



Zmluva o spracúvaní údajov

ÚČEL A PORADIE PRIORÍT

Táto Zmluva o spracúvaní údajov spolu s jej prílohami a akýmkoľvek dokumentom, na ktorý výslovne odkazuje (ďalej len „DPA“), sa považuje za súčasť zmluvy o poskytovaní služieb medzi spoločnosťou Iron Mountain a Zákazníkom (ďalej len „Zmluva“). Na práva a povinnosti zmluvných strán podľa tejto DPA sa vzťahujú a riadia ich zmluvné podmienky Zmluvy.

Ak sú akékoľvek zmluvné podmienky tejto DPA v rozpore so zmluvnými podmienkami uvedenými v Zmluve, zmluvné podmienky uvedené v tejto DPA budú rozhodujúce s ohľadom na predmet tejto DPA. Táto DPA ruší a nahrádza všetky predchádzajúce zmluvy o spracúvaní údajov a doložky o ochrane údajov alebo súkromia medzi zmluvnými stranami v súvislosti so Službami poskytovanými na základe tejto Zmluvy.

VŠEOBECNÉ PODMIENKY

1. VYMEDZENIE POJMOV

Pokiaľ to nie je výslovne uvedené v tejto Zmluve, všetky pojmy s veľkým začiatočným písmenom budú mať rovnaký význam, aký im bol udelený v tejto Zmluve.

„**Prevádzkovateľ**“ je fyzická alebo právnická osoba, orgán verejnej moci, úrad alebo iný subjekt, ktorý samostatne alebo spoločne s inými určuje účely a prostriedky Spracúvania Osobných údajov;

„**Osobné údaje Zákazníka**“ znamenajú Osobné údaje patriace alebo zhromaždené Zákazníkom alebo jeho pridruženými spoločnosťami, ktoré sa spracúvajú ako súčasť Služieb;

„**Dotknutá osoba**“ znamená identifikovanú alebo identifikovateľnú fyzickú osobu;

„**Právne predpisy o ochrane údajov**“ znamená všetky príslušné zákony a nariadenia týkajúce sa Spracúvania osobných údajov, ktoré môžu existovať v príslušných jurisdikciách, okrem iného aj vrátane nariadenia GDPR EÚ (Nariadenie (EÚ) 2016/679), GDPR Spojeného kráľovstva (GDPR uplatniteľné ako súčasť vnútroštátnych právnych predpisov Spojeného kráľovstva na základe oddielu 3 zákona Európskej únie (o vystúpení) z roku 2018 a v znení zmien a doplnení nariadení o ochrane údajov, súkromia a elektronických komunikáciách (dodatky atď.) nariadenia (pri odchode z EÚ) z roku 2019 (v znení neskorších predpisov)), zákon o ochrane údajov z roku 2018, FADP (švajčiarsky federálny zákon o ochrane údajov), zákony USA o ochrane osobných údajov, LGPD (brazílsky všeobecný zákon o ochrane údajov), PIPL (zákon Čínskej ľudovej republiky o ochrane osobných údajov) a akékoľvek právne predpisy a/alebo nariadenie zavádzané alebo vytvorené v súlade s nimi, alebo ktoré menia, nahrádzajú, opätovne prijímajú alebo konsolidujú akékoľvek z nich, prípadne vrátane usmernení a kódexov postupov vydaných orgánmi dohľadu;

„**Osobné údaje**“ znamenajú akékoľvek údaje týkajúce sa Dotknutej osoby;

„**Sprostredkovateľ**“ znamená fyzickú alebo právnickú osobu, orgán verejnej moci, úrad alebo iný subjekt, ktorý spracúva Osobné údaje v mene Prevádzkovateľa;

„**Spracúvanie**“ znamená akúkoľvek operáciu alebo súbor operácií, ktoré sa vykonávajú s Osobnými údajmi alebo súbormi Osobných údajov, či už automatizovanými prostriedkami alebo inak, ako je zhromažďovanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prispôsobovanie alebo zmena, vyhľadávanie, prehliadanie, používanie, zverejňovanie prenosom, šírenie alebo iné sprístupňovanie, zosúlaďovanie alebo kombinovanie, obmedzovanie, vymazávanie alebo ničenie;

„**Porušenie bezpečnosti**“ znamená akékoľvek náhodné alebo nezákonné poškodenie, zničenie, stratu, zmenu alebo neoprávnené zverejnenie alebo prístup k Osobným údajom Zákazníka, ktoré spoločnosť Iron Mountain, jej zamestnanci alebo subdodávatelia spracúvajú v priebehu poskytovania Služieb;

„**Služby**“ znamenajú akékoľvek služby poskytované spoločnosťou Iron Mountain alebo jej pridruženými spoločnosťami zákazníkovi alebo jeho pridruženým spoločnostiam na základe Zmluvy;

„**Zákony USA o ochrane osobných údajov**“ znamenajú všetky zákony USA na ochranu súkromia a údajov, ktoré sa vzťahujú na Spracúvanie osobných údajov podľa tejto Zmluvy, okrem iného aj vrátane tých, ktoré sa môžu priebežne meniť, rušiť alebo nahradiť: (1) Kalifornský zákon o ochrane osobných údajov spotrebiteľov zmenený a doplnený Kalifornským zákonom o ochrane osobných údajov a všetkými zavedenými predpismi, ktoré sa toho týkajú (spolu „**CCPA**“); (2) Zákon o ochrane osobných údajov štátu Colorado (ďalej len „**CPA**“), (3) Zákon o ochrane osobných údajov štátu Virginia (ďalej len „**CDPA**“); (4) Zákon o ochrane osobných údajov spotrebiteľov štátu Utah (ďalej len „**UCPA**“) a (5) Zákon o ochrane osobných údajov štátu Connecticut (ďalej len „**CTDPA**“).

2. ROZSAH PLATNOSTI A PODROBNOSTI SPRACÚVANIA ÚDAJOV

- 2.1 Táto DPA sa vzťahuje na Osobné údaje Zákazníka spracúvané spoločnosťou Iron Mountain ako Sprostredkovateľom v rámci poskytovania Služieb podľa tejto Zmluvy v mene Zákazníka.
- 2.2 Spoločnosť Iron Mountain môže zhromažďovať a spracúvať osobné údaje zamestnancov Zákazníka a jeho pridružených spoločností ako Prevádzkovateľ na oprávnené obchodné účely, ako je riadenie zmlúv a vzťahov so zákazníkmi, a v súlade s právnymi predpismi o ochrane údajov a oznámením o ochrane osobných údajov spoločnosti Iron Mountain dostupným na webových stránkach spoločnosti Iron Mountain a inými platnými zásadami ochrany osobných údajov. Povinnosti spoločnosti Iron Mountain stanovené v tejto DPA sa nevzťahujú na spracúvanie takýchto Osobných údajov.
- 2.3 Predmetom spracúvania Osobných údajov je poskytovanie Služieb. Práva a povinnosti Zákazníka a spoločnosti Iron Mountain sú stanovené v tejto DPA. V prílohe 1 tejto DPA sa uvádza povaha, trvanie a účel spracúvania, typy Osobných údajov Zákazníkov, ktoré spoločnosť Iron Mountain spracúva, a kategórie Dotknutých osôb, ktorých Osobné údaje sa spracúvajú.
- 2.4 Keď spoločnosť Iron Mountain spracúva Osobné údaje Zákazníka v priebehu poskytovania Služieb, spoločnosť Iron Mountain:
- 2.4.1 spracúva Osobné údaje Zákazníka iba v súlade so zdokumentovanými pokynmi Zákazníka. Ak sa od spoločnosti Iron Mountain vyžaduje, aby spracúvala Osobné údaje Zákazníka na akýkoľvek iný účel podľa právnych predpisov, ktoré sa vzťahujú na spoločnosť Iron Mountain, spoločnosť Iron Mountain bude o tejto požiadavke najskôr informovať Zákazníka, pokiaľ to takéto zákony nezakazujú z dôležitých dôvodov verejného záujmu, a
- 2.4.2 bude vždy dodržiavať platné právne predpisy o ochrane údajov a okamžite o tom informuje Zákazníka, ak podľa názoru spoločnosti Iron Mountain pokyn na Spracúvanie Osobných údajov Zákazníka zadaný Zákazníkom porušuje platné právne predpisy o ochrane údajov.
- 2.5 Pokyny Zákazníka budú pre spoločnosť Iron Mountain záväzné, pokiaľ vykonanie pokynov nevyžaduje poskytovanie služieb podľa Zmluvy a ak Zákazník nesúhlasí s platbou servisných poplatkov za takéto služby.
- 2.6 Spoločnosť Iron Mountain zabezpečí, aby pracovníci, ktorí majú prístup k osobným údajom Zákazníka, podliehali záväznej povinnosti zachovávať mlčanlivosť v súvislosti s týmito Osobnými údajmi Zákazníka a prijme primerané opatrenia na zabezpečenie spoľahlivosti a spôsobilosti zamestnancov spoločnosti Iron Mountain, ktorí majú prístup k Osobným údajom Zákazníka.

3. POSKYTOVANIE POMOCI ZÁKAZNÍKOM

- 3.1 Spoločnosť Iron Mountain poskytne zákazníkovi pomoc, pričom vždy zohľadní povahu Spracúvania:
- 3.1.1 vhodnými technickými a organizačnými opatreniami a pokiaľ je to možné, pri plnení povinností Zákazníka reagovať na žiadosti Dotknutých osôb, ktoré si uplatňujú svoje práva;
- 3.1.2 pri zabezpečovaní súladu s povinnosťami Zákazníka (ako je bezpečnosť spracúvania, oznamovanie porušenia povinností týkajúcich sa Osobných údajov dozornému orgánu, oznamovanie porušenia povinností týkajúcich sa Osobných údajov Dotknutej osobe, posúdenie vplyvu na ochranu Osobných údajov a predchádzajúca konzultácia s dozornými orgánmi, keď by Spracúvanie mohlo viesť k vysokému riziku v prípade, že by prevádzkovateľ neprijal opatrenia na zmiernenie rizika), pričom sa zohľadňujú informácie, ktoré má spoločnosť Iron Mountain k dispozícii a
- 3.1.3 sprístupnením všetkých informácií, o ktoré Zákazník odôvodnene žiada, aby mohol preukázať, že jeho povinnosti pri výbere a vymenovaní spoločnosti Iron Mountain boli splnené.

4. BEZPEČNOSTNÉ OPATRENIA

- 4.1 S ohľadom na bežné prevádzkové postupy, náklady na implementáciu a povahu, rozsah, kontext a účely spracúvania, spoločnosť Iron Mountain zavedie vhodné a primerané technické a organizačné opatrenia určené na ochranu dôvernosti, integrity a dostupnosti Osobných údajov Zákazníka a na ochranu Osobných údajov Zákazníka pred neoprávneným alebo nezákonným Spracúvaním a pred náhodnou stratou, zničením, poškodením, zmenou alebo zverejnením. Bezpečnostné normy spoločnosti Iron Mountain sú uvedené v Prílohe 2 tejto DPA.

- 4.2 Zákazník je výlučne zodpovedný za posúdenie toho, či tieto technické a organizačné opatrenia spĺňajú požiadavky Zákazníka.

5. DODRŽIAVANIE PRÁVNÝCH PREDPISOV

Zákazník a jeho pridružené spoločnosti: (i) budú spracúvať osobné údaje Zákazníka v súlade s právnymi predpismi o ochrane údajov; (ii) sú oprávnení dávať spoločnosti Iron Mountain písomné pokyny na Spracúvanie Osobných údajov Zákazníka v súvislosti so Službami (vrátane pokynov v mene akejkoľvek tretej strany, ktorá je prevádzkovateľom Osobných údajov Zákazníka); a (iii) si vždy ponechajú kontrolu a právomoc nad Osobnými údajmi Zákazníka v súvislosti so Spracúvaním.

6. SUBSPRACÚVANIE

- 6.1 Zákazník berie na vedomie a súhlasí s tým, že spoločnosť Iron Mountain môže zapojiť materskú spoločnosť, pridružené spoločnosti a iných ďalších sprostredkovateľov tretích strán (vrátane ďalších sprostredkovateľov tretích strán zapojených pridruženými spoločnosťami alebo materskou spoločnosťou spoločnosti Iron Mountain) na účely Spracúvania Osobných údajov Zákazníka podľa tejto DPA s výhradou článku 6.2 nižšie.
- 6.2 Zoznam ďalších sprostredkovateľov schválených Zákazníkom k dátumu tejto DPA je k dispozícii [tu](#)¹. Spoločnosť Iron Mountain môže kedykoľvek nahradiť alebo vymenovať nového ďalšieho sprostredkovateľa za predpokladu, že Zákazník dostane písomné oznámenie pätnásť (15) dní vopred a nebude v rámci tohto časového rámca namietat' proti takýmto zmenám z preukázateľných dôvodov súvisiacich s ochranou údajov. Aby Zákazník mohol dostávať tieto e-mailové upozornenia, musí sa prihlásiť a spravovať akékoľvek existujúce predplatné v rámci služieb oznámení spoločnosti Iron Mountain prostredníctvom tejto [webovej stránky](#)².
- 6.3 Ak sa Zákazník neprihlási na odber tejto oznamovacej služby, spoločnosť Iron Mountain nenesie zodpovednosť za chýbajúce oznámenie ďalších sprostredkovateľov a všetky takéto termíny sa budú považovať za schválené Zákazníkom. Ak Zákazník z preukázateľných dôvodov súvisiacich s ochranou údajov písomne podá námietku voči vymenovaniu náhradného alebo nového ďalšieho sprostredkovateľa do pätnásť (15) dní vopred, spoločnosť Iron Mountain vynaloží primerané úsilie, aby Zákazníkovi sprístupnila zmenu Služby alebo odporučila zmenu konfigurácie Zákazníka alebo používania Služieb, v každom prípade s cieľom vyhnúť sa spracúvaniu Osobných údajov Zákazníka zo strany ďalšieho sprostredkovateľa, voči ktorému je námietka vznesená, na posúdenie a schválenie Zákazníkom. Ak Zákazník neschváli akékoľvek takéto zmeny navrhnuté spoločnosťou Iron Mountain do pätnásť (15) dní, spoločnosť Iron Mountain môže na základe písomného oznámenia Zákazníkovi okamžite ukončiť Službu alebo časť Služby, ktorú spoločnosť Iron Mountain nemôže poskytnúť bez použitia namietaného ďalšieho sprostredkovateľa. Takýmto ukončením nie sú dotknuté žiadne nadobudnuté práva ani záväzky strán za predpokladu, že spoločnosť Iron Mountain alebo jej pridružené spoločnosti nebudú v súvislosti s takýmto ukončením zmluvy platiť žiadne poplatky za ukončenie, výdavky ani iné kompenzácie a Zákazník sa okamžite zaväzuje prevziať majetok, ktorý poskytol spoločnosti Iron Mountain ako súčasť ukončených Služieb v súlade s podmienkami Zmluvy a na vlastné náklady.
- 6.4 Spoločnosť Iron Mountain zabezpečí, aby každá zmluva s ďalšími sprostredkovateľmi v rozsahu platnosti tejto DPA obsahovala ustanovenia, ktoré sú vo všetkých podstatných ohľadoch rovnaké ako ustanovenia tejto DPA a sú také, ako to vyžadujú platné právne predpisy o ochrane údajov. Ak ďalší sprostredkovateľ spoločnosti Iron Mountain pôsobí, že spoločnosť Iron Mountain poruší svoje záväzky vyplývajúce z tejto DPA alebo z akýchkoľvek platných právnych predpisov o ochrane údajov, spoločnosť Iron Mountain bude v plnej miere zodpovedná voči Zákazníkovi za splnenie záväzkov spoločnosti Iron Mountain podľa týchto podmienok.

7. PORUŠENIA ZABEZPEČENIA

- 7.1 V prípade podozrenia z porušenia zabezpečenia spoločnosť Iron Mountain:
- 7.1.1 okamžite prijme opatrenia na vyšetrovanie podozrenia na Porušenie zabezpečenia a identifikáciu, prevenciu a zmiernenie účinkov podozrenia na Porušenie zabezpečenia a nápravu Porušenia zabezpečenia;
- 7.1.2 bezodkladne upovedomí Zákazníka, keď bude mať primeraný stupeň istoty, že došlo k porušeniu zabezpečenia, a poskytne Zákazníkovi podrobný opis Porušenia zabezpečenia vrátane informácií primerane potrebných na to, aby si Zákazník splnil oznamovacie povinnosti podľa právnych predpisov o ochrane údajov.

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-KSV6FFlot0PGng&r=JTizF2zjl-gYEg5GmWmZcbbq-d-hqyVuleEIP9Eu7Nvw&m=NB4wllSphmYGqqrvtYNU-28S8AAU6-YibdZ3Yg_2F68&s=xNzeKlzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

- 7.2 Zákazník súhlasí s tým, že spoločnosť Iron Mountain môže poskytovať údaje podľa článku 7.1.2 postupne. V takých prípadoch, keď spoločnosť Iron Mountain nemá prístup k určitým údajom uvedeným v článku 7.1.2 alebo ich Zákazníkovi nemôže poskytnúť, bude o tom Zákazníka informovať a nebude niesť žiadnu zodpovednosť za neposkytnutie takýchto údajov.

8. AUDITY

Spoločnosť Iron Mountain umožní Zákazníkovi a jeho príslušným audítorom alebo splnomocneným zástupcom po tom, čo spoločnosti Iron Mountain predložia oznámenie aspoň desať (10) pracovných dní vopred, vykonať audity alebo kontroly počas trvania Zmluvy za predpokladu, že spoločnosť Iron Mountain nebude musieť poskytnúť ani povoliť prístup k údajom týkajúcim sa: (i) iných zákazníkov spoločnosti Iron Mountain; (ii) akýchkoľvek neverejných externých správ spoločnosti Iron Mountain; a (iii) akýchkoľvek interných správ pripravených oddelením pre interný audit alebo oddelením dodržiavania predpisov spoločnosti Iron Mountain. Účely auditu alebo kontroly podľa tohto článku sa obmedzia na overenie, či spoločnosť Iron Mountain spracúva Osobné údaje Zákazníka v súlade so svojimi povinnosťami podľa tejto DPA. Okrem prípadov, keď dôjde k porušeniu zabezpečenia, za obdobie dvanástich (12) mesiacov bude vykonaný najviac jeden takýto audit.

9. MEDZINÁRODNÉ PRENOSY ÚDAJOV (OBMEDZENÉ PRENOSY)

- 9.1 Zákazník týmto v príslušnom rozsahu súhlasí a povoľuje medzinárodné prenosy Osobných údajov Zákazníka subjektom uvedeným v článku 6.2 a v súlade s Prílohou 3 na poskytovanie služieb. Zákazník a spoločnosť Iron Mountain sa dohodli, že:

- 9.1.1 budú dodržiavať platné právne predpisy o ochrane údajov v súvislosti s takýmito prenosmi;
- 9.1.2 okrem iného aj s ohľadom na i) kategórie osobných údajov zákazníka, ii) krajiny, ktorých vnútroštátne zákony nemusia poskytovať úroveň ochrany osobných údajov, ktorá je porovnateľná s úrovňou ochrany osobných údajov v rámci platných zákonov EÚ/Spojeného kráľovstva (ďalej len „**tretia krajina**“) iii) príslušné technické a organizačné opatrenia uvedené v článku 7 a iv) príslušné strany podieľajúce sa na spracúvaní takýchto Osobných údajov Zákazníka, vykonali posúdenie vhodnosti príslušného mechanizmu prenosu prijatého podľa tejto zmluvy, ak sa to vyžaduje podľa zákona, a určili, že takýto mechanizmus prenosu je vhodne navrhnutý na zabezpečenie toho, aby sa Osobným údajom prenášaným v súlade s touto DPA poskytovala v cieľovej krajine úroveň ochrany, ktorá je v podstate rovnocenná s úrovňou ochrany zaručenou podľa právnych predpisov o ochrane údajov.

10. ZODPOVEDNOSŤ A ODŠKODNENIE

- 10.1 Bez ohľadu na čokoľvek, čo je v Zmluve uvedené inak, v prípade porušenia zabezpečenia spôsobeného priamo porušením povinností spoločnosti Iron Mountain podľa tejto DPA, spoločnosť Iron Mountain uhradí Zákazníkovi v rozsahu povolenom príslušným zákonom priame, preukázateľné, nevyhnutné a odôvodnené vynaložené náklady Zákazníka v súvislosti s tretími stranami pri (a) vyšetrovaní takéhoto porušenia zabezpečenia, (b) príprave a odoslaní oznámení takýmto Dotknutým osobám a regulačným orgánom, ako to vyžadujú právne predpisy o ochrane údajov, (c) poskytovaní Služieb monitorovania kreditu takýmto jednotlivcom, ako to vyžaduje zákon na obdobie menej ako dvanásť (12) mesiacov, a (d) úhrade časti regulačných pokút, penále alebo sankcií uložených dozorným orgánom, pri ktorých dozorný orgán uvedie, že je priamo zodpovedná spoločnosť Iron Mountain.
- 10.2 V prípade, že Dotknutá osoba vznesie voči jednej alebo oboch zmluvným stranám nárok na odškodnenie za údajné porušenie právnych predpisov o ochrane údajov (ďalej len „**nároky Dotknutej osoby**“) a ak je to povolené, každá zmluvná strana bude riadiť svoju obhajobu takéhoto nároku (alebo časť obhajoby) a bude výlučne zodpovedná za vlastné náklady, výdavky a záväzky s tým súvisiace, vrátane poplatkov za právne zastupovanie alebo akýchkoľvek poplatkov, ktoré jej prisúdil súd alebo ktoré uhradila v rámci vyrovnaní, to však za predpokladu, že ak je každá zo strán zodpovedná za časť alebo ak je niektorá zo strán zodpovedná za celú výšku škody, ktorú utrpela Dotknutá osoba v súvislosti s tým istým incidentom alebo sériou incidentov, a Dotknutá osoba získala plnú náhradu škody len od jednej strany (ďalej len „**Odškodňujúca strana**“), potom bude Odškodňujúca strana oprávnená žiadať od druhej zmluvnej strany späť tú časť náhrady, ktorá zodpovedá škode spôsobenej touto druhou stranou. Odškodňujúca strana môže uplatniť svoj nárok voči druhej zmluvnej strane len do 12 mesiacov po incidente, a to v rozsahu povolenom príslušným zákonom.
- 10.3 V maximálnom rozsahu povolenom príslušnými zákonmi, sa obmedzenia zodpovednosti a akékoľvek vylúčenia škôd uvedené v Zmluve vzťahujú na celkovú zodpovednosť za všetky nároky Zákazníka vyplývajúce z tejto DPA a/alebo Zmluvy voči spoločnosti Iron Mountain alebo v súvislosti s nimi. Tieto obmedzenia zodpovednosti a vylúčenia škôd sa vzťahujú na všetky nároky, či už vyplývajúce zo zmluvy, deliktu alebo akejkoľvek inej teórie zodpovednosti, a akýkoľvek odkaz na zodpovednosť spoločnosti Iron Mountain znamená súhrnnú zodpovednosť spoločnosti Iron Mountain a všetkých pridružených spoločností Iron Mountain za nároky zo strany Zákazníka a všetkých ostatných pridružených spoločností Zákazníka. V rozsahu vyžadovanom príslušnými zákonmi nie je cieľom tohto článku na (i) upraviť ani obmedziť zodpovednosť strán za nároky Dotknutých osôb vznesené voči zmluvnej strane v

prípade spoločnej a nerozdielnej zodpovednosti ani (ii) obmedziť zodpovednosť ktorejkoľvek zo strán za zaplatenie pokút uložených takejto zmluvnej strane regulačným orgánom.

- 10.4 V článkoch 10.1 až 10.3 sa uvádza jediný a výhradný opravný prostriedok každej zmluvnej strany a výhradná zodpovednosť každej zmluvnej strany za akúkoľvek stratu, škodu, výdavky alebo zodpovednosť v súvislosti s touto DPA.

11. ŽIADOSTI ORGÁNOV VEREJNEJ MOCI

- 11.1 V rozsahu, ktorý je právne prípustný, a s výhradou článkov 11.2 až 11.5 nižšie spoločnosť Iron Mountain súhlasí s tým, že bude informovať Zákazníka, ak:

11.1.1 dostane právne záväznú žiadosť od orgánu verejnej moci vrátane súdnych orgánov podľa zákonov krajiny určenia o poskytnutie Osobných údajov Zákazníka prenesených v súlade so Zmluvou alebo

11.1.2 sa dozvie o akomkoľvek priamom prístupe orgánov verejnej moci k Osobným údajom Zákazníka preneseným v súlade so Zmluvou a podľa zákonov danej krajiny určenia.

- 11.2 Ak má spoločnosť Iron Mountain zakázané informovať zákazníka podľa zákonov krajiny určenia, súhlasí s tým, že vynaloží maximálne úsilie na získanie výnimky zo zákazu s cieľom čo najskôr poskytnúť čo najviac informácií.

- 11.3 Spoločnosť Iron Mountain súhlasí s tým, že preskúma zákonnosť žiadosti o sprístupnenie, najmä to, či zostáva v rámci právomocí udelených žiadajúcemu orgánu verejnej moci, a spochybní žiadosť, ak dospeje k záveru, že existujú primerané dôvody domnievať sa, že žiadosť je podľa zákonov cieľovej krajiny nezákonná. Nezverejní požadované Osobné údaje Zákazníka, pokiaľ to nebude musieť urobiť podľa platných procesných pravidiel.

- 11.4 Spoločnosť Iron Mountain súhlasí s tým, že pri odpovedi na žiadosť o sprístupnenie poskytne minimálne množstvo údajov, ktoré sú prípustné na základe primeraného výkladu žiadosti.

- 11.5 Spoločnosť Iron Mountain súhlasí s tým, že bude uchovávať údaje podľa tohto článku počas trvania Zmluvy a na požiadanie ich sprístupní príslušnému dozornému orgánu.

12. RÔZNE

- 12.1 V závislosti od povahy Služieb poskytovaných spoločnosťou Iron Mountain po ukončení/uplynutí platnosti Zmluvy na základe konkrétnych pokynov Zákazníka a v súlade s podmienkami Zmluvy spoločnosť Iron Mountain buď vymaže/zničí všetky Osobné údaje Zákazníka, alebo ich vráti Zákazníkovi alebo tretej strane určenej Zákazníkom. Osobné údaje akéhokoľvek Zákazníka, ktoré sú súčasťou majetku Zákazníka a v mene Zákazníka uchovávané spoločnosťou Iron Mountain, sa vrátia Zákazníkovi v súlade s dohodnutým plánom odchodu alebo prechodu a dohodnutými nákladmi, ako je stanovené v Zmluve alebo v inom platnom zmluvnom dokumente. Vo všetkých ostatných prípadoch, ak v Zmluve nie je uvedené ustanovenie o vymazaní/zničení alebo vrátení Osobných údajov Zákazníka a Zákazník neposkytne žiadne pokyny týkajúce sa vymazania/zničenia alebo vrátenia jeho Osobných údajov do pätnástich (15) dní od ukončenia/uplynutia platnosti Zmluvy, spoločnosť Iron Mountain zašle Zákazníkovi písomné oznámenie, v ktorom ho požiada, aby do 15 (pätnástich) dní poskytol konkrétne pokyny týkajúce sa vymazania/zničenia alebo vrátenia jeho Osobných údajov, a informuje Zákazníka o všetkých príslušných poplatkoch za bezpečné zničenie alebo iných poplatkoch splatných Zákazníkom. Ak Zákazník neposkytne písomné pokyny v tejto lehote pätnástich (15) dní a v rovnakej lehote nezplatí príslušné poplatky, oprávňuje týmto spoločnosť Iron Mountain, aby po ukončení Zmluvy naďalej spracúvala, vymazávala a ničila všetky Osobné údaje Zákazníka na základe jej vlastného rozhodnutia a na náklady Zákazníka.

- 12.2 Bez ohľadu na článok 12.1 spoločnosť Iron Mountain neporuší svoje povinnosti týkajúce sa vymazania Osobných údajov Zákazníka uchovávaných na záložných páskach, pokiaľ sú takéto záložné pásky prepísané (a tým sa Osobné údaje Zákazníka vymažú) v rámci bežnej obchodnej činnosti.

- 12.3 Okrem Štandardných zmluvných doložiek (ako sú definované v Prílohe 3 tejto DPA) sa táto DPA a akýkoľvek spor, nárok alebo konflikt vyplývajúci z tejto DPA alebo s ňou súvisiaci alebo jej porušenie, ukončenie alebo platnosť riadia ustanovením o voľbe práva v Zmluve, a akýkoľvek spor, konflikt alebo nárok vyplývajúci z tejto DPA alebo v súvislosti s ňou sa budú primárne riešiť prostredníctvom akéhokoľvek definovaného postupu riešenia sporov uvedeného v Zmluve.

- 12.4 Každá zmluvná strana môže priebežne písomne oznámiť druhej zmluvnej strane akékoľvek úpravy tejto DPA, ktoré zmluvná strana odôvodnene považuje za potrebné na splnenie požiadaviek právnych predpisov o ochrane údajov alebo akéhokoľvek rozhodnutia dozorného orgánu alebo príslušného súdu. Všetky takéto úpravy nadobudnú účinnosť iba vtedy, ak sú uvedené vo vzájomne schválenom dodatku k tejto DPA podpísanom obidvoma zmluvnými stranami a v rozsahu, ktorý je v ňom uvedený, s výnimkou prípadov, keď jedna zmluvná strana bude druhú zmluvnú protistranu informovať o novej právnej požiadavke a pošle taký dodatok, ktorý bude obsahovať iba potrebné zmeny, ktoré je možné prijať bez formálneho súhlasu, t. j. nevznesením námietky v určitej lehote, pričom v takom stave sa budú považovať za vzájomne odsúhlasené dodatky k tejto DPA.

PRÍLOHA 1

Podrobnosti o spracúvaní a prenose údajov (ak je to relevantné)

A. ZOZNAM ZMLUVNÝCH STRÁN:

Zmluvné strany tejto DPA a úlohy Vývozcu údajov a Dovožcu údajov sú uvedené v Zmluve a prípadne v Prílohe 3 (Medzinárodné prenosy údajov).

B. OPIS SPRACÚVANIA/PRENOSU (ak je to relevantné):

Kategórie Dotknutých osôb, ktorých údaje sa spracúvajú/prenášajú:

V závislosti od povahy Služieb spoločnosti Iron Mountain a podnikania Zákazníka môže Zákazník odovzdať spoločnosti Iron Mountain Osobné údaje patriace rôznym kategóriám Dotknutých osôb, ktorých rozsah určuje a kontroluje Zákazník podľa vlastného uváženia. Medzi takéto kategórie Dotknutých osôb môžu patriť: minulí a súčasní zamestnanci, minulí a súčasní dodávatelia alebo konzultanti, agentúrni dodávatelia alebo konzultanti a externí vyslaní pracovníci, uchádzači o zamestnanie a kandidáti, študenti a dobrovoľníci, jednotlivci identifikovaní zamestnancami alebo dôchodcami ako príjemcovia, manžel/manželka, druh/družka, závislé osoby a kontaktné osoby pre núdzové prípady, dôchodcovia, minulí a súčasní riaditelia a funkcionári, akcionári, vlastníci dlhopisov, majitelia účtov, koncoví používatelia/spotrebitelia (dospelí, deti), pacienti (dospelí, deti), okoloidúci (v prípade použitia priemyselných kamier) a používatelia webovej lokality.

Kategórie spracúvaných/prenášaných Osobných údajov:

V závislosti od povahy Služieb spoločnosti Iron Mountain a podnikania Zákazníka môže Zákazník poskytnúť spoločnosti Iron Mountain Osobné údaje patriace do rôznych kategórií Osobných údajov, ktorých rozsah určuje a kontroluje Zákazník podľa vlastného uváženia. Kategórie ako také môžu zahŕňať Osobné údaje týkajúce sa Zákazníka a/alebo jeho vlastných klientov, zamestnancov atď.

Prenášané citlivé údaje (ak je to relevantné):

V závislosti od povahy Služieb spoločnosti Iron Mountain a podnikania Zákazníka môže Zákazník poskytnúť spoločnosti Iron Mountain citlivé údaje, ktorých rozsah určuje a kontroluje Zákazník podľa vlastného uváženia.

Ak je to relevantné, frekvencia prenosu (napr. či sa údaje prenášajú jednorazovo alebo nepretržite):

Prenos prebieha nepretržite.

Povaha Spracúvania:

zhromažďovanie, zaznamenávanie, organizovanie, štruktúrovanie, uchovávanie, prispôsobovanie alebo zmena, vyhľadávanie, prehliadanie, používanie, zverejňovanie prenosom, šírenie alebo iné sprístupňovanie, zosúladovanie alebo kombinovanie, obmedzovanie, vymazávanie alebo ničenie.

Účel/-y spracúvania/prenosu údajov (ak je to relevantné) a ďalšieho Spracúvania:

Poskytovanie Služieb, ako je uvedené v Zmluve.

Uchovávanie údajov:

Spoločnosť Iron Mountain bude uchovávať Osobné údaje počas trvania Služieb ponúkaných Zákazníkovi a dotedy, kým nebudú Osobné údaje vrátené alebo zničené v súlade s článkom 12.1 tejto DPA.

Ak je to relevantné, v prípade prenosov (ďalším) sprostredkovateľom tiež uveďte predmet, povahu a trvanie Spracúvania:

Počas trvania Zmluvy so Zákazníkom poskytujú ďalší sprostredkovatelia okrem iného Informačné technológie (IT) a konzultačné služby vrátane globálnej podpory IT, hlásenia udalostí a služieb správy.

C. PRÍSLUŠNÝ DOZORNÝ ORGÁN

Ako je uvedené v Prílohe 3 (Medzinárodné prenosy údajov), ak je to relevantné.

PRÍLOHA 2

TECHNICKÉ A ORGANIZAČNÉ OPATRENIA („BEZPEČNOSTNÉ OPATRENIA“)

1. PROGRAM A ZÁSADY INFORMAČNEJ BEZPEČNOSTI

Spoločnosť Iron Mountain bude udržiavať program informačnej bezpečnosti pomocou príslušných fyzických, technických a administratívnych kontrol, ktoré sú navrhnuté tak, aby spĺňali priemyselné normy. Program informačnej bezpečnosti zahŕňa:

- 1.1 dokumentáciu, internú publikáciu a komunikáciu o zásadách, normách a postupoch informačnej bezpečnosti spoločnosti Iron Mountain;
- 1.2 zdokumentované jasné pridelenie zodpovednosti a právomocí na vytvorenie a udržiavanie programu informačnej bezpečnosti;
- 1.3 pravidelné testovanie kľúčových kontrol, systémov a postupov programu informačnej bezpečnosti;
- 1.4 administratívne, technické a prevádzkové opatrenia určené na ochranu všetkých Osobných údajov Zákazníka s využitím praktík, postupov a procesov opísaných v tejto prílohe o bezpečnosti v rozsahu, v akom sú relevantné a v akom sa vzťahujú na formát, v ktorom sa Osobné údaje Zákazníka uchovávajú.

2. HODNOTENIE RIZIKA

Spoločnosť Iron Mountain bude udržiavať program hodnotenia rizík informačnej bezpečnosti určený na identifikáciu a posúdenie rozumne predvídateľných interných a externých rizík a zraniteľností, ktoré by mohli ovplyvniť bezpečnosť, dôvernosť a/alebo integritu Osobných údajov Zákazníka. Spoločnosť Iron Mountain každoročne alebo vždy, keď dôjde k podstatnej zmene rizika alebo zraniteľnosti Osobných údajov Zákazníka, vyhodnotí a aktualizuje, ak je to potrebné, primerané a vhodné, účinnosť súčasného programu informačnej bezpečnosti na obmedzenie takýchto rizík.

3. SPRÁVA PROSTRIEDKOV NA SPRACÚVANIE INFORMÁCIÍ A FYZICKÝCH MÉDIÍ

- 3.1 Správa prostriedkov na spracúvanie informácií. Spoločnosť Iron Mountain udržiava program správy inventára majetku na riadenie fyzických, technických a administratívnych kontrol týkajúcich sa majetku spoločnosti Iron Mountain na spracúvanie informácií (napr. počítače, servery, úložné zariadenia, komunikačné siete, osobné počítače, notebooky a periférne zariadenia).

Program riadenia inventarizácie prostriedkov zahŕňa:

- 3.1.1 zdokumentované pridelenie vlastníctva prostriedkov personálu spoločnosti Iron Mountain s cieľom zabezpečiť primeranú klasifikáciu informácií, určenie obmedzení prístupu a zhodnotenie kontroly prístupu;
 - 3.1.2 sanitáciu prostriedkov pred ich likvidáciou v súlade s usmernením NIST 800-88;
 - 3.1.3 požiadavku oprávnenia manažmentu pred odstránením zariadenia alebo softvéru, ktorý nie je pridelený konkrétnej osobe z priestorov spoločnosti Iron Mountain.
- 3.2 Kontroly. Kontroly spoločnosti Iron Mountain zahŕňajú:
 - 3.2.1 prevádzkové postupy a technické kontroly určené na ochranu dokumentov, počítačových médií, vstupných/výstupných/záložných údajov a systémovej dokumentácie pred neoprávneným zverejnením, úpravou a zničením;
 - 3.2.2 postupy na bezpečnú likvidáciu elektronických alebo fyzických médií obsahujúcich Osobné údaje Zákazníka;
 - 3.2.3 zavedený proces sledovania všetkých fyzických médií Zákazníka od počiatočnej úschovy v spoločnosti Iron Mountain až po trvalé stiahnutie alebo zničenie.

4. OPATRENIA NA ZABEZPEČENIE PRACOVNEJ SILY

- 4.1 Dôvernosť. Spoločnosť Iron Mountain bude primerane vyžadovať, aby všetci zamestnanci spoločnosti Iron Mountain vrátane zamestnancov na dobu určitú a zmluvných zamestnancov súhlasili so zachovaním dôvernosti Osobných údajov Zákazníka a dodržiavali interné požiadavky spoločnosti Iron Mountain na bezpečnosť informácií a prijateľné používanie.
- 4.2 Zásady bezpečnostných previerok. Spoločnosť Iron Mountain má pre svojich zamestnancov zavedené zásady bezpečnostných previerok a testovania na drogy (iba v USA). Spoločnosť Iron Mountain bude pokračovať v zachovávaní týchto zásad počas platnosti Zmluvy. Požiadavky zásad zahŕňajú okrem iného testy na drogy (iba USA), overenie totožnosti zamestnancov, vyhľadávanie v registri trestov, overovanie zamestnania, vyhľadávanie v štátnych zoznamoch/zoznamoch hľadaných teroristov, ako aj overovanie vzdelania určitých zamestnancov, udeľovanie vodičského oprávnenia a históriu priestupkov u žiadateľov o vodičské oprávnenie a existujúcich vodičov. Keď sa pri bezpečnostnej previerke zistia znevažujúce informácie, spoločnosť Iron Mountain vykoná individuálne posúdenie v súlade s platnými pracovnoprávnymi postupmi a osvedčenou praxou.
- 4.3 Spolupráca so subdodávateľmi. Spoločnosť Iron Mountain bude od každého subdodávateľa, ktorý vykonáva Služby podľa Zmluvy, žiadať, aby dodržiaval podobné obmedzenia, ako sú tie, ktoré sú uvedené v tomto článku, pokiaľ ide o zamestnancov subdodávateľov, ktorí budú vykonávať Služby podľa Zmluvy, ktorých súčasťou je Spracúvanie Osobných údajov Zákazníka.

- 4.4 Školenie na zvyšovanie povedomia o bezpečnosti. Minimálne raz ročne spoločnosť Iron Mountain zorganizuje všeobecné školenie na zvyšovanie povedomia o bezpečnosti a školenie týkajúce sa bezpečnosti na konkrétnych pozíciách pre všetkých zamestnancov spoločnosti Iron Mountain s prístupom k Osobným údajom Zákazníka. Spoločnosť Iron Mountain bude viesť prezenčné záznamy s menami zamestnancov spoločnosti Iron Mountain a dátumom každého školenia na zvyšovanie povedomia o bezpečnosti. Spoločnosť Iron Mountain bude pravidelne kontrolovať a aktualizovať svoj školiaci program na zvyšovanie povedomia o bezpečnosti.
- 4.5 Prepúšťanie zamestnancov spoločnosti Iron Mountain. Spoločnosť Iron Mountain vedie disciplinárne postupy, ktoré sa vzťahujú na zamestnancov spoločnosti Iron Mountain, ktorí porušia bezpečnostné požiadavky uvedené v tejto Zmluve.
- 4.6 Ukončenie prístupu pri ukončení pracovného pomeru/preradení. Po ukončení pracovného pomeru alebo preradení na pozíciu, pri ktorej nie je potrebný prístup k Osobným údajom Zákazníka, sa prístup zamestnanca spoločnosti Iron Mountain k Osobným údajom Zákazníka okamžite zruší.

5. FYZICKÁ A ENVIRONMENTÁLNA BEZPEČNOSŤ

- 5.1 Fyzické bezpečnostné kontroly. Zariadenia spoločnosti Iron Mountain využívajú fyzické kontroly, pri ktorých sa primerane obmedzuje prístup k Osobným údajom Zákazníka, vrátane protokolov kontroly prístupu, fyzických bariér, ako sú uzamknuté zariadenia a priestory, prístupové preukazy zamestnancov, denníky návštev, prístupové preukazy návštevníkov, čítačky kariet, kamery na monitorovanie a alarmy na detekciu vniknutia, ak to spoločnosť Iron Mountain považuje za vhodné. Všetci návštevníci sa musia zaregistrovať a musia byť vždy sprevádzaní.
- 5.2 Podporné nástroje. Spoločnosť Iron Mountain zavedie opatrenia určené na ochranu svojich zariadení obsahujúcich Osobné údaje Zákazníkov a systémov pred výpadkami elektrickej energie, telekomunikácií, dodávok vody, kanalizácie, vykurovania, vetrania a klimatizácie, podľa potreby.
- 5.3 Bezpečnosť prenosovej sústavy. Spoločnosť Iron Mountain zavedie opatrenia určené na ochranu fyzickej bezpečnosti svojej sieťovej infraštruktúry a telekomunikačných systémov pred zachytením a poškodením prenosu.
- 5.4 Externé zariadenie. V prípade, že spoločnosť Iron Mountain externe zabezpečuje funkcie, ktoré si vyžadujú použitie externého zariadenia na podporu Služieb, všetky externé zariadenia, na ktorých sa uchováva osobné údaje Zákazníka, musia byť chránené rovnakým zabezpečením, aké sa používa pre zariadenia na pracovisku používané na rovnaký účel.
- 5.5 Fyzický prístup k prostriedkom na spracúvanie informácií. Spoločnosť Iron Mountain bude uchovávať záznamy o zamestnancoch spoločnosti Iron Mountain s oprávnením na fyzický prístup k počítačovému prostrediu kontrolovanému spoločnosťou Iron Mountain, ktoré spoločnosť Iron Mountain používa na poskytovanie Služieb, počas jedného roka a na žiadosť Zákazníka v súvislosti s porušením bezpečnosti a v súlade s bezpečnostnými zásadami spoločnosti Iron Mountain, poskytne Zákazníkovi prístup k nahliadnutiu do auditovateľných záznamov takýchto zamestnancov spoločnosti Iron Mountain.
- 5.6 Obmedzený fyzický prístup. Spoločnosť Iron Mountain obmedzí fyzický prístup do zariadení kontrolovaných spoločnosťou Iron Mountain, ktoré spracúvajú Osobné údaje Zákazníkov, na tých zamestnancov spoločnosti Iron Mountain a oprávnených jednotlivcov, ktorí takýto prístup potrebujú. Spoločnosť Iron Mountain musí mať zavedený schvaľovací postup na schvaľovanie a sledovanie žiadostí o fyzický prístup k takýmto zariadeniam.
- 5.7 Opravy a úpravy. Spoločnosť Iron Mountain má viesť záznamy o všetkých opravách a úpravách všetkých fyzických komponentov, ktoré súvisia s bezpečnosťou, vrátane hardvéru, stien, dverí a zámkov zabezpečených oblastí v zariadeniach, kde sú uložené Osobné údaje Zákazníka.
- 5.8 Záznamy. Je potrebné viesť záznamy o pohybe hardvéru a elektronických médiách a o všetkých zodpovedných osobách.

6. RIADENIE PREVÁDZOK NA KOMUNIKÁCIU A SPRACÚVANIE INFORMÁCIÍ

- 6.1 Štandardy konfigurácie zariadení. Spoločnosť Iron Mountain vytvorí, zavedie a bude udržiavať postupy správy systému, ktoré spĺňajú priemyselné štandardy, okrem iného aj vrátane posilnenia systému, opráv systému a zariadení (operačný systém a aplikácie) a správnej inštalácie a aktualizácií antivírusových programov.
- 6.2 Kontrola zmien v systémoch spracúvania informácií. Spoločnosť Iron Mountain musí mať zavedený interný formálny proces riadenia zmien v systémoch na spracúvanie informácií a komunikačných sieťových systémov a požiadavky spoločnosti Iron Mountain na zmenu musia byť zdokumentované, otestované a schválené pred zavedením akýchkoľvek nových kompetencií spracúvania informácií alebo sieťovej komunikácie, opráv systému alebo zmien existujúcich systémov.
- 6.3 Rozdelenie povinností. Spoločnosť Iron Mountain rozdelí povinnosti a oblasti zodpovednosti tak, aby žiadna osoba nemala výhradnú možnosť upravovať systémy na spracúvanie informácií, ktoré majú prístup k Osobným údajom Zákazníka.
- 6.4 Oddelenie vývojového a výrobného prostredia. Vývojové, testovacie a výrobné prostredie spoločnosti Iron Mountain pre systémy spracúvania informácií musia byť logicky alebo fyzicky oddelené.
- 6.5 Riadenie technickej architektúry. Spoločnosť Iron Mountain zavedie proces riadenia konfigurácie na určenie, riadenie a kontrolu komponentov systému na spracúvanie informácií používaných na poskytovanie Služieb a technickej infraštruktúry takýchto komponentov.

- 6.6 Detekcia narušenia. Spoločnosť Iron Mountain bude nepretržite monitorovať počítačové systémy a postupy, či nedošlo k pokusom o narušenie alebo skutočným narušeniam alebo porušeniam bezpečnosti, a upozorní Zákazníka na akýkoľvek neoprávnený prístup k jeho Osobným údajom.
- 6.7 Bezpečnosť siete. Spoločnosť Iron Mountain zabezpečí zavedenie týchto zariadení:
- 6.7.1 pokiaľ ide o prostredie/-a, ktoré hosťuje spoločnosť Iron Mountain a ktoré sa používa/-jú na poskytovanie Služieb, výstražné udalosti systému detekcie narušenia siete („IDS“) a snímače prevencie narušenia („IPS“), ktoré sa zaznamenávajú, pričom sa denne vydávajú správy na preskúmanie (spoločne známe ako „IDS/IPS“);
- 6.7.2 pokiaľ ide o prostredie/-a, ktoré hosťuje spoločnosť Iron Mountain a ktoré sa používa/-jú na poskytovanie Služieb, IDS/IPS, ktoré sa aktualizuje/-jú nie menej často ako raz za týždeň, ale čo najskôr po prijatí aktualizácií, a okamžité spustenie najnovších signatúr alebo pravidiel týkajúcich sa hrozieb;
- 6.7.3 vysoko rizikové porty na externe orientovaných systémoch nie sú prístupné z internetu;
- 6.7.4 sieťové pripojenia spoločnosti Iron Mountain sa zaprotokolujú a zaznamenávajú do súborov protokolov;
- 6.7.5 nasadenie firewallu/-ov navrhnutého/-ých na ochranu a kontrolu všetkej prichádzajúcej a odchádzajúcej prevádzky sieťových služieb medzi určenými bodmi siete;
- 6.7.6 sprísnenie zásad na určenie vstupných a výstupných sieťových portov alebo prevádzky služieb pre všetky systémy vo vlastníctve alebo správe spoločnosti Iron Mountain, ktoré sú zdokumentované a schválené v rámci programu informačnej bezpečnosti;
- 6.7.7 sieťové a diagnostické porty, ktoré sú riadne zabezpečené a
- 6.7.8 zásady, postupy a technické kontroly, ktoré sú navrhnuté na prevenciu, zisťovanie a odstraňovanie škodlivého kódu alebo známych útokov na informačné systémy spoločnosti Iron Mountain.
- 6.8 Zašifrované overovacie údaje. Spoločnosť Iron Mountain zabezpečí, aby sa autentifikačné údaje prenášané prostredníctvom sieťových zariadení spoločnosti Iron Mountain pri prenose šifrovali.
- 6.9 Bezpečná správa siete. Siete spoločnosti Iron Mountain budú primerane riadené a kontrolované na ochranu pred známymi hrozbami a zachovanie bezpečnosti všetkých aplikácií a údajov spravovaných spoločnosťou Iron Mountain v sieti alebo pri prenose cez sieť. Zavedú sa technické kontroly a bezpečné komunikačné protokoly na zamedzenie neobmedzenému pripojeniu k nedôveryhodným sieťam alebo verejne prístupným serverom.
- 6.10 Ochrana pred vírusmi. Spoločnosť Iron Mountain zavedie a bude udržiavať program riadenia ochrany pred vírusmi vrátane ochrany proti malvéru, aktuálnych súborov s podpismi alebo alternatívnej ochrany pred novými hrozbami, opravami a definíciami vírusov pre servery a pracovné stanice spravované spoločnosťou Iron Mountain, ktoré sa používajú na uchovávanie osobných údajov zákazníka alebo na prístup k nim.
- 6.11 Webová stránka – šifrovanie klienta. Spoločnosť Iron Mountain zabezpečí, aby na každej z jej webových lokalít bola zapnutá funkcia Secure Sockets Layering (SSL) a aby obsahovala platný certifikát SSL, ktorý vyžaduje kontrolu dôvernosti, overovania alebo autorizácie.
- 6.12 Zálohovanie informácií. Spoločnosť Iron Mountain vytvorí vhodné záložné kópie systémových súborov. Okrem toho spoločnosť Iron Mountain vypracuje a bude udržiavať postupy obnovy po havárii. Ďalšie podrobnosti nájdete v časti „Obnova po havárii“ nižšie.
- 6.13 Elektronické údaje počas prenosu. Spoločnosť Iron Mountain použije na ochranu osobných údajov zákazníka prenášaných cez verejné siete, ak pochádzajú z infraštruktúry, ktorú hosťuje spoločnosť Iron Mountain, šifrovanie pomocou štandardného algoritmu s minimálnou dĺžkou kľúča 128 bitov.
- 6.14 Kryptografické kontroly. Spoločnosť Iron Mountain bude dodržiavať zdokumentované zásady používania kryptografických kontrol. Kryptografické kontroly spoločnosti Iron Mountain:
- 6.14.1 musia byť navrhnuté tak, aby primerane chránili dôvernosť a integritu Osobných údajov Zákazníka, ktoré spoločnosť Iron Mountain spracúva, prenáša alebo uchováva v akomkoľvek zdieľanom sieťovom prostredí v súlade s podmienkami Zmluvy;
- 6.14.2 sa musia používať v prostredí/-iach, ktoré hosťuje spoločnosť Iron Mountain a ktoré sa používa/-jú na poskytovanie služieb, na Osobné údaje Zákazníka pri prenose cez nedôveryhodné siete (t. j. siete, ktoré spoločnosť Iron Mountain nemá pod zákonnou kontrolou) alebo do nich vrátane sietí používaných na odosielanie údajov do podnikovej siete Zákazníka zo siete spoločnosti Iron Mountain, v každom prípade za predpokladu, že Zákazník spolupracuje pri správe šifrovacích kľúčov potrebných na dešifrovanie prenosov prijatých Zákazníkom; a
- 6.14.3 musia obsahovať zdokumentované postupy správy šifrovacích kľúčov na podporu bezpečnosti kryptografických technológií;
- 6.14.4 musia zahŕňať šifrovanie všetkých Osobných údajov Zákazníka na prenosných počítačoch alebo iných prenosných zariadeniach.
- 6.15 Požiadavky na zaznamenávanie. Spoločnosť Iron Mountain zabezpečí:
- 6.15.1 zaznamenávanie a kontrolu významných bezpečnostných a systémových udalostí;
- 6.15.2 uchovávanie záznamov z auditu minimálne jeden rok pre systémy v prostredí/-iach, ktoré spoločnosť Iron Mountain hosťuje a používa na poskytovanie služieb;
- 6.15.3 posúdenie záznamov z auditu systému s ohľadom na anomálie a
- 6.15.4 primeranú ochranu zaznamenávacích zariadení a informácií o systémoch pred manipuláciou a neoprávneným prístupom.
- 6.16 Synchronizácia sieťového času. Spoločnosť Iron Mountain bude synchronizovať systémové hodiny všetkých systémov na spracúvanie údajov pomocou spoločného autoritatívneho zdroja času.

- 6.17 Oddelenie v sieťach. Spoločnosť Iron Mountain vhodne oddelí súvisiace skupiny informačných služieb, používateľov a informačné systémy v sieťach.

7. KONTROLA PRÍSTUPU

- 7.1 Zásady kontroly prístupu. Spoločnosť Iron Mountain udržiava zásady riadenia prístupu v súvislosti s prostriedkami na spracúvanie informácií, ktoré spoločnosť Iron Mountain formálne schvaľuje, zverejňuje a zavádza.
- 7.2 Povolenie logického prístupu. Spoločnosť Iron Mountain bude mať zavedený proces schvaľovania žiadostí o logický prístup k Osobným údajom Zákazníka a žiadostí o prístup do systémov spoločnosti Iron Mountain určených na používanie v rámci Služieb.
- 7.3 Kontrola a posúdenie prístupu. Spoločnosť Iron Mountain poskytne prístup k Osobným údajom Zákazníka iba aktívnym zamestnancom spoločnosti Iron Mountain vrátane zamestnancov na dobu určitú a zmluvných zamestnancov a aktívnym používateľským účtom, ktorí takýto prístup potrebujú, aby mohli vykonávať svoju pracovnú funkciu. Všetky privilegované prístupy sa musia byť posúdiť a potvrdiť, aby boli v súlade s aktuálnou pracovnou úlohou, a zdokumentovať aspoň raz štvrtročne.
- 7.4 Kontrola prístupu tretích strán. Pred udelením prístupu do informačných systémov spoločnosti Iron Mountain, ktoré majú prístup k Osobným údajom Zákazníka, externým stranám spoločnosť Iron Mountain zaistí, aby boli zavedené príslušné kontroly.
- 7.5 Kontrola prístupu k operačným systémom. Spoločnosť Iron Mountain bude kontrolovať prístup k operačným systémom (softvérovým aj hardvérovým operačným systémom) vyžadovaním bezpečného prihlasovacieho procesu, ktorý jednoznačne identifikuje osobu, ktorá sa prihlasuje do operačného systému.
- 7.6 Mobilné počítačové zariadenia. Spoločnosť Iron Mountain bude mať zavedené zásady alebo postupy určené na ochranu mobilných počítačových zariadení spoločnosti Iron Mountain pred neoprávneným prístupom. Takéto zásady alebo postupy sa týkajú fyzickej ochrany, kontroly prístupu a bezpečnostných kontrol, ako je šifrovanie, ochrana pred vírusmi a zálohovanie zariadení.
- 7.7 Izolácia systémov Zákazníka. Spoločnosť Iron Mountain v rámci svojho hosťovského/-ých prostredia/-í používaného/-ých na poskytovanie Služieb logicky oddelí a segreguje Osobné údaje Zákazníka od všetkých ostatných údajov.
- 7.8 Účty. V súvislosti s účtami spoločnosť Iron Mountain:
- 7.8.1 bude vyžadovať overenie totožnosti každého zamestnanca spoločnosti Iron Mountain, ktorý žiada o prístup k systémom spoločnosti Iron Mountain, ktoré spracúvajú Osobné údaje Zákazníka, a zakáže používanie zdieľaných používateľských účtov alebo používateľských účtov so všeobecnými prihlasovacími údajmi (t. j. identifikátormi) na prístup k Osobným údajom alebo systémom Zákazníka;
- 7.8.2 bude vyžadovať, aby všetky identifikátory používateľských účtov vrátane privilegovaných účtov boli prepojené priamo s osobou (a nie s pozíciou);
- 7.8.3 ak predvolené administrátorské účty nebudú deaktivované alebo odstránené, bude vyžadovať použitie dočasných hesiel, identifikátorov odhlasovania alebo podobných kontrol pre predvolený prístup administrátorského účtu;
- 7.8.4 bude vyžadovať, aby sa neaktívne bežné účty po 90 dňoch nečinnosti zablokovali alebo deaktivovali;
- 7.8.5 zakáže prístup k účtu po viacerých neúspešných pokusoch o prístup;
- 7.8.6 bude vyžadovať jedinečné identifikátory a silné heslá, ktoré zahŕňajú minimálne tieto požiadavky: minimálne 8 znakov; musia sa meniť každých 90 dní; a majú požiadavky na zložitosť;
- 7.8.7 zakáže zamestnancom poskytovať heslá iným osobám alebo si ich zapisovať.
- 7.9 Kontroly bezobslužných systémov. Spoločnosť Iron Mountain použije šetrič obrazovky chránené heslom pre všetky systémy, ktoré sú ponechané bez dozoru a v ktorých sa 30 minút nevykonávala žiadna činnosť.

8. VÝVOJ A ÚDRŽBA AKVIZÍCIE INFORMAČNÝCH SYSTÉMOV

- 8.1 Bezpečnosť vývoja systémov. Spoločnosť Iron Mountain zabezpečí, aby bola bezpečnosť súčasťou vývoja a prevádzky všetkých informačných systémov, a zverejní a bude udržiavať interné metodiky bezpečného kódovania založené na bezpečnostných štandardoch vývoja aplikácií.
- 8.2 Správa zabezpečenia softvéru. Informačné systémy spoločnosti Iron Mountain (vrátane operačných systémov, infraštruktúry, obchodných aplikácií, služieb a aplikácií vyvinutých používateľmi) budú navrhnuté tak, aby boli v súlade so štandardmi informačnej bezpečnosti.
- 8.3 Sieťové schémy. Spoločnosť Iron Mountain bude vyvíjať, dokumentovať a udržiavať fyzické a logické schémy sieťových zariadení a prevádzky.
- 8.4 Hodnotenie zraniteľnosti aplikácií/etický hacking. Spoločnosť Iron Mountain bude minimálne raz ročne vykonávať hodnotenia zraniteľnosti aplikácií v hosťovanom/-ých prostredí/-iach používanom/-ých na poskytovanie služieb, ktoré spracúvajú Osobné údaje Zákazníkov. Podrobné výsledky sú dôverné a chránené údaje spoločnosti Iron Mountain a nebudú sa nikomu poskytovať.
- 8.5 Testovanie a kontrola zmien. Spoločnosť Iron Mountain pred nasadením skontroluje a otestuje zmeny aplikácií a operačných systémov a zabezpečí, aby nemali nepriaznivý vplyv na Osobné údaje ani systémy Zákazníka.

9. OBNOVA PO HAVÁRII

Spoločnosť Iron Mountain bude dodržiavať plán obnovy po havárii vrátane replikácie systémov a elektronických údajov používaných na podporu Služieb do záložného dátového centra. Replikácia systémov a elektronických údajov nezahŕňa Osobné údaje Zákazníka, ktoré sú fyzicky uložené v zariadení spoločnosti Iron Mountain. Spoločnosť Iron Mountain bude dodržiavať plán kontinuity podnikania na obnovenie dôležitých obchodných oddelení. Spoločnosť Iron Mountain vykoná test obnovy po havárii najmenej raz za dvanásť (12) mesiacov.

10. EXTERNÉ AUDITY A HODNOTENIA

Bezpečnostné protokoly spoločnosti Iron Mountain sú navrhnuté tak, aby boli v súlade s priemyselnými štandardmi. Spoločnosť Iron Mountain poskytne Zákazníkovi všetky správy z nezávislých auditov, ktoré si objednal u tretej strany (napr. PCI, ISO27001, SOC2 atď.), ktoré sa týkajú Služieb v regióne, v ktorom sú takéto Služby poskytované (ďalej len „Správa z auditu“). Spoločnosť Iron Mountain poskytne všetky takéto správy, ktoré boli zadané tak, aby boli určené pre zákazníkov, bez ohľadu na výsledky správy. Spoločnosť Iron Mountain nebude povinná poskytnúť výsledky interného auditu alebo výsledky iných nezávislých hodnotení, ktoré boli zadané so zámerom, aby boli pre spoločnosť Iron Mountain dôverné. Zákazníkovi a jeho externým audítorom budú na požiadanie poskytnuté kópie Správy z auditu. Akákoľvek Správa z auditu alebo iný výsledok vygenerovaný prostredníctvom testov alebo auditov povinných v tejto časti sa bude považovať za dôvernú informáciu spoločnosti Iron Mountain. Zákazník má právo poskytnúť kópiu takejto Správy z auditu všetkým príslušným zákazníkom alebo regulačným orgánom Zákazníka, pričom sa na ňu vzťahujú ustanovenia o zachovaní dôvernosti, ktoré sú rovnako prísne ako ustanovenia uvedené v tejto Zmluve. Na žiadosť Zákazníka spoločnosť Iron Mountain písomne potvrdí, že od vypracovania takejto Správy z auditu nenastali žiadne zmeny v príslušných zásadách, postupoch a interných kontrolách, ktoré nepresiahnu viac ako tri mesiace od konca vykazovaného obdobia Správy z auditu.

PRÍLOHA 3

Medzinárodné prenosy údajov

1. VYMEDZENIE POJMOV

„**Štandardné zmluvné doložky EÚ z roku 2021**“ znamenajú štandardné zmluvné doložky o prenose Osobných údajov do tretích krajín podľa nariadenia GDPR prijaté Európskou komisiou podľa Vykonávacieho rozhodnutia Komisie (EÚ) 2021/914 dostupné [tu](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)³.

„**Dodatok pre Spojené kráľovstvo z roku 2022**“ znamená šablónu dodatku B.1.0 vydanú Úradom komisára Spojeného kráľovstva pre informácie a predloženú 2. februára 2022 Parlamentu v súlade s článkom 119A Zákona o ochrane údajov z roku 2018, v znení prípadnej revízie podľa článku 18, dostupný [tu](https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf)⁴.

„**Osobné údaje zákazníka z EÚ**“ znamenajú spracúvanie Osobných údajov Zákazníka, na ktoré sa pred ich spracúvaním spoločnosťou Iron Mountain vzťahovali zákony o ochrane údajov Európskej únie alebo členského štátu Európskej únie alebo Európskeho hospodárskeho priestoru;

„**Chránená oblasť**“ znamená:

- i. v prípade Osobných údajov Zákazníkov z EÚ členské štáty Európskej únie a Európskeho hospodárskeho priestoru a akúkoľvek krajinu, územie, sektor alebo medzinárodnú organizáciu, v súvislosti s ktorými platí rozhodnutie o primeranosti podľa článku 45 nariadenia GDPR;
- ii. v prípade Osobných údajov Zákazníkov zo Spojeného kráľovstva Spojené kráľovstvo a akúkoľvek krajinu, územie, sektor alebo medzinárodnú organizáciu, v súvislosti s ktorými platí rozhodnutie o primeranosti podľa predpisov Spojeného kráľovstva o primeranosti;
- iii. v prípade Osobných údajov švajčiarskych Zákazníkov akúkoľvek krajinu, územie, sektor alebo medzinárodnú organizáciu, ktorá je uznaná za primeranú podľa právnych predpisov Švajčiarska;
- iv. v prípade akýchkoľvek iných osobných údajov zákazníka prenášaných mimo jurisdikcie, ktorá poskytuje podobnú ochranu ako EÚ, Spojené kráľovstvo alebo Švajčiarsko, akúkoľvek krajinu, územie, sektor alebo medzinárodná organizácia, ktorá je uznaná za primeranú podľa zákonov takejto jurisdikcie.

„**Štandardné zmluvné doložky**“ znamenajú spoločne Štandardné zmluvné doložky EÚ z roku 2021 a Dodatok Spojeného kráľovstva z roku 2022.

„**Osobné údaje Zákazníkov zo Švajčiarska**“ znamená Spracúvanie Osobných údajov Zákazníkov, na ktoré sa pred ich Spracúvaním spoločnosťou Iron Mountain vzťahovali švajčiarske zákony o ochrane údajov.

„**Osobné údaje Zákazníkov zo Spojeného kráľovstva**“ znamená Spracúvanie Osobných údajov Zákazníkov, na ktoré sa pred ich Spracúvaním spoločnosťou Iron Mountain vzťahovali zákony Spojeného kráľovstva o ochrane údajov.

2. INÉ USTANOVENIA

- 2.1 Táto Príloha 3 obsahuje nasledujúce časti: (i) Časť A – Prenosy Osobných údajov Zákazníkov z EÚ; (ii) Časť B – Prenosy Osobných údajov Zákazníkov zo Švajčiarska; (iii) Časť C – Prenos Osobných údajov Zákazníkov zo Spojeného kráľovstva, ktorá sa bude vzťahovať na prenos Osobných údajov Zákazníkov spoločnosťou Iron Mountain v súvislosti s jej Službami.
- 2.2 Štandardné zmluvné doložky sa vzťahujú na spoločnosť Iron Mountain a jej pridružené spoločnosti ako „dovozcov údajov“ a na Zákazníka a jeho pridružené spoločnosti ako „vývozcov údajov“.
- 2.3 Podpis a dátum Zmluvy predstavujú všetky povinné podpisy a dátumy pre Štandardné zmluvné doložky.
- 2.4 V prípade, že zmluvné strany prenesú Osobné údaje Zákazníkov z EÚ, Spojeného kráľovstva alebo Švajčiarska mimo chránenú oblasť a príslušné rozhodnutie Európskej komisie alebo iný platný spôsob primeranosti podľa platných právnych predpisov o ochrane údajov, na ktorý sa spoločnosť Iron Mountain pri prenose údajov spoliehala, sa považuje za neplatný alebo že akýkoľvek dozorný orgán požaduje pozastavenie prenosu osobných údajov vykonaného na základe takéhoto rozhodnutia, zmluvné strany budú spolupracovať a umožnia použitie alternatívneho mechanizmu prenosu. Zmluvné strany sa tiež dohodli, že príslušné záruky používané na uľahčenie medzinárodných prenosov v tejto Prílohe 3 nie sú výhradné a že zmluvné strany môžu využívať ďalšie mechanizmy prenosu, ako je napríklad rámec ochrany osobných údajov medzi EÚ a USA.

ČASŤ A – PRENOSY OSOBNÝCH ÚDAJOV ZÁKAZNÍKOV V EÚ

Ak a v rozsahu, v akom Zákazník alebo jeho Pridružené spoločnosti prenášajú Osobné údaje Zákazníka z EÚ mimo Chránenej oblasti spoločnosti Iron Mountain alebo jej Pridruženým spoločnostiam v súvislosti so Službami

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>

spoločnosti Iron Mountain podľa zmluvy, bude sa uplatňovať táto Časť A Prílohy 3 a Zmluvné strany sa dohodli takto:

- Výber štandardných zmluvných doložiek.** Text z MODULU DVA Štandardných zmluvných doložiek EÚ z roku 2021 sa použije v prípade, že Zákazník alebo ktorákoľvek z jeho Pridružených spoločností je Prevádzkovateľom a spoločnosť Iron Mountain alebo ktorákoľvek z jej Pridružených spoločností je Sprostredkovateľom; text z MODULU TRI Štandardných zmluvných doložiek EÚ z roku 2021 sa použije v prípade, že Zákazník alebo ktorákoľvek z jeho Pridružených spoločností je Sprostredkovateľom a spoločnosť Iron Mountain alebo ktorákoľvek z jej Pridružených spoločností je Ďalším sprostredkovateľom. Príslušné ustanovenia v Štandardných zmluvných doložkách EÚ z roku 2021 sú do tejto DPA začlenené formou odkazu a sú jej neoddeliteľnou súčasťou. Neuplatňujú sa žiadne iné moduly ani doložky označené ako nepovinné v Štandardných zmluvných doložkách EÚ z roku 2021. Informácie požadované na účely Dodatkov k Štandardným zmluvným doložkám EÚ z roku 2021 sú uvedené v Prílohe 1 – Opis spracúvania/prenosu, v Prílohe 2 – Technické a organizačné opatrenia a v článku 6.2 DPA – Zoznam ďalších sprostredkovateľov.
- Použitie ďalších sprostredkovateľov.** Na účely článku 9 Štandardných zmluvných doložiek EÚ z roku 2021 sa použije možnosť 2 (Všeobecné písomné splnomocnenie) na používanie ďalších sprostredkovateľov na poskytovanie Služieb. Zákazník berie na vedomie a súhlasí s tým, že spoločnosť Iron Mountain môže zapojiť nových ďalších sprostredkovateľov prostredníctvom mechanizmu dohodnutého v článku 6 tejto DPA a že lehota na predloženie žiadostí o zmeny ďalších sprostredkovateľov bude pätnásť (15) dní.
- Rozhodné právo a voľba súdu.** Na účely článku 17 Štandardných zmluvných doložiek EÚ z roku 2021 (rozhodné právo) sa použije možnosť 2 rozhodného práva a tieto doložky sa budú riadiť právom členského štátu EÚ, v ktorom má vývozca údajov sídlo, a to v rozsahu umožňujúcom práva oprávnených tretích strán. Na účely článku 18 Štandardných zmluvných doložiek EÚ z roku 2021 (voľba súdu a súdnej právomoci) budú to súdy členského štátu EÚ, v ktorom má vývozca údajov sídlo.
- Potvrdenie o vymazaní.** Na účely článku 8.5 a článku 16 písm. d) Štandardných zmluvných doložiek EÚ z roku 2021 spoločnosť Iron Mountain poskytne Zákazníkovi potvrdenie o vymazaní Osobných údajov iba na základe písomnej žiadosti Zákazníka.
- Porušenia ochrany osobných údajov.** Na účely článku 8.6 písm. c) Štandardných zmluvných doložiek EÚ z roku 2021 sa porušenia ochrany osobných údajov budú riešiť v súlade s postupom dohodnutým v článku 7 DPA.
- Audity.** Na účely článku 8.9 Štandardných zmluvných doložiek EÚ z roku 2021 sa audity týchto doložiek vykonajú v súlade s postupom auditu dohodnutým v Zmluve.
- Sťažnosti.** Na účely článku 11 Štandardných zmluvných doložiek EÚ z roku 2021 bude spoločnosť Iron Mountain informovať Zákazníka, ak v súvislosti s Osobnými údajmi zákazníkov z EÚ dostane sťažnosť od Dotknutej osoby, a túto sťažnosť oznámi Zákazníkovi v súlade s postupom dohodnutým v Zmluve.
- Dozorný orgán.** V prípade Štandardných zmluvných doložiek EÚ z roku 2022 sa príslušný dozorný orgán určí v súlade s článkom 13 Štandardných zmluvných doložiek EÚ.

ČASŤ B – PRENOSY OSOBNÝCH ÚDAJOV ZÁKAZNÍKOV ZO ŠVAJČIARSKA

Ak a v rozsahu, v akom Zákazník alebo jeho pridružené spoločnosti vykonajú prenos Osobných údajov zákazníkov zo Švajčiarska mimo chránenej oblasti spoločnosti Iron Mountain alebo ich pridruženým spoločnostiam v súvislosti so Službami spoločnosti Iron Mountain podľa Zmluvy, bude sa uplatňovať táto Časť B Prílohy 3 a zmluvné strany sa dohodli takto:

- Výber štandardných zmluvných doložiek.** Štandardné zmluvné doložky EÚ z roku 2021 a príslušné ustanovenia v Časti A sa budú uplatňovať, ak je Zákazník alebo akákoľvek z jeho pridružených spoločností Prevádzkovateľom a spoločnosť Iron Mountain alebo akákoľvek z jej pridružených spoločností Sprostredkovateľom a/alebo Zákazník alebo akákoľvek z jeho pridružených spoločností je Sprostredkovateľom a spoločnosť Iron Mountain alebo akákoľvek z jej pridružených spoločností je Ďalším sprostredkovateľom, s výnimkou toho, že:
 - príslušným dozorným orgánom podľa článku 13 Štandardných zmluvných doložiek EÚ z roku 2021 bude Švajčiarska federálna komisia pre ochranu údajov a informácií;
 - rozhodným právom pre zmluvné nároky podľa článku 17 Štandardných zmluvných doložiek EÚ z roku 2021 je švajčiarske právo a miesto súdnej právomoci pre konania medzi stranami podľa článku 18 b) budú švajčiarske súdy.
- Odkazy na nariadenie GDPR EÚ v Štandardných zmluvných doložkách EÚ z roku 2021 sa majú chápať ako odkazy na FADP.

3. Pojem „členský štát“ v Štandardných zmluvných doložkách EÚ z roku 2021 sa nesmie vykladať tak, aby znemožnili Dotknutým osobám vo Švajčiarsku podať žalobu v rámci svojich práv v mieste ich obvyklého pobytu (Švajčiarsko) v súlade s článkom 18 c) Štandardných zmluvných doložiek EÚ z roku 2021.

ČASŤ C – PRENOSY OSOBNÝCH ÚDAJOV ZÁKAZNÍKOV ZO SPOJENÉHO KRÁĽOVSTVA

Ak a v rozsahu, v akom Zákazník alebo jeho pridružené spoločnosti vykonajú prenos Osobných údajov zo Spojeného kráľovstva mimo chránenej oblasti spoločnosti Iron Mountain alebo jej pridruženým spoločnostiam v súvislosti so Službami spoločnosti Iron Mountain podľa Zmluvy, bude sa uplatňovať táto Časť C Prílohy 3 a zmluvné strany sa dohodli takto:

1. **Výber štandardných zmluvných doložiek.** Štandardné zmluvné doložky EÚ z roku 2021, príslušné ustanovenia v Časti A a Dodatok pre Spojené kráľovstvo z roku 2022 sa uplatňujú v prípade, že Zákazník alebo akákoľvek z jeho pridružených spoločností je Prevádzkovateľom a spoločnosť Iron Mountain alebo akákoľvek z jej pridružených spoločností je Sprostredkovateľom a/alebo Zákazník alebo akákoľvek jeho pridružených spoločností je Sprostredkovateľom a spoločnosť Iron Mountain alebo akákoľvek z jej pridružených spoločností je Ďalším sprostredkovateľom.
2. **Časť 1: Tabuľka 1 – 3 Dodatku pre Spojené kráľovstvo z roku 2022:** Informácie o zmluvných stranách – Tabuľka 1; Vybrané SCC, moduly a vybrané doložky a informácie v Dodatku vrátane Prílohy 1A: Zoznam zmluvných strán, Príloha 1B: Opis prenosu a Príloha 1C: Technické a organizačné opatrenia na zaistenie bezpečnosti údajov – Tabuľka 3, sa považujú za vykonané odkazom na túto Prílohu 3 vrátane Časti A, Tabuľky 4 Dodatku pre Spojené kráľovstvo: Zákazník a spoločnosť Iron Mountain berú na vedomie a súhlasia s tým, že Dodatok pre Spojené kráľovstvo môže vypovedať ktorákoľvek zo zmluvných strán.
3. **Časť 2:** Povinné ustanovenia Dodatku pre Spojené kráľovstvo: Zákazník a spoločnosť Iron Mountain berú na vedomie a súhlasia so záväznými ustanoveniami Dodatku pre Spojené kráľovstvo.
4. **Dozorný orgán.** Úrad komisára Spojeného kráľovstva pre informácie bude konať ako príslušný dozorný orgán.

ČASŤ D – PRENOSY OSOBNÝCH ÚDAJOV INÝCH ZÁKAZNÍKOV

Ak a v rozsahu, v akom Zákazník alebo jeho pridružené spoločnosti vykonajú prenos Osobných údajov Zákazníka, pričom sa na spoločnosť Iron Mountain alebo jej pridružené spoločnosti ČASTI A – C v súvislosti so Službami spoločnosti Iron Mountain podľa Zmluvy nevzťahujú, bude sa uplatňovať Časť A Prílohy 3 v rozsahu príslušnom a uplatniteľnom podľa platných právnych predpisov o ochrane údajov. V opačnom prípade, v rozsahu, v akom sa na prenos osobných údajov zákazníka do krajiny, ktorá neposkytuje primeranú úroveň ochrany osobných údajov z pohľadu vývozu údajov, vyžadujú akékoľvek náhradné alebo dodatočné príslušné záruky alebo postupy prenosu podľa právnych predpisov o ochrane údajov, zmluvné strany súhlasia s tými, že ich zavedú čo najskôr a zdokumentujú takéto požiadavky na zavedenie v prílohe k tejto DPA.

PRÍLOHA 4

HIPAA – Zmluva obchodných partnerov (ďalej len „BAA,,)

Táto BAA dopĺňa a mení všetky súčasné alebo budúce Zmluvy uzavreté medzi spoločnosťou Iron Mountain a jej pridruženými spoločnosťami a Zákazníkom a jeho pridruženými spoločnosťami, na základe ktorých spoločnosť Iron Mountain alebo jej pridružené spoločnosti poskytujú Zákazníkovi alebo jeho pridruženým spoločnostiam určité Služby, ktoré vyžadujú zapojenie Obchodného partnera a/alebo zverejnenie PHI v mene Chráneného subjektu. S výnimkou rozsahu upraveného v tejto BAA zostávajú všetky zmluvné podmienky uvedené v Zmluve v plnej platnosti a účinnosti a riadia sa nimi Služby poskytované Zákazníkovi spoločnosťou Iron Mountain.

Spoločnosť Iron Mountain a Zákazník uzatvárajú túto BAA, aby si obe zmluvné strany splnili svoje príslušné povinnosti, ktoré nadobudnú účinnosť a budú pre strany záväzné podľa pravidiel ochrany súkromia, bezpečnosti a oznamovania porušenia zákona HIPAA spolu s akýmikoľvek vykonávacími predpismi vrátane tých, ktoré boli zavedené ako súčasť súhrnného nariadenia (spoločne označované ako „Pravidlá HIPAA“), podľa ktorého sú Zákazník a jeho pridružené spoločnosti „Chráneným subjektom“ alebo „Obchodným partnerom“ a spoločnosť Iron Mountain a jej pridružené spoločnosti sú „Obchodným partnerom“ Zákazníka. Na účely tejto Zmluvy sa všetky odkazy na Obchodného partnera nižšie považujú za odkazy na spoločnosť Iron Mountain alebo jej príslušnú pridruženú spoločnosť.

1. VYMEDZENIE POJMOV

Pojmy s veľkým začiatočným písmenom používané, ale inak neurčené v tejto BAA, majú rovnaký význam, aký je týmto pojmom priradený v pravidlách HIPAA alebo v Zmluve, podľa toho, čo je relevantné.

„**Pravidlo oznamovania porušenia**“ znamená pravidlo pre oznamovanie porušenia nezabezpečených chránených zdravotných údajov v 45 CFR § 164, podčasti D.

„**Obchodný partner**“ znamená vyššie uvedený subjekt obchodného partnera v rozsahu, v akom prijíma, uchováva alebo prenáša chránené zdravotné údaje pri poskytovaní Služieb Zákazníkom.

„**HIPAA**“ znamená zákon o prenosnosti a zúčtovateľnosti zdravotného poistenia z roku 1996.

„**HITECH Act**“ znamená platné ustanovenia zákona o zdravotníckych informačných technológiách pre ekonomické a klinické zdravotníctvo, ktoré sú začlenené do amerického zákona o obnove a opätovnom investovaní z roku 2009, vrátane všetkých vykonávacích predpisov.

„**Pravidlo ochrany osobných údajov**“ znamená normy ochrany osobných údajov individuálne identifikovateľných zdravotných údajov v 45 CFR § 160 a § 164, podčastiach A a E.

„**Chránené zdravotné údaje**“ alebo „**PHI**“ budú mať rovnaký význam ako výraz „chránené zdravotné údaje“ v 45 CFR § 160.103 a budú obmedzené na PHI vytvorené Obchodným partnerom v mene Zákazníka alebo prijaté od Zákazníka alebo v jeho mene v súlade so Zmluvou.

„**Bezpečnostné pravidlo**“ znamená Bezpečnostné normy na ochranu elektronických chránených zdravotných údajov v 45 CFR §160 a §164, podčasti A a C.

2. POVINNOSTI A AKTIVITY OBCHODNÉHO PARTNERA

- 2.1. Obchodný partner súhlasí s tým, že nebude používať ani ďalej zverejňovať PHI inak, než to povoľuje alebo vyžaduje táto BAA alebo ako to vyžaduje zákon.
- 2.2. Obchodný partner súhlasí s tým, že bude používať primerané záruky a podľa potreby dodržiavať podčasť C 45 CFR § 164, pokiaľ ide o elektronické PHI, aby zabránil použitiu alebo zverejneniu PHI iným spôsobom, ako je stanovené v tejto BAA alebo Zmluve. Zmluvné strany však berú na vedomie a súhlasia s tým, že za dodržiavanie požiadaviek podľa 45 CFR § 164.312 na zavedenie šifrovacích alebo dešifrovacích mechanizmov pre elektronické PHI uchovávané na fyzických médiách (napr. páskach), ktoré Zákazník uchováva u Obchodného partnera je zodpovedný Zákazník, a nie Obchodný partner.
- 2.3. Obchodný partner súhlasí s tým, že bezodkladne oznámi Zákazníkovi akýkoľvek bezpečnostný incident, porušenie alebo iné použitie alebo zverejnenie PHI, o ktorom sa dozvie a ktoré nie je povolené ani požadované podľa tejto BAA alebo Zmluvy. V prípade porušenia sa takéto oznámenie vykoná v súlade s pravidlami HIPAA a tak, ako sa to od Obchodného partnera vyžaduje, okrem iného aj podľa 45 CFR 164.410, v žiadnom prípade však nie viac ako tri (3) pracovné dni potom, ako Obchodný partner ukončil svoje interné vyšetrovanie a potvrdil, že došlo k porušeniu. Obchodný partner poskytne primeranú pomoc a súčinnosť pri vyšetrovaní každého takéhoto Porušenia a zdokumentuje konkrétne Úložiská, ktoré boli ohrozené, totožnosť každej neoprávnenej tretej strany, ktorá mohla získať prístup k PHI alebo získať PHI, ak je známa, a akékoľvek kroky, ktoré Obchodný partner prijal na zmiernenie účinkov takéhoto Porušenia.
- 2.4. Obchodný partner v súlade s 45 CFR 164.502 písm. e) bod 1 ii) a 164.308 písm. b) bod 2 podľa potreby zabezpečí, aby Obchodný partner, ktorý je subdodávateľom, ktorý vytvára, prijíma, udržiava alebo

prenáša PHI v mene Obchodného partnera na účely pomoci pri poskytovaní Služieb v súlade so Zmluvou, súhlasí s rovnakými obmedzeniami, podmienkami a požiadavkami, ktoré sa vzťahujú na Obchodného partnera v súvislosti s takýmito PHI prostredníctvom tejto BAA.

- 2.5. Ak má Obchodný partner v úschove PHI v určenom súbore záznamov týkajúcich sa jednotlivcov a ak o to Zákazník požiada, Obchodný partner súhlasí s tým, že Zákazníkovi poskytne prístup k takýmto PHI vyhľadanim a poskytnutím takýchto PHI v súlade s podmienkami Zmluvy, aby Zákazník mohol jednotlivcovi odpovedať s cieľom splniť požiadavky 45 CFR § 164.524.
- 2.6. Obchodný partner súhlasí s tým, že ak sú potrebné zmeny a doplnenia PHI v určenom súbore záznamov v úschove Obchodného partnera a ak Zákazník dá Obchodnému partnerovi pokyn na vyhľadanie takýchto PHI v súlade so Zmluvou, Obchodný partner takúto službu vykoná, aby Zákazník mohol vykonať akékoľvek zmeny a doplnenia týchto PHI, o ktoré môže žiadať Zákazník alebo jednotlivec podľa 45 CFR §164.526.
- 2.7. Obchodný partner súhlasí s tým, že zdokumentuje a sprístupní Zákazníkovi informácie potrebné na evidenciu zverejnených PHI za predpokladu, že Zákazník poskytol Obchodnému partnerovi informácie dostatočné na to, aby Obchodný partner mohol určiť, ktoré záznamy alebo údaje prijaté od Zákazníka alebo v jeho mene prostredníctvom Obchodného partnera obsahujú PHI. Dokumentácia zverejnených informácií bude obsahovať také informácie, ktoré sú potrebné na to, aby Zákazník mohol odpovedať na žiadosť jednotlivca o evidenciu zverejňovania PHI v súlade s 45 CFR §164.528 alebo inými ustanoveniami pravidiel HIPAA.
- 2.8. Ak nie je v Zmluve výslovne dohodnuté inak, Obchodný partner bude bezodkladne informovať Zákazníka o všetkých žiadostiach jednotlivcov o prístup k PHI alebo o ich oboznámenie sa s nimi alebo o ich opravu bez toho, aby na takéto žiadosti odpovedal, pričom Zákazník bude zodpovedný za prijatie a odpoveď na všetky takéto žiadosti jednotlivcov.
- 2.9. V rozsahu, v akom Obchodný partner musí plniť jednu alebo viaceré povinnosti Zákazníka podľa podčasti E článku 45 CFR § 164, musí Obchodný partner pri plnení týchto povinností dodržiavať požiadavky podčasti E, ktoré sa vzťahujú na Zákazníka.
- 2.10. Obchodný partner súhlasí s tým, že svoje interné postupy, účtovné knihy a záznamy sprístupní Tajomníkovi na účely stanovenia súladu s pravidlami HIPAA.

3. POVOLENÉ POUŽITIE A ZVEREJNENIE ZO STRANY OBCHODNÉHO PARTNERA

- 3.1. Obchodný partner môže podľa potreby používať alebo zverejniť PHI na poskytovanie Služieb uvedených v tejto Zmluve.
- 3.2. Obchodný partner môže používať alebo zverejňovať PHI tak, ako to vyžaduje zákon.
- 3.3. Obchodný partner súhlasí s tým, že vynaloží primerané úsilie na obmedzenie PHI na minimum potrebné na dosiahnutie zamýšľaného účelu použitia, zverejnenia alebo žiadosti.
- 3.4. Obchodný partner nesmie používať ani zverejňovať PHI spôsobom, ktorý by porušoval podčasť E 45 CFR § 164, ak to urobí Zákazník.
- 3.5. Obchodný partner môže zverejniť PHI na účely riadneho riadenia a správy Obchodného partnera alebo na plnenie zákonných povinností Obchodného partnera za predpokladu, že zverejnené informácie vyžaduje zákon alebo že Obchodný partner získa primerané záruky od osoby, ktorej sa informácie poskytujú, že informácie zostanú dôverné a použijú sa alebo ďalej zverejnia len v súlade so zákonom alebo na účely, na ktoré boli danej osobe poskytnuté, a osoba bude Obchodného partnera informovať o všetkých prípadoch, v prípade ktorých vie, že došlo k porušeniu dôvernosti informácií.

4. POVINNOSTI ZÁKAZNÍKA

- 4.1. Zákazník nesmie nariadiť Obchodnému partnerovi, aby konal spôsobom, ktorý by nebol v súlade s pravidlami HIPAA.
- 4.2. Zákazník oznámi obchodnému partnerovi akékoľvek obmedzenie (obmedzenia) v jeho oznámení o postupoch ochrany osobných údajov Zákazníka v súlade s 45 CFR § 164.520 v rozsahu, v akom takéto obmedzenie môže ovplyvniť používanie alebo zverejňovanie PHI Obchodným partnerom.
- 4.3. Zákazník je povinný informovať Obchodného partnera o všetkých zmenách alebo zrušení povolenia jednotlivca na používanie alebo zverejňovanie PHI v rozsahu, v akom môžu tieto zmeny ovplyvniť používanie alebo zverejňovanie PHI Obchodným partnerom.
- 4.4. Zákazník písomne oznámi Obchodnému partnerovi akékoľvek obmedzenie používania alebo zverejňovania PHI, s ktorým Zákazník súhlasil v súlade s 45 CFR § 164.522 v rozsahu, v akom takéto obmedzenie môže ovplyvniť používanie alebo zverejňovanie PHI Obchodným partnerom.

5. OBDOBIE PLATNOSTI A UKONČENIE ZMLUVY

- 5.1. Obdobie platnosti tejto BAA sa začína dátumom nadobudnutia účinnosti a automaticky sa skončí po tom, čo nastane neskoršia z týchto udalostí: (i) uplynutie platnosti Zmluvy alebo (ii) keď sa všetky PHI poskytnuté Zákazníkom Obchodnému partnerovi zničia alebo vráti Zákazníkovi.
- 5.2. Keď sa zmluvná strana dozvie o podstatnom porušení BAA druhou zmluvnou stranou, zmluvná strana, ktorá neporušila Zmluvu, poskytne zmluvnej strane, ktorá porušila Zmluvu, príležitosť na nápravu porušenia. Ak zmluvná strana, ktorá porušila Zmluvu, neodstráni porušenie do tridsiatich (30) dní po tom, čo zmluvná strana, ktorá porušila Zmluvu, dostala písomné oznámenie od zmluvnej strany, ktorá neporušila Zmluvu, s podrobnosťami o takomto závažnom porušení, má zmluvná strana, ktorá

neporušila Zmluvu, právo ukončiť túto BAA a Zmluvu v súlade s jej podmienkami, alebo ak ukončenie nie je možné, nahlásiť problém Tajomníkovi alebo akémukoľvek inému príslušnému orgánu.

5.3. Účinek ukončenia zmluvy:

5.3.1.1. Okrem prípadov uvedených v bode 5.3.2 nižšie, po ukončení tejto BAA z akéhokoľvek dôvodu Obchodný partner vráti alebo zničí všetky PHI prijaté od Zákazníka v súlade so Zmluvou. Toto ustanovenie sa vzťahuje na PHI, ktoré sú v držbe subdodávateľov alebo zástupcov Obchodného partnera. Obchodný partner si neoponcháva žiadne kópie PHI.

5.3.1.2. V prípade, že Obchodný partner rozhodne, že vrátenie alebo zničenie PHI je neuskutočniteľné, Obchodný partner pošle Zákazníkovi oznámenie o podmienkach, ktoré znemožňujú ich vrátenie alebo zničenie. Na základe oznámenia Zákazníkovi Obchodný partner rozšíri ochranu tejto BAA na takéto PHI a obmedzí ďalšie použitie a zverejnenie takýchto PHI na tie účely, ktoré znemožňujú ich vrátenie alebo zničenie, pokiaľ bude Obchodný partner takéto PHI uchovávať v súlade s podmienkami Zmluvy.

6. RÔZNE

6.1. Odškodnenie. Obchodný partner sa zaväzuje odškodniť zákazníka v prípade akýchkoľvek pokút alebo sankcií uložených Zákazníkovi v dôsledku akéhokoľvek exekučného konania začatého Tajomníkom alebo akejkolvek občianskoprávnej žaloby podanej Generálnym prokurátorom štátu Zákazníkom, pričom takéto konanie alebo žaloba vyplýva priamo a výlučne z akéhokoľvek konania alebo opomenutia zo strany Obchodného partnera, ktoré je buď porušením Pravidiel HIPAA, alebo podstatným porušením tejto BAA (ďalej len „nárok“). Obchodný partner nie je povinný odškodniť Zákazníka za akúkoľvek časť takýchto pokút alebo sankcií vyplývajúcich z (i) porušenia pravidiel HIPAA alebo tejto BAA Zákazníkom alebo (ii) z jeho nedbanlivosti alebo úmyselného konania alebo opomenutia. Vyššie uvedený záväzok odškodnenia je výslovne podmienený tým, že zákazník udelí Obchodnému partnerovi právo podľa voľby a na náklady Obchodného partnera a s právnym zástupcom podľa vlastného výberu riadiť obhajobu akéhokoľvek takéhoto nároku alebo sa na nej zúčastniť, to však za predpokladu, že pokiaľ je akýkoľvek takýto nárok súčasťou väčšieho konania alebo žaloby, právo Obchodného partnera riadiť obhajobu alebo sa na nej zúčastniť je obmedzené na tento nárok, a nie na rozsiahlejšie konanie alebo žalobu. V prípade, že Obchodný partner využije svoju možnosť kontroly obhajoby, potom (i) Obchodný partner bez predchádzajúceho písomného súhlasu Zákazníka neurovná žiaden nárok, ktorý si vyžaduje akékoľvek priznanie zavinenia zo strany Zákazníka, (ii) Zákazník má právo zúčastniť sa na vlastné náklady na nároku alebo žalobe a (iii) Zákazník je povinný spolupracovať s Obchodným partnerom, ak sa to od neho bude odôvodnene požadovať. Vyššie uvedené je jediným a výhradným opravným prostriedkom Zákazníka a výhradnou zodpovednosťou Obchodného partnera za akúkoľvek stratu, poškodenie, výdavky alebo zodpovednosť Zákazníka za akékoľvek nároky v súvislosti s touto BAA.

6.2. Súdny príkaz na nápravu. Obchodný partner berie na vedomie, že akékoľvek neoprávnené použitie alebo zverejnenie PHI z jeho strany môže spôsobiť Zákazníkovi nenapraviteľnú ujmu, za ktorú bude Zákazník oprávnený, ak sa tak rozhodne, požiadať o súdny príkaz na nápravu alebo iné spravodlivé odškodnenie.

6.3. Regulačné odkazy. Odkaz v tejto BAA na časť pravidiel HIPAA znamená tú časť zákona HIPAA, pravidlo ochrany osobných údajov, bezpečnostné pravidlo, zákon HITECH ACT alebo konečné súhrnné pravidlá v znení neskorších predpisov a účinnosti, ktoré je potrebné dodržiavať.

6.4. Dodatok. Zmluvné strany sa dohodli, že v dobrej viere budú rokovať o akýchkoľvek zmenách a doplneniach tejto BAA, ktoré môžu byť priebežne potrebné na to, aby Zákazník alebo Obchodný partner spĺňali požiadavky pravidiel HIPAA. Ak zmluvné strany nedokážu dosiahnuť vzájomnú dohodu o podmienkach akejkoľvek takejto zmeny a doplnenia do šesťdesiatich (60) dní od dátumu prijatia takejto písomnej žiadosti predloženej Zákazníkom Obchodnému partnerovi, potom má ktorákoľvek zo zmluvných strán právo ukončiť túto BAA a Zmluvu na základe písomného oznámenia druhej zmluvnej strane, ktoré nesmie byť predložené neskôr ako tridsať (30) dní vopred.

6.5. Žiadni príjemcovia tretích strán. Žiadne ustanovenie vyjadrené alebo zahrnuté v tejto BAA nemá za cieľ udeľovať, a ani žiadne ustanovenie v tejto Zmluve neudeľuje žiadnej inej osobe ako Zákazníkovi, Obchodnému partnerovi a ich príslušným nástupcom alebo postupníkom žiadne práva, opravné prostriedky, povinnosti alebo záväzky.

6.6. Nezávislý dodávateľ. Obchodný partner vrátane jeho riaditeľov, vedúcich pracovníkov, zamestnancov a zástupcov je nezávislým dodávateľom, ale nie zástupcom (ako je uvedené vo federálnom zákone o zastúpení) Zákazníka alebo jeho zamestnanca. Bez toho, aby sa obmedzil všeobecný charakter vyššie uvedeného, Zákazník nebude mať žiadne právo kontrolovať, riadiť ani inak ovplyvňovať konanie Obchodného partnera v priebehu poskytovania Služieb, inak ako prostredníctvom presadzovania tejto BAA alebo Zmluvy, alebo ich vzájomných zmien a doplnení.

6.7. Prednosť: celistvosť Zmluvy. Akákoľvek nejasnosť v tejto BAA bude vyriešená tak, aby strany mohli dodržiavať pravidlá HIPAA. Táto BAA predstavuje úplnú dohodu medzi zmluvnými stranami s ohľadom na predmet tejto zmluvy a nahrádza všetky predchádzajúce oznámenia, vyhlásenia, zmluvy a dohody týkajúce sa pravidiel HIPAA vrátane všetkých predchádzajúcich zmlúv o obchodnom partnerstve medzi zmluvnými stranami.