Smlouva o zpracování Údajů

ÚČEL A POŘADÍ PRIORIT

Tato Smlouva o Zpracování Údajů, spolu s přílohami a všemi dokumenty, na které je výslovně odkazováno (dále jen „**DPA**“), je považována za součást smlouvy o poskytování služeb mezi společností Iron Mountain a Zákazníkem (dále jen „**Smlouva**“). Podmínky Smlouvy se vztahují na práva a povinnosti smluvních stran podle této DPA a řídí se jimi.

Pokud jsou některé podmínky obsažené v této DPA v rozporu s podmínkami ve Smlouvě, jsou rozhodujícími podmínkami ve vztahu k předmětu této DPA podmínky uvedené v této DPA. Touto DPA se ruší a nahrazují veškeré předchozí smlouvy o zpracování údajů nebo doložky o ochraně osobních údajů či soukromí mezi stranami v souvislosti se Službami poskytovaným podle Smlouvy.

OBECNÉ PODMÍNKY

1. DEFINICE

Není-li v tomto dokumentu výslovně uvedeno jinak, mají všechny pojmy psané velkými písmeny stejný význam, jaký jim byl dán ve Smlouvě.

„**Správce**“ znamená fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný Subjekt, který sám nebo společně s jinými Subjekty určuje účely a prostředky Zpracování Osobních Údajů;

„**Osobními Údaji Zákazníka**“ se rozumí Osobní Údaje, které patří Zákazníkovi či jeho přidruženým společnostem nebo jsou jimi shromažďovány a zpracovávány v rámci Služeb;

„**Subjekt Údajů**“ znamená identifikovanou nebo identifikovatelnou fyzickou osobu;

„**Právními Předpisy o Ochraně Údajů**“ se rozumí všechny platné zákony a předpisy týkající se Zpracování Osobních Údajů, které mohou existovat v příslušných jurisdikcích, mimo jiné včetně EU GDPR (nařízení (EU) 2016/679), GDPR Spojeného království (GDPR ve znění platném jako součást britského vnitrostátního práva na základě oddílu 3 zákona o Evropské unii (o vystoupení) z roku 2018 a ve znění Zákona o Ochraně Údajů, Soukromí a Elektronických Komunikacích (Dodatky atd.) nařízení z roku 2019 (Odchod z EU) (v platném znění)), Zákona o ochraně Údajů z roku 2018, FADP (švýcarský federální Zákon o Ochraně Osobních Údajů), amerických státních Zákonů o Ochraně Osobních Údajů, LGPD (brazilský obecný Zákon o Ochraně Údajů), PIPL (Zákon Čínské lidové republiky o Ochraně Osobních Údajů) a veškerých právních předpisů a/nebo nařízení, které je zavádějí či jsou vydány na jejich základě, nebo které je mění, nahrazují, nově schvalují či sdružují některé z nich, včetně případných pokynů a kodexů postupů vydaných dozorovými úřady;

„**Osobními Údaji**“ se rozumí informace týkající se Subjektu Údajů;

„**Zpracovatelem**“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný Subjekt, který Zpracovává Osobní Údaje jménem Správce;

„**Zpracováním**“ se rozumí operace nebo soubor operací prováděných s Osobními Údaji nebo jejich soubory, ať již automatizovanými prostředky či nikoli, jako je shromažďování, zaznamenávání, uspořádání, strukturování, ukládání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, zveřejňování přenosem, šíření nebo jiné zpřístupnění, řazení nebo kombinace, omezování, výmaz nebo likvidace;

„**Porušením Zabezpečení**“ se rozumí náhodné nebo nezákonné poškození, zničení, ztráta, změna nebo neoprávněné zpřístupnění Osobních Údajů Zákazníka, které společnost Iron Mountain, její zaměstnanci nebo subdodavatelé Zpracovávají v průběhu poskytování Služeb;

„**Služby**“ znamenají služby poskytované společností Iron Mountain nebo jejími přidruženými společnostmi Zákazníkovi či jeho přidruženým společnostem podle Smlouvy;

„**Státní zákony USA o Ochraně Soukromí**“ znamenají všechny zákony států USA o ochraně soukromí a ochraně Údajů, které se vztahují na Zpracování Osobních Údajů podle Smlouvy, mimo jiné včetně jejich občasných změn, doplňků nebo nahrazení: (1) kalifornský zákon o ochraně Osobních Údajů spotřebitelů, ve

znění kalifornského Zákona o Právech na Ochranu Osobních Údajů a veškerých prováděcích předpisů týkajících se tohoto zákona (společně dále jen jako „**CCPA**“); (2) Zákon státu Colorado o Ochraně Osobních Údajů (dále jen jako „**CPA**“), (3) Zákon státu Virginie o Ochraně Údajů Spotřebitelů (dále jen jako „**CDPA**“); (4) Zákon státu Utah o Ochraně Osobních Údajů spotřebitelů (dále jen jako „**UCPA**“); a (5) Zákon státu Connecticut o Ochraně Osobních Údajů („**CTDPA**“).

2. ROZSAH A PODROBNOSTI ZPRACOVÁNÍ ÚDAJŮ

2.1 Tato DPA se vztahuje na Osobní Údaje Zákazníka zpracovávané společností Iron Mountain jako Zpracovatelem při poskytování Služeb podle Smlouvy jménem Zákazníka.

2.2 Společnost Iron Mountain může shromažďovat a Zpracovávat Osobní Údaje zaměstnanců Zákazníka a jeho přidružených společností jako Správce Údajů pro legitimní obchodní účely, jako je řízení smluv a vztahů se zákazníky a v souladu s Právními Předpisy o Ochraně Osobních Údajů a oznámením o ochraně osobních údajů společnosti Iron Mountain, které jsou k dispozici na jejich webových stránkách a dalšími platnými zásadami ochrany osobních údajů. Povinnosti společnosti Iron Mountain stanovené touto DPA se nevztahují na Zpracování těchto Osobních Údajů.

2.3 Předmětem Zpracování Osobních Údajů je poskytování Služeb. Práva a povinnosti Zákazníka a společnosti Iron Mountain jsou stanoveny v této DPA. V příloze 1 této DPA je uvedena povaha, doba trvání a účel Zpracování, typy Osobních Údajů Zákazníků, které společnost Iron Mountain Zpracovává a kategorie Subjektů Údajů, jejichž Osobní Údaje jsou Zpracovávány.

2.4 Pokud společnost Iron Mountain v průběhu poskytování služeb Zpracovává Osobní Údaje Zákazníků:

2.4.1 bude je Zpracovávat pouze v souladu se zdokumentovanými pokyny Zákazníka. Vyžadují-li právní předpisy, které společnost Iron Mountain musí dodržovat, Zpracování Osobních Údajů Zákazníka pro jiné účely, bude o tomto požadavku Zákazníka informovat předem, pokud to tyto právní předpisy z důležitých důvodů v rámci veřejného zájmu nezakazují; a

2.4.2 vždy bude dodržovat platné Právní Předpisy o Ochraně Osobních Údajů a neprodleně informuje Zákazníka, pokud podle jejího názoru pokyn ke Zpracování Osobních Údajů Zákazníka porušuje platné Právní Předpisy o Ochraně Osobních Údajů.

2.5 Pokyny Zákazníka jsou pro společnost Iron Mountain závazné, pokud splnění pokynů nevyžaduje poskytnutí nějaké služby podle Smlouvy a Zákazník nesouhlasí s úhradou poplatků za takovou službu.

2.6 Společnost Iron Mountain zajistí, aby pracovníci, kteří mají přístup k Osobním Údajům Zákazníka podléhali závazné povinnosti mlčenlivosti o nich, a přijme veškerá přiměřená opatření k zajištění důvěryhodnosti a způsobilosti všech svých zaměstnanců s přístupem k Osobním Údajů Zákazníků.

3. POSKYTOVÁNÍ POMOCI ZÁKAZNÍKŮM

3.1 Společnost Iron Mountain poskytne Zákazníkovi pomoc, vždy s ohledem k povaze Zpracování:

3.1.1 prostřednictvím technických a organizačních opatření, a v rámci možností při plnění povinností Zákazníka reagovat na žádosti Subjektů Údajů uplatňujících svá práva;

3.1.2 při zajišťování souladu s povinnostmi Zákazníka (jako je zabezpečení Zpracování, ohlášení porušení zabezpečení Osobních Údajů dozorovému úřadu, sdělení porušení zabezpečení Osobních Údajů Subjektu Údajů, posouzení vlivu na ochranu údajů a předchozí konzultace s dozorovými úřady, pokud by Zpracování vedlo k vysokému riziku v případě, že Správce nepřijme opatření ke zmírnění rizika), s přihlédnutím k informacím, které má společnost Iron Mountain k dispozici; a

3.1.3 zpřístupněním Zákazníkovi veškerých informací, které si přiměřeně vyžádá, aby mohl prokázat, že povinnosti při výběru a jmenování společnosti Iron Mountain byly splněny.

4. BEZPEČNOSTNÍ OPATŘENÍ

4.1 S ohledem na běžné provozní postupy, náklady na provedení a povahu, rozsah, kontext i účely Zpracování, zavede společnost Iron Mountain vhodná a přiměřená technická i organizační opatření určená k ochraně důvěrnosti, integrity a dostupnosti Osobních Údajů Zákazníků jejich ochraně před neoprávněným nebo nezákonným Zpracováním a náhodnou ztrátou, zničením, poškozením, změnou či zveřejněním. Bezpečnostní standardy společnosti Iron Mountain jsou stanoveny v Příloze 2 této DPA.

4.2 Je výhradní odpovědností Zákazníka posoudit, zda tato technická a organizační opatření splňují jeho požadavky.

5. DODRŽOVÁNÍ ZÁKONŮ

Zákazník a jeho přidružené společnosti jsou: (i) povinni Zpracovávat své Osobní Údaje v souladu s Právními Předpisy o Ochraně Údajů; (ii) oprávněni dávat společnosti Iron Mountain písemné pokyny ohledně Zpracování svých Osobních Údajů v souvislosti se Službami (a to i jménem Subjektu třetí

strany, která je Správcem Osobních Údajů Zákazníka); a (iii) povinni mít vždy kontrolu nad svými Osobními Údaji v souvislosti se Zpracováním.

6. DÍLČÍ ZPRACOVÁNÍ

6.1 Zákazník bere na vědomí a souhlasí s tím, že společnost Iron Mountain může pro účely Zpracování jeho Osobních Údajů podle této DPA s výhradou ustanovení 6.2 níže zapojit svou mateřskou společnost, své přidružené společnosti a další dílčí Zpracovatele třetích stran (včetně dílčích Zpracovatelů třetích stran zapojených přidruženými společnostmi nebo mateřskou společností Iron Mountain).

6.2 Seznam dílčích Zpracovatelů schválených Zákazníkem ke dni účinnosti této DPA je k dispozici zde[1]. Společnost Iron Mountain může kdykoli nahradit nebo jmenovat nového dílčího Zpracovatele za předpokladu, že Zákazník obdrží patnáct (15) dní předem písemné oznámení, a že v této lhůtě nevznese proti takovým změnám námitky z prokazatelných důvodů souvisejících s ochranou údajů. K tomu, aby Zákazník dostával tato e-mailová oznámení, musí se prostřednictvím této webové stránky[2]přihlásit k odběru služby e-mailových oznámení společnosti Iron Mountain a spravovat veškeré stávající předplatné.

6.3 Pokud se Zákazník k odběru této oznamovací služby nepřihlásí, společnost Iron Mountain nenese odpovědnost za chybějící oznámení dílčího Zpracovatele a všechna taková jmenování budou považována za Zákazníkem schválená**.** Pokud Zákazník z prokazatelných důvodů souvisejících s ochranou údajů písemně vznese námitku proti jmenování náhradního nebo nového dílčího Zpracovatele do patnácti (15) dnů po předchozím písemném oznámení, společnost Iron Mountain vynaloží přiměřené úsilí, aby Zákazníkovi poskytla změnu Služeb nebo doporučila změnu konfigurace či používání Služeb, v každém případě, aby zabránila Zpracování Osobních Údajů Zákazníka dílčím Zpracovatelem, proti kterému byla námitka vznesena. Pokud Zákazník neschválí žádnou z navrhovaných změn společností Iron Mountain do patnácti (15) dnů a vznese námitky proti dílčímu Zpracovateli, může společnost Iron Mountain Zákazníkovi na základě písemného oznámení okamžitě ukončit poskytování Služby nebo její části, kterou nemůže poskytovat bez účasti tohoto dílčího Zpracovatele. Takovým ukončením nejsou dotčena nabytá práva ani závazky stran za předpokladu, že společnosti Iron Mountain ani její přidružené společnosti nebudou v souvislosti s takovým ukončením platit poplatky, výdaje ani jiné kompenzace za ukončení, a že Zákazník neprodleně převezme aktiva, která společnosti Iron Mountain poskytl v rámci těchto ukončených služeb, v souladu s podmínkami Smlouvy a na vlastní náklady.

6.4 Společnost Iron Mountain zajistí, aby smlouva s dílčími Zpracovateli podle této DPA obsahovala ustanovení, která jsou ve všech podstatných ohledech stejná jako ustanovení této DPA, a aby byla v souladu platnými Právními Předpisy o Ochraně Údajů. Pokud dílčí Zpracovatel zapříčiní porušení povinností ze strany společnosti Iron Mountain podle této DPA nebo Právních Předpisů o Ochraně Údajů, zůstává společnost Iron Mountain vůči Zákazníkovi plně odpovědná za plnění svých povinností podle těchto podmínek.

7. PORUŠENÍ ZABEZPEČENÍ

7.1 V případě podezření na Porušení Zabezpečení, společnost Iron Mountain:

7.1.1 neprodleně přijme opatření k prošetření podezření na Porušení Zabezpečení, k jeho identifikaci, prevenci a zmírnění účinků a k nápravě;

7.1.2 informuje Zákazníka bez zbytečného odkladu, jakmile získá přiměřenou míru jistoty, že došlo k Porušení Zabezpečení, a poskytne mu jeho podrobný popis, včetně informací přiměřeně nezbytných k tomu, aby Zákazník splnil ohlašovací povinnosti podle Právních Předpisů o Ochraně Údajů.

7.2 Zákazník souhlasí s tím, že společnost Iron Mountain může informace podle bodu 7.1.2 poskytovat postupně. V případech, kdy společnost Iron Mountain nemá přístup k určitým informacím uvedeným v bodě 7.1.2 nebo je nemůže Zákazníkovi poskytnout, bude o tom Zákazníka informovat a neponese odpovědnost za jejich neposkytnutí.

8. AUDITY

Společnost Iron Mountain umožní Zákazníkovi a jeho příslušným auditorům nebo oprávněným zástupcům po předchozím upozornění nejméně deset (10) pracovních dnů předem provádět audity nebo inspekce po dobu platnosti Smlouvy, přičemž není povinna poskytnout ani umožnit přístup k informacím týkajících se: i) jiných Zákazníků společnosti Iron Mountain; ii) neveřejných externích zpráv společnosti Iron Mountain; a iii) interních zpráv vypracovaných při interních auditech nebo oddělením pro dodržování předpisů společnosti Iron Mountain. Účely auditu nebo inspekce podle tohoto bodu jsou

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

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

omezeny na ověření toho, zda společnost Iron Mountain zpracovává Osobní Údaje Zákazníků v souladu se svými povinnostmi podle této DPA. S výjimkou případů, kdy dojde k Porušení Zabezpečení, nebude proveden více než jeden takový audit za dvanáct (12) měsíců.

9. MEZINÁRODNÍ PŘEDÁVÁNÍ ÚDAJŮ (OMEZENÁ PŘEDÁVÁNÍ)

9.1 Zákazník tímto v příslušném rozsahu povoluje a souhlasí s mezinárodním předáváním svých Osobních Údajů za účelem poskytování Služeb subjektům uvedeným v bodě 6.2 a v souladu s Přílohou 3 a Zákazník i společnost Iron Mountain souhlasí s následujícím:

9.1.1 budou dodržovat v souvislosti s tímto předáváním platné Právní Předpisy o Ochraně Údajů;

9.1.2 přičemž mimo jiné berou v úvahu i) kategorie Osobních Údajů Zákazníka, ii) země, jejichž vnitrostátní právní předpisy, pokud jde o rozsah, nemusí poskytovat srovnatelnou úroveň ochrany Osobních Údajů s právními předpisy EU/UK (dále jen „**Třetí Země**“), iii) příslušná technická a organizační opatření uvedená v oddíle 7 a iv) příslušné strany podílející se na Zpracování těchto Osobních Údajů Zákazníka provedou posouzení vhodnosti příslušného mechanismu předávání přijatého podle tohoto dokumentu, pokud to vyžaduje zákon a rozhodnou, že tento mechanismus je vhodně navržen tak, aby zajistil Osobním Údajům předávaným v souladu s touto DPA v cílové zemi v podstatě rovnocennou úroveň ochrany, jaká je zaručena Právními Předpisy o Ochraně Údajů.

10. ODPOVĚDNOST A ODŠKODNĚNÍ

10.1 Bez ohledu na cokoli, co je v rozporu se Smlouvou, v případě Porušení Zabezpečení způsobeného přímo porušením povinností společnosti Iron Mountain podle této DPA, společnost Iron Mountain uhradí Zákazníkovi v rozsahu povoleném příslušnými právními předpisy přímé, prokazatelné, nezbytné a přiměřeně vynaložené náklady třetí strany (a) na vyšetřování takového Porušení Zabezpečení, (b) přípravu a rozesílání oznámení těm Subjektům Údajů a regulačním orgánům, u kterých to vyžadují Právní Předpisy o Ochraně Údajů, (c) po dobu nepřesahující dvanáct (12) měsíců poskytování služeb monitorování úvěruschopnosti těm osobám, u kterých to vyžadují právní předpisy a (d) na úhradu části regulačních pokut, penále, nebo sankcí uložených dozorovým úřadem, za které je podle dozorového úřadu odpovědná přímo společnost Iron Mountain.

10.2 V případě, že Subjekt Údajů vznese vůči jedné nebo oběma stranám nárok z důvodu údajného porušení Právních Předpisů o Ochraně Údajů (dále jen „**Nároky Subjektu Údajů**“), pokud je to přípustné, každá strana bude řídit svou vlastní obhajobu proti takovému nároku (nebo svou část obhajoby) a zůstává odpovědná výhradně za své vlastní náklady, výdaje a závazky s tím spojené, včetně právních poplatků nebo jiných částek, které jí byly soudně přiznány nebo vyplaceny v rámci vyrovnání, avšak za předpokladu, že každá ze stran je odpovědná za část nebo kterákoli ze stran je odpovědná za plnou výši škody, kterou utrpěl Subjekt Údajů v souvislosti se stejným incidentem nebo sérii incidentů a získal plnou náhradu pouze od jedné strany (dále jen „**Odškodňující Strana**“), pak je Odškodňující Strana oprávněna požadovat zpět od druhé strany tu část náhrady škody, která odpovídá škodě způsobené touto druhou stranou. Odškodňující Strana může vznést svůj nárok vůči druhé straně pouze do 12 měsíců po incidentu, a to v rozsahu povoleném platnými právními předpisy.

10.3 V maximálním rozsahu povoleném platnými zákony se omezení odpovědnosti a případné vyloučení náhrady škody vůči společnosti Iron Mountain uvedené ve Smlouvě řídí celkovou odpovědností za všechny nároky Zákazníka vyplývající z této DPA a/nebo Smlouvy nebo s nimi související. Tato omezení odpovědnosti a vyloučení náhrady škody se vztahují na všechny nároky, ať už vznikly na základě smlouvy, deliktu nebo jiné teorie odpovědnosti, a odkaz na odpovědnost společnosti Iron Mountain znamená souhrnnou odpovědnost společnosti Iron Mountain a všech jejich přidružených společností za nároky Zákazníka a všech jeho ostatních přidružených společností. V rozsahu požadovaném platnými právními předpisy není účelem tohoto oddílu i) měnit nebo omezovat odpovědnost stran za Nároky Subjektů Údajů vznesené vůči straně v případě společné a nerozdílné odpovědnosti nebo ii) omezovat odpovědnost kterékoli strany za zaplacení pokut uložených této straně regulačním orgánem.

10.4 V ustanoveních 10.1 až 10.3 je uveden jediný a výhradní prostředek nápravy každé strany a výhradní odpovědnost každé strany za ztrátu, škodu, výdaje nebo odpovědnost v souvislosti s touto DPA.

11. ŽÁDOSTI ORGÁNŮ VEŘEJNÉ MOCI

11.1 Společnost Iron Mountain se zavazuje, že v zákonem povoleném rozsahu a s výhradou níže uvedených bodů 11.2 až 11.5 bude Zákazníka informovat, pokud:

11.1.1 obdrží právně závaznou žádost orgánu veřejné moci, včetně soudních orgánů, podle právních předpisů cílové země o zpřístupnění Osobních Údajů Zákazníka podle této Smlouvy; nebo

11.1.2 se dozví o přímém přístupu orgánů veřejné moci k Osobním Údajům Zákazníků předaným na základě Smlouvy v souladu se zákony dané země.

11.2 Pokud je společnosti Iron Mountain podle právních předpisů cílové země zakázáno informovat Zákazníka, zavazuje se vynaložit maximální úsilí k získání výjimky ze zákazu s cílem sdělit co nejvíce informací co nejdříve.

11.3 Společnost Iron Mountain se zavazuje přezkoumat zákonnost žádosti o zpřístupnění, zejména zda zůstává v pravomocí udělených žádajícímu orgánu veřejné moci, a napadnout žádost, pokud dojde k závěru, že existují přiměřené důvody domnívat se, že žádost je podle právních předpisů dané země nezákonná. Požadované Osobní Údaje Zákazníka nezpřístupní, dokud k tomu nebude vyzvána podle platných procesních pravidel.

11.4 Společnost Iron Mountain se zavazuje, že v odpovědi na žádost o zpřístupnění informací poskytne minimální povolené množství informací na základě přiměřeného výkladu žádosti.

11.5 Společnost Iron Mountain se zavazuje uchovávat informace podle tohoto bodu po dobu trvání Smlouvy a na požádání je zpřístupní příslušnému dozorovému úřadu.

12. RŮZNÉ

12.1 S ohledem na povahu poskytovaných Služeb společnost Iron Mountain po ukončení/vypršení platnosti Smlouvy na základě konkrétního pokynu Zákazníka a v souladu s podmínkami Smlouvy buď vymaže/zničí nebo vrátí Zákazníkovi či jím určené třetí straně všechny jeho Osobní Údaje. Osobní Údaje Zákazníka obsažené v aktivu Zákazníka uloženého společností Iron Mountain jménem Zákazníka mu budou vráceny v souladu s dohodnutým plánem výstupu nebo přechodu a s výhradou dohodnutých nákladů, jak stanoví Smlouva nebo jiný platný smluvní dokument. Ve všech ostatních případech, kdy Smlouva neupravuje vymazání/zničení nebo vrácení Osobních Údajů Zákazníka a Zákazník k tomu do patnácti (15) dnů od ukončení/vypršení Smlouvy neposkytne žádné pokyny, požádá společnost Iron Mountain Zákazníka písemně, aby konkrétní pokyny k vymazání/zničení nebo vrácení svých Osobních Údajů zaslal do patnácti (15) dnů, a informuje Zákazníka o všech příslušných nebo jiných poplatcích, které je třeba za bezpečné zničení uhradit. Pokud Zákazník v patnáctidenní (15) lhůtě neposkytne písemně pokyny, ani nezaplatí příslušné poplatky ve stejné lhůtě, pak tímto opravňuje společnost Iron Mountain, aby po ukončení Smlouvy podle své vlastní volby a na náklady Zákazníka i nadále Osobní Údaje Zákazníka zpracovávala, vymazala nebo zničila.

12.2 Bez ohledu na Ustanovení bodu 12.1 společnost Iron Mountain neporuší své povinnosti týkající se vymazání Osobních Údajů Zákazníka uchovávaných na záložních páskách, pokud jsou tyto záložní pásky v rámci běžného provozu přepsány (a tím odstraněny Osobní Údaje Zákazníka).

12.3 S výjimkou Standardních Smluvních Doložek (jak jsou definovány v Příloze 3 této DPA) se tato DPA a veškeré spory, nároky nebo rozpory z vyplývající z této DPA nebo s ní související, či její porušení, ukončení nebo platnost řídí ustanovením o volbě práva uvedeným ve Smlouvě; a veškeré spory, nároky nebo rozpory vyplývající z této DPA nebo s ní související se bude primárně řešit prostřednictvím postupu pro řešení sporů definovaného ve Smlouvě.

12.4 Každá ze stran může čas od času písemně informovat druhou stranu o změnách této DPA, které přiměřeně považuje za nezbytné pro splnění požadavků Právních Předpisů o Ochraně Údajů nebo rozhodnutí dozorového úřadu či soudu. Takové změny budou účinné pouze tehdy, pokud se obě strany vzájemně dohodnou na rozsahu a podepíší dodatek k této DPA, s výjimkou případů, kdy jedna strana informuje druhou o nových zákonných požadavcích a předloží dodatek, který obsahuje pouze nezbytné změny, a který lze přijmout bez formálního souhlasu, tj. nevznesení námitek v určité lhůtě se považuje za vzájemně dohodnuté dodatky k této DPA.

PŘÍLOHA 1

Podrobnosti o Zpracování a Předávání Údajů (případně)

A. SEZNAM SMLUVNÍCH STRAN:

Smluvní strany této DPA a případné funkce vývozce a dovozce Údajů jsou uvedeny ve Smlouvě a v Příloze 3 (Mezinárodní Předávání Údajů).

B. POPIS ZPRACOVÁNÍ/PŘEDÁVÁNÍ (případně)**:**

Kategorie Subjektů Údajů, jejichž Osobní Údaje jsou zpracovávány/předávány:

V závislosti na povaze Služeb společnosti Iron Mountain a obchodní činnosti Zákazníka může Zákazník předávat společnosti Iron Mountain Osobní Údaje týkající se různých kategorií Subjektů Údajů, jejichž rozsah určuje a řídí on sám podle svého výhradního uvážení. Mezi kategorie Subjektů Údajů mohou patřit: bývalí a současní zaměstnanci; bývalí a současní dodavatelé nebo konzultanti; dodavatelé nebo konzultanti a externí pracovníci dodaní agenturou; uchazeči a zájemci o zaměstnání; studenti a dobrovolníci; osoby označené zaměstnanci nebo důchodci za oprávněné osoby, manželé/manželky, partneři ve společné domácnosti/partneři podle občanského práva, závislé osoby a kontakty pro naléhavé případy; důchodci; bývalí a současní ředitelé a vedoucí pracovníci; akcionáři; držitelé dluhopisů; majitelé účtů; koncoví uživatelé/spotřebitelé (dospělí, děti); pacienti (dospělí, děti); kolemjdoucí (kamery CCTV); a uživatelů webových stránek.

Kategorie zpracovávaných/předávaných Osobních Údajů:

V závislosti na povaze Služeb společnosti Iron Mountain a obchodní aktivitě Zákazníka může Zákazník společnosti Iron Mountain předávat různé kategorie Osobních Údajů, jejichž rozsah určuje a kontroluje on sám podle svého vlastního uvážení. Kategorie mohou zahrnovat Osobní Údaje týkající se Zákazníka a/nebo jeho vlastních klientů, zaměstnanců atd.

Předávané citlivé údaje (případné)**:**

V závislosti na povaze služeb společnosti Iron Mountain a obchodní aktivitě Zákazníka může Zákazník společnosti Iron Mountain předávat citlivé Údaje, jejichž rozsah určuje a kontroluje on sám podle svého vlastního uvážení.

Případná četnost předávání (např. zda jsou údaje předávány jednorázově nebo průběžně):

předávání probíhá průběžně.

Povaha Zpracování:

shromažďování, zaznamenávání, uspořádání, strukturování, ukládání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, zveřejňování přenosem, šíření nebo jiný způsob zpřístupnění, seřazení nebo kombinace, omezení, výmaz nebo zničení.

Účel(y) zpracování/předávání údajů (případně) **a další Zpracování:**

poskytování Služeb uvedených ve Smlouvě.

Uchovávání Údajů:

Osobní Údaje bude společnost Iron Mountain uchovávat po dobu trvání Služeb nabízených Zákazníkovi a do doby, kdy bude nucena je vrátit nebo zničit v souladu s bodem 12.1 této DPA.

V případě předávání (dílčím) Zpracovatelům uveďte také předmět, povahu a dobu trvání Zpracování:

Po dobu trvání Smlouvy se Zákazníkem poskytují dílčí Zpracovatelé mimo jiné informační technologie (IT) a konzultační služby, včetně globální podpory IT, hlášení událostí a služby správy.

C. PŘÍSLUŠNÝ DOZOROVÝ ÚŘAD

Jak je uvedeno v Příloze 3, případně (Mezinárodní Předávání Údajů).

PŘÍLOHA 2

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ („BEZPEČNOSTNÍ OPATŘENÍ“)

1. PROGRAM A ZÁSADY ZABEZPEČENÍ INFORMACÍ

Společnost Iron Mountain musí udržovat program zabezpečení informací prostřednictvím vhodných fyzických, technických a administrativních kontrol, navržených tak, aby byly splněny standardy v rámci odvětví. Program zabezpečení informací musí zahrnovat:

1.1 dokumentaci, interní publikace a komunikace zásad, norem a postupů zabezpečení informací společnosti Iron Mountain;

1.2. zdokumentované, jasné přiřazení odpovědnosti a pravomocí k vytvoření a udržování programu zabezpečení informací;

1.3 pravidelné testování klíčových kontrol, systémů a postupů programu zabezpečení informací;

1.4 administrativní, technická a provozní opatření určená k ochraně všech Osobních Údajů Zákazníka s využitím praktik, postupů a procesů popsaných v této Příloze o Zabezpečení v rozsahu, v jakém jsou relevantní a použitelné pro formát, v němž jsou uchovávány.

2. HODNOCENÍ RIZIK

Společnost Iron Mountain musí udržovat program hodnocení rizik zabezpečení informací určený k identifikaci a posouzení rozumně předvídatelných interních i externích rizik a zranitelností, které by mohly ovlivnit bezpečnost, důvěrnost a/nebo integritu Osobních Údajů Zákazníka. Společnost Iron Mountain bude každoročně nebo vždy, když dojde k podstatné změně rizika nebo zranitelnosti Osobních Údajů Zákazníka vyhodnocovat a podle potřeby přiměřeně a vhodně aktualizovat účinnost stávajícího programu zabezpečení informací s cílem omezit tato rizika.

3. SPRÁVA AKTIV PRO ZPRACOVÁNÍ INFORMACÍ A FYZICKÝCH MÉDIÍ

3.1 Správa aktiv pro zpracování informací. Společnost Iron Mountain udržuje program správy inventáře aktiv, kterým řídí fyzické, technické a administrativní kontroly týkající se aktiv pro zpracování informací (jako jsou počítače, servery, úložná zařízení, komunikační sítě, osobní počítače, notebooky a periferní zařízení).

Program správy inventáře aktiv zahrnuje následující:

3.1.1 dokumentované přidělení vlastnictví aktiv pracovníkům společnosti Iron Mountain, aby byla zajištěna vhodná klasifikace informací, určeno omezení přístupu a revize kontroly přístupu.

3.1.2 Sanitace aktiv před jejich likvidací v souladu s NIST 800-88.

3.1.3 Požadavek na svolení vedení před odstraněním zařízení nebo softwaru, který není přidělen konkrétní osobě, z prostor společnosti Iron Mountain.

3.2 Kontroly. Mezi kontrolní prvky společnosti Iron Mountain patří následující:

3.2.1 provozní postupy a technické kontroly určené k ochraně dokumentů, počítačových médií, vstupních/výstupních/záložních dat a systémové dokumentace před neoprávněným zveřejněním, úpravou a zničením.

3.2.2 Postupy pro bezpečnou likvidaci elektronických nebo fyzických médií obsahujících Osobní Údaje Zákazníka.

3.2.3 Zavedený proces pro sledování všech fyzických médií Zákazníka od prvotního držení společností Iron Mountain až po trvalé stažení nebo zničení.

4. BEZPEČNOSTNÍ OPATŘENÍ PRO PRACOVNÍKY

4.1 Zachování důvěrnosti. Společnost Iron Mountain bude přiměřeně vyžadovat od svých zaměstnanců, včetně dočasných i smluvních, aby souhlasili se zachováním důvěrnosti Osobních Údajů Zákazníků a dodržovali interní požadavky společnosti Iron Mountain na zabezpečení a přijatelné používání informací.

4.2 Zásady prověřování minulosti. Společnost Iron Mountain má pro své zaměstnance zavedeny zásady pro vyšetřování profesní historie a testování návykových látek (pouze v USA). Společnost Iron Mountain bude dodržovat tyto zásady po dobu trvání Smlouvy. Mezi požadavky těchto zásad patří mimo jiné kontroly na přítomnost drog (pouze v USA), ověřování totožnosti zaměstnanců, vyhledávání v trestním rejstříku, prověřování zaměstnání, prověřování vládních/teroristických seznamů, jakož i u některých zaměstnanců ověření vzdělání a u uchazečů o pozici řidiče a stávajících řidičů získání řidičského oprávnění a historie přestupků. Pokud jsou při prověření minulosti zjištěny negativní informace, provede společnost Iron Mountain individuální vyhodnocení v souladu s platnými pracovněprávními předpisy a osvědčenými postupy.

4.3 Spolupráce se subdodavateli. Společnost Iron Mountain bude vyžadovat od každého subdodavatele, aby všichni jeho zaměstnanci, kteří se podílejí na poskytování Služeb spojených se Zpracováním Osobních Údajů Zákazníka podle Smlouvy dodržovali omezení podobná těm, která jsou uvedená v tomto bodě.

4.4 Školení o bezpečnosti. Nejméně jednou ročně uskuteční společnost Iron Mountain školení pro všechny své zaměstnance, kteří mají přístup k Osobním Údajům Zákazníků, o bezpečnosti a specifická bezpečnostní školení podle jejich úkolů. Společnost Iron Mountain povede záznamy se jmény všech

zúčastněných zaměstnanců a datum každého školení o bezpečnosti. Společnost Iron Mountain bude svůj program školení o bezpečnosti pravidelně kontrolovat a aktualizovat.

4.5 Propuštění zaměstnanců společnosti Iron Mountain. Společnost Iron Mountain uplatní disciplinární postup vůči všem svým zaměstnancům, kteří poruší bezpečnostní požadavky uvedené v tomto dokumentu.

4.6 Ukončení přístupu po ukončení pracovního poměru/přeřazení na jinou pozici. Po ukončení pracovního poměru nebo přeřazení na jinou pozici, která nevyžaduje přístup k Osobním Údajům Zákazníka, bude přístup zaměstnance společnosti Iron Mountain k Osobním Údajům Zákazníka neprodleně zrušen.

5. FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

5.1 Kontroly fyzické bezpečnosti. Zařízení společnosti Iron Mountain podléhají fyzickým kontrolám, které přiměřeně omezují přístup k Osobním Údajům Zákazníků, včetně protokolů kontroly přístupu, fyzických bariér, jako jsou uzamčená zařízení a prostory, přístupové karty zaměstnanců, návštěvní deníky, přístupové karty návštěvníků, čtečky karet, kamery pro video zabezpečení a alarmy pro detekci vniknutí. Všichni návštěvníci musí být vždy zapsáni a doprovázeni.

5.2 Podpůrné nástroje. Společnost Iron Mountain zavede opatření určená k ochraně svých zařízení obsahujících Osobní Údaje Zákazníků a systémů před výpadky napájení, telekomunikací, vodou, kanalizací, vytápěním, větráním a klimatizací podle potřeby.

5.3 Zabezpečení přenosového systému. Společnost Iron Mountain přijme opatření určená k ochraně fyzické bezpečnosti své síťové infrastruktury a telekomunikačních systémů před odposlechem a poškozením přenosu.

5.4 Zařízení mimo pracoviště. V případě, že společnost Iron Mountain externě zajišťuje funkce vyžadující použití zařízení mimo pracoviště na podporu služeb, musí být takové zařízení mimo pracoviště obsahující Osobní Údaje Zákazníků chráněno stejným zabezpečením jako zařízení na pracovišti používané pro stejné účely.

5.5 Fyzický přístup k majetku pro zpracování informací. Společnost Iron Mountain bude uchovávat záznamy o svých zaměstnancích, kteří mají oprávnění fyzicky přistupovat ke kontrolovanému počítačovému prostředí používaného k poskytování služeb po dobu jednoho roku a Zákazníkovi na jeho žádost poskytne přístup k prohlížení auditovatelných záznamů těchto svých zaměstnanců v souvislosti s Porušením Zabezpečení a v souladu se svými bezpečnostními zásadami.

5.6 Omezený fyzický přístup. Společnost Iron Mountain omezí fyzický přístup do vlastních zařízení na Zpracovávání Osobních Údajů Zákazníků pouze na ty své zaměstnance a oprávněné osoby, které mají pro takový přístup obchodní potřebu. Společnost Iron Mountain zavede schvalovací proces pro schvalování a sledování žádostí o fyzický přístup k takovým zařízením.

5.7 Opravy a úpravy. Společnost Iron Mountain zaznamená veškeré opravy a úpravy fyzických součástí, včetně hardwaru, zdí, dveří a zámků zabezpečených prostor se zařízeními, kde jsou uloženy Osobní Údaje Zákazníků.

5.8 Záznamy. Povede záznamy o pohybech hardwaru a elektronických médií a o všech, kteří jsou za ně odpovědní.

6. ŘÍZENÍ OPERACÍ KOMUNIKACÍ A ZPRACOVÁNÍ INFORMACÍ

6.1 Standardy konfigurace zařízení. Společnost Iron Mountain vytvoří, zavede a bude udržovat postupy správy systému, které odpovídají standardům v rámci odvětví, mimo jiné včetně zpevnění systému, záplatování systému a zařízení (operačního systému a aplikací) a správné instalace a aktualizace antivirových programů.

6.2 Řízení změn systémů zpracování informací. Společnost Iron Mountain musí mít zaveden interní formální proces řízení žádostí o změny v systémech pro zpracování informací a komunikační sítě a žádosti o změnu musí být zdokumentovány, testovány a schváleny před zavedením jakýchkoli nových funkcí zpracování informací nebo komunikačních sítí, systémových oprav nebo změn stávajících systémů.

6.3 Oddělení povinností. Společnost Iron Mountain oddělí povinnosti a odpovědnosti jednotlivých osob tak, aby žádná jedna osoba, která má přístup k Osobním Údajům Zákazníků, neměla výhradní možnost měnit systémy zpracování informací.

6.4 Oddělení vývojového a produkčního prostředí. Vývojová, testovací a produkční prostředí systémů zpracování informací společnosti Iron Mountain musí být logicky nebo fyzicky oddělena.

6.5 Správa technické architektury. Společnost Iron Mountain zavede proces správy konfigurace, aby definovala, spravovala a kontrolovala komponenty systému zpracování informací používané k poskytování služeb a technickou infrastrukturu těchto komponent.

6.6 Detekce narušení. Společnost Iron Mountain bude nepřetržitě monitorovat počítačové systémy a procesy, zda nedochází k pokusům o narušení nebo skutečným narušení zabezpečení a bude Zákazníka informovat o jakémkoli neoprávněném přístupu k jeho Osobním Údajům.

6.7 Zabezpečení sítě. Společnost Iron Mountain zajistí zavedení následujících opatření:

6.7.1 pokud jde o prostředí hostované společností Iron Mountain k poskytování služeb, systém detekce narušení sítě (dále jen zkr. „IDS“) a senzory prevence narušení (dále jen zkr. „IPS“) zaznamenávající výstražné události a vydávající denní zprávy pro kontrolu (souhrnně označované jako „IDS/IPS“);

6.7.2 pokud jde o prostředí hostované společností Iron Mountain k poskytování Služeb, aktualizace zpráv IDS/IPS nejméně jednou týdně, ale i dříve, ihned po obdržení aktualizací a okamžité spuštění nejnovějších signatur hrozeb či pravidel;

6.7.3 vysoce rizikové porty v systémech orientovaných na externí uživatele nejsou přístupné na internetu;

6.7.4 síťová připojení společnosti Iron Mountain jsou nahrávána a zaznamenávána v souborech protokolu;

6.7.5 nasazení brány (bran) firewall určené k ochraně a kontrole veškerého příchozího a odchozího provozu síťových služeb mezi definovanými body sítě;

6.7.6 zásady zabezpečení pro definování příchozích a odchozích síťových portů nebo služebního provozu pro všechny systémy, které společnost Iron Mountain vlastní nebo spravuje, a které jsou zdokumentovány a schváleny v rámci programu zabezpečení informací;

6.7.7 síťové a diagnostické porty, které jsou řádně zabezpečeny; a

6.7.8 zásady, postupy a technické kontroly, jejichž cílem je předcházet škodlivým kódům nebo známým útokům na informační systémy společnosti Iron Mountain, odhalovat je a odstraňovat.

6.8 Šifrované ověřovací pověření. Společnost Iron Mountain zajistí zašifrování ověřovacích pověření při tranzitu přes své sítě.

6.9 Zabezpečená správa sítě. Sítě společnosti Iron Mountain musí být rozumně řízeny a kontrolovány tak, aby byly chráněny před známými hrozbami, a aby byla zajištěna bezpečnost všech aplikací a dat spravovaných společností Iron Mountain v síti nebo v tranzitu po síti. Budou zavedeny technické kontroly a zabezpečené komunikační protokoly, které zakazují neomezené připojení k nedůvěryhodným sítím nebo veřejně přístupným serverům.

6.10 Ochrana proti virům. Společnost Iron Mountain zavede a bude udržovat antivirový řídící program, včetně ochrany proti malwaru, aktuálních souborů s podpisy nebo alternativní ochrany proti vznikajícím hrozbám, záplatám a definicím virů, pro spravované servery a pracoviště používané k ukládání nebo přístupu k Osobním Údajům Zákazníků.

6.11 Webové stránky – šifrování klientů. Společnost Iron Mountain zajistí, aby pro každou z jejích webových stránek byla povolena funkce Secure Sockets Layering (SSL) a obsahovala platný certifikát SSL vyžadující kontrolu důvěrnosti, autentizace nebo autorizace.

6.12 Zálohování informací. Společnost Iron Mountain vytvoří příslušné záložní kopie systémových souborů. Kromě toho společnost Iron Mountain vyvine a zachová postupy obnovy po havárii. Další podrobnosti naleznete v části „Obnova po havárii“ níže.

6.13 Elektronické informace při tranzitu. Společnost Iron Mountain využívá šifrování s algoritmem standardním pro dané odvětví s minimální délkou klíče 128 bitů k ochraně Osobních Údajů Zákazníků přenášených po veřejných sítích v době, kdy pocházejí infrastruktury hostované společností Iron Mountain.

6.14 Kryptografické ovládání. Společnost Iron Mountain se bude řídit zdokumentovanými zásadami používání kryptografických ovládacích prvků. Kryptografické ovládací prvky společnosti Iron Mountain musí:

6.14.1 být navrženy tak, aby přiměřeně chránily důvěrnost a integritu Osobních Údajů Zákazníků, které společnost Iron Mountain zpracovává, přenáší nebo uchovává v prostředí sdílené sítě, v souladu s podmínkami Smlouvy;

6.14.2 v prostředí hostovaném společností Iron Mountain používané k poskytování služeb, být aplikovány na Osobní Údaje Zákazníka při přenosu přes nebo do „nedůvěryhodných“ sítí (tj. sítí, které Iron Mountain nemá právně pod kontrolou), včetně těch, které se používají k odesílání dat do podnikové sítě Zákazníka ze sítě společnosti Iron Mountain, v každém případě s výhradou spolupráce zákazníka při správě šifrovacích klíčů nezbytných k dešifrování přenosů přijatých zákazníkem; a

6.14.3 zahrnovat dokumentované postupy správy šifrovacích klíčů na podporu zabezpečení kryptografických technologií.

6.14.4 zahrnovat šifrování veškerých Osobních Údajů Zákazníků do notebooků nebo jiných přenosných zařízení.

6.15 Požadavky na protokolování. Společnost Iron Mountain zajistí následující:

6.15.1 významné bezpečnostní a systémové události jsou zaznamenávány a kontrolovány;

6.15.2 auditní protokoly jsou uchovávány minimálně po dobu jednoho roku pro systémy v prostředí hostovaném společností Iron Mountain, které využívá k poskytování služeb;

6.15.3 protokoly systémového auditu jsou přezkoumávány kvůli anomáliím; a

6.15.4 Protokolovací zařízení a systémové informace jsou přiměřeně chráněny před neoprávněným zásahem i neoprávněným přístupem.

6.16 Síťová synchronizace času. Společnost Iron Mountain bude synchronizovat systémové hodiny všech systémů zpracování informací pomocí společného autoritativního časového zdroje.

6.17 Segregace na sítích. Společnost Iron Mountain bude v sítích odpovídajícím způsobem oddělovat související skupiny informačních služeb, uživatelů a informačních systémů.

7. ŘÍZENÍ PŘÍSTUPU

7.1 Zásady řízení přístupu. Společnost Iron Mountain dodržuje zásady řízení přístupu, pokud jde o aktiva pro zpracování informací, které sama formálně schvaluje, zveřejňuje a implementuje.

7.2 Schválení logického přístupu. Společnost Iron Mountain musí mít zaveden schvalovací proces pro žádosti o logický přístup k Osobním Údajům Zákazníků a žádosti o přístup ke svým systémům určeným pro použití ve Sužbách.

7.3 Řízení přístupu a kontrola přístupu. Společnost Iron Mountain umožní přístup k Osobním Údajům Zákazníků pouze svým aktivním zaměstnancům, včetně dočasných a smluvních zaměstnanců a aktivním uživatelům účtů, kteří takový přístup potřebují k výkonu své pracovní funkce. Veškerý privilegovaný přístup musí být přezkoumán a potvrzen tak, aby byl v souladu s aktuální úlohou v zaměstnání a alespoň čtvrtletně zdokumentován.

7.4 Řízení přístupu třetích stran. Předtím, než společnost Iron Mountain udělí externím stranám, které mají přístup k Osobním Údajům Zákazníků přístup do svých informačních systémů, zavede vhodné kontrolní mechanismy.

7.5 Řízení přístupu k operačním systémům. Společnost Iron Mountain musí řídit přístup k operačním systémům (softwarovým i hardwarovým) tak, že bude vyžadovat bezpečný přihlašovací proces, který jedinečně identifikuje osobu přistupující k operačnímu systému.

7.6 Mobilní výpočetní zařízení. Společnost Iron Mountain zavede zásady nebo postupy určené k ochraně svých mobilních výpočetních zařízení před neoprávněným přístupem. Tyto zásady nebo postupy se budou zabývat fyzickou ochranou, kontrolou přístupu a bezpečnostními kontrolami, jako je šifrování, protivirová ochrana a zálohování zařízení.

7.7 Izolace zákaznických systémů. Společnost Iron Mountain v rámci svého hostovaného prostředí používaného k poskytování služeb logicky oddělí a segreguje Osobní Údaje Zákazníků od všech ostatních informací.

7.8 Účty. Společnost Iron Mountain učiní v souvislosti s účty následující:

7.8.1 vyžádá si ověření totožnosti každého svého zaměstnance, který usiluje o přístup k jejím systémům pro zpracovávání Osobních Údajů Zákazníků a zakáže používání sdílených uživatelských účtů nebo uživatelských účtů s obecnými přihlašovacími Údaji (tj. ID) pro přístup k Osobním Údajům Zákazníků nebo systémům.

7.8.2 bude požadovat, aby všechna ID uživatelských účtů, včetně privilegovaných účtů, byla vždy vázána přímo k určité osobě (nikoli k pozici).

7.8.3 pokud nejsou výchozí administrační účty zakázány nebo odstraněny, je nutné pro přístup k výchozímu administračnímu účtu použít dočasná hesla, odškrtávací ID nebo podobné kontroly.

7.8.4 bude požadovat, aby neaktivní běžné účty byly po 90 dnech nečinnosti uzamčeny nebo deaktivovány.

7.8.5 zakáže přístup k účtu po několika neúspěšných pokusech o něj.

7.8.6 bude vyžadovat jedinečné identifikační kódy a silná hesla, která budou obsahovat: minimálně 8 znaků; budou měněna každých 90 dní a splní požadavky na složitost.

7.8.7 zakáže zaměstnancům sdílet hesla nebo si je zapisovat.

7.9 Ovládání systémů bez dozoru. Společnost Iron Mountain musí používat spořič obrazovky chráněný heslem pro všechny systémy, které jsou ponechány bez dozoru a nevykazují žádnou činnost po dobu 30 minut.

8. VÝVOJ A ÚDRŽBA ZÍSKÁVÁNÍ INFORMAČNÍCH SYSTÉMŮ

8.1 Zabezpečení vývoje systémů. Společnost Iron Mountain zajistí, aby zabezpečení bylo součástí vývoje a provozu všech informačních systémů a zveřejní a dodrží interní metodiky bezpečného kódování založené na bezpečnostních normách pro vývoj aplikací.

8.2 Správa zabezpečení softwaru. Informační systémy společnosti Iron Mountain (včetně operačních systémů, infrastruktury, podnikových aplikací, služeb a aplikací vyvíjených uživateli) musí být navrženy tak, aby byly v souladu se standardy zabezpečení informací.

8.3 Síťové diagramy. Společnost Iron Mountain vyvine, zdokumentuje a bude udržovat fyzické a logické diagramy síťových zařízení a provozu.

8.4 Hodnocení zranitelnosti aplikací/etické hackování. Společnost Iron Mountain alespoň jednou ročně provede hodnocení zranitelnosti u aplikací, které Zpracovávají Osobní Údaje Zákazníků v hostovaném prostředí (hostovaných prostředích) k poskytování služeb. Podrobné výsledky jsou důvěrnými a chráněnými informacemi společnosti Iron Mountain a nebudou poskytnuty.

8.5 Změna testování a kontrola. Společnost Iron Mountain přezkoumá a otestuje změny aplikací a operačních systémů před jejím nasazením, aby zajistila, že nedojde k nepříznivému vlivu na Osobní Údaje Zákazníků nebo systémů.

9. OBNOVENÍ PO HAVÁRII

Společnost Iron Mountain musí udržovat plán obnovy po havárii, včetně replikace systémů a elektronických dat používaných na podporu služeb do záložního datového centra. Replikace systémů a elektronických dat nezahrnuje Osobní Údaje Zákazníků, které jsou fyzicky uloženy v zařízeních společnosti Iron Mountain. Společnost Iron Mountain udržuje plán provozu pro obnovu zásadních podnikových funkcí. Společnost Iron Mountain bude provádět testování obnovy po havárii nejméně jednou za dvanáct (12) měsíců.

10. EXTERNÍ AUDITY A HODNOCENÍ

Bezpečnostní protokoly společnosti Iron Mountain jsou navrženy tak, aby byly v souladu se standardy v rámci odvětví. Společnost Iron Mountain poskytne Zákazníkovi zprávy nezávislého auditu třetí strany, které si nechala

vypracovat (např. PCI, ISO27001, SOC2 atd.), vztahující se ke Službám v regionu, kde jsou takové Služby poskytovány (dále jen „Zpráva Auditora“). Společnost Iron Mountain poskytne všechny tyto zprávy zadané s úmyslem být poskytnuty Zákazníkovi, bez ohledu na jejich výsledky. Společnost Iron Mountain nebude povinna poskytnout výsledky interních auditů ani výsledky jiných nezávislých hodnocení, které byly zadány s úmyslem být důvěrnou informací pro společnost. Zákazníkovi a jeho externím auditorům budou na požádání poskytnuty kopie Zprávy Auditora. Zpráva Auditora nebo jiné výsledky získané při testování či auditech vyžadovaných v tomto oddíle budou považovány za důvěrné informace společnosti Iron Mountain. Zákazník má právo poskytnout kopii takové Zprávy Auditora všem příslušným zákazníkům nebo regulačním orgánům Zákazníka, s výhradou ustanovení o důvěrnosti, která jsou stejně přísná jako ustanovení v tomto dokumentu. Na žádost Zákazníka společnost Iron Mountain písemně potvrdí, že od dokončení takové Zprávy Auditora nedošlo ke změnám v příslušných zásadách, postupech a vnitřních kontrolách, a to nejdéle do tří měsíců od konce vykazovaného období Zprávy Auditora.

PŘÍLOHA 3

Mezinárodní Předávání Údajů

1. DEFINICE

„**Standardní Smluvní Doložky EU 2021**“ znamenají standardní smluvní doložky pro předávání Osobních Údajů do třetích zemí podle GDPR, přijaté Evropskou komisí podle Prováděcího Rozhodnutí Komise (EU) 2021/914, které jsou k dispozici zde[3] .

„**Dodatkem Spojeného království z roku 2022**“ se rozumí vzorový Dodatek B.1.0 vydaný Úřadem komisaře pro informace Spojeného království a předložený Parlamentu v souladu se Zákonem s119A o Ochraně Údajů 2018 ze dne 2. února 2022, který může být revidován podle Oddílu 18, a který je k dispozici zde[4] .

„**Osobními Údaji Zákazníků EU**“ se rozumí Zpracování Osobních Údajů Zákazníků, na které se před jejich zpracováním společností Iron Mountain vztahovaly zákony o ochraně Údajů Evropské unie nebo práva některého z členských států EU či Evropského hospodářského prostoru;

„**Chráněnou Oblastí**“ se rozumí:

i. v případě Osobních Údajů Zákazníků v EU, členské státy Evropské unie a Evropského hospodářského prostoru a každá země, území, zóna nebo mezinárodní organizace, pro kterou platí rozhodnutí o odpovídající ochraně podle čl. 45 GDPR;

ii. v případě Osobních Údajů Zákazníků ze Spojeného království, Spojené království a každá země, území, zóna nebo mezinárodní organizace, pro kterou platí rozhodnutí o odpovídající ochraně podle nařízení Spojeného království o odpovídající úrovni ochrany;

iii. v případě Osobních Údajů švýcarských Zákazníků, každá země, území, zóna nebo mezinárodní organizace, která je uznávaná podle švýcarských zákonů jako odpovídající;

iv. v případě jiných Osobních Údajů Zákazníků předávaných mimo jurisdikci, která nabízí podobnou ochranu jako ochrana Osobních Údajů Zákazníků v EU, Spojeném království nebo Švýcarsku, každá země, území, zóna nebo mezinárodní organizace, která je podle zákonů takové jurisdikce uznávaná jako odpovídající;

„**Standardními Smluvními Doložkami**“ se souhrnně rozumí Standardní Smluvní Doložky EU z roku 2021 a Dodatek Spojeného království z roku 2022.

„**Osobními Údaji švýcarského Zákazníka**“ se rozumí Zpracování Osobních Údajů Zákazníků, na které se vztahovaly švýcarské zákony o ochraně osobních údajů před jejich Zpracováním společností Iron Mountain;

„**Osobními Údaji Zákazníků ze Spojeného království**“ se rozumí Zpracování Osobních Údajů Zákazníků, na které se vztahovaly zákony o ochraně osobních údajů Spojeného království před jejich zpracováním společností Iron Mountain;

2. RŮZNÉ

2.1 Tato Příloha 3 obsahuje následující části: (i) část A – Předávání Osobních Údajů Zákazníků z EU; (ii) část B – Předávání Osobních Údajů švýcarských Zákazníků; (iii) část C – Předávání Osobních Údajů Zákazníků ze Spojeného království, které se použijí podle potřeby na předávání Osobních Údajů Zákazníků společností Iron Mountain v souvislosti s jejími Službami.

2.2 Standardní Smluvní Doložky platí pro společnost Iron Mountain a její přidružené společnosti jako pro „dovozce Údajů“ a pro Zákazníka a jeho přidružené společnosti jako pro „vývozce Údajů“.

2.3 Podpis a datování Smlouvy představují všechny požadované podpisy a data pro Standardní Smluvní Doložky.

2.4 V případě, že smluvní strany předávají Osobní Údaje Zákazníků z EU, Spojeného království nebo Švýcarska mimo Chráněnou Oblast a příslušné rozhodnutí Evropské komise nebo jiná platná metoda přiměřenosti podle platných Právních předpisů o Ochraně Osobních Údajů, na níž se společnost Iron Mountain při předávání Údajů spoléhala, je považována za neplatnou, nebo pokud dozorový úřad požaduje pozastavení předávání Osobních Údajů na základě takového rozhodnutí, budou smluvní strany spolupracovat a usnadní použití alternativního mechanismu předávání. Strany se rovněž dohodly, že vhodné záruky používané k usnadnění mezinárodního předávání uvedené v této Příloze 3 nejsou výlučné, a že mohou využívat další mechanismy předávání, např. rámec EU-USA pro Ochranu Osobních Údajů.

ČÁST A – PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ ZÁKAZNÍKŮ Z EU

[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

Pokud a v rozsahu, v jakém Zákazník nebo jeho Přidružené společnosti předávají v souvislosti se Službami podle Smlouvy společnosti Iron Moutain či jejím Přidruženým společnostem Osobní Údaje Zákazníků z EU mimo Chráněnou Oblast, platí tato část A Přílohy 3 a Strany se dohodly následovně:

1. **Výběr Standardních Smluvních Doložek.** Text MODULU DVA Standardních Smluvních Doložek EU 2021 se použije v případě, že Zákazník nebo některá z jeho Přidružených společností je Správcem a společnost Iron Mountain nebo některá z jejich Přidružených společností je Zpracovatelem; text MODULU TŘI Standardních Smluvních Doložek EU 2021 se použije v případě, že Zákazník nebo některá z jeho Přidružených společností je Zpracovatelem a společnost Iron Mountain nebo některá z jejich Přidružených společností je dílčím Zpracovatelem. Příslušná ustanovení obsažená ve Standardních Smluvních doložkách EU 2021 jsou do této DPA začleněna odkazem a jsou její nedílnou součástí. Žádné další moduly ani ustanovení označená ve Standardních Smluvních Doložkách EU 2021 jako nepovinná platit nebudou. Informace požadované pro účely příloh Standardních Smluvních Doložek EU 2021 jsou uvedeny v Příloze 1 – Popis Zpracování/předávání, Příloze 2 – Technická a organizační opatření a ustanovení 6.2 DPA – Seznam dílčích Zpracovatelů.

2. **Využívání dílčích Zpracovatelů.** Při využití dílčích Zpracovatelů k poskytování Služeb bude pro účely ustanovení 9 Standardních Smluvních Doložek EU 2021 platit možnost 2 (Obecné Písemné Oprávnění). Zákazník bere na vědomí a souhlasí s tím, že společnost Iron Mountain může zapojit nové dílčí Zpracovatele prostřednictvím mechanismu dohodnutého v ustanovení 6 této DPA, a že lhůta pro podání žádostí dílčím Zpracovatelům o změnu je patnáct (15) dnů.

3. **Rozhodné právo a volba soudní příslušnosti.** Pro účely ustanovení 17 Standardních Smluvních Doložek EU 2021 (Rozhodné Právo) bude platit varianta 2 rozhodného práva a tyto doložky se budou v rozsahu, v jakém to umožňují práva oprávněné třetí strany řídit právem členského státu EU, v němž sídlí vývozce Údajů. Pro účely ustanovení 18 Standardních Smluvních Doložek EU 2021 (Volba Soudní Příslušnosti a Jurisdikce) to budou soudy členského státu EU, v němž sídlí vývozce údajů.

4. **Potvrzení o výmazu.** Pro účely ustanovení 8.5 a 16(d) Standardních Smluvních Doložek EU 2021 poskytne společnost Iron Mountain Zákazníkovi potvrzení o výmazu Osobních Údajů pouze na jeho písemnou žádost.

5. **Porušení zabezpečení osobních údajů.** Porušení zabezpečení osobních údajů budou pro účely ustanovení 8.6(c) Standardních Smluvních Doložek EU 2021 řešeny v souladu s mechanismem dohodnutým v ustanovení 7 DPA.

6. **Audity.** Audity budou pro účely ustanovení 8.9 Standardních Smluvních Doložek EU 2021 prováděny v souladu s auditním mechanismem dohodnutým ve Smlouvě.

7. **Stížnosti.** Pro účely ustanovení 11 Standardních Smluvních Doložek EU 2021 společnost Iron Mountain informuje Zákazníka, pokud obdrží stížnost od Subjektu Údajů týkající se Osobních Údajů Zákazníka ze EU, a sdělí tuto stížnost Zákazníkovi v souladu s mechanismem dohodnutým ve Smlouvě.

8. **Dozorový úřad.** V případě Standardních Smluvních Doložek EU 2022 bude příslušný dozorový úřad určen v souladu s ustanovením 13 Standardních Smluvních Doložek EU.

ČÁST B – PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ ŠVÝCARSKÝCH ZÁKAZNÍKŮ

Pokud a v rozsahu, v jakém Zákazník nebo jeho přidružené společnosti předávají v souvislosti se Službami podle Smlouvy společnosti Iron Moutain či jejím přidruženým společnostem Osobní Údaje švýcarských Zákazníků mimo Chráněnou Oblast, platí tato Část B Přílohy 3 a strany se dohodly následovně:

1. **Výběr Standardních Smluvních Doložek.** Standardní Smluvní Doložky EU 2021 a příslušná ustanovení podle Části A budou platit v případech, kdy je Zákazník nebo některá z jeho Přidružených společností Správcem a společnost Iron Mountain nebo některá z jejích Přidružených společností Zpracovatelem a/nebo Zákazník nebo některá z jeho Přidružených společností Zpracovatelem a společnost Iron Mountain nebo některá z jejích přidružených společností dílčím Zpracovatelem s výjimkou následujících případů:

   a. příslušným dozorovým úřadem podle ustanovení 13 Standardních Smluvních Doložek EU 2021 je švýcarská Federální komise pro ochranu osobních údajů a informací;

   b. rozhodným právem pro smluvní nároky podle ustanovení 17 Standardních Smluvních Doložek EU 2021 je švýcarské právo a místem jurisdikce pro žaloby mezi stranami podle ustanovení 18 (b) jsou švýcarské soudy.

2. Odkazy na nařízení GDPR EU ve Standardních Smluvních Doložkách EU 2021 je třeba chápat jako odkazy na FADP.

3. V souladu s ustanovením 18 (c) Standardních Smluvních Doložek EU 2021 nelze pojem „členský stát“ ve Standardních Smluvních Doložkách EU 2021 vykládat tak, že by vylučoval Subjekty Údajů ve Švýcarsku z možnosti domáhat se svých práv v místě svého obvyklého sídla (Švýcarsko).

ČÁST C – PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ ZÁKAZNÍKŮ ZE SPOJENÉHO KRÁLOVSTVÍ

Pokud a v rozsahu, v jakém Zákazník nebo jeho Přidružené společnosti předávají v souvislosti se Službami podle Smlouvy společnosti Iron Moutain či jejím Přidruženým společnostem Osobní Údaje Zákazníků ze Spojeného království mimo Chráněnou Oblast, platí tato Část C přílohy 3 a Strany se dohodly následovně:

1. **Výběr standardních smluvních doložek.** Standardní Smluvní Doložky EU 2021, příslušná ustanovení podle Části A a Dodatek 2022 Spojeného království budou platit v případech, kdy je Zákazník nebo některá z jeho Přidružených společností Správcem a společnost Iron Mountain nebo některá z jejích Přidružených společností Zpracovatelem a/nebo Zákazník nebo některá z jeho Přidružených společností Zpracovatelem a společnost Iron Mountain nebo některá z jejích Přidružených společností dílčím Zpracovatelem.

2. **Část 1: Tabulka 1-3 Dodatku 2022 Spojeného království:** Informace o Stranách – tabulka 1; vybrané SCC, moduly a vybraná ustanovení; a informace v příloze, včetně přílohy 1A: Seznam Stran, Příloha 1B: Popis Předávání a Příloha 1C: Technická a organizační opatření k zajištění bezpečnosti údajů – Tabulka 3 budou považována za splněná odkazem na tuto Přílohu 3, včetně Části A. Tabulka 4 dodatku Spojeného království: Zákazník a společnost Iron Mountain berou na vědomí a souhlasí s tím, že Dodatek Spojeného království může být vypovězen kteroukoli ze Stran.

3. **Část 2:** Povinná ustanovení Dodatku Spojeného království: Zákazník a společnost Iron Mountain berou na vědomí závazné podmínky Dodatku Spojeného království a souhlasí s nimi.

4. **Dozorový úřad.** Úřad komisaře pro informace Spojeného království bude vystupovat jako příslušný dozorový úřad.

ČÁST B – PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ OSTATNÍCH ZÁKAZNÍKŮ

Pokud a v rozsahu, v jakém Zákazník nebo jeho přidružené společnosti předávají společnosti Iron Mountain nebo jejím přidruženým společnostem Osobní Údaje v souvislosti s jejími Službami podle Smlouvy, na které se nevztahuje ČÁST A-C, bude platit Část A Přílohy 3 v rozsahu, který je relevantní a použitelný podle příslušných Právních Předpisů o Ochraně Údajů. V opačném případě, pokud jsou pro předávání Osobních Údajů Zákazníka do země, která neposkytuje odpovídající úroveň ochrany Osobních Údajů z pohledu vývozce údajů, vyžadována náhradní nebo dodatečná vhodná ochranná opatření či mechanismy předávání podle Právních Předpisů o Ochraně Údajů, se strany dohodly, že je zavedou co nejdříve a zdokumentují tyto požadavky na zavedení v příloze k této DPA.

PŘÍLOHA 4

HIPAA – Smlouva o spolupráci s obchodními partnery (dále jen „smlouva BAA“)

Tato smlouva BAA doplňuje a mění všechny současné nebo budoucí Smlouvy uzavřené mezi společností Iron Mountain, jejími přidruženými společnostmi a Zákazníkem i jeho přidruženými společnostmi, na jejichž základě společnost Iron Mountain nebo její přidružené společnosti poskytují určité služby Zákazníkovi či jeho přidruženým společnostem, přičemž tyto Služby vyžadují, aby obchodní partner používal a/nebo zveřejňoval PHI jménem Krytého Subjektu. S výjimkou rozsahu upraveného v této smlouvě BAA zůstávají všechny podmínky stanovené ve Smlouvě v plné platnosti a účinnosti a řídí se jimi Služby, které společnost Iron Mountain poskytuje Zákazníkovi.

Společnost Iron Mountain a Zákazník uzavírají tuto smlouvu BAA, aby obě strany mohly plnit své příslušné povinnosti, jakmile nabudou účinnosti a budou pro ně závazné podle pravidel HIPAA o ochraně soukromí, bezpečnosti a oznamování porušení spolu s veškerými prováděcími předpisy včetně těch, které byly zavedeny jako součást souhrnného pravidla (dále společně jen jako „Pravidla HIPAA"), podle nichž je Zákazník a jeho přidružené společnosti „Krytým Subjektem“ nebo „Obchodním Partnerem" a společnost Iron Mountain a její přidružené společnosti jsou „Obchodním Partnerem“ Zákazníka. Pro účely této Smlouvy budou veškeré odkazy na Obchodního Partnera dále považovány za odkazy na společnost Iron Mountain nebo její příslušnou přidruženou společnost.

1. DEFINICE

Pojmy psané velkými písmeny, které jsou použity, ale nejsou jinak definovány v této smlouvě BAA, mají stejný význam, jaký je jim připisován v Pravidlech HIPAA nebo ve Smlouvě, podle toho, co je relevantní.

„**Pravidlo pro Oznamování Porušení**“ znamená pravidlo pro Oznamování Porušení Nezabezpečených Chráněných Zdravotních Informací v 45 CFR §164, Podčást D.

„**Obchodním Partnerem**“ se rozumí výše uvedený subjekt Obchodního Partnera v rozsahu, v jakém při poskytování služeb Zákazníkům přijímá, uchovává nebo předává Chráněné Zdravotní Informace.

„**HIPAA**“ znamená Zákon z roku 1996 o přenositelnosti a odpovědnosti zdravotního pojištění.

„**Zákon HITECH**“ znamená platná ustanovení Zákona o zdravotnických informačních technologiích pro ekonomické a klinické zdraví, jak je začleněn do amerického Zákona o obnově a reinvesticích z roku 2009, včetně veškerých prováděcích předpisů.

„**Pravidlo o Ochraně Osobních Údajů**“ znamená Standardy pro ochranu osobně identifikovatelných zdravotních informací podle 45 CFR §160 a §164, dílčích částí A a E.

„**Chráněné Zdravotní Informace**“ nebo „**PHI**“ mají stejný význam jako pojem „chráněné zdravotní informace“ v 45 CFR §160.103 a jsou omezeny na chráněné zdravotní informace vytvořené Obchodním Partnerem jménem Zákazníka nebo získané od Zákazníka či jeho jménem podle Smlouvy.

„**Bezpečnostní Pravidlo**“ znamená Bezpečnostní standardy pro ochranu elektronických chráněných zdravotních informací podle 45 CFR §160 a §164, Podčástí A a C.

2. POVINNOSTI A ČINNOSTI OBCHODNÍHO PARTNERA

2.1. Obchodní Partner souhlasí s tím, že nebude Používat ani dále Zveřejňovat Chráněné Zdravotní Informace jinak, než jak je povoleno nebo vyžadováno touto smlouvou BAA nebo zákonem.

2.2. Obchodní Partner souhlasí s tím, že bude používat vhodná ochranná opatření a případně dodržovat Podčást C 45 CFR § 164, pokud jde o elektronické PHI, aby zabránil použití nebo zpřístupnění PHI jiným způsobem, než jak je stanoví tato BAA nebo Smlouva; strany však uznávají a souhlasí s tím, že za splnění požadavků podle 45 CFR § 164.312 na zavedení šifrovacích nebo dešifrovacích mechanismů pro elektronické PHI uchovávané na fyzických médiích (např. páskách) uložených Zákazníkem u Obchodního Partnera odpovídá Zákazník, nikoli Obchodní Partner.

2.3. Obchodní Partner se zavazuje neprodleně oznámit Zákazníkovi jakýkoli Bezpečnostní Incident, Porušení nebo jiné Použití či Zpřístupnění PHI, o kterém se dozví, a které není povoleno nebo vyžadováno touto BAA nebo Smlouvou. V případě Porušení musí být toto oznámení učiněno v souladu s Pravidly HIPAA a tak, jak je požadováno po obchodním partnerovi, mimo jiné v souladu s 45 CFR 164.410, ale v žádném případě ne později než tři (3) pracovní dny poté, co Obchodní Partner dokončil své interní šetření a potvrdil, že k Porušení došlo. Obchodní Partner poskytne při vyšetřování takového Porušení náležitou pomoc a spolupráci a zdokumentuje konkrétní Úložiště, která byla ohrožena, totožnost případné neoprávněné třetí strany, která mohla získat přístup k PHI nebo je získala, a opatření, která podnikl Obchodní Partner s cílem zmírnit dopad takového Porušení.

2.4. V souladu s 45 CFR 164.502(e)(1)(ii) a 164.308(b)(2), podle potřeby, Obchodní Partner zajistí, aby kdokoli z obchodních partnerů, který je subdodavatelem a vytváří, přijímá, uchovává nebo předává PHI jeho jménem za účelem pomoci při poskytování Služeb podle Smlouvy, souhlasil se stejnými

omezeními, podmínkami a požadavky, které se vztahují Obchodního Partnera v souvislosti s těmito PHI prostřednictvím této smlouvy BAA.

2.5. Pokud má Obchodní Partner v souvislosti s Osobami PHI ve své péči jako Určený Záznamový Soubor a Zákazník o ně požádá, zavazuje se Obchodní Partner poskytnout Zákazníkovi přístup tak, že získá a dodá tyto PHI v souladu s podmínkami Smlouvy, aby Zákazník mohl odpovědět Osobě a splnil tak požadavky 45 CFR §164.524.

2.6. Obchodní Partner souhlasí s tím, že pokud je vyžadována oprava PHI, které má ve své péči jako Určený Záznamový Soubor, a Zákazník Obchodnímu Partnerovi nařídí, aby poskytl tyto PHI v souladu se Smlouvou, Obchodní Partner provede takovou službu, aby Zákazník mohl provést změny těchto PHI, které může vyžadovat Zákazník nebo Osoba podle 45 CFR §164.526.

2.7. Obchodní Partner souhlasí s tím, že zdokumentuje a zpřístupní Zákazníkovi informace potřebné k vyúčtování Zpřístupnění PHI za předpokladu, že Zákazník mu poskytne dostatečné informace k tomu, aby určil, které záznamy nebo údaje přijaté od Zákazníka nebo jeho jménem obsahují PHI. Dokumentace o Zpřístupnění bude obsahovat takové informace, které by vyžadoval Zákazník, aby reagoval na žádost Osoby o vyúčtování Zpřístupnění PHI v souladu s 45 CFR §164.528 nebo jinými ustanoveními pravidel HIPAA.

2.8. Není-li ve Smlouvě výslovně dohodnuto jinak, Obchodní Partner neprodleně oznámí Zákazníkovi žádosti Osob o přístup k PHI, jejich znalost nebo opravu, aniž by na takové žádosti reagoval, a Zákazník ponese odpovědnost za přijetí a reakci na takové žádosti těchto Osob.

2.9. V rozsahu, v jakém má Obchodní Partner splnit jednu nebo více povinností Zákazníka podle Podčásti E zákona 45 CFR § 164, musí dodržet požadavky Podčásti E, které se vztahují na Zákazníka při plnění takových povinností.

2.10. Obchodní Partner souhlasí s tím, že zpřístupní své interní postupy, knihy a záznamy Tajemníkovi za účelem určení souladu s Pravidly HIPAA.

3. POVOLENÁ POUŽITÍ A ZPŘÍSTUPNĚNÍ OBCHODNÍM PARTNEREM

3.1. Obchodní Partner může používat nebo zpřístupňovat PHI podle potřeby k provádění Služeb uvedených ve Smlouvě.

3.2. Obchodní Partner může používat nebo zpřístupňovat PHI v souladu se zákonem.

3.3. Obchodní Partner souhlasí s tím, že vynaloží přiměřené úsilí k omezení PHI na minimum nezbytné k dosažení zamýšleného účelu Použití, Zpřístupnění nebo žádosti.

3.4. Obchodní Partner nesmí používat ani zpřístupňovat PHI způsobem, který by porušil Podčást E zákona 45 CFR §164, pokud tak učiní Zákazník.

3.5. Obchodní Partner může Zpřístupnit PHI za účelem svého řádného řízení a správy nebo plnění svých zákonných povinností za předpokladu, že Zpřístupnění je vyžadováno zákonem nebo že Obchodní Partner získá od osoby, které jsou informace zpřístupněny, přiměřené ujištění, že informace zůstanou důvěrné a budou použity nebo dále zpřístupněny pouze v souladu se zákonem nebo pro účely, pro které byly osobě sděleny, a že tato osoba Obchodnímu Partnerovi oznámí všechny případy, o nichž ví, že byla porušena důvěrnost informací.

4. POVINNOSTI ZÁKAZNÍKA

4.1. Zákazník nesmí dát Obchodnímu Partnerovi pokyn, aby jednal způsobem, který není v souladu s Pravidly HIPAA.

4.2. Zákazník je povinen informovat Obchodního Partnera o jakémkoli omezení ve svém oznámení o postupech v oblasti ochrany soukromí Zákazníka v souladu s 45 CFR §164.520, v rozsahu, v jakém může mít takové omezení vliv na Používání nebo Zpřístupnění PHI Obchodním Partnerem.

4.3. Zákazník je povinen informovat Obchodního Partnera o změnách nebo odvolání souhlasu Osoby s Použitím nebo Zpřístupněním svých PHI v rozsahu, v jakém mohou mít takové změny vliv na Používání nebo Zpřístupnění PHI Obchodním Partnerem.

4.4. Zákazník písemně oznámí Obchodnímu Partnerovi veškerá omezení týkající se Používání nebo Zpřístupnění PHI, s nimiž Zákazník souhlasil v souladu s 45 CFR §164.522, v rozsahu, v jakém může mít toto omezení vliv na Používání nebo Zpřístupnění PHI Obchodním Partnerem.

5. DOBA A UKONČENÍ PLATNOSTI

5.1. Doba platnosti této smlouvy BAA začíná Datem Účinnosti a končí automaticky, jakmile nastane některá z pozdějších následujících situací: (i) vypršení platnosti Smlouvy nebo (ii) když budou zničeny nebo vráceny Zákazníkovi všechny PHI, které Zákazník poskytl Obchodnímu Partnerovi.

5.2. Pokud se některá smluvní strana dozví o závažném porušení smlouvy BAA, poskytne smluvní strana, která porušení nezpůsobila druhé smluvní straně možnost toto porušení napravit. Pokud porušující strana toto porušení nenapraví do třiceti (30) od obdržení písemného oznámení druhé smluvní strany uvádějící podrobnosti o takovém závažném porušení, má neporušující strana právo vypovědět tuto BAA a Smlouvu podle podmínek Smlouvy nebo, není-li ukončení proveditelné, má právo oznámit problém Tajemníkovi nebo jinému příslušnému orgánu.

5.3. <u>Účinek ukončení:</u>

5.3.1.1. S výjimkou případů uvedených níže v bodě 5.3.2 po ukončení této smlouvy BAA z jakéhokoli důvodu Obchodní Partner vrátí nebo zničí všechny PHI obdržené od Zákazníka v souladu se Smlouvou. Toto ustanovení se vztahuje na PHI, které jsou v

držení subdodavatelů nebo zástupců Obchodního Partnera. Obchodní Partner si nesmí ponechat žádné kopie PHI.

5.3.1.2. V případě, že Obchodní Partner zjistí, že vrácení nebo zničení PHI je neproveditelné, oznámí Zákazníkovi podmínky, které to znemožňují. Na základě oznámení Zákazníkovi Obchodní Partner rozšíří ochranu této BAA na takové PHI a omezí jejich další Použití a Zpřístupnění na ty účely, kvůli nimž je navrácení nebo zničení neproveditelné, dokud takové PHI udržuje v souladu s podmínkami Smlouvy.

6. RŮZNÉ

6.1. Zbavení odpovědnosti. Obchodní Partner souhlasí s tím, že Zákazníka zbaví odpovědnosti za pokuty nebo penále, které byly Zákazníkovi uloženy v důsledku donucovacího řízení zahájeného Tajemníkem nebo které proti němu zahájil státní generální právní zástupce v občanskoprávním řízení a které je výsledkem řízení nebo žaloby přímo a výhradně vyplývající z jednání nebo opomenutí Obchodního Partnera a je buď porušením Pravidel HIPAA, nebo závažným porušením této smlouvy BAA (dále jen „Nárok“). Obchodní Partner není povinen Zákazníka zbavit odpovědnosti za část těchto pokut nebo sankcí vyplývajících z (i) porušení Pravidel HIPAA nebo této smlouvy BAA Zákazníkem nebo (ii) nedbalostního nebo úmyslného jednání či opomenutí Zákazníka. Výše uvedená povinnost zbavení odpovědnosti je výslovně podmíněna tím, že Zákazník Obchodnímu Partnerovi udělí právo, na základě jeho volby a na náklady a s právním zástupcem podle vlastního výběru, kontrolovat nebo se podílet na obraně proti takovému Nároku, avšak za předpokladu, že v rozsahu, v jakém je takový Nárok součástí rozsáhlejšího řízení nebo žaloby, právo Obchodního Partnera na kontrolu nebo účast je omezeno pouze na Nárok, nikoli na rozsáhlejší řízení nebo žalobu. V případě, že Obchodní Partner využije své možnosti řídit obranu, pak i) nevypořádá pohledávku vyžadující přiznání zavinění ze strany Zákazníka bez jeho předchozího písemného souhlasu, ii) Zákazník má právo podílet se na nároku nebo žalobě na vlastní náklady a iii) Zákazník bude s Obchodním Partnerem podle přiměřených požadavků spolupracovat. Výše je uveden výhradní a výlučný prostředek nápravy Zákazníka a výhradní odpovědnost Obchodního Partnera za ztrátu, škodu, výdaje nebo odpovědnost Zákazníka v souvislosti s Nároky souvisejícími s touto smlouvou BAA.

6.2. Soudní příkaz zdržet se jednání. Obchodní Partner bere na vědomí, že neoprávněné Použití nebo Zpřístupnění PHI Obchodním Partnerem může Zákazníkovi způsobit nenapravitelnou škodu, na základě čehož je podle vlastního rozhodnutí oprávněn usilovat o soudní příkaz ke zdržení se jednání nebo o jinou spravedlivou úlevu.

6.3. Regulační odkazy. Odkazem na část Pravidel HIPAA v této BAA se rozumí část HIPAA, Pravidla o ochraně soukromí, Bezpečnostního pravidla, Zákona HITECH nebo závěrečných Souhrnných pravidel v platném a účinném znění, jejíž dodržování je vyžadováno.

6.4. Změny. Smluvní strany se dohodly, že budou v dobré víře jednat o změnách této smlouvy BAA, které mohou být čas od času vyžadovány, aby Zákazník nebo Obchodní Partner splňovali požadavky Pravidel HIPAA. Pokud smluvní strany nedosáhnou vzájemné dohody o podmínkách takové změny do šedesáti (60) dnů od data obdržení takové písemné žádosti předložené Zákazníkem Obchodnímu Partnerovi, má kterákoli ze smluvních stran právo ukončit tuto BAA a Smlouvu na základě písemné výpovědi doručené druhé straně nejméně třicet (30) dnů předem.

6.5. Žádné oprávněné třetí strany. Nic z toho, co je v této smlouvě BBA vyjádřeno nebo naznačeno, nemá zakládat ani nezakládá práva, prostředky nápravy, povinnosti ani odpovědnost jiným osobám než Zákazníkovi, Obchodnímu Partnerovi a jejich příslušným nástupcům nebo postupníkům.

6.6. Nezávislý dodavatel. Obchodní Partner, včetně svých ředitelů, vedoucích pracovníků, zaměstnanců a zástupců, je nezávislým dodavatelem a není zástupcem (jak je definován ve federálním obecném právu o zastupování) Zákazníka ani jedním z jeho zaměstnanců. Aniž by tím byla omezena obecnost výše uvedeného bodu, Zákazník nemá právo ovládat, řídit ani jinak ovlivňovat jednání Obchodního Partnera při poskytování služeb jinak než prostřednictvím prosazování této BAA nebo Smlouvy či jejich vzájemných změn.

6.7. Priorita, úplná dohoda. Jakékoli nejasnosti v této smlouvě BAA budou řešeny tak, aby smluvní strany dodržely Pravidla HIPAA. Tato smlouva BAA představuje úplnou dohodu mezi stranami, pokud jde o její předmět, a nahrazuje veškerou předchozí komunikaci, prohlášení, dohody a ujednání týkající se Pravidel HIPAA, včetně veškerých předchozích dohod o společném podniku mezi stranami.