tiesību Akti**" ir visi Amerikas Savienoto Valstu štata privātuma un datu aizsardzības tiesību akti, kas ir piemērojami Personas Datu Apstrādei saskaņā ar Līgumu, tostarp bez ierobežojumiem, un kas laiku pa laikam var tikt grozīti, aizstāti: (1) Kalifornijas Patērētāju privātuma likums, kas grozīts ar Kalifornijas Privātuma tiesību likumu, un visi ar to saistītie īstenošanas noteikumi (kopā — California Privacy Rights Act jeb

“**CCPA**”); (2) Kolorādo Privātuma likums (Colorado Privacy Act jeb “**CPA”**), (3) Virdžīnijas Patērētāju datu aizsardzības likums (Consumer Data Protection Ac jeb “**CDPA**”); (4) Jūtas Patērētāju privātuma likums (Utah Consumer Privacy Act jeb “**UCPA**”); un (5) Konektikutas datu privātuma likums (Connecticut Data Privacy Act jeb “**CTDPA**”).

2. TVĒRUMS UN DATU APSTRĀDES INFORMĀCIJA

2.1 Šī DAL attiecas uz Klienta Personas Datiem, ko Iron Mountain apstrādā kā Apstrādātājs, sniedzot Pakalpojumus saskaņā ar Līgumu Klienta vārdā.

2.2 Iron Mountain var vākt un Apstrādāt Klienta un tā saistīto uzņēmumu darbinieku Personas Datus kā Pārzinis likumīgiem uzņēmējdarbības nolūkiem, piemēram, līgumu un klientu attiecību pārvaldībai, un saskaņā ar Datu Aizsardzības Tiesību Aktiem un Iron Mountain Privātuma paziņojumu, kas pieejams Iron Mountain tīmekļa vietnēs, un citām piemērojamām privātuma politikām. Iron Mountain pienākumi, kas noteikti šajā DAL, neattiecas uz šādu Personas Datu apstrādi.

2.3 Personas Datu Apstrādes priekšmets ir Pakalpojumu sniegšana. Klienta un Iron Mountain tiesības un pienākumi ir noteikti šajā DAL. Šī DAL 1. pielikums nosaka Apstrādes būtību, ilgumu un nolūku, Klienta Personas Datu Iron Mountain Apstrādes veidus un Datu Subjektu kategorijas, kuru Personas Dati tiek Apstrādāti.

2.4 Kad Iron Mountain Pakalpojumu sniegšanas laikā Apstrādā Klientu Personas Datus, Iron Mountain veiks turpmāk minēto.

2.4.1 Apstrādās Klienta Personas Datus tikai saskaņā ar dokumentētiem Klienta norādījumiem. Ja Iron Mountain jāapstrādā Klienta Personas Dati jebkādiem citiem nolūkiem saskaņā ar tiesību aktiem, uz kuriem attiecas Iron Mountain, Iron Mountain vispirms informēs Klientu par šo prasību, ja vien šāds(-i) tiesību akts(-i) to neaizliedz svarīgu sabiedrības interešu dēļ.

2.4.2 Vienmēr ievērojiet piemērojamos Datu Aizsardzības Tiesību Aktus un nekavējoties informējiet Klientu, ja, pēc Iron Mountain domām, Klienta sniegtais norādījums par Klienta Personas Datu apstrādi pārkāpj piemērojamos Datu Aizsardzības Tiesību Aktus.

2.5 Klienta norādījumi būs saistoši uzņēmumam Iron Mountain, ja vien norādījumu izpildei nav nepieciešama pakalpojuma sniegšana saskaņā ar Līgumu un Klients nepiekrīt maksāt pakalpojumu maksu par šādiem pakalpojumiem.

2.6 Iron Mountain nodrošina, ka personālam, kuram nepieciešams piekļūt Klienta Personas Datiem, ir saistošs pienākums ievērot konfidencialitāti attiecībā uz šādiem Klienta Personas Datiem, un veic saprātīgus pasākumus, lai nodrošinātu Iron Mountain personāla uzticamību un kompetenci, kuriem ir piekļuve Klienta Personas Datiem.

3. PALĪDZĪBAS SNIEGŠANA KLIENTAM

3.1 Iron Mountain sniedz palīdzību Klientam, vienmēr ņemot vērā Apstrādes raksturu:

3.1.1 ar atbilstošiem tehniskiem un organizatoriskiem pasākumiem un iespēju robežās, pildot Klienta pienākumus atbildēt uz Datu Subjektu pieprasījumiem, kuri īsteno savas tiesības;

3.1.2 nodrošinot Klienta pienākumu izpildi (piemēram, Apstrādes drošība, Personas Datu aizsardzības pārkāpuma paziņošana uzraudzības iestādei, Personas Datu aizsardzības pārkāpuma paziņošana Datu Subjektam, ietekmes uz datu aizsardzību novērtējums un iepriekšēja apspriešanās ar uzraudzības iestādēm, ja Apstrāde radītu augstu risku, ja Pārzinis neveiks pasākumus riska mazināšanai), ņemot vērā Iron Mountain pieejamo informāciju; un

3.1.3 nododot Klientam pieejamu visu informāciju, ko Klients pamatoti pieprasa, lai ļautu Klientam pierādīt, ka tā pienākumi, izvēloties un ieceļot Iron Mountain, ir izpildīti.

4.DROŠĪBAS PASĀKUMI

4.1. Ņemot vērā parastās darbības procedūras, ieviešanas izmaksas un apstrādes veidu, tvērumu, kontekstu un nolūkus, Iron Mountain īsteno atbilstošus un saprātīgus tehniskos un organizatoriskos pasākumus, kas paredzēti, lai aizsargātu Klienta Personas Datu konfidencialitāti, integritāti un pieejamību un aizsargātu Klienta Personas Datus pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu, bojājumiem, pārveidošanu vai izpaušanu. Iron Mountain drošības standarti ir izklāstīti šī DAL 2. pielikumā.

4.2. Tikai Klients ir atbildīgs par to, vai šie tehniskie un organizatoriski pasākumi atbilst Klienta prasībām.

5. ATBILSTĪBA TIESĪBU AKTIEM

Klients un tā saistītie uzņēmumi: (i) apstrādā Klienta Personas Datus saskaņā ar Datu Aizsardzības Tiesību Aktiem; (ii) ir pilnvarots sniegt Iron Mountain rakstiskus norādījumus par Klienta Personas Datu Apstrādi saistībā ar Pakalpojumiem (tostarp jebkuras trešās personas subjekta vārdā, kas ir Klienta

Personas Datu Pārzinis); un (iii) vienmēr saglabā kontroli un pilnvaras pār Klienta Personas Datiem saistībā ar Apstrādi.

6. APAKŠAPSTRĀDE

6.1. Klients atzīst un piekrīt, ka Iron Mountain var piesaistīt savu mātesuzņēmumu, tā saistītos uzņēmumus un citus trešo personu apakšapstrādātājus (tostarp trešo personu apakšapstrādātājiem, ko iesaistījuši Iron Mountain saistītie uzņēmumi vai mātesuzņēmumi), lai saskaņā ar šo DAL apstrādātu Klienta Personas Datus, ievērojot tālāk minēto 6.2. punktu.

6.2. Klienta apstiprināto apakšapstrādātāju saraksts šī DAL datumā ir pieejams šeit[1]. Iron Mountain var jebkurā laikā nomainīt vai iecelt jaunu apakšapstrādātāju, ja Klients tiek informēts piecpadsmit (15) dienas iepriekš un Klients neiebilst pret šādām izmaiņām, pamatojoties uz pierādāmu ar datu aizsardzību saistītu iemeslu dēļ. Lai saņemtu šos e-pasta paziņojumus, Klients abonē un pārvalda jebkuru esošo Iron Mountain paziņojumu pakalpojuma abonementu, izmantojot šo tīmekļa lapu[2].

6.3. Ja Klients neabonē šo paziņojumu pakalpojumu, Iron Mountain nav atbildīgs par apakšprocesora paziņojuma trūkumu, un visas šādas tikšanās tiks uzskatītas par Klienta pilnvarotām. Ja Klients piecpadsmit (15) dienu laikā iepriekš rakstiski iebilst, pamatojoties uz pierādāmiem ar datu aizsardzību saistītiem iemesliem, pret aizstājēja vai jauna apakšapstrādātāja iecelšanu, tad Iron Mountain pieliks saprātīgas pūles, lai padarītu Klientam pieejamas izmaiņas Pakalpojumos vai ieteiktu izmaiņas Klienta konfigurācijā vai Pakalpojumu lietošanā, katrā gadījumā izvairīties no Klienta Personas Datu Apstrādes, ko veic apakšapstrādātājs, kuram iesniegts iebildums, lai to izskatītu un apstiprinātu. Ja Klients piecpadsmit (15) dienu laikā neapstiprina šādas Iron Mountain ierosinātās izmaiņas, Iron Mountain, iesniedzot Klientam rakstisku paziņojumu, var nekavējoties izbeigt Pakalpojumu vai Pakalpojuma daļu, ko Iron Mountain nevar nodrošināt, neizmantojot apakšapstrādātāju, kuram ir iebildums. Šāda izbeigšana neskar jebkādas pušu uzkrātās tiesības un saistības ar nosacījumu, ka Iron Mountain vai Iron Mountain saistītie uzņēmumi nemaksās nekādas izbeigšanas maksas, izdevumus vai citas kompensācijas saistībā ar šādu izbeigšanu, un Klients nekavējoties pārņem īpašumā īpašumus, ko tas ir piešķīris Iron Mountain kā daļu no pārtrauktajiem Pakalpojumiem, ievērojot Līguma noteikumus un uz Klienta paša rēķina.

6.4. Iron Mountain nodrošina, ka visos līgumos ar apakšapstrādātājiem, kas ietilpst šī DAL darbības jomā, ir ietverti noteikumi, kas visos būtiskajos aspektos ir tādi paši kā šajā DAL un atbilst piemērojamajiem Datu aizsardzības tiesību aktiem. Ja Iron Mountain apakšapstrādātāja dēļ Iron Mountain pārkāpj savus pienākumus saskaņā ar šo DAL vai jebkuru piemērojamo Datu aizsardzības tiesību aktu, Iron Mountain joprojām ir pilnībā atbildīgs pret Klientu par Iron Mountain saistību izpildi saskaņā ar šiem noteikumiem.

7. DROŠĪBAS PĀRKĀPUMI

7.1. Ja ir aizdomas par Drošības pārkāpumu, Iron Mountain:

7.1.1. nekavējoties veiks pasākumus, lai izmeklētu iespējamo Drošības pārkāpumu un identificētu, novērstu un mazinātu iespējamā Drošības pārkāpuma sekas un novērstu Drošības pārkāpumu;

7.1.2. bez nepamatotas kavēšanās paziņos Klientam, tiklīdz tam ir pietiekama pārliecība, ka ir noticis Drošības pārkāpums, un sniegs Klientam detalizētu Drošības pārkāpuma aprakstu, tostarp informāciju, kura ir pamatoti nepieciešama, lai Klients izpildītu ziņošanas pienākumus saskaņā ar Datu aizsardzības tiesību aktiem.

7.2. Klients piekrīt, ka Iron Mountain informāciju saskaņā ar 7.1.2. punktu var sniegt pakāpeniski. Šādos gadījumos, kad Iron Mountain nav piekļuves vai nevar sniegt Klientam noteiktu informāciju, kas minēta 7.1.2. punktā, Iron Mountain attiecīgi informēs Klientu, un Iron Mountain nav atbildīgs par šādas informācijas nesniegšanu.

8. REVĪZIJAS

Iron Mountain ļaus Klientam un tā attiecīgajiem auditoriem vai pilnvarotajiem aģentiem, paziņojot Iron Mountain vismaz desmit (10) darba dienas iepriekš, veikt revīzijas vai pārbaudes Līguma darbības laikā, ar nosacījumu, ka Iron Mountain nav jāsniedz informācija vai jāatļauj piekļuve tai informācijai par: (i) citiem Iron Mountain klientiem; (ii) jebkuru no Iron Mountain nepubliskiem ārējiem ziņojumiem; un (iii) jebkuriem iekšējiem ziņojumiem, ko sagatavojusi Iron Mountain iekšējās revīzijas vai atbilstības funkcija. Revīzijas vai pārbaudes nolūki saskaņā ar šo klauzulu aprobežojas ar pārbaudi, vai Iron Mountain apstrādā Klienta Personas Datus saskaņā ar saviem pienākumiem saskaņā ar šo DAL. Izņemot

[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=xNzeKIzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

gadījumus, kad ir noticis Drošības pārkāpums, divpadsmit (12) mēnešu periodā nedrīkst veikt vairāk nekā vienu šādu revīziju.

9. STARPTAUTISKA DATU PĀRSŪTĪŠANA (IEROBEŽOTA PĀRSŪTĪŠANA)

9.1. Ciktāl tas ir piemērojams, Klients piekrīt un atļauj Klienta Personas Datu starptautisku pārsūtīšanu struktūrām, kas noteiktas 6.2. sadaļā un saskaņā ar 3. pielikumu, lai sniegtu Pakalpojumus, un Klients un Iron Mountain vienojas:

9.1.1. ievērot piemērojamos Datu aizsardzības tiesību aktus attiecībā uz šādu pārsūtīšanu;

9.1.2. ka viņiem ir, bez ierobežojumiem ņemot vērā: i) Klienta Personas Datu kategorijas; ii) valstis, kuru nacionālie tiesību akti nevar nodrošināt personas datu aizsardzības līmeni, kas ir salīdzināms ar ES/AK tiesību aktu ("**Trešās valstis**") darbības jomas līmeni; iii) attiecīgos tehniskos un organizatoriskos pasākumus, kas noteikti 7. sadaļā; un iv) attiecīgās puses, kuras piedalās šādu Klienta Personas Datu apstrādē, ir veikušas attiecīgos nosūtīšanas mehānisma, kas pieņemts saskaņā ar šo noteikumu, atbilstības novērtējumu, ja to pieprasa tiesību akti, un ir noteikušas, ka šāds pārsūtīšanas mehānisms ir atbilstoši izstrādāts, lai nodrošinātu, ka saskaņā ar šo DAL pārsūtītajiem Personas Datiem galamērķa valstī tiek nodrošināts aizsardzības līmenis, kas būtībā ir līdzvērtīgs Datu Aizsardzības Tiesību Aktos garantētajam.

10. ATBILDĪBA UN ZAUDĒJUMU ATLĪDZINĀŠANA

10.1. Neatkarīgi no tā, ka Līgumā ir norādīts pretējais, Drošības pārkāpuma gadījumā, ko tieši izraisījis Iron Mountain pienākumu pārkāpums saskaņā ar šo DAL, Iron Mountain, ciktāl to pieļauj piemērojamie tiesību akti, atlīdzina Klientam tiešās, pārbaudāmās, nepieciešamās un pamatoti radušās trešās personas izmaksas Klientam saistībā ar: a) šāda Drošības pārkāpuma izmeklēšanu; b) paziņojumu sagatavošanu un nosūtīšanu šādiem Datu Subjektiem un regulatīvajām iestādēm saskaņā ar Datu aizsardzības tiesību aktiem; c) kredītu uzraudzības pakalpojumu sniegšanu šādām personām saskaņā ar tiesību aktiem uz laiku, kas nepārsniedz divpadsmit (12) mēnešus; un d) uzraudzības iestādes noteikto regulējošo naudas sodu, sodu vai sankciju daļas samaksu, par kuru uzraudzības iestāde norāda, ka uzņēmums Iron Mountain ir tieši atbildīgs.

10.2. Ja Datu Subjekts ceļ prasību pret vienu vai abām pusēm par iespējamu datu aizsardzības tiesību aktu pārkāpumu ("**Datu Subjekta Prasības**"), kur tas ir atļauts, katra puse kontrolē savu aizstāvību pret jebkuru šādu prasību (vai tās daļu no aizstāvības) un ir pilnībā atbildīga par savām izmaksām, izdevumiem un saistībām, kas ar to saistīti, tostarp par juridiskajām maksām vai jebkādām summām, ko tai piespriedusi tiesa vai ko tā piešķīrusi izlīgumā, tomēr ar nosacījumu, ka katra puse ir atbildīga par daļu vai jebkura no pusēm ir atbildīga par pilnu zaudējumu apmēru, kas Datu Subjektam nodarīts par vienu un to pašu incidentu vai incidentu sēriju, un Datu Subjekts ir atguvis pilnu kompensāciju tikai no vienas puses("**Atlīdzinātāja Puse"**), tad Atlīdzinātājai Pusei ir tiesības pieprasīt atpakaļ no otras puses to kompensācijas daļu, kas atbilst šīs otras puses nodarītajam kaitējumam. Atlīdzinātāja puse var celt prasību pret otru pusi tikai 12 mēnešu laikā pēc incidenta, ciktāl to pieļauj piemērojamie tiesību akti.

10.3. Ciktāl to pieļauj piemērojamie tiesību akti, atbildības ierobežojumi un jebkādi zaudējumu atlīdzināšanas izņēmumi, kas noteikti Līgumā, regulē kopējo atbildību par visām Klienta prasībām, kuras izriet no vai ir saistītas ar šo DAL un/vai Līgumu pret Iron Mountain. Šie atbildības ierobežojumi un zaudējumu atlīdzināšanas izņēmumi attiecas uz visām prasībām neatkarīgi no tā, vai tās rodas saskaņā ar līgumu, deliktu vai jebkuru citu atbildības teoriju, un jebkura atsauce uz Iron Mountain atbildību nozīmē Iron Mountain un visu Iron Mountain saistīto uzņēmumu kopējo atbildību par Klienta un visu citu Klienta saistīto uzņēmumu prasībām. Ciktāl to prasa piemērojamie tiesību akti, šī sadaļa nav paredzēta, lai (i) mainītu vai ierobežotu pušu atbildību par Datu Subjekta prasībām, kuras celtas pret pusi, ja pastāv solidāra atbildība, vai (ii) ierobežotu katras puses atbildību maksāt sodus, ko šai pusei uzlikusi regulējošā iestāde.

10.4. 10.1.–10.3. punktā ir norādīts katras puses vienīgais un ekskluzīvais tiesiskās aizsardzības līdzeklis un katras puses vienīgā atbildība par jebkādiem zaudējumiem, bojājumiem, izdevumiem vai saistībām saistībā ar šo DAL.

11. VALSTS IESTĀDES PIEPRASĪJUMI

11.1. Ciktāl tas ir likumīgi atļauts un ievērojot tālāk minētos 11.2.–11.5. punktus, Iron Mountain piekrīt informēt Klientu, ja:

11.1.1. Tas saņem juridiski saistošu pieprasījumu no valsts iestādes, tostarp tiesu iestādēm, saskaņā ar galamērķa valsts tiesību aktiem par Klienta Personas Datu izpaušanu, kas nodoti saskaņā ar Līgumu. vai

11.1.2. Tam kļūst zināms par jebkādu tiešu valsts iestāžu piekļuvi Klienta Personas Datiem, kas nodoti atbilstoši Līgumam saskaņā ar galamērķa valsts tiesību aktiem.

11.2. Ja uzņēmumam Iron Mountain ir aizliegts informēt Klientu saskaņā ar galamērķa valsts tiesību aktiem, Iron Mountain piekrīt pielikt visas pūles, lai panāktu atteikšanos no aizlieguma, lai pēc iespējas ātrāk paziņotu pēc iespējas vairāk informācijas.

11.3. Iron Mountain piekrīt pārskatīt informācijas izpaušanas pieprasījuma likumību, jo īpaši, vai tas paliek pieprasījuma iesniedzējai valsts iestādei piešķirto pilnvaru robežās, un apstrīdēt pieprasījumu, ja tas secina, ka ir pamatots iemesls uzskatīt, ka pieprasījums ir nelikumīgs saskaņā ar galamērķa valsts tiesību aktiem. Tas neizpauž pieprasītos Klienta Personas Datus, kamēr tas nav jādara saskaņā ar piemērojamajiem procedūras noteikumiem.

11.4. Iron Mountain piekrīt sniegt minimālo pieļaujamo informācijas apjomu, atbildot uz informācijas izpaušanas pieprasījumu, pamatojoties uz saprātīgu pieprasījuma interpretāciju.

11.5. Iron Mountain piekrīt saglabāt informāciju saskaņā ar šo punktu Līguma darbības laikā un pēc pieprasījuma darīt to pieejamu kompetentajai uzraudzības iestādei.

12. DAŽĀDI

12.1. Ņemot vērā Iron Mountain sniegto Pakalpojumu raksturu, Līguma izbeigšanas/termiņa beigās, pamatojoties uz īpašu Klienta norādījumu un ievērojot Līguma noteikumus, Iron Mountain vai nu dzēš/iznīcina vai atdod Klientam vai Klienta norādītai trešajai personai visus Klienta Personas Datus. Jebkuri Klienta Personas Dati, kas ir ietverti Klienta īpašumā, ko Iron Mountain glabā Klienta vārdā, tiks atgriezti Klientam saskaņā ar saskaņotu izejas vai pārejas plānu un saskaņā ar saskaņotām izmaksām, kā noteikts Līgumā vai citā piemērojamā Līguma dokumentā. Visos citos gadījumos, ja Līgumā nav runāts par Klienta Personas Datu dzēšanu/iznīcināšanu vai atdošanu un Klients nedod nekādus norādījumus par Klienta Personas Datu dzēšanu/iznīcināšanu vai atgriešanu piecpadsmit (15) dienu laikā pēc Līguma izbeigšanas/termiņa beigām, Iron Mountain nosūta Klientam rakstisku paziņojumu, pieprasot piecpadsmit (15) dienu laikā saņemt konkrētus norādījumus par to, vai dzēst/iznīcināt vai atgriezt Klienta Personas Datus, un informējot Klientu par visām piemērojamām drošas iznīcināšanas vai citām maksām, kas Klientam jāmaksā. Ja Klients nesniedz rakstiskus norādījumus šajā piecpadsmit (15) dienu laikā un nesamaksā piemērojamo maksu šajā pašā termiņā, tad Klients ar šo pilnvaro Iron Mountain turpināt apstrādāt, dzēst, iznīcināt visus Klienta Personas Datus pēc Līguma izbeigšanas pēc Iron Mountain izvēles un uz Klienta rēķina.

12.2. Neatkarīgi no 12.1. punkta Iron Mountain nepārkāps savus pienākumus attiecībā uz Klientu Personas Datu dzēšanu, kas saglabāti dublējumkopiju kasetēs, kamēr šādas dublējuma lentes tiek ignorētas (un līdz ar to Klienta Personas Dati tiek dzēsti) parastās uzņēmējdarbības gaitā.

12.3. Izņemot Līguma tipveida klauzulas (kā noteikts šī DAL 3.pielikumā), šo DAL un jebkuru strīdu, prasību vai pretrunu, kas izriet no šī DAL vai ir saistīts ar to, vai tā pārkāpšanu, izbeigšanu vai spēkā esamību, regulē Līguma tiesību aktu izvēles noteikums; un jebkuru strīdu, pretrunu vai prasību, kas izriet no šī DAL vai saistībā ar to, galvenokārt centīsies atrisināt, izmantojot jebkuru noteiktu strīdu izšķiršanas procesu, kas ietverts Līgumā.

12.4. Katra puse var laiku pa laikam rakstiski paziņot otrai pusei par jebkādām izmaiņām šajā DAL, ko puse pamatoti uzskata par nepieciešamām, lai izpildītu Datu aizsardzības tiesību aktu prasības vai jebkuru uzraudzības iestādes vai kompetentas tiesas lēmumu. Jebkuri šādi grozījumi stājas spēkā tikai tad, ja un tādā apjomā, kas noteikts abpusēji saskaņotā šī DAL grozījumā, ko īstenojušas abas puses, izņemot gadījumus, kad viena puse informē otru pusi par jebkuru jaunu juridisku prasību un nosūta šādu grozījumu, kas ietver tikai nepieciešamās izmaiņas un kurus var pieņemt, tam formāli nepiekrītot, t. i., neceļot iebildumus noteiktā termiņā, tiek uzskatīti par savstarpēji saskaņotiem šī DAL grozījumiem.

1. PIELIKUMS

Detalizēta informācija par Apstrādi un Datu pārsūtīšanu (ja piemērojams)

A. PUŠU SARAKSTS.

Šīs DAL puses un Datu nosūtītāja un Datu saņēmēja lomas ir noteiktas Līgumā un 3. pielikumā (Starptautiskā datu pārsūtīšana), ja piemērojams.

B. APSTRĀDES/PĀRSŪTĪŠANAS APRAKSTS (ja piemērojams).

Datu Subjektu kategorijas, kuru Personas Dati tiek apstrādāti/pārsūtīti.

Atkarībā no Iron Mountain Pakalpojumu veida un Klienta uzņēmējdarbības Klients var iesniegt Iron Mountain Personas Datus, kas pieder dažādām Datu Subjektu kategorijām, kuru apjomu Klients nosaka un kontrolē pēc saviem ieskatiem. Datu Subjektu kategorijās var ietilpt: bijušie un esošie darbinieki; bijušie un esošie darbuzņēmēji vai konsultanti; aģentūras nodrošināti darbuzņēmēji vai konsultanti un ārējie norīkotie darbinieki; darba pretendenti un kandidāti; studenti un brīvprātīgie; personas, kuras darbinieki vai pensionāri identificējuši kā labuma guvējus, laulātais, ģimenes loceklis/civilpartneris, apgādājamie un ārkārtas kontaktpersonas; pensionāri; bijušie un esošie direktori un amatpersonas; akcionāri; obligāciju turētāji; kontu turētāji; galalietotāji/patērētāji (pieaugušie, bērni); pacienti (pieaugušie, bērni); garāmejošie (videonovērošanas kameras); un tīmekļa vietnes lietotāji.

Apstrādāto/pārsūtīto personas datu kategorijas.

Atkarībā no Iron Mountain Pakalpojumu veida un Klienta uzņēmējdarbības Klients var iesniegt Iron Mountain Personas Datus, kas pieder dažādām Personu Datu kategorijām, kuru apjomu Klients nosaka un kontrolē pēc saviem ieskatiem. Kā tādas kategorijas var ietvert Personas Datus, kas attiecas uz Klientu un/vai paša Klienta klientiem, darbiniekiem utt.

Pārsūtīti sensitīvi dati (ja piemērojams).

Atkarībā no Iron Mountain pakalpojumu veida un Klienta uzņēmējdarbības Klients var iesniegt Iron Mountain sensitīvus datus, kuru apjomu Klients nosaka un kontrolē pēc saviem ieskatiem.

Ja piemērojams, pārsūtīšanas biežums (piemēram, vai dati tiek pārsūtīti vienreizēji vai nepārtraukti).

Pārsūtīšana notiek nepārtraukti.

Apstrādes veids.

Savākšana, ierakstīšana, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, izguve, konsultēšana, izmantošana, izpaušana, nosūtot, izplatot vai citādi padarot pieejamu, saskaņošana vai apvienošana, ierobežošana, dzēšana vai iznīcināšana.

Datu apstrādes/pārsūtīšanas (ja piemērojams) un turpmākās apstrādes nolūks(-i).

Pakalpojumu sniegšana, kā noteikts Līgumā.

Datu glabāšana.

Iron Mountain glabās Personas Datus Klientam piedāvāto Pakalpojumu laikā un līdz tam laikam, kad Personas Dati tiek atgriezti vai iznīcināti, kā noteikts saskaņā ar šī DAL 12.1. punktu.

Ja piemērojams, nosūtot (apakš)apstrādātājiem, norādiet arī Apstrādes priekšmetu, veidu un ilgumu.

Līguma ar Klientu darbības laikā apakšapstrādātāji cita starpā sniedz informācijas tehnoloģiju (IT) un konsultāciju pakalpojumus, tostarp globālo IT atbalstu, notikumu ziņošanas un pārvaldības pakalpojumus.

C. KOMPETENTĀ UZRAUDZĪBAS IESTĀDE

Kā noteikts 3. pielikumā (Starptautiskā Datu pārsūtīšana), ja piemērojams.

2. PIELIKUMS

TEHNISKIE UN ORGANIZATORISKIE PASĀKUMI ("DROŠĪBAS PASĀKUMI")

1. INFORMĀCIJAS DROŠĪBAS PROGRAMMA UN POLITIKA

Iron Mountain uztur informācijas drošības programmu ar atbilstošu fizisko, tehnisko un administratīvo kontroli, kas ir izstrādāta, lai atbilstu nozares standartiem. Informācijas drošības programmā iekļauj:

1.1. Iron Mountain informācijas drošības politiku, standartu un procedūru dokumentācija, iekšējā publikācija un saziņa;

1.2. dokumentētu, skaidru atbildības un pilnvaru sadalījumu informācijas drošības programmas izveidei un uzturēšanai;

1.3. regulāru informācijas drošības programmas galveno vadības ierīču, sistēmu un procedūru testēšanu;

1.4. administratīvos, tehniskos un operatīvos pasākumus, kas paredzēti, lai aizsargātu visus Klienta Personas Datus, izmantojot šajā drošības pielikumā aprakstītās prakses, procedūras un procesus, ciktāl tie ir būtiski un piemērojami formātam, kādā tiek uzturēti Klienta Personas Dati.

2. RISKA NOVĒRTĒŠANA

Iron Mountain uztur informācijas drošības riska novērtēšanas programmu, kura izstrādāta, lai identificētu un novērtētu saprātīgi paredzamus iekšējos un ārējos riskus un ievainojamības, kas varētu ietekmēt Klienta Personas Datu drošību, konfidencialitāti un/vai integritāti. Iron Mountain novērtē un atjaunina, ja nepieciešams, saprātīgi un piemēroti, pašreizējās informācijas drošības programmas efektivitāti šādu risku ierobežošanai katru gadu vai ikreiz, kad notiek būtiskas izmaiņas saistībā ar Klienta Personas Datu risku vai ievainojamību.

3. INFORMĀCIJAS APSTRĀDES LĪDZEKĻU UN FIZISKO DATU NESĒJU PĀRVALDĪBA

3.1. Informācijas apstrādes aktīvu pārvaldība. Iron Mountain uztur aktīvu krājumu pārvaldības programmu, lai pārvaldītu fizisko, tehnisko un administratīvo kontroli attiecībā uz Iron Mountain informācijas apstrādes aktīviem (piemēram, datoriem, serveriem, atmiņas ierīcēm, sakaru tīkliem, personālajiem datoriem, klēpjdatoriem un perifērijas ierīcēm).
Aktīvu krājumu pārvaldības programma ietver:

- 3.1.1. Dokumentēta īpašuma īpašumtiesību piešķiršanu Iron Mountain personālam, lai nodrošinātu atbilstošu informācijas klasifikāciju, piekļuves ierobežojumu noteikšanu un piekļuves kontroles pārskatīšanu.
- 3.1.2. Aktīvu dezinfekciju pirms to atsavināšanas saskaņā ar NIST 800-88.
- 3.1.3. Prasību saņemt pārvaldības atļauju pirms tāda aprīkojuma vai programmatūras noņemšanas no Iron Mountain telpām, kuras nav piešķirtas konkrētai personai.

3.2. Kontroles. Iron Mountain kontroles ietver:

- 3.2.1. Darbības procedūras un tehniskās kontroles, kas paredzētas, lai aizsargātu dokumentus, datoru datu nesējus, ievades/izvades/dublējuma datus un sistēmas dokumentāciju pret neatļautu izpaušanu, pārveidošanu un iznīcināšanu.
- 3.2.2. Elektronisko vai fizisko datu nesēju, kas satur Klienta Personas Datus, drošas iznīcināšanas procedūras.
- 3.2.3. Izveidotu procesu visu Klienta fizisko datu nesēju izsekošanai no sākotnējās Iron Mountain glabāšanas līdz pastāvīgai izņemšanai vai iznīcināšanai.

4. DARBASPĒKA DROŠĪBAS PASĀKUMI

4.1. Konfidencialitāte. Iron Mountain pamatoti pieprasa, lai visi Iron Mountain darbinieki, tostarp pagaidu darbinieki un līgumdarbinieki, piekristu glabāt Klienta Personas Datu konfidencialitāti un ievērot Iron Mountain iekšējās informācijas drošības un pieņemamas lietošanas prasības.

4.2. Iepriekšējās darbības pārbaudes politika. Iron Mountain darbinieki ir pakļauti iepriekšējās darbības pārbaudes un narkotiku testēšanas politikai (tikai ASV).Iron Mountain turpinās uzturēt šādu politiku Līguma darbības laikā. Politikas prasības ietver, bet ne tikai, narkotiku pārbaudi (tikai ASV), personāla identitātes verifikāciju, sodāmības reģistra meklēšanu, nodarbinātības pārbaudes, valdības/teroristu novērošanas saraksta meklēšanu, kā arī noteiktu darbinieku izglītības verifikāciju, kā arī autovadītāju apliecību un pārkāpumu vēsturi autovadītāju kandidātiem un esošajiem autovadītājiem. Ja iepriekšējās darbības pārbaudē tiek atklāta nievājoša informācija, Iron Mountain veic individuālu novērtējumu saskaņā ar piemērojamajiem darba tiesību aktiem un paraugpraksi.

4.3. Darbs ar apakšuzņēmējiem. Iron Mountain pieprasa, lai jebkurš apakšuzņēmējs, kas sniedz Pakalpojumus saskaņā ar Līgumu, ievērotu līdzīgus ierobežojumus, kādi noteikti šajā Sadaļā, attiecībā uz jebkuru apakšuzņēmēja personālu, kas saskaņā ar Līgumu veiks pakalpojumus, kas ietver Klienta Personas Datu Apstrādi.

4.4. Drošības izpratnes apmācība. Vismaz reizi gadā uzņēmums Iron Mountain visiem Iron Mountain darbiniekiem, kuriem ir piekļuve Klienta Personas Datiem, rīko vispārīgas drošības izpratnes apmācības un īpašas drošības apmācības par piemērojamām lomām. Iron Mountain uztur ierakstus, kuros norādīti šādu Iron Mountain darbinieku vārdi, kas apmeklējuši, un katras drošības izpratnes apmācības datums. Iron Mountain regulāri pārskata un atjaunina savu drošības izpratnes apmācības programmu.

4.5. Iron Mountain personāla atlaišana. Iron Mountain uztur disciplināro procesu, kas tiek piemērots Iron Mountain darbiniekiem, kuri pārkāpj šeit noteiktās drošības prasības.

4.6. Piekļuves pārtraukšana pēc izbeigšanas/pārcelšanas. Pārtraucot darba attiecības vai pārceļot uz citu amatu, kuram nav nepieciešama piekļuve Klienta Personas Datiem, Iron Mountain darbinieka piekļuve klienta Personas Datiem tiek nekavējoties atsaukta.

5. FIZISKĀ UN VIDES DROŠĪBA

5.1. Fiziskās drošības kontrole. Iron Mountain telpās tiek izmantotas fiziskas kontroles, kuras saprātīgi ierobežo piekļuvi Klienta Personas Datiem, tostarp, ja Iron Mountain uzskata par piemērotu, piekļuves kontroles protokoli, fiziski šķēršļi, piemēram, bloķētas telpas un zonas, darbinieku piekļuves žetoni, apmeklētāju žurnālus, apmeklētāju piekļuves žetoni, karšu lasītāji, videonovērošanas kameras un ielaušanās atklāšanas trauksmes signāli. Visiem apmeklētājiem jāpierakstās un tie vienmēr ir jāpavada.

5.2. Atbalsta utilītprogrammas. Iron Mountain izmanto pasākumus, kuri paredzēti, lai aizsargātu tās iekārtas, kurās ir Klienta Personas Dati, un sistēmas no strāvas, telekomunikāciju, ūdens apgādes, kanalizācijas, apkures, ventilācijas un gaisa kondicionēšanas traucējumiem, ja piemērojams.

5.3. Pārvades sistēmas drošība. Iron Mountain izmanto pasākumus, kuri paredzēti, lai aizsargātu tā tīkla infrastruktūras un telekomunikāciju sistēmu fizisko drošību no pārraides pārtveršanas un bojājumiem.

5.4. Izbraukuma aprīkojums. Gadījumā, ja Iron Mountain izmanto ārpakalpojumus funkcijas, kuru nodrošināšanai pakalpojumu atbalstam jāizmanto izbraukuma aprīkojums, visas izbraukuma iekārtas, kurās tiek glabāti Klienta Personas Dati, ir aizsargātas ar drošību, kas ir līdzvērtīga tai, ko izmanto uz vietas esošajām iekārtām, ko izmanto tiem pašiem nolūkiem.

5.5. Fiziska piekļuve informācijas apstrādes līdzekļiem. Iron Mountain vienu gadu glabā ierakstus par Iron Mountain darbiniekiem, kuriem ir atļauts fiziski piekļūt Iron Mountain kontrolētajai(-ām) datoru videi(-ēm), ko izmanto Iron Mountain, lai sniegtu Pakalpojumus vienu gadu un pēc Klienta pieprasījuma saistībā ar Drošības pārkāpumu un saskaņā ar Iron Mountain drošības politikām nodrošinātu piekļuvi Klientam, lai skatītu šādu Iron Mountain darbinieku pārbaudāmos ierakstus.

5.6. Fiziskā piekļuve ierobežota. Iron Mountain ierobežo fizisku piekļuvi Iron Mountain kontrolētajām iekārtām, kuras apstrādā Klientu Personas Datus, līdz tiem Iron Mountain darbiniekiem un pilnvarotām personām, kurām šāda piekļuve ir nepieciešama uzņēmējdarbībā. Iron Mountain ir apstiprinājuma process, lai autorizētu un izsekotu pieprasījumus fiziskai piekļuvei šādām telpām.

5.7. Remonts un modifikācijas. Uzņēmums Iron Mountain reģistrē visus ar drošību saistītos remontdarbus un jebkādu fizisko komponentu modifikācijas, tostarp aparatūru, sienas, durvis un drošo zonu slēdzenes telpās, kurās tiek glabāti Klienta Personas Dati.

5.8. Ieraksti. Saglabāt aparatūras un elektronisko plašsaziņas līdzekļu kustību un par to atbildīgo personu uzskaiti.

6. SAZIŅAS UN INFORMĀCIJAS APSTRĀDES OPERĀCIJU VADĪBA

6.1. Ierīces konfigurācijas standarti. Iron Mountain izveido, ievieš un uztur sistēmas administrēšanas procedūras, kuras atbilst nozares standartiem, tostarp bez ierobežojumiem sistēmas nostiprināšanu, sistēmas un ierīču ielāpojumu (operētājsistēmas un lietojumprogrammas) un pareizu pretvīrusu instalēšanu un atjauninājumus.

6.2. Informācijas apstrādes sistēmu izmaiņu kontrole. Iron Mountain ievieš iekšēju formālu izmaiņu pārvaldības pieprasījumu procesu informācijas apstrādes un sakaru tīklu sistēmām, un Iron Mountain izmaiņu pieprasījumi jādokumentē, jāpārbauda un jāapstiprina pirms jebkādu jaunu informācijas apstrādes vai tīkla sakaru iespēju, sistēmas ielāpu vai esošo sistēmu izmaiņu ieviešanas.

6.3. Pienākumu noškiršana. Iron Mountain nodala pienākumus un atbildības jomas, lai nevienai personai nebūtu vienīga iespēja mainīt informācijas apstrādes sistēmas, kas piekļūst Klienta Personas Datiem.

6.4. Izstrādes un ražošanas vides atdalīšana. Iron Mountain informācijas apstrādes sistēmu izstrādes, testēšanas un ražošanas vidēm jābūt loģiski vai fiziski nodalītām.

6.5. Tehniskās arhitektūras vadība. Iron Mountain izveido konfigurācijas pārvaldības procesu, lai definētu, pārvaldītu un kontrolētu informācijas apstrādes sistēmas komponentus, kas tiek izmantoti Pakalpojumu sniegšanai, un šādu komponentu tehnisko infrastruktūru.

6.6. Ielaušanās noteikšana. Iron Mountain pastāvīgi uzrauga datorsistēmas un procesus, lai atklātu mēģinājumus vai faktiski veiktu drošības ielaušanos vai pārkāpumus, un informē Klientu par jebkādu nesankcionētu piekļuvi Klienta Personas Datiem.

6.7. Tīkla drošība. Iron Mountain jānodrošina, lai:

6.7.1. Attiecībā uz Iron Mountain mitināto vidi(-ēm), ko izmanto Pakalpojumu sniegšanai, būtu tīkla ielaušanās noteikšanas sistēma (intrusion detection system jeb “IDS”) un ielaušanās novēršanas sensori (intrusion prevention sensors jeb “IPS”), brīdinājuma notikumi, kas tiek reģistrēti, ar ikdienas pārskatiem, kas tiek izsniegti pārskatīšanai (kopā saukti par “IDS/IPS”).

6.7.2. Attiecībā uz Iron Mountain mitināto vidi(-ēm), ko izmanto Pakalpojumu sniegšanai, būtu IDS/IPS, kas tiek atjaunināti ne retāk kā reizi nedēļā, bet cik drīz vien iespējams pēc atjauninājumu saņemšanas, un tūlītēju jaunāko draudu parakstu vai noteikumu izpildi.

6.7.3. Augsta riska pieslēgvietas uz āru vērstām sistēmām nav pieejamas no interneta.

6.7.4. Iron Mountain tīkla savienojumi tiek reģistrēti un reģistrēti žurnālfailos.

6.7.5. Būtu ugunsmūra(-u) izvietošana, kas izstrādāta, lai aizsargātu un pārbaudītu visu ienākošo un izejošo tīkla pakalpojumu trafiku starp noteiktiem tīkla punktiem.

6.7.6. Būtu stingrākas politikas ienākošā un izejošā tīkla portu vai pakalpojumu trafika noteikšanai visām Iron Mountain piederošajām vai pārvaldītajām sistēmām, kas ir dokumentētas un autorizētas informācijas drošības programmā.
6.7.7. Būtu tīkla un diagnostikas porti, kas ir pareizi nodrošināti; un
6.7.8. Būtu ieviestas šādas politikas, procedūras un tehniskās kontroles, kas paredzētas, lai novērstu, atklātu un noņemtu ļaunprātīgu kodu vai zināmus uzbrukumus Iron Mountain informācijas sistēmām.

6.8. Šifrēti autentifikācijas akreditācijas dati. Iron Mountain nodrošina, ka autentifikācijas akreditācijas dati, kas tiek pārsūtīti pa Iron Mountain tīkla ierīcēm, tiek šifrēti sūtīšanas laikā.

6.9. Droša tīkla administrēšana. Iron Mountain tīkli ir saprātīgi jāpārvalda un jākontrolē, lai aizsargātu pret zināmiem draudiem un uzturētu drošību visām Iron Mountain pārvaldītajām lietojumprogrammām un datiem tīklā. Ievieš tehniskās kontroles un drošus sakaru protokolus, lai aizliegtu neierobežotus savienojumus ar neuzticamiem tīkliem vai publiski pieejamiem serveriem.

6.10. Aizsardzība pret vīrusu. Iron Mountain ievieš un uztur pretvīrusu pārvaldības programmu, tostarp aizsardzību pret ļaunprātīgu programmatūru, atjauninātus parakstu failus vai alternatīvu aizsardzību pret jauniem draudiem, ielāpus un vīrusu definīcijas Iron Mountain pārvaldītajiem serveriem un darbstacijām, ko izmanto, lai izvietotu vai piekļūtu Klienta Personas Datiem.

6.11. Tīmekļa Vietne – Klienta šifrēšana. Iron Mountain nodrošina, ka katrai vietnei ir iespējota Drošligzdu slāņa (Secure Sockets Layering jeb SSL) funkcija un tajā ir derīgs SSL sertifikāts, kam nepieciešama konfidencialitāte, autentifikācija vai autorizācijas kontrole.

6.12. Informācijas dublēšana. Iron Mountain izveido atbilstošas sistēmas failu rezerves kopijas. Turklāt Iron Mountain izstrādā un uztur avārijas seku novēršanas procedūras. Plašāku informāciju skatiet tālāk sadaļā “Atkopšana katastrofu gadījumos”.

6.13. Elektroniskā informācija tranzītā. Iron Mountain izmanto šifrēšanu ar nozares standarta algoritmu ar vismaz 128 bitu atslēgas garumu, lai aizsargātu Klienta Personas Datus, kas tiek pārsūtīti pa publiskajiem tīkliem, ja tie ir iegūti no Iron Mountain mitinātās infrastruktūras.

6.14. Kriptogrāfiskās vadīklas. Iron Mountain ievēro dokumentētu politiku attiecībā uz kriptogrāfijas vadīkļu izmantošanu. Iron Mountain kriptogrāfijas vadīklas:
6.14.1. Ir izstrādātas, lai saprātīgi aizsargātu to Klienta Personas Datu konfidencialitāti un integritāti, ko Iron Mountain apstrādā, pārsūta vai glabā jebkurā koplietojamā tīkla vidē saskaņā ar Līguma noteikumiem.
6.14.2. Jāpiemēro Pakalpojumu sniegšanai izmantotajā(-ās) Iron Mountain mitinātajā(-s) vidē(-ēs) Klienta Personas Datiem, kuri tiek pārsūtīti pa vai uz “neuzticamiem” tīkliem (t. i., tīkliem, kurus Iron Mountain juridiski nekontrolē), tostarp tiem, kas tiek izmantoti datu nosūtīšanai uz Klienta korporatīvo tīklu no Iron Mountain tīkla, katrā gadījumā ievērojot Klienta sadarbību šifrēšanas atslēgu pārvaldībā, kas nepieciešamas, lai atšifrētu Klienta saņemtos sūtījumus; un
6.14.3. Ietver dokumentētu šifrēšanas atslēgu pārvaldības praksi, lai atbalstītu kriptogrāfijas tehnoloģiju drošību.
6.14.4. Ietver visu Klienta Personas Datu šifrēšanu klēpjdatoros vai citās pārnēsājamās ierīcēs.

6.15. Žurnālu prasības. Iron Mountain jānodrošina, ka:
6.15.1. Nozīmīgi drošības un sistēmu notikumi tiek reģistrēti un pārskatīti.
6.15.2. Revīziju žurnāli tiek glabāti vismaz vienu gadu sistēmām Iron Mountain mitinātā vidē(-ās), ko Iron Mountain izmanto pakalpojumu sniegšanai.
6.15.3. Tiek pārskatīti sistēmas revīzijas žurnāli, lai noteiktu anomālijas; un
6.15.4. Žurnālu iekārtas un sistēmu informācija ir pietiekami aizsargāta pret manipulācijām un neatļautu piekļuvi.

6.16. Tīkla laika sinhronizācija. Iron Mountain sinhronizē visu informācijas apstrādes sistēmu sistēmas pulksteņus, izmantojot kopīgu autoritatīvu laika avotu.

6.17. Segregācija tīklos. Iron Mountain pienācīgi nodala saistītās informācijas pakalpojumu grupas, lietotājus un informācijas sistēmas tīklos.

7. PIEKĻUVES KONTROLE

7.1. Piekļuves kontroles politika. Iron Mountain uztur piekļuves kontroles politikas attiecībā uz informācijas apstrādes līdzekļiem, kurus Iron Mountain oficiāli apstiprina, publicē un ievieš.

7.2. Loģiskās piekļuves autorizācija. Iron Mountain ir jāapstiprina loģiski piekļuves pieprasījumi Klienta Personas Datiem un pieprasījumi piekļūt Iron Mountain sistēmām, kas paredzētas izmantošanai Pakalpojumos.

7.3. Piekļuves kontrole un piekļuves apskats. Iron Mountain piešķir piekļuvi Klienta Personas Datiem tikai aktīviem Iron Mountain darbiniekiem, tostarp pagaidu darbiniekiem un līgumdarbiniekiem, un aktīvo lietotāju kontiem, kuriem šāda piekļuve ir nepieciešama, lai veiktu savus amata pienākumus. Visas priviliģētās piekļuves jāpārskata un jāapstiprina, lai tās atbilstu pašreizējai darba lomai, un jādokumentē vismaz reizi ceturksnī.

7.4. Trešās personas piekļuves kontrole. Pirms piekļuves piešķiršanas ārējām pusēm Iron Mountain informācijas sistēmām, kas piekļūst Klienta Personas Datiem, Iron Mountain nodrošina, ka ir ieviestas atbilstošas kontroles.

7.5. Operētājsistēmu piekļuves kontrole. Iron Mountain kontrolē piekļuvi operētājsistēmām (gan programmatūras, gan aparatūras operētājsistēmām), pieprasot drošu pieteikšanās procesu, kas unikāli identificē personu, kura piekļūst operētājsistēmai.

7.6. Mobilās skaitļošanas ierīces. Iron Mountain būs politika vai procedūra, kas paredzēta, lai aizsargātu Iron Mountain mobilās skaitļošanas ierīces no nesankcionētas piekļuves. Šāda politika vai procedūras attiecas uz fizisko aizsardzību, piekļuves kontroli un drošības kontroli, piemēram, šifrēšanu, aizsardzību pret vīrusiem un ierīces dublēšanu.

7.7. Klientu sistēmu izolācija. Iron Mountain savā mitinātajā vidē, ko izmanto Pakalpojumu sniegšanai, loģiski nodala un nošķir Klienta Personas Datus no visas pārējās informācijas.

7.8. Konti. Iron Mountain attiecībā uz kontiem veic turpmākās darbības.

7.8.1. Pieprasīt katra Iron Mountain darbinieka identitātes autentifikāciju, kurš meklē piekļuvi Iron Mountain sistēmām, kuras apstrādā Klienta Personas Datus, un aizliedz izmantot koplietotus lietotāju kontus vai lietotāju kontus ar vispārīgiem akreditācijas datiem (t. i., ID), lai piekļūtu Klienta Personas Datiem vai sistēmām.

7.8.2. Pieprasīt, lai visi lietotāju kontu ID, tostarp priviliģētie konti, būtu tieši saistīti ar personu (nevis ar amatu).

7.8.3. Ja noklusējuma administrēšanas konti nav atspējoti vai noņemti, pieprasīt izmantot pagaidu paroles, pārbaudīt ID vai līdzīgas vadīklas noklusējuma administrēšanas konta piekļuvei.

7.8.4. Pieprasīt, lai neaktīvie regulārie konti tiktu bloķēti vai atspējoti pēc 90 dienu neaktivitātes.

7.8.5. Aizliegt piekļuvi kontam pēc vairākiem neveiksmīgiem piekļuves mēģinājumiem.

7.8.6. Nepieciešami unikāli identifikatori un spēcīgas paroles, kas ietver vismaz šādu informāciju: minimālais 8 rakstzīmju skaits; jāmaina ik pēc 90 dienām; un tiem ir sarežģītības prasības.

7.8.7. Aizliegt darbiniekiem koplietot vai pierakstīt paroles.

7.9. Vadības ierīces bez uzraudzības sistēmām. Iron Mountain izmanto ar paroli aizsargātu ekrānsaudzētāju visām sistēmām, kuras ir atstātas bez uzraudzības un kurās 30 minūtes nav bijušas nekādas darbības.

8. INFORMĀCIJAS SISTĒMU IEGĀDES IZSTRĀDE UN UZTURĒŠANA

8.1. Sistēmu izstrādes drošība. Iron Mountain nodrošina, ka drošība ir daļa no visas informācijas sistēmu izstrādes un darbības, un publicē un ievēro iekšējās drošas kodēšanas metodoloģijas, kuru pamatā ir lietojumprogrammu izstrādes drošības standarti.

8.2. Programmatūras drošības pārvaldība. Iron Mountain informācijas sistēmas (tostarp operētājsistēmas, infrastruktūra, uzņēmuma lietojumprogrammas, pakalpojumi un lietotāju izstrādātās lietojumprogrammas) ir izstrādātas tā, lai tās atbilstu informācijas drošības standartiem.

8.3. Tīkla diagrammas. Iron Mountain izstrādā, dokumentē un uztur tīkla ierīču un trafika fiziskās un loģiskās diagrammas.

8.4. Lietojumprogrammu ievainojamības novērtējumi/ētiskā uzlaušana. Iron Mountain vismaz reizi gadā veic ievainojamības novērtējumus lietojumprogrammām savā mitinātajā vidē, ko izmanto, lai sniegtu pakalpojumus, kas Apstrādā Klienta Personas Datus. Detalizēti rezultāti ir Iron Mountain konfidenciāla un patentēta informācija, un tie netiks sniegti.

8.5. Izmaiņu pārbaude un pārskatīšana. Iron Mountain pirms izvietošanas pārskata un testē lietojumprogrammu un operētājsistēmu izmaiņas, lai nodrošinātu, ka netiek negatīvi ietekmēti Klienta Personas Dati vai sistēmas.

9. KATASTROFU SEKU LIKVIDĒŠANA

Iron Mountain uztur avārijas seku novēršanas plānu, tostarp pakalpojumu atbalstam izmantoto sistēmu un elektronisko datu replikāciju rezerves datu centrā. Sistēmu un elektronisko datu pavairošana neietver Klienta Personas Datus, kas fiziski tiek glabāti Iron Mountain objektā. Iron Mountain uzturēs uzņēmējdarbības nepārtrauktības plānu svarīgu uzņēmuma struktūrvienību atjaunošanai. Iron Mountain veiks avārijas seku testus ne retāk kā reizi divpadsmit (12) mēnešos.

10. ĀRĒJĀS REVĪZIJAS UN NOVĒRTĒJUMI

Iron Mountain drošības protokoli ir izstrādāti tā, lai tie atbilstu nozares standartiem. Iron Mountain nodrošinās Klientam visus trešās personas neatkarīgus revīzijas ziņojumus, ko tas ir pasūtījis (piemēram, PCI, ISO27001, SOC2 utt.), kas attiecas uz Pakalpojumiem reģionā, kurā šādi Pakalpojumi tiek sniegti (“Revīzijas ziņojums”).Iron Mountain sniegs visus šādus ziņojumus, kas pasūtīti ar nolūku būt vērsti uz klientu, neatkarīgi no ziņojuma rezultātiem. Iron Mountain nebūs jāiesniedz iekšējās revīzijas rezultāti vai rezultāti no citiem neatkarīgiem novērtējumiem, kas tika pasūtīti, lai tie būtu konfidenciāli Iron Mountain. Klientam un tā ārējiem auditoriem pēc pieprasījuma tiks izsniegtas Revīzijas ziņojuma kopijas. Jebkurš Revīzijas ziņojums vai cits rezultāts, kas iegūts, veicot testus vai revīzijas, kas prasīti šajā sadaļā, tiks uzskatīti par Iron Mountain Konfidenciālo informāciju. Klientam ir tiesības iesniegt šādas Revīzijas ziņojuma kopiju jebkuram Klienta klientam vai regulatoram, ievērojot konfidencialitātes noteikumus, kas ir tikpat ierobežojoši kā šeit minētie. Pēc Klienta pieprasījuma Iron Mountain rakstiski apstiprina, ka attiecīgajās politikās, procedūrās un iekšējā kontrolē nav notikušas izmaiņas kopš jebkura šāda Revīzijas ziņojuma pabeigšanas, bet ne ilgāk kā trīs mēnešus no Revīzijas ziņojuma pārskata perioda beigām.

3. PIELIKUMS

Starptautiskā datu pārsūtīšana

1. DEFINĪCIJAS

"**2021. gada ES līguma standartklauzulas**" ir līguma standartklauzulas par Personas Datu pārsūtīšanu uz trešām valstīm saskaņā ar VDAR, ko Eiropas Komisija ir pieņēmusi saskaņā ar Komisijas Īstenošanas lēmumu (ES) 2021/914, un ir pieejami šeit[3].

"**Apvienotās Karalistes 2022. gada papildinājums**" ir Apvienotās Karalistes Informācijas komisāra biroja izdevusi un parlamentā iesniegta veidne B.1.0. papildinājuma veidne saskaņā ar 2018. gada datu aizsardzības likuma s119A 2022. gada 2. februārī, jo tas var tikt pārskatīts saskaņā ar tā 18. sadaļu, kas pieejams šeit[4].

"**ES Klienta Personas Dati**" ir Klienta Personas Datu Apstrāde, kurai pirms to apstrādes Iron Mountain bija piemērojami Eiropas Savienības vai Eiropas Savienības dalībvalsts vai Eiropas Ekonomikas zonas datu aizsardzības tiesību akti;

"**Aizsargātā zona**" nozīmē:

i. ES Klienta Personas Datu gadījumā Eiropas Savienības un Eiropas Ekonomikas zonas dalībvalstis un jebkura valsts, teritorija, nozare vai starptautiska organizācija, attiecībā uz kuru ir spēkā VDAR 45. panta atbilstības lēmums;

ii. Apvienotās Karalistes Klienta Personas Datu gadījumā Apvienotā Karaliste un jebkura valsts, teritorija, nozare vai starptautiska organizācija, attiecībā uz kuru ir spēkā lēmums par atbilstību saskaņā ar Apvienotās Karalistes pietiekamības noteikumiem;

iii. Šveices Klienta Personas Datu gadījumā jebkura valsts, teritorija, nozare vai starptautiska organizācija, kas ir atzīta par atbilstošu saskaņā ar Šveices tiesību aktiem;

iv. jebkādu citu Klienta Personas Datu gadījumā, kas tiek pārsūtīti ārpus jurisdikcijas, kas piedāvā līdzīgu aizsardzību kā ES, Apvienotās Karalistes vai Šveices Klienta Personas Datiem, jebkura valsts, teritorija, nozare vai starptautiska organizācija, kas ir atzīta par atbilstošu saskaņā ar šādas jurisdikcijas tiesību aktiem.

"**Līguma standartklauzulas**" kopā ir 2021. gada ES līguma standartklauzulas un Apvienotās Karalistes 2022. gada papildinājums.

"**Šveices Klienta Personas Dati**" nozīmē Klienta Personas Datu Apstrādi, uz kuru bija piemērojami Šveices datu aizsardzības tiesību akti, pirms tos apstrādāja Iron Mountain.

"**Apvienotās Karalistes Klienta Personas Dati**" ir Klienta Personas Datu Apstrāde, kurai bija piemērojami Apvienotās Karalistes datu aizsardzības tiesību akti, pirms tos apstrādāja Iron Mountain.

2. DAŽĀDI

2.1. Šajā 3. pielikumā ir iekļautas šādas daļas: (i) A daļa – ES Klientu Personas Datu pārsūtīšana; (ii) B daļa – Šveices Klienta Personas Datu pārsūtīšana; (iii) C daļa — Apvienotās Karalistes Klienta Personas Datu nosūtīšana, kas attiecīgi attiecas uz Iron Mountain veikto Klienta Personas Datu pārsūtīšanu saistībā ar saviem Pakalpojumiem.

2.2. Līguma standartklauzulas attiecas uz Iron Mountain un tā saistītajiem uzņēmumiem kā "datu saņēmēju" un Klientu un tā saistītajiem uzņēmumiem kā "datu nosūtītāju".

2.3. Līguma parakstīšana un datējums ir visi nepieciešamie paraksti un datumi Līguma standartklauzulām.

2.4. Gadījumā, ja puses nodod ES, Apvienotās Karalistes vai Šveices Klientu Personas Datus ārpus aizsargājamās teritorijas un attiecīgu Eiropas Komisijas lēmumu vai citu derīgu atbilstības metodi saskaņā ar piemērojamajiem datu aizsardzības tiesību aktiem, uz kuru Iron Mountain ir paļāvies datu pārsūtīšanai, tiek uzskatīts par nederīgu vai ka jebkura uzraudzības iestāde pieprasa apturēt Personas Datu pārsūtīšanu, kas veikta saskaņā ar šādu lēmumu, tad puses sadarbojas un veicina alternatīva nodošanas mehānisma izmantošanu. Puses arī vienojas, ka atbilstošie drošības pasākumi, kas izmantoti, lai veicinātu starptautisku pārsūtīšanu šajā 3. pielikumā, nav ekskluzīvi un ka puses var izmantot papildu pārsūtīšanas mehānismus, piemēram, ES un ASV datu privātuma regulējumu.

A. DAĻA – ES KLIENTA PERSONAS DATU PĀRSŪTĪŠANA

Ja un ciktāl klients vai tā saistītie uzņēmumi nodod ES Klienta Personas Datus ārpus aizsargājamās teritorijas Iron Mountain vai tā saistītajiem uzņēmumiem saistībā ar Iron Mountain pakalpojumiem saskaņā ar Līgumu, tiek piemērota šī 3. pielikuma A. daļa, un Puses vienojas par turpmāk minēto.

[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. **Līguma standartklauzulu izvēle.** 2021. gada ES līguma standartklauzulu OTRĀ MODUĻA teksts tiek piemērots, ja Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Pārzinis un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs; teksts no 2021. gada ES līguma standartklauzulu TREŠĀ MODUĻA ir piemērojams, ja Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir Apakšapstrādātājs. Attiecīgie noteikumi, kas ietverti 2021. gada ES līguma standartklauzulās, ir iekļauti šajā DAL ar atsauci un ir šī DAL neatņemama sastāvdaļa. Nekādus citus moduļus vai klauzulas, kas 2021. gada ES līguma standartklauzulās atzīmētas kā neobligātas, nepiemēro.2021. gada ES līguma standartklauzulas pielikumu vajadzībām nepieciešamā informācija ir noteikta 1. pielikumā – Apstrādes/nodošanas apraksts, 2. pielikumā – Tehniskie un organizatoriski pasākumi un DAL 6.2. punktā – Apakšapstrādātāju saraksts

2. **Apakšapstrādātāju izmantošana.** 2021. gada ES līguma standartklauzulu 9. klauzulas vajadzībām tiek piemērota 2. iespēja (vispārēja rakstiska pilnvara) apakšapstrādātāju izmantošanai Pakalpojumu sniegšanai. Klients atzīst un piekrīt, ka Iron Mountain var piesaistīt jaunus apakšapstrādātājus, izmantojot mehānismu, par kuru panākta vienošanās šī DAL 6. punktā, un ka termiņš izmaiņu pieprasījumu iesniegšanai apakšapstrādātājiem ir piecpadsmit (15) dienas.

3. **Piemērojamie tiesību akti un foruma izvēle.** 2021. gada ES līguma standartklauzulu (vadošo tiesību) 17. klauzulas vajadzībām piemēro 2. iespēju, kas regulē tiesību aktus, un šīs klauzulas reglamentē tās ES dalībvalsts tiesību akti, kurā datu nosūtītājs ir reģistrēts, ciktāl tas pieļauj trešās personas labuma guvēju tiesības.2021. gada ES līguma standartklauzulu 18. klauzulas (foruma un jurisdikcijas izvēle) nozīmē tās ir tās ES dalībvalsts tiesas, kurā datu nosūtītājs ir reģistrēts.

4. **Dzēšanas apliecinājums.** 2021. gada ES līguma standartklauzulu 8.5. punkta un 16. d) punkta nolūkos Iron Mountain izsniedz Klientam Personas Datu dzēšanas apliecinājumu tikai pēc Klienta rakstiska pieprasījuma.

5. **Personas datu pārkāpumi.** 2021. gada ES līguma standartklauzulu 8.6. punkta c) apakšpunkta nolūkos personas datu aizsardzības pārkāpumus apstrādā saskaņā ar DAL 7. punktā saskaņoto mehānismu.

6. **Revīzijas.** 2021. gada ES līguma standartklauzulu 8.9. punkta ietvaros šajā punktā minētās revīzijas tiek veiktas saskaņā ar Līgumā saskaņoto revīziju mehānismu.

7. **Sūdzības.** 2021. gada ES līguma standartklauzulu 11. punkta vajadzībām, Iron Mountain informē Klientu, ja tas saņem sūdzību no Datu Subjekta par ES Klienta Personas Datiem, un paziņo sūdzību Klientam saskaņā ar Līgumā saskaņoto mehānismu.

8. **Uzraudzības iestāde.** 2022. gada ES līguma standartklauzulām attiecīgo kompetento uzraudzības iestādi nosaka saskaņā ar ES līguma standartklauzulu 13. punktu.

B. DAĻA – ŠVEICES KLIENTA PERSONAS DATU PĀRSŪTĪŠANA

Ja un ciktāl Klients vai tā saistītie uzņēmumi nodod Šveices Klienta Personas Datus ārpus Aizsargājamās Teritorijas uzņēmumam Iron Mountain vai tā saistītajiem uzņēmumiem saistībā ar Iron Mountain pakalpojumiem saskaņā ar Līgumu, tiek piemērota šī 3. pielikuma B. daļa, un Puses vienojas par turpmāk minēto.

1. **Līguma standartklauzulu izvēle.** 2021. gada ES līguma standartklauzulas un attiecīgie A. daļas noteikumi tiek piemēroti, ja Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Pārzinis, un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs, un/vai Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs, un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir apakšapstrādātājs, izņemot:

   a. kompetentā uzraudzības iestāde saskaņā ar 2021. gada ES līguma standartklauzulu 13. punktu ir Šveices Federālā datu aizsardzības un informācijas komisija;

   b. piemērojamie tiesību akti līgumiskām prasībām saskaņā ar 2021. gada ES līguma standartklauzulu 17. punktu ir Šveices tiesību akti, un jurisdikcijas vieta prasībām starp pusēm saskaņā ar 18. punkta b) apakšpunktu ir Šveices tiesas.

2. Atsauces uz ES VDAR 2021. gada ES līguma standartklauzulās jāsaprot kā atsauces uz FADP.

3. Jēdziens "dalībvalsts" 2021. gada ES līguma standartklauzulās nav jāinterpretē tādējādi, ka saskaņā ar 2021. gada ES līguma standartklauzulu 18. punkta c) apakšpunktu Datu Subjektiem Šveicē nav iespējas celt prasību tiesā par savām tiesībām viņu pastāvīgās dzīvesvietas vietā (Šveicē).

C. DAĻA – APVIENOTĀS KARALISTES KLIENTA PERSONAS DATU PĀRSŪTĪŠANA

Ja un ciktāl Klients vai tā Saistītie Uzņēmumi nodod Apvienotās Karalistes Personas Datus ārpus Aizsargājamās Teritorijas uzņēmumam Iron Mountain vai tā Saistītajiem Uzņēmumiem saistībā ar Iron Mountain pakalpojumiem saskaņā ar Līgumu, tiek piemērota šī 3. pielikuma C. daļa, un Puses vienojas par turpmāk minēto.

1. **Līguma standartklauzulu izvēle.** 2021. gada ES līguma standartklauzulas, attiecīgie A. daļas noteikumi un 2022. gada Apvienotās Karalistes papildinājums tiek piemēroti, ja Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Pārzinis, un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs, un/vai Klients vai kāds no tā Saistītajiem Uzņēmumiem ir Apstrādātājs, un Iron Mountain vai kāds no tā Saistītajiem Uzņēmumiem ir apakšapstrādātājs.

2. **1. daļa. Apvienotās Karalistes 2022. gada papildinājuma 1.–3. tabula.** Informācija par pusēm – 1. tabula; Atlasītie SCC, moduļi un atlasītās klauzulas; un papildinājuma informācija, tostarp 1.A pielikums: Pušu saraksts, 1.B pielikums: Pārsūtīšanas apraksts un 1.C pielikums: Tehniskie un organizatoriski pasākumi datu drošības nodrošināšanai – 3. tabulu uzskata par pabeigtu, atsaucoties uz šo 3. pielikumu, tostarp A. daļu. Apvienotās Karalistes papildinājuma 4. tabula: Klients un Iron Mountain atzīst un piekrīt, ka Apvienotās Karalistes papildinājumu var izbeigt jebkura Puse.

3. **2. daļa.** Apvienotās Karalistes papildinājuma obligātie noteikumi: Klients un Iron Mountain atzīst un piekrīt Apvienotās Karalistes papildinājuma obligātajiem noteikumiem.

4. **Uzraudzības iestāde.** Apvienotās Karalistes Informācijas komisāra birojs darbojas kā kompetenta uzraudzības iestāde.

D. DAĻA – CITU KLIENTA PERSONAS DATU PĀRSŪTĪŠANA

Ja un ciktāl Klients vai tā saistītie uzņēmumi nodod uzņēmumam Iron Mountain vai tā saistītajiem uzņēmumiem Klienta Personas Datus, uz kuriem neattiecas A–C. DAĻA, saistībā ar Iron Mountain Pakalpojumiem saskaņā ar Līgumu, 3. pielikuma A. daļa tiek piemērota tiktāl, ciktāl tas ir būtiski un piemērojams saskaņā ar piemērojamajiem Datu Aizsardzības Tiesību Aktiem. Pretējā gadījumā, ciktāl saskaņā ar Datu Aizsardzības Tiesību Aktiem ir nepieciešami jebkādi aizstājēji vai papildu atbilstoši aizsardzības vai pārsūtīšanas mehānismi, lai pārsūtītu Klienta Personas Datus uz valsti, kas no datu nosūtītāja viedokļa nenodrošina atbilstošu Personas Datu aizsardzības līmeni, puses vienojas to īstenot, cik drīz vien iespējams, un dokumentēt šādas ieviešanas prasības šī DAL pielikumā.

4. PIELIKUMS

HIPAA – Uzņēmuma partneru līgums (Business Associate Agreement jeb "BAA")

Šis BAA papildina un groza visus pašreizējos vai turpmākos līgumus, kas noslēgti starp Iron Mountain un tā saistītajiem uzņēmumiem un Klientu un tā saistītajiem uzņēmumiem, saskaņā ar kuru Iron Mountain vai tā saistītie uzņēmumi sniedz noteiktus Pakalpojumus Klientam vai tā saistītajiem uzņēmumiem, kuri, lai nodrošinātu Pakalpojumus, paredz, ka Darījuma Partnerim ir Jāizmanto un/vai Jāatklāj PHI Attiecinātās Vienības vārdā. Izņemot šajā BAA mainītos apmērus, visi Līgumā noteiktie noteikumi un nosacījumi paliek spēkā un attiecas uz Iron Mountain Klientam sniegtajiem Pakalpojumiem.

Iron Mountain un Klients noslēdz šo BAA, lai abas puses izpildītu savus attiecīgos pienākumus, tiklīdz tie stājas spēkā un pusēm ir saistoši saskaņā ar HIPAA Privātuma, Drošības un Pārkāpumu Paziņošanas Noteikumiem, kā arī visiem īstenošanas noteikumiem, tostarp tiem, kas ieviesti kā daļa no Omnibus noteikuma (kopā saukti par "HIPAA noteikumiem"), saskaņā ar kuru Klients un tā saistītie uzņēmumi ir "Attiecinātā vienība" vai "Darījuma Partneris" un Iron Mountain un tā saistītie uzņēmumi ir Klienta "Darījuma Partneris". Šī Līguma izpratnē visas turpmākās atsauces uz Darījuma Partneri tiks uzskatītas par atsaucēm uz Iron Mountain vai tā piemērojamo saistīto uzņēmumu.

1. DEFINĪCIJAS

Šajā BAA lietotajiem jēdzieniem, kuri izcelti ar lieliem sākuma burtiem, kas nav definēti citādi, ir tāda pati nozīme, kāda jēdzieniem, kas piešķirta HIPAA noteikumos vai Līgumā, ja piemērojams.

"**Pārkāpumu paziņošanas noteikums**" ir noteikums par Pārkāpumu Paziņošanu nedrošai aizsargātai veselības informācijai saskaņā ar 45 CFR 164. panta D apakšsadaļu.

"**Darījuma Partneris**" ir iepriekš norādītā Darījuma Partnera vienība tādā apjomā, kādā tā saņem, uztur vai nosūta Aizsargātu informāciju par veselību, sniedzot Pakalpojumus Klientiem.

"**HIPAA**" ir 1996. gada Veselības apdrošināšanas pārnesamības un atbildības likums (Health Insurance Portability and Accountability Act).

"**HITECH likums**" ir piemērojamie Likuma par veselības informācijas tehnoloģiju ekonomiskajai un klīniskajai veselībai (Health Information Technology for Economic and Clinical Health Act) piemērojamie noteikumi, kas iekļauti 2009. gada Amerikas Atgūšanas un reinvestēšanas likumā (Recovery and Reinvestment Act), kā arī visi īstenošanas noteikumi.

"**Privātuma noteikums**" ir individuāli identificējamas veselības informācijas privātuma aizsardzības standarti 45 CFR 160. un 164. panta, A un E apakšsadaļās.

"**Aizsargātā veselības informācija**" jeb "**PHI**" (Protected Health Information) ir tāda pati nozīme kā jēdzienam "aizsargāta informācija par veselību" 45 CFR 160.103. pantā, un tā attiecas tikai uz PHI, ko izveidojis Darījuma Partneris Klienta vārdā vai saņemts no Klienta vai viņa vārdā saskaņā ar Līgumu.

"**Drošības noteikums**" ir drošības standarti elektroniski aizsargātas veselības informācijas aizsardzībai saskaņā ar 45 CFR 160. un 164. panta, A un C apakšsadaļu.

2. DARĪJUMA PARTNERA PIENĀKUMI UN DARBĪBAS

2.1. Darījuma Partneris piekrīt neizmantot vai turpmāk neizpaust PHI citādi, kā to atļauj vai pieprasa šis BAA vai kā noteikts likumā.

2.2. Darījuma Partneris piekrīt izmantot atbilstošus drošības pasākumus un ievērot C apakšnodaļas 45 CFR 164. panta C apakšsadaļu attiecībā uz elektroniskajiem PHI, lai novērstu PHI izmantošanu vai izpaušanu, kas nav paredzēta šajā BAA vai Līgumā; tomēr puses atzīst un vienojas, ka Klients, nevis Darījuma Partneris ir atbildīgs par prasību izpildi saskaņā ar 45 CFR 164.312. pantu, lai ieviestu šifrēšanas vai atšifrēšanas mehānismus elektroniskajiem PHI, kas tiek uzturēti fiziskajos datu nesējos (piem., kasetēs), ko Klients glabā kopā ar Darījuma Partneri.

2.3. Darījuma Partneris piekrīt nekavējoties ziņot Klientam par jebkuru Drošības Incidentu, Pārkāpumu vai citu PHI Izmantošanu vai Izpaušanu, par kuru tas kļūst zināms un kas nav atļauts vai pieprasīts saskaņā ar šo BAA vai Līgumu. Pārkāpuma gadījumā šāds paziņojums jāsniedz saskaņā ar HIPAA noteikumiem un saskaņā ar Darījuma Partnera prasībām, tostarp bez ierobežojumiem saskaņā ar 45 CFR 164.410. pantu, bet nekādā gadījumā ne vēlāk kā trīs (3) darba dienas pēc tam, kad Darījuma Partneris ir pabeidzis iekšējo izmeklēšanu un apstiprinājis, ka ir noticis Pārkāpums. Darījuma Partneris sniegs saprātīgu palīdzību un sadarbosies jebkura šāda Pārkāpuma izmeklēšanā un dokumentēs konkrētos Depozītus, kuri ir apdraudēti, jebkuras nesankcionētas trešās personas identitāti, kas, iespējams, ir piekļuvusi PHI vai saņēmusi to, un visas darbības, ko Darījuma Partneris ir veicis, lai mazinātu šāda Pārkāpuma sekas.

2.4. Darījuma Partneris saskaņā ar 45 CFR 164.502. panta (e)(1)(ii). apakšpunktu un 164.308. panta (b)(2). apakšpunktu, ja piemērojams, nodrošina, ka jebkuram Darījuma Partnerim, kas ir

apakšuzņēmējs, kas izveido, saņem, uztur vai pārsūta PHI Darījuma Partnera vārdā, lai palīdzētu sniegt Pakalpojumus saskaņā ar Līgumu, piekrīt tiem pašiem ierobežojumiem, nosacījumiem un prasībām, kas attiecas uz Darījuma Partneri attiecībā uz šādu PHI, izmantojot šo BAA.

2.5. Ja Darījuma Partnerim ir PHI pārziņā noteiktā ierakstu kopā attiecībā uz Fiziskām Personām un ja Klients to pieprasa, Darījuma Partneris piekrīt nodrošināt Klientam piekļuvi šādiem PHI, izgūstot un piegādājot šādus PHI saskaņā ar Līguma noteikumiem un nosacījumiem, lai Klients varētu atbildēt Fiziskai Personai, lai izpildītu 45 CFR 164.524. panta prasības.

2.6. Darījuma Partneris piekrīt, ka, ja ir nepieciešami PHI grozījumi norādītajā ierakstu komplektā, kas atrodas Darījuma Partnera pārziņā, un, ja Klients uzdod Darījuma Partnerim izgūt šādu PHI saskaņā ar Līgumu, Darījuma Partneris veic šādu Pakalpojumu, lai Klients varētu veikt jebkādus grozījumus šajā PHI, ko var pieprasīt Klients vai Fiziska Persona saskaņā ar 45 CFR 164.526. pantu.

2.7. Darījuma Partneris piekrīt dokumentēt un darīt pieejamu Klientam informāciju, kas nepieciešama, lai nodrošinātu PHI atklātās informācijas uzskaiti, ar nosacījumu, ka Klients ir sniedzis Darījuma Partnerim informāciju, kas ir pietiekama, lai ļautu Darījuma Partnerim noteikt, kuri ieraksti vai dati, ko Darījuma Partneris saņēmis no Klienta vai tā vārdā, satur PHI. Informācijas izpaušanas dokumentācijā jāietver tāda informācija, kas būtu nepieciešama, lai Klients atbildētu uz Fiziskas Personas pieprasījumu par PHI izpaušanas uzskaiti saskaņā ar 45 CFR 164.528. pantu vai citiem HIPAA noteikumu noteikumiem.

2.8. Ja vien Līgumā nav skaidri noteikts citādi, Darījuma Partneris nekavējoties informē Klientu par visiem Fizisku Personu pieprasījumiem piekļūt PHI, uzzināt vai labot to, neatbildot uz šādiem pieprasījumiem, un Klients ir atbildīgs par šādu Individuālu pieprasījumu saņemšanu un atbildēšanu uz tiem.

2.9. Ciktāl Darījuma Partnerim jāpilda viens vai vairāki Klienta pienākumi saskaņā ar 45 CFR 164. panta E apakšsadaļu, Darījuma Partnerim jāievēro E apakšsadaļas prasības, kuras attiecas uz Klientu, pildot šādu(-s) pienākumu(-s).

2.10. Darījuma Partneris piekrīt darīt savu iekšējo praksi, žurnālus un ierakstus pieejamus sekretāram, lai noteiktu atbilstību HIPAA noteikumiem.

3. DARĪJUMA PARTNERA ATĻAUTĀ IZMANTOŠANA UN IZPAUŠANA

3.1. Darījuma Partneris var izmantot vai izpaust PHI, ja nepieciešams, lai sniegtu Līgumā noteiktos Pakalpojumus.

3.2. Darījuma Partneris var izmantot vai izpaust PHI, kā noteikts likumā.

3.3. Darījuma Partneris piekrīt pielikt saprātīgas pūles, lai ierobežotu PHI līdz minimumam, kas nepieciešams, lai sasniegtu paredzēto Lietošanas, Izpaušanas vai Pieprasījuma nolūku.

3.4. Darījuma Partneris nedrīkst izmantot vai izpaust PHI tādā veidā, kas pārkāptu CFR 45. 164. panta E. apakšsadaļu, ja to dara Klients.

3.5. Darījuma Partneris var izpaust PHI, lai pareizi pārvaldītu, administrētu vai veiktu Darījuma Partnera juridiskos pienākumus, ar nosacījumu, ka Informācijas Izpaušana ir nepieciešama saskaņā ar likumu, vai Darījuma Partneris iegūst pamatotas garantijas no personas, kurai informācija tiek izpausta, ka informācija paliks konfidenciāla un tiks izmantota vai turpmāk izpausta tikai saskaņā ar likumu vai nolūkiem, kādiem tā tika atklāta personai, un persona paziņo Darījuma Partnerim par visiem gadījumiem, par kuriem tai ir zināms, ka informācijas konfidencialitāte ir pārkāpta.

4. KLIENTA PIENĀKUMI

4.1. Klients nedrīkst likt Darījuma Partnerim rīkoties veidā, kas neatbilst HIPAA noteikumiem.

4.2. Klients informē Darījuma Partneri par jebkādiem ierobežojumiem savā paziņojumā par Klienta privātuma praksi saskaņā ar 45 CFR 164.520. pantu, ciktāl šāds ierobežojums var ietekmēt Darījuma Partnera PHI izmantošanu vai izpaušanu.

4.3. Klients informē Darījuma Partneri par jebkādām izmaiņām vai atsaukšanu, kas attiecas uz Personas atļauju izmantot vai izpaust savu PHI, ciktāl šādas izmaiņas var ietekmēt Darījuma Partnera PHI izmantošanu vai izpaušanu.

4.4. Klients rakstiski informē Darījuma Partneri par visiem PHI izmantošanas vai izpaušanas ierobežojumiem, kuriem Klients ir piekritis saskaņā ar 45 CFR 164.522. pantu, ciktāl šāds ierobežojums var ietekmēt Darījuma Partnera PHI Izmantošanu vai Izpaušanu.

5. TERMIŅS UN IZBEIGŠANA

5.1. Šī BAA darbības termiņš sākas no Spēkā Stāšanās Datuma un beidzas automātiski (i) Līguma termiņa beigās vai (ii) ja visi PHI, ko Klients sniedzis Darījuma Partnerim, tiek iznīcināti vai atdoti Klientam.

5.2. Pusei uzzinot par otras puses būtisku BAA pārkāpumu, pusei, kura nav atbildīga par pārkāpumu, jānodrošina iespēja pārkāpējai pusei pārkāpumu novērst. Ja pārkāpēja puse nav novērsusi pārkāpumu trīsdesmit (30) dienu laikā pēc tam, kad pārkāpēja puse ir saņēmusi rakstisku paziņojumu no puses, kura nav atbildīga par pārkāpumu, ar detalizētu informāciju, kura nav atbildīga par pārkāpumu, ir tiesības izbeigt šo BAA un Līgumu saskaņā ar Līguma noteikumiem vai, ja izbeigšana nav iespējama, ziņot par problēmu Sekretāram vai jebkurai citai kompetentai iestādei.

5.3. Pārtraukšanas sekas.

5.3.1.1. Izņemot 5.3.2. apakšpunktā tālāk norādītos gadījumus, pēc šī BAA darbības pārtraukšanas jebkura iemesla dēļ Darījuma Partnerim jāatdod vai jāiznīcina visi no Klienta saņemtie PHI saskaņā ar Līgumu. Šis noteikums attiecas uz PHI, kas ir

Darījuma Partnera apakšuzņēmēju vai aģentu īpašumā. Darījuma Partneris neglabā nekādas PHI kopijas.

5.3.1.2. Gadījumā, ja Darījuma Partneris konstatē, ka PHI atgriešana vai iznīcināšana nav iespējama, Darījuma Partneris sniedz Klientam paziņojumu par nosacījumiem, kuru dēļ atgriešana vai iznīcināšana nav iespējama. Darījuma Partnerim, saņemot paziņojumu Klientam, jāpaplašina šī BAA aizsardzība attiecībā uz šādiem PHI un jāierobežo turpmāka šādu PHI Izmantošana un Izpaušana šiem nolūkiem, kas padara atgriešanu vai iznīcināšanu neiespējamu, kamēr Darījuma Partneris uztur šādu PHI saskaņā ar Līguma noteikumiem.

6. DAŽĀDI

6.1. Zaudējumu atlīdzināšana. Darījuma Partneris piekrīt atlīdzināt Klientam jebkādus naudas sodus vai sodus, kas Klientam uzlikti jebkura Sekretāra uzsākta izpildes procesa rezultātā, vai jebkura civilprasība, ko štata Ģenerālprokurors cēlis pret Klientu un kuras process vai darbība izriet tieši un vienīgi no jebkuras Darījuma Partnera darbības vai bezdarbības, kas ir vai nu HIPAA noteikumu pārkāpums, vai būtisks šī BAA pārkāpums ("Prasība").Darījuma Partnerim nav pienākuma atlīdzināt Klientam jebkādu šādu naudas sodu vai sodu daļu, kas izriet no (i) Klienta HIPAA noteikumu vai šī BAA pārkāpuma vai (ii) Klienta nolaidīgas vai tīšas darbības vai bezdarbības. Iepriekšminētais atlīdzības pienākums ir nepārprotami atkarīgs no tā, vai Klients piešķir Darījuma Partnerim tiesības pēc Darījuma Partnera izvēles un rēķina un ar paša izvēlētu juristkonsultantu kontrolēt vai piedalīties jebkuras šādas Prasības aizstāvēšanā, tomēr ar nosacījumu, ka, ciktāl jebkura šāda Prasība ir daļa no lielākas procedūras vai darbības, Darījuma Partnera tiesības kontrolēt vai piedalīties ir ierobežotas attiecībā uz Prasību, nevis uz plašāku procesu vai darbību. Gadījumā, ja Darījuma Partneris izmanto savu izvēli kontrolēt aizsardzību, tad (i) Darījuma Partneris bez iepriekšējas rakstiskas piekrišanas nerisina nevienu prasību, kas prasa Klienta vainas atzīšanu; (ii) Klientam ir tiesības uz sava rēķina piedalīties prasības vai lietas izskatīšanā; un (iii) Klientam jāsadarbojas ar Darījuma Partneri, kā tas ir pamatoti pieprasīts. Iepriekš minētais nosaka Klienta vienīgo un ekskluzīvo tiesiskās aizsardzības līdzekli un Darījuma Partnera vienīgo atbildību par jebkādiem zaudējumiem, bojājumiem, izdevumiem vai Klienta atbildību par jebkādām Prasībām saistībā ar šo BAA.

6.2. Pagaidu tiesiskās aizsardzības līdzekļi. Darījuma Partneris atzīst, ka jebkura Darījuma Partnera nesankcionēta PHI Izmantošana vai Izpaušana var nodarīt Klientam neatgriezenisku kaitējumu, par kuru Klientam ir tiesības, ja tas tā vēlas, pieprasīt rīkojumu vai citu taisnīgu atbalstu.

6.3. Normatīvās atsauces. Atsauce šajā BAA uz kādu HIPAA Noteikumu sadaļu nozīmē to HIPAA, Privātuma Noteikumu, Drošības Noteikumu, HITECH LIKUMA sadaļu vai galīgos Omnibus Noteikumus, kas ir grozīti un ir spēkā un kuriem ir nepieciešama atbilstība.

6.4. Grozījumi. Puse piekrīt godprātīgi vienoties par visiem šī BAA grozījumiem, kas laiku pa laikam var būt nepieciešami, lai Klients vai Darījuma Partneris atbilstu HIPAA Noteikumu prasībām. Ja puses nevar panākt savstarpēju vienošanos par jebkuru šādu grozījumu nosacījumiem sešdesmit (60) dienu laikā pēc jebkura šāda rakstiska pieprasījuma saņemšanas, ko Klients ir iesniedzis Darījuma Partnerim, tad jebkurai pusei ir tiesības izbeigt šo BAA un Līgumu, par to ne mazāk kā trīsdesmit (30) dienas iepriekš rakstiski brīdinot otru pusi.

6.5. Nav trešo personu labuma guvēju. Nekas, kas izteikts vai netieši norādīts šajā BAA, nav paredzēts nevienai personai, izņemot Klientu, Darījuma Partnerus un to attiecīgos pēctečus vai cesijas, jebkādas tiesības, tiesiskās aizsardzības līdzekļus, pienākumus vai saistības.

6.6. Neatkarīgs līgumslēdzējs. Darījuma Partneris, tostarp tā direktori, amatpersonas, darbinieki un aģenti, ir neatkarīgs līgumslēdzējs, nevis Klienta aģents (kā definēts federālajā likumā par pārstāvniecību) vai tā darbaspēka loceklis. Neierobežojot iepriekšminētā vispārīgumu, Klientam nav tiesību kontrolēt, vadīt vai citādi ietekmēt Darījuma Partnera uzvedību pakalpojumu sniegšanas laikā, izņemot, īstenojot šo BAA vai Līgumu, vai savstarpēji grozot tos.

6.7. Prioritāte; Viss līgums. Jebkādas neskaidrības šajā BAA jāatrisina, lai ļautu pusēm ievērot HIPAA Noteikumus. Šis BAA veido visu pušu vienošanos attiecībā uz šī līguma priekšmetu, un tā aizstāj visus iepriekšējos paziņojumus, paziņojumus, līgumus un vienošanās, kas attiecas uz HIPAA Noteikumiem, tostarp jebkuru un visus iepriekšējos Darījuma Partneru līgumus starp pusēm.