Ugovor o obradi podataka

SVRHA I RASPORED PO PRVENSTVU

Ovaj Ugovor o obradi podataka, zajedno s njegovim prilozima i svim dokumentima izričito je unakrsno-referencirano ("**DPA**"), smatra se dijelom ugovora o uslugama između Iron Mountaina i Korisnika ("**Ugovor**"). Odredbe i uvjeti Ugovora primjenjuju se i njima se uređuju prava i obveze stranaka prema ovom DPA.

Ako su bilo koje odredbe i uvjeti sadržani u ovom DPA u suprotnosti s odredbama i uvjetima navedenim u Ugovoru, odredbe i uvjeti navedeni u ovom DPA bit će kontrolne odredbe i uvjeti u odnosu na predmet ovog DPA. Ovaj DPA nadjačava i zamjenjuje sve prethodne ugovore o obradi podataka ili klauzule o zaštiti podataka ili privatnosti između stranaka u vezi s Uslugama koje se pružaju prema Ugovoru.

OPĆI UVJETI

1. DEFINICIJE

Osim ako nije izričito definirano ovdje, svi izrazi napisani velikim slovima imat će ista značenja koja su im dana u Ugovoru.

"**Voditelj obrade podataka**" označava fizičku ili pravnu osobu, javno tijelo, agenciju ili drugo tijelo koje, samostalno ili zajedno s drugima, određuje svrhe i načine obrade osobnih podataka;

"**Osobni podaci korisnika**" znači Osobni podaci koji pripadaju ili su prikupljeni od stranke Korisnika ili njegovih podružnica Obrađenih kao dio Usluga;

"**Subjekt podataka**" označava identificiranu ili fizičku osobu koja se može identificirati;

"Zakoni o zaštiti podataka" znači sve primjenjive zakone i propise koji se odnose na obradu osobnih podataka koji mogu postojati u relevantnim jurisdikcijama, uključujući, ali ne ograničavajući se na, EU GDPR (Uredba (EU) 2016/679), UK GDPR (GDPR primjenjiv kao dio domaćeg zakona Ujedinjenog Kraljevstva na temelju odjeljka 3 Zakona o (povlačenju) Europske unije iz 2018. i izmijenjenog i dopunjenog Uredbama o zaštiti podataka, privatnosti i elektroničkim komunikacijama (amandmani itd.) (izlazak iz EU) iz 2019. (s izmjenama i dopunama)), zaštita podataka Zakon iz 2018., FADP (Švicarski savezni zakon o zaštiti podataka), Državni zakoni SAD-a o privatnosti, LGPD (Brazilski opći zakon o zaštiti podataka), PIPL (Zakon o zaštiti osobnih podataka Narodne Republike Kine) i svi zakoni i/ili propisi koji ih provode ili donose u skladu s njima, ili koji mijenjaju, zamjenjuju, ponovno donose ili konsolidira bilo koji od njih, uključujući, gdje je primjenjivo, vodič i kodekse prakse koje izdaju nadzorna tijela;

"**Osobni podaci**" znači sve informacije koje se odnose na subjekta podataka;

"**Obrađivač podataka**" označava fizičku ili pravnu osobu, javno tijelo, agenciju ili drugo tijelo koje obrađuje osobne podatke u ime Voditelja obrade podataka;

"**Obrada**" je svaka radnja ili skup radnji koji se izvršava kakve osobne podatke ili i predmeta Osobnim podacima, bez obzira obavlja li se automatizirano ili ne, kao što je prikupljanje, bilježenje, organizaciju, strukturiranje, pohranu, prilagodbu ili izmjenu, povrat, savjetovanje, uporabu, otkrivanje prijenosom, priopćavanje ili stavljanje na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

"**Povreda sigurnosti**" znači svako slučajno ili nezakonito oštećenje, uništenje, gubitak, izmjenu ili neovlašteno otkrivanje ili pristup Osobnim podacima korisnika koje Iron Mountain, njegovo osoblje ili podizvođači obrađuju tijekom pružanja Usluga;

"**Usluge**" označava sve usluge koje Iron Mountain ili njegove podružnice pružaju Korisniku ili njegovim podružnicama prema Ugovoru;

"**Državni zakoni SAD-a o privatnosti**" označava sve državne zakone Sjedinjenih Država o privatnosti i zaštiti podataka koji su primjenjivi na obradu osobnih podataka prema Ugovoru, uključujući bez ograničenja, i koji se mogu povremeno izmijeniti ili zamijeniti: (1) Kalifornijski zakon o privatnosti potrošača, s izmjenama i dopunama

Kalifornijskim zakonom o pravima na privatnost, i svi provedbeni propisi koji se odnose na isti (zajedno, "**CCPA**"); (2) Zakon o privatnosti u Coloradu ("**CPA**"), (3) Zakon o zaštiti podataka potrošača Virginije ("**CDPA**"); (4) Zakon o zaštiti privatnosti potrošača Utaha ("**UCPA**"); i (5) Zakon o zaštiti podataka u Connecticutu ("**CTDPA**").

2. OPSEG I DETALJI OBRADE PODATAKA

2.1 Ovaj DPA primjenjivat će se na Osobne podatke korisnika koje obrađuje Iron Mountain kao izvršitelj obrade podataka tijekom pružanja Usluga prema Ugovoru u ime Korisnika.

2.2 Iron Mountain može prikupljati i obrađivati osobne podatke Korisnika i zzaposlenika njegovih podružnica kao Voditelj obrade podataka u legitimne poslovne svrhe, kao što je upravljanje ugovorima i odnosima s klijentima, te u skladu sa Zakonom o zaštiti podataka i Obavijesti o privatnosti tvrtke Iron Mountain dostupne na web stranicama Iron Mountain i drugim primjenjivim politikama privatnosti. Obveze tvrtke Iron Mountain navedene u ovom DPA neće se primjenjivati na obradu takvih osobnih podataka.

2.3 Predmet obrade osobnih podataka je izvedba Usluga. Prava i obveze Korisnika i Iron Mountaina navedeni su u ovom DPA. Dodatak 1 ovog DPA utvrđuje prirodu, trajanje i svrhu obrade, vrste obrade Osobnih podataka korisnika Iron Mountaina, procese i kategorije subjekata podataka čiji se osobni podaci obrađuju.

2.4 Kada Iron Mountain obrađuje Osobne podatke korisnika tijekom pružanja usluga, Iron Mountain će:

2.4.1 obrađivati Osobne podatke korisnika samo u skladu s dokumentiranim uputama Korisnika. Ako se od tvrtke Iron Mountain zahtijeva obrada Osobnih podataka korisnika u bilo koju drugu svrhu prema zakonu kojem podliježe Iron Mountain, Iron Mountain će prvo obavijestiti Korisnika o ovom zahtjevu, osim ako takav zakon(i) to zabranjuje(u) zbog važnih razloga od javnog interesa; i

2.4.2 Uvijek se pridržavajte važećih zakona o zaštiti podataka i odmah obavijestite Korisnika ako, po mišljenju tvrtke Iron Mountain, upute za obradu Osobnih podataka korisnika koje je dao Korisnik krše važeće zakone o zaštiti podataka.

2.5 Upute Korisnika bit će obvezujuće za tvrtku Iron Mountain osim ako izvršenje uputa zahtijeva pružanje usluge prema Ugovoru, a Korisnik ne pristaje platiti naknade za usluge za takve usluge.

2.6 Iron Mountain će osigurati da osoblje kojem je potreban pristup Osobnim podacima korisnika podliježe obvezujućoj obvezi povjerljivosti u pogledu takvih Osobnih podataka korisnika te poduzeti razumne korake kako bi se osigurala pouzdanost i kompetentnost osoblja Iron Mountaina koje ima pristup Osobnim podacima korisnika.

3. PRUŽANJE KORISNIČKE POMOĆI

3.1 Iron Mountain će pružiti pomoć Korisniku, uvijek uzimajući u obzir prirodu Obrade:

3.1.1 odgovarajućim tehničkim i organizacijskim mjerama i u mjeri u kojoj je to moguće, u ispunjavanju obveza Korisnika da odgovori na zahtjeve Subjekata podataka koji ostvaruju svoja prava;

3.1.2 u osiguravanju usklađenosti s obvezama Korisnika (kao što je sigurnost obrade, obavijest nadzornom tijelu o povredi osobnih podataka, obavještavanje subjekta podataka o povredi osobnih podataka, procjena učinka zaštite podataka i prethodno savjetovanje s nadzornim tijelima kada bi obrada dovesti do visokog rizika u nedostatku mjera koje je voditelj obrade podataka poduzeo za ublažavanje rizika), uzimajući u obzir informacije dostupne Iron Mountainu; i

3.1.3 stavljanjem na raspolaganje Korisniku svih informacija koje Korisnik razumno zahtijeva kako bi Korisniku omogućio da dokaže ispunjavanje svojih obveza pri odabiru i imenovanju Iron Mountaina.

4. SIGURNOSNE MJERE

4.1 Uzimajući u obzir uobičajene operativne postupke, troškove provedbe i prirodu, opseg, kontekst i svrhe obrade, Iron Mountain će provesti odgovarajuće i razumne tehničke i organizacijske mjere namijenjene zaštiti povjerljivosti, integriteta i dostupnosti Osobnih podataka korisnika i radi zaštite Osobnih podataka korisnika od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja, oštećenja, izmjene ili otkrivanja. Sigurnosni standardi tvrtke Iron Mountain navedeni su u Dodatku 2 ovog DPA.

4.2 Isključiva je odgovornost Korisnika da ocijeni zadovoljavaju li ove tehničke i organizacijske mjere zahtjeve Korisnika.

5. USKLAĐENOST SA ZAKONIMA

Korisnik i njegov podružnice će: (i) Obrađivati Osobne podatke korisnika u skladu sa Zakonom o zaštiti podataka; (ii) biti ovlašteni za davanje pisanih uputa tvrtki Iron Mountain o obradi Osobnih podataka korisnika u vezi s uslugama (uključujući u ime bilo kojeg subjekta treće strane koji je voditelj obrade Osobnih podataka korisnika); i (iii) u svakom trenutku zadržati kontrolu i ovlasti nad Osobnim podacima korisnika u vezi s Obradom.

6. PODOBRADA

6.1 Korisnik potvrđuje i slaže se da Iron Mountain može angažirati svoju matičnu tvrtku, svoje podružnice i druge podizvršitelje obrade trećih strana (uključujući podizvršitelje obrade trećih strana koje angažiraju Iron Mountainove podružnice ili matična tvrtka) u svrhu obrade Osobnih podataka korisnika prema ovom DPA podložno klauzuli 6.2 u nastavku.

6.2 Popis podizvršitelja obrade koje je Korisnik odobrio od datuma ovog DPA je dostupan ovdje[1]. Iron Mountain može u bilo kojem trenutku zamijeniti ili imenovati novog podizvršitelja obrade pod uvjetom da je Korisnik petnaest (15) dana unaprijed pismeno obaviješten i da se Korisnik ne protivi takvim promjenama na dokazivim osnovama u vezi sa zaštitom podataka unutar tog vremenskog okvira. Kako bi primao ove obavijesti e-poštom, Korisnik će se pretplatiti i upravljati postojećom pretplatom na uslugu obavijesti Iron Mountain putem ove web stranice[2].

6.3 Ako se Korisnik ne uspije pretplatiti na ovu uslugu obavijesti, Iron Mountain neće biti odgovoran za nedostatak obavijesti podizvršitelja obrade i sva takva imenovanja smatrat će se ovlaštenima od strane Korisnika**.** Ako se Korisnik pismeno na dokazivim osnovama koje se odnose na zaštitu podataka usprotivi imenovanju zamjene ili novog podizvršitelja obrade unutar petnaest (15) dana prije pisane obavijesti, tada će tvrtka Iron Mountain poduzeti razumne napore kako bi Korisniku omogućio promjenu u Uslugama ili preporučiti promjenu Korisnikove konfiguracije ili upotrebe Usluga, u svakom slučaju kako bi se izbjegla obrada Osobnih podataka korisnika od strane podizvršitelja obrade kojem je uložen prigovor na razmatranje i odobrenje Korisnika. Ako Korisnik ne odobri takve promjene koje je predložio Iron Mountain u roku od petnaest (15) dana, Iron Mountain može, davanjem pismene obavijesti Korisniku, odmah prekinuti Uslugu ili dio Usluge koji Iron Mountain ne može pružiti bez korištenja Podizvršitelja obrade za kojeg je uložen prigovor. Takav raskid ne dovodi u pitanje bilo koja stečena prava i obveze stranaka, pod uvjetom da Iron Mountain ili njegove podružnice neće platiti nikakve naknade za raskid, troškove ili drugu naknadu u vezi s takvim raskidom i Korisnik će odmah preuzeti imovinu koju je dao Iron Mountainu kao dio prekinutih Usluga, podložno uvjetima Ugovora i o vlastitom trošku Korisnika.

6.4 Iron Mountain će osigurati da bilo koji ugovor s Podizvršiteljima obrade u opsegu ovog DPA sadrži odredbe koje su u svim suštinskim aspektima iste kao one u ovom DPA i u skladu s važećim zakonima o zaštiti podataka. Ako Podizvršitelj obrade Iron Mountaina prouzroči da Iron Mountain prekrši svoje obveze prema ovom DPA ili bilo kojem primjenjivom zakonodavstvu o zaštiti podataka, Iron Mountain će ostati u potpunosti odgovoran Korisniku za ispunjenje obveza Iron Mountaina prema ovim uvjetima.

7. POVREDE SIGURNOSTI

7.1 U slučaju sumnje na povrede sigurnosti, Iron Mountain će:

7.1.1 odmah poduzeti mjere za istraživanje sumnje na povredu sigurnosti i identificiranje, sprječavanje i ublažavanje učinaka sumnje na povredu sigurnosti i otklanjanje povrede sigurnosti;

7.1.2 obavijestiti Korisnika bez nepotrebnog odgađanja nakon što ima razuman stupanj sigurnosti da je došlo do povrede sigurnosti i pružiti Korisniku detaljan opis povrede sigurnosti uključujući informacije koje su razumno potrebne da bi Korisnik ispunio obveze izvješćivanja prema Zakonu o zaštiti podataka.

7.2 Korisnik se slaže da Iron Mountain može pružiti informacije prema klauzuli 7.1.2 u fazama. U takvim slučajevima kada Iron Mountain nema pristup ili ne može pružiti određene informacije navedene u klauzuli 7.1.2 Korisniku, Iron Mountain će obavijestiti Korisnika u skladu s tim i Iron Mountain neće snositi nikakvu odgovornost za nedostavljanje takvih informacija.

8. REVIZIJE

Iron Mountain će dopustiti Korisniku i njegovim odgovarajućim revizorima ili ovlaštenim agentima, nakon pružanja obavijesti u roku od najmanje deset (10) radnih dana Iron Mountainu za provođenje revizija ili inspekcija tijekom trajanja Ugovora, pod uvjetom da se od Iron Mountaina neće zahtijevati pružanje ili dopuštanje pristupa informacijama koje se tiču: (i) ostalih korisnika Iron Mountaina; (ii) svih nejavnih vanjskih izvješća Iron Mountaina; i (iii) svih internih izvješća sastavljenih od strane interne revizije ili odjela za usklađenost tvrtke Iron Mountain. Svrha revizije ili inspekcije u skladu s ovom klauzulom bit će ograničena na provjeru obrađuje li Iron Mountain Osobne podatke korisnika u skladu sa svojim obvezama prema ovom DPA. Osim u slučajevima kada je došlo do povrede sigurnosti, neće se provesti više od jedne takve revizije u bilo kojem razdoblju od dvanaest (12) mjeseci.

---

[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=

9. MEĐUNARODNI PRIJENOSI PODATAKA (OGRANIČENI PRIJENOSI)

9.1 U mjeri u kojoj je to primjenjivo, Korisnik ovime pristaje i odobrava međunarodne prijenose Osobnih podataka korisnika subjektima kako je navedeno u odjeljku 6.2 i u skladu s Dodatkom 3 za pružanje Usluga, a Korisnik i Iron Mountain su suglasni da:

9.1.1 se pridržavaju važećih zakona o zaštiti podataka u vezi s takvim prijenosima;

9.1.2 uzimaju u obzir, bez ograničenja, i) kategorije Osobnih podataka korisnika, ii) zemlje čiji nacionalni zakoni možda ne pružaju razinu zaštite Osobnih podataka koja je usporediva s onima iz zakona EU/UK ("**Treća zemlja**") u opsegu, iii) relevantne tehničke i organizacijske mjere navedene u Odjeljku 7 i iv) relevantne stranke koje sudjeluju u obradi takvih Osobnih podataka korisnika, provele su procjenu prikladnosti relevantnog mehanizma prijenosa koji je ovdje usvojen kada to zahtijeva zakon i utvrdili da je takav mehanizam prijenosa prikladno osmišljen kako bi se osiguralo da Osobni podaci koji se prenose u skladu s ovim DPA imaju razinu zaštite u odredišnoj zemlji koja je u biti jednaka onoj zajamčenoj prema Zakonu o zaštiti podataka.

10. ODGOVORNOST I NAKNADA ŠTETE

10.1 Bez obzira na sve što je u suprotnosti u Ugovoru, u slučaju povrede sigurnosti uzrokovane izravno kršenjem obveza Iron Mountaina prema ovom DPA, Iron Mountain će nadoknaditi Korisniku u mjeri dopuštenoj primjenjivim zakonom za izravne, provjerljive, potrebne i razumno nastale troškove treće strane Korisnika u (a) istrazi takve povrede sigurnosti, (b) pripremi i slanju obavijesti takvim Subjektima podataka i regulatornim tijelima u skladu sa Zakonom o zaštiti podataka, (c) pružanje usluga kreditnog praćenja takvim pojedincima u skladu sa zakonom u razdoblju koje ne prelazi dvanaest (12) mjeseci i (d) plaćanje dijela regulatornih kazni, naknada ili sankcija koje je izreklo nadzorno tijelo za koje nadzorno tijelo navodi da je Iron Mountain izravno odgovoran.

10.2 U slučaju da subjekt podataka podnese tužbu protiv jedne ili obje stranke zbog navodnog kršenja zakona o zaštiti podataka ("**Potraživanja subjekta podataka**") kada je to dopušteno, svaka će stranka kontrolirati vlastitu obranu od bilo koje takve tužbe (ili svog dijela obrane) i ostaje isključivo odgovorna za vlastite troškove, izdatke i obveze u vezi s time, uključujući pravne troškove ili bilo koje iznose koji joj se dodjeljuju od strane suda ili u nagodbi, međutim, pod uvjetom da je svaka stranka odgovorna za dio ili je bilo koja stranka odgovorna za puni iznos štete koju je Subjekt podataka pretrpio za isti incident ili niz incidenata i Subjekt podataka je dobio punu naknadu od samo jedne stranke ("**Stranka koja daje odštetu**"), onda će Stranka koja daje odštetu imati pravo tražiti povrat od druge stranke onaj dio naknade koji odgovara šteti koju je prouzročila ta druga stranka. Stranka koja daje odštetu može podnijeti zahtjev drugoj stranci samo u roku od 12 mjeseci nakon incidenta, u mjeri dopuštenoj važećim zakonom.

10.3 U najvećoj mjeri dopuštenoj važećim zakonima, ograničenja odgovornosti i sva isključenja od šteta navedenih u Ugovoru uređuju ukupnu odgovornost Iron Mountaina za sva potraživanja Korisnika koja proizlaze iz ili su povezana s ovim DPA i/ili Ugovorom. Ova ograničenja odgovornosti i isključenja od šteta primjenjuju se na sve zahtjeve, bilo da proizlaze iz ugovora, prekršaja ili bilo koje druge teorije odgovornosti, a svako pozivanje na odgovornost tvrtke Iron Mountain znači ukupnu odgovornost tvrtke Iron Mountain i svih njezinih podružnica zajedno za potraživanja od strane Korisnika i svih drugih podružnica Korisnika. U mjeri u kojoj to zahtijevaju primjenjivi zakoni, ovaj odjeljak nema namjeru (i) mijenjati ili ograničavati odgovornost stranaka za Potraživanja subjekta podataka protiv stranke kada postoji zajednička i solidarna odgovornost ili (ii) ograničavati odgovornost bilo koje stranke za plaćanje kazne koje je takvoj stranci izreklo regulatorno tijelo.

10.4 Članci 10.1 do 10.3 navode jedini i isključivi pravni lijek svake stranke i isključivu odgovornost svake stranke za gubitak, štetu, trošak ili odgovornost u vezi s ovim DPA.

11. ZAHTJEVI JAVNE VLASTI

11.1 U mjeri u kojoj je to zakonski dopušteno i podložno klauzulama 11.2 do 11.5 u nastavku, Iron Mountain pristaje obavijestiti Korisnika ako:

11.1.1 primi pravno obvezujući zahtjev od javnog tijela, uključujući pravosudna tijela, prema zakonima odredišne zemlje za otkrivanje Osobnih podataka korisnika prenesenih u skladu s Ugovorom; ili

11.1.2 postane svjestan bilo kakvog izravnog pristupa javnih tijela prenesenim Osobnim podacima korisnika na temelju Ugovora u skladu sa zakonima zemlje odredišta.

11.2 Ako je tvrtki Iron Mountain zabranjeno obavijestiti Korisnika u skladu sa zakonima zemlje odredišta, Iron Mountain pristaje uložiti sve moguće napore da postigne odricanje od zabrane, s ciljem priopćavanja što više informacije što je prije moguće.

11.3 Tvrtka Iron Mountain suglasna je preispitati zakonitost zahtjeva za otkrivanje, posebice ostaje li on u okviru ovlasti koje su dane javnom tijelu koje je podnijelo zahtjev, te osporiti zahtjev ako na razumnoj osnovi zaključi da zahtjev nezakonit prema zakonima zemlje odredišta. Neće otkriti tražene Osobne podatke korisnika sve dok to ne bude potrebno u skladu s primjenjivim pravilima postupaka.

11.4 Tvrtka Iron Mountain pristaje pružiti minimalnu količinu informacija koja je dopuštena kada odgovara na zahtjev za otkrivanje, na temelju razumnog tumačenja zahtjeva.

11.5 Tvrtka Iron Mountain pristaje čuvati podatke u skladu sa stavcima (a) do (c) za vrijeme trajanja Ugovora te ih na zahtjev staviti na raspolaganje nadležnom nadzornom tijelu.

12. RAZNO

12.1 Ovisno o prirodi usluga koje pruža tvrtka Iron Mountain, po raskidu/isteku Ugovora, na temelju posebnih uputa Korisnika i podložno uvjetima Ugovora, Iron Mountain će izbrisati/uništiti ili vratiti Korisniku ili trećoj strani koju je Korisnik odredio sve Osobne podatke korisnika. Svi Osobni podaci korisnika sadržani unutar sredstava Korisnika koje Iron Mountain pohranjuje u njegovo ime bit će mu vraćeni u skladu s dogovorenim izlaznim ili tranzicijskim planom i podložno dogovorenim troškovima, kako je navedeno u Ugovoru ili drugom važećem ugovornom dokumentu. U svim drugim slučajevima ako se Ugovorom ne spominje brisanje/uništenje ili povrat Osobnih podataka korisnika i Korisnik ne pruži nikakve upute u vezi s brisanjem/uništenjem ili vraćanjem Osobnih podataka korisnika u roku od petnaest (15) dana od raskida/isteka Ugovora, Iron Mountain će poslati pisanu obavijest Korisniku tražeći da primi u roku od 15 (petnaest) dana s posebnim uputama da li izbrisati/uništiti ili vratiti Osobne podatke korisnika i informirati Korisnika o svim primjenjivim naknadama za sigurno uništavanje ili drugim naknadama koje Korisnik plaća. Ako Korisnik ne dostavi pisane upute u roku od petnaest (15) dana i ne plati primjenjive naknade unutar istog razdoblja, Korisnik ovime ovlašćuje Iron Mountain da dalje obrađuje, briše, uništava sve Osobne podatke korisnika nakon prestanka Ugovora po izboru Iron Mountaina i na trošak Korisnika.

12.2 Bez obzira na klauzulu 12.1, Iron Mountain neće prekršiti svoje obveze u pogledu brisanja Osobnih podataka korisnika koji se čuvaju na sigurnosnim kopijama sve dok se takve sigurnosne kopije poništavaju (a time i Osobni podaci korisnika brišu) u uobičajenom tijeku poslovanja.

12.3 Osim standardnih ugovornih klauzula (kao što je definirano u Dodatku 3 ovog DPA), ovaj DPA i svaki spor, zahtjev ili kontroverza proizašli iz ili u vezi s ovim DPA, ili njegovo kršenje, raskid ili valjanost, regulirani su izborom zakonske odredbe Ugovora; a svaki spor, kontroverza ili zahtjev koji proizlazi iz ili u vezi s ovim DPA prvenstveno će se nastojati riješiti kroz bilo koji definirani postupak rješavanja sporova sadržan u Ugovoru.

12.4 Svaka stranka može s vremena na vrijeme pismeno obavijestiti drugu stranku o svim izmjenama ovog DPA za koje stranka razumno smatra da su potrebne za rješavanje zahtjeva Zakona o zaštiti podataka ili bilo koje odluke nadzornog tijela ili suda. Sve takve izmjene stupaju na snagu samo ako i u mjeri navedenoj u međusobno dogovorenim izmjenama i dopunama ovog DPA koji su izvršile obje stranke, osim kada jedna stranka obavijesti drugu o bilo kakvom novom zakonskom zahtjevu i pošalje takve izmjene i dopune koje uključuju samo potrebne izmjene i koji se mogu prihvatiti bez formalnog pristanka na to, tj. ne podnoseći prigovor u određenom roku, smatraju se međusobno dogovorenim izmjenama i dopunama ovog DPA.

DODATAK 1

Pojedinosti o obradi i prijenosu podataka (ako je primjenjivo)

A. POPIS STRANAKA:

Stranke u ovom DPA i uloge Izvoznika podataka i Uvoznika podataka navedeni su u Ugovoru i Dodatku 3 (Međunarodni prijenosi podataka), ako je primjenjivo.

B. OPIS OBRADE/PRIJENOSA (ako je primjenjivo):

Kategorije subjekata podataka čiji se osobni podaci obrađuju/prenose:

Ovisno o prirodi usluga Iron Mountaina i poslovanju Korisnika, Korisnik može podnijeti Osobne podatke koji pripadaju različitim kategorijama ispitanika Iron Mountainu, čiji opseg određuje i kontrolira Korisnik prema vlastitom nahođenju. Kao takve, kategorije subjekata podataka mogu uključivati: bivše i sadašnje zaposlenike; bivše i sadašnje izvođače ili konzultante; izvođače ili konzultante koje osigurava agencija i vanjski ustupljene suradnike; kandidate za posao; studente i dobrovoljce; pojedince koje su zaposlenici ili umirovljenici identificirali kao korisnike, supružnike, obiteljske/građanske partnere, uzdržavane osobe i kontakte za hitne slučajeve; umirovljenike; bivše i sadašnje direktore i službenike; dioničare; vlasnike obveznica; vlasnike računa; krajnje korisnike/potrošače (odrasli, djeca); bolesnike (odrasli, djeca); prolaznike (CCTV kamere); i korisnike web stranice.

Kategorije osobnih podataka koji se obrađuju/prenose:

Ovisno o prirodi usluga Iron Mountaina i poslovanju Korisnika, Korisnik može podnijeti Osobne podatke koji pripadaju različitim kategorijama osobnih podataka Iron Mountainu, čiji opseg određuje i kontrolira Korisnik prema vlastitom nahođenju. Kao takve, kategorije mogu uključivati osobne podatke koji se odnose na Korisnika i/ili njegove vlastite klijente, zaposlenike itd.

Preneseni osjetljivi podaci (ako je primjenjivo):

Ovisno o prirodi usluga Iron Mountaina i poslovanju Korisnika, Korisnik može podnijeti osjetljive podatke Iron Mountainu, čiji opseg određuje i kontrolira Korisnik prema vlastitom nahođenju.

Ako je primjenjivo, učestalost prijenosa (npr. prenose li se podaci jednokratno ili kontinuirano):

Prijenos se odvija kontinuirano.

Priroda obrade:

Prikupljanje, evidentiranje, organizacija, strukturiranje, pohrana, prilagodba ili promjena, povrat, savjetovanje, uporaba, otkrivanje prijenosom, širenje ili na drugi način stavljanje na raspolaganje, usklađivanje ili kombinacija, ograničavanje, brisanje ili uništavanje.

Svrha(e) obrade/prijenosa podataka (ako je primjenjivo) i daljnja obrada:

Pružanje Usluga kako je navedeno u Ugovoru.

Zadržavanje podataka:

Iron Mountain će zadržati osobne podatke za vrijeme trajanja Usluga koje se nude korisniku i do trenutka kada se osobni podaci vrate ili unište kako je određeno u skladu s člankom 12.1 ovog DPA.

Ako je primjenjivo, za prijenose podizvršiteljima obrade, navedite predmet, prirodu i trajanje obrade:

Za vrijeme trajanja Ugovora s Korisnikom, Podizvršitelji obrade pružaju, između ostalog, usluge informacijske tehnologije (IT) i savjetodavne usluge, uključujući globalnu IT podršku, usluge izvještavanja o događajima i upravljanja.

C. NADLEŽNO NADZORNO TIJELO

Kako je navedeno u Dodatku 3 (Međunarodni prijenosi podataka), ako je primjenjivo.

DODATAK 2

TEHNIČKE I ORGANIZACIJSKE MJERE ("SIGURNOSNE MJERE")

1. PROGRAM I POLITIKA INFORMACIJSKE SIGURNOSTI

Iron Mountain će održavati program informacijske sigurnosti s odgovarajućim fizičkim, tehničkim i administrativnim kontrolama koje su dizajnirane da zadovolje industrijske standarde. Program informacijske sigurnosti uključuje:

1.1 Dokumentaciju, internu publikaciju i komunikaciju politika, standarda i postupaka informacijske sigurnosti Iron Mountaina;

1.2. Dokumentirana, jasna dodjela odgovornosti i ovlasti za uspostavu i održavanje programa informacijske sigurnosti;

1.3 Redovito testiranje ključnih kontrola, sustava i procedura programa informacijske sigurnosti;

1.4 Administrativne, tehničke i operativne mjere osmišljene za zaštitu svih Osobnih podataka korisnika korištenjem praksi, postupaka i procesa opisanih u ovom Sigurnosnom dodatku, u mjeri u kojoj su relevantne i primjenjive na format u kojem se održavaju Osobni podaci korisnika.

2. PROCJENA RIZIKA

Iron Mountain će održavati program procjene rizika informacijske sigurnosti osmišljen za prepoznavanje i procjenu razumno predvidljivih unutarnjih i vanjskih rizika i ranjivosti koji bi mogli utjecati na sigurnost, povjerljivost i/ili integritet Osobnih podataka korisnika. Iron Mountain će procijeniti i ažurirati, gdje je to potrebno, razumno i prikladno, učinkovitost trenutnog programa informacijske sigurnosti za ograničavanje takvih rizika, na godišnjoj osnovi ili kad god dođe do materijalne promjene u riziku ili ranjivosti Osobnih podataka korisnika.

3. UPRAVLJANJE SREDSTVIMA ZA OBRADU INFORMACIJA I FIZIČKIM MEDIJIMA

3.1 Upravljanje sredstvima za obradu informacija. Iron Mountain održava program za upravljanje inventarom imovine za upravljanje fizičkim, tehničkim i administrativnim kontrolama u vezi s imovinom za obradu informacija tvrtke Iron Mountain (kao što su računala, poslužitelji, uređaji za pohranu, komunikacijske mreže, osobna računala, prijenosna računala i periferni uređaji).
Program upravljanja zalihama imovine uključuje sljedeće:

3.1.1 Dokumentiranu dodjelu vlasništva imovine osoblju Iron Mountaina kako bi se osigurala odgovarajuća klasifikacija informacija, određivanje ograničenja pristupa i pregled kontrola pristupa.

3.1.2 Sanitizacija imovine prije njenog odlaganja u skladu s NIST 800-88.

3.1.3 Zahtjev za ovlaštenjem uprave prije uklanjanja opreme ili softvera koji nisu dodijeljeni određenoj osobi iz objekata Iron Mountaina.

3.2 Kontrole. Kontrole Iron Mountaina uključuju sljedeće:

3.2.1 Operativne postupke i tehničke kontrole osmišljene za zaštitu dokumenata, računalnih medija, ulaznih/izlaznih/sigurnosnih podataka i dokumentacije sustava od neovlaštenog otkrivanja, izmjene i uništenja.

3.2.2 Postupke za sigurno odlaganje elektroničkih ili fizičkih medija koji sadrže Osobne podatke korisnika.

3.2.3 Uspostavljeni postupak za praćenje svih fizičkih medija Korisnika od početnog čuvanja Iron Mountaina do trajnog povlačenja ili uništenja.

4. MJERE ZAŠTITE RADNE SNAGE

4.1 Povjerljivost. Iron Mountain razumno će zahtijevati da svi zaposlenici Iron Mountaina, uključujući privremene i ugovorne zaposlenike, pristanu na održavanje povjerljivosti Osobnih podataka korisnika i pridržavaju se internih zahtjeva za sigurnost informacija i prihvatljivu upotrebu tvrtke Iron Mountain.

4.2 Politika pozadinske istrage. Iron Mountain ima politiku pozadinske istrage i politiku testiranja na droge (samo u SAD-u) na snazi za svoje zaposlenike. Iron Mountain će nastaviti održavati takve politike za vrijeme trajanja Ugovora. Zahtjevi pravila uključuju, ali nisu ograničeni na provjeru na droge (samo u SAD-u), provjeru identiteta osoblja, pretragu kaznenih dosjea, provjeru zaposlenja, pretragu popisa za vladin/nadzor terorista, kao i provjeru obrazovanja za određene zaposlenike te povijest vozačke dozvole i prekršaja za kandidate za vozače i postojeće vozače. Kada se pogrešne informacije identificiraju tijekom pozadinske istrage, Iron Mountain provodi individualiziranu procjenu, u skladu s primjenjivim zakonima o radu i najboljim praksama.

4.3 Rad s podizvođačima. Iron Mountain će zahtijevati od bilo kojeg podizvođača koji pruža Usluge prema Ugovoru da se pridržava ograničenja sličnih onima navedenima u ovom odjeljku u odnosu na bilo koje osoblje podizvođača koje će pružati Usluge prema Ugovoru koje uključuju obradu Osobnih podataka korisnika.

4.4 Obuka za podizanje svijesti o sigurnosti. Najmanje jednom godišnje, Iron Mountain provodi opću obuku za podizanje svijesti o sigurnosti i sigurnosnu obuku primjenjivu na određene uloge za sve zaposlenike Iron Mountaina koji imaju pristup Osobnim podacima korisnika. Iron Mountain će voditi evidenciju koja prikazuje imena takvih zaposlenika Iron Mountaina koji su prisutni i datum svake obuke za podizanje

svijesti o sigurnosti. Iron Mountain će rutinski pregledavati i ažurirati svoj program obuke za podizanje svijesti o sigurnosti.

4.5 Otpuštanje osoblja Iron Mountaina. Iron Mountain održava disciplinski postupak koji se primjenjuje na zaposlenike Iron Mountaina koji krše sigurnosne zahtjeve navedene u ovom Ugovoru.

4.6 Prestanak pristupa nakon raskida/ponovne dodjele. Nakon raskida ili preraspodjele na ulogu koja ne zahtijeva pristup Osobnim podacima korisnika, pristup zaposlenika tvrtke Iron Mountain Osobnim podacima korisnika bit će odmah opozvan.

5. FIZIČKA SIGURNOST I SIGURNOST OKOLIŠA

5.1 Kontrole fizičke sigurnosti. Objekti Iron Mountaina koriste fizičke kontrole koje razumno ograničavaju pristup Osobnim podacima korisnika, uključujući, kako Iron Mountain smatra prikladnim, protokole kontrole pristupa, fizičke barijere kao što su zaključani objekti i područja, bedževi za pristup zaposlenika, zapisnici posjetitelja, bedževi za pristup posjetitelja, čitači kartica, kamere za videonadzor i protuprovalne alarme. Svi posjetitelji moraju se prijaviti i imati pratnju u svakom trenutku.

5.2 Pomoćni programi. Iron Mountain će primijeniti mjere osmišljene za zaštitu svojih objekata koji sadrže Osobne podatke korisnika i sustave od kvarova napajanja, telekomunikacija, vodoopskrbe, kanalizacije, grijanja, ventilacije i klimatizacije, prema potrebi.

5.3 Sigurnost prijenosnog sustava. Iron Mountain će primijeniti mjere namijenjene zaštiti fizičke sigurnosti svoje mrežne infrastrukture i telekomunikacijskih sustava od presretanja prijenosa i oštećenja.

5.4 Vanjska oprema. U slučaju da Iron Mountain vanjskim izvršiteljima povjeri funkcije koje zahtijevaju korištenje opreme izvan lokacije kao podršku uslugama, sva oprema izvan lokacije koja pohranjuje Osobne podatke korisnika bit će zaštićena sigurnošću koja je jednaka onoj koja se koristi za opremu na lokaciji koja se koristi u istu svrhu.

5.5 Fizički pristup sredstvima za obradu informacija. Iron Mountain će čuvati evidenciju zaposlenika Iron Mountaina ovlaštenih za fizički pristup računalnom(im) okruženju(ima) pod kontrolom Iron Mountaina koje Iron Mountain koristi za pružanje Usluga jednu godinu i, na zahtjev Korisnika u vezi s kršenjem sigurnosti, i podložno sigurnosnim politikama Iron Mountaina, omogućiti pristup Korisniku za pregled evidencije takvih zaposlenika Iron Mountaina koja se može provjeriti.

5.6 Ograničenje fizičkog pristupa. Iron Mountain će ograničiti fizički pristup objektima pod kontrolom Iron Mountaina koji obrađuju Osobne podatke korisnika na one zaposlenike Iron Mountaina i ovlaštene pojedince koji imaju poslovnu potrebu za takvim pristupom. Iron Mountain će imati postupak odobrenja za autorizaciju i praćenje zahtjeva za fizički pristup takvim objektima.

5.7 Popravci i izmjene. Iron Mountain će zabilježiti sve sigurnosne popravke i izmjene na svim fizičkim komponentama, uključujući hardver, zidove, vrata i brave sigurnih područja unutar objekata u kojima se pohranjuju Osobni podaci korisnika.

5.8 Zapisi. Održavat će se evidencija kretanja hardvera i elektroničkih medija i svih osoba odgovornih za to.

6. UPRAVLJANJE POSLOVIMA U VEZI KOMUNIKACIJA I OBRADE INFORMACIJA

6.1 Standardi konfiguracije uređaja. Iron Mountain će kreirati, implementirati i održavati postupke administracije sustava koji zadovoljavaju industrijske standarde, uključujući, bez ograničenja, očvršćivanje sustava, zakrpe sustava i uređaja (operativni sustav i aplikacije) te pravilnu instalaciju i ažuriranja antivirusnog programa.

6.2 Kontrola promjena sustava obrade informacija. Iron Mountain će imati uspostavljen interni formalni postupak za upravljanje zahtjevima za obradu informacija i komunikacijske mrežne sustave, a zahtjevi za promjene Iron Mountaina bit će dokumentirani, testirani i odobreni prije implementacije bilo koje nove obrade informacija ili mogućnosti mrežne komunikacije, zakrpa sustava ili promjene postojećih sustava.

6.3 Podjela dužnosti. Iron Mountain će razdvojiti dužnosti i područja odgovornosti tako da niti jedna osoba nema isključivu mogućnost izmjene sustava za obradu informacija koji pristupaju Osobnim podacima korisnika.

6.4 Razdvajanje razvojnog i proizvodnog okruženja. Razvojna, testna i proizvodna okruženja tvrtke Iron Mountain za sustave obrade informacija moraju biti logički ili fizički odvojena.

6.5 Upravljanje tehničkom arhitekturom. Iron Mountain će uspostaviti proces upravljanja konfiguracijom za definiranje, upravljanje i kontrolu komponenti sustava za obradu informacija koje se koriste za pružanje Usluga i tehničke infrastrukture takvih komponenti.

6.6 Otkrivanje upada. Iron Mountain će kontinuirano nadzirati računalne sustave i procese radi pokušaja ili stvarnih sigurnosnih upada ili kršenja i obavijestiti Korisnika o bilo kakvom neovlaštenom pristupu Osobnim podacima korisnika.

6.7 Sigurnost mreže. Iron Mountain će osigurati primjenu sljedećeg:

- 6.7.1 Što se tiče okruženja hostiranih u Iron Mountainu koja se koriste za pružanje Usluga, sustav za otkrivanje upada u mrežu ("IDS") i senzori za sprječavanje upada ("IPS") upozoravaju na događaje koji se bilježe, s dnevnim izvješćima izdanim za pregled (zajednički poznati kao "IDS/IPS");
- 6.7.2 Što se tiče okruženja hostiranih u Iron Mountainu koja se koriste za pružanje Usluga, IDS/IPS koji se ažuriraju ne rjeđe nego jednom tjedno, ali što je prije razumno moguće nakon primitka ažuriranja, i brzo pokretanje najnovijih definicija prijetnji ili pravila;
- 6.7.3 Priključci visokog rizika na vanjskim sustavima nisu dostupni s interneta;
- 6.7.4 Mrežne veze Iron Mountaina se vode i bilježe u datotekama dnevnika;

6.7.5 Postavljanje vatrozida osmišljenog za zaštitu i pregled cjelokupnog dolaznog i odlaznog prometa mrežnih usluga između definiranih mrežnih točaka;

6.7.6 Politike očvršćivanja za definiranje ulaznih i izlaznih mrežnih priključaka ili servisnog prometa za sve sustave u vlasništvu ili kojima upravlja Iron Mountain koji su dokumentirani i ovlašteni unutar programa informacijske sigurnosti;

6.7.7 Mrežni i dijagnostički priključci koji su ispravno osigurani; i

6.7.8 Politike, procedure i tehničke kontrole koje su osmišljene za sprječavanje, otkrivanje i uklanjanje zlonamjernog koda ili poznatih napada na informacijske sustave Iron Mountaina.

6.8 Šifrirane vjerodajnice za provjeru autentičnosti. Iron Mountain će osigurati da su vjerodajnice za autentifikaciju koje se prenose preko mrežnih uređaja Iron Mountaina šifrirane tijekom prijenosa.

6.9 Sigurna mrežna administracija. Mreže Iron Mountaina bit će razumno upravljane i kontrolirane radi zaštite od poznatih prijetnji i održavanja sigurnosti za sve aplikacije i podatke kojima upravlja Iron Mountain na mreži ili u prijenosu preko mreže. Implementirat će se tehničke kontrole i sigurni komunikacijski protokoli kako bi se zabranile neograničene veze s nepouzdanim mrežama ili javno dostupnim poslužiteljima.

6.10 Zaštita od virusa. Iron Mountain implementirat će i održavati antivirusni program upravljanja, uključujući zaštitu od zlonamjernog softvera, ažurirane datoteke potpisa ili alternativnu zaštitu od novih prijetnji, zakrpa i definicija virusa, za poslužitelje i radne stanice kojima upravlja Iron Mountain koji se koriste za smještaj ili pristup Osobnim podacima korisnika.

6.11 Web stranica – enkripcija klijenta. Iron Mountain će osigurati da je za svaku od svojih web stranica omogućen sigurnosni protokol Secure Sockets Layering (SSL) i da sadrži važeći SSL certifikat koji zahtijeva kontrolu povjerljivosti, provjere autentičnosti ili autorizacije.

6.12 Sigurnosna kopija informacija. Iron Mountain će izraditi odgovarajuće sigurnosne kopije sistemskih datoteka. Osim toga, Iron Mountain će razviti i održavati postupke oporavka od katastrofe, pogledajte odjeljak "Oporavak od katastrofe" u nastavku za više detalja.

6.13 Elektroničke informacije u prijenosu. Iron Mountain će koristiti enkripciju s industrijskim standardnim algoritmom s minimalnom duljinom ključa od 128 bita za zaštitu Osobnih podataka korisnika koji se prenose preko javnih mreža kada potječu iz infrastrukture koju hostira Iron Mountain.

6.14 Kriptografske kontrole. Iron Mountain će slijediti dokumentiranu politiku o korištenju kriptografskih kontrola. Kriptografske kontrole Iron Mountaina će:

6.14.1 Biti dizajnirane za razumnu zaštitu povjerljivosti i integriteta Osobnih podataka korisnika koje Iron Mountain obrađuje, prenosi ili pohranjuje u svim zajedničkim mrežnim okruženjima u skladu s uvjetima Ugovora;

6.14.2 Primijeniti, u host okruženju(ima) Iron Mountaina koje(a) se koristi(e) za pružanje usluga, na Osobne podatke korisnika u prijenosu preko ili na "nepouzdane" mreže (tj. mreže koje Iron Mountain zakonski ne kontrolira), uključujući one koje se koriste za slanje podataka na korporativnu mrežu Korisnika sa mreže Iron Mountaina, podložno, u svakom slučaju, suradnji Korisnika u upravljanju ključevima za šifriranje potrebnim za dešifriranje prijenosa koje Korisnik prima; i

6.14.3 Uključiti dokumentirane prakse upravljanja ključem šifriranja za podršku sigurnosti kriptografskih tehnologija.

6.14.4 Uključiti enkripciju svih Osobnih podataka korisnika na prijenosnim računalima ili drugim prijenosnim uređajima.

6.15 Zahtjevi za bilježenje. Iron Mountain će osigurati sljedeće:

6.15.1 Značajni sigurnosni i sistemski događaji se bilježe i pregledavaju;

6.15.2 Revizijski zapisnici se čuvaju najmanje godinu dana za sustave u okruženju(ima) koje(a) Iron Mountain koristi za pružanje usluga;

6.15.3 Dnevnici revizije sustava se pregledavaju zbog anomalija; i

6.15.4 Objekti zapisnika i podaci o sustavima razumno su zaštićeni od manipulacije i neovlaštenog pristupa.

6.16 Mrežna sinkronizacija vremena. Iron Mountain će sinkronizirati sistemske satove svih sustava za obradu informacija koristeći zajednički mjerodavni izvor vremena.

6.17 Segregacija na mrežama. Iron Mountain će na odgovarajući način odvojiti povezane grupe informacijskih usluga, korisnika i informacijskih sustava na mrežama.

7. KONTROLA PRISTUPA

7.1 Mjere kontrole pristupa. Iron Mountain održava mjere kontrole pristupa u pogledu sredstava za obradu informacija koje Iron Mountain formalno odobrava, objavljuje i provodi.

7.2 Logička autorizacija pristupa. Iron Mountain će imati postupak odobravanja za logičke zahtjeve za pristup Osobnim podacima korisnika i zahtjeve za pristup Iron Mountain sustavima namijenjenim za korištenje u Uslugama.

7.3 Kontrola i pregled pristupa. Iron Mountain će omogućiti pristup Osobnim podacima korisnika samo svojim aktivnim zaposlenicima, uključujući privremene i ugovorne zaposlenike te aktivnim korisničkim računima kojima je takav pristup potreban kako bi obavljali svoju radnu funkciju. Svi povlašteni pristupi moraju se pregledati i potvrditi da su u skladu s trenutnom radnom ulogom i dokumentirati barem jednom u tromjesečju.

7.4 Kontrola pristupa trećih strana. Prije odobravanja pristupa informacijskim sustavima Iron Mountaina za vanjske strane koje pristupaju Osobnim podacima korisnika, Iron Mountain će osigurati da postoje odgovarajuće kontrole.

7.5 Kontrola pristupa operativnim sustavima. Iron Mountain će kontrolirati pristup operativnim sustavima (i softverskim i hardverskim operativnim sustavima) zahtijevajući siguran proces prijave koji jedinstveno identificira osobu koja pristupa operativnom sustavu.

7.6 Mobilni računalni uređaji. Iron Mountain će imati politiku ili proceduru osmišljenu za zaštitu mobilnih računalnih uređaja Iron Mountaina od neovlaštenog pristupa. Takve politike ili postupci odnose se na fizičku zaštitu, kontrolu pristupa i sigurnosne kontrole kao što su enkripcija, zaštita od virusa i sigurnosna kopija uređaja.

7.7 Izolacija korisničkih sustava. Iron Mountain će, unutar svojih hostiranih okruženja koja se koriste za pružanje Usluga, logički odvojiti i razdvojiti Osobne podatke korisnika od svih ostalih informacija.

7.8 Računi. Iron Mountain će učiniti sljedeće u vezi s računima:

7.8.1 Zahtijevati autentifikaciju identiteta svakog zaposlenika Iron Mountaina koji traži pristup sustavima Iron Mountaina koji obrađuju Osobne podatke korisnika i zabraniti korištenje zajedničkih korisničkih računa ili korisničkih računa s generičkim vjerodajnicama (tj. ID-ovima) za pristup Osobnim podacima korisnika ili sustavima.

7.8.2 Zahtijevati da svi ID-ovi korisničkih računa, uključujući povlaštene račune, budu izravno povezani s osobom (za razliku od položaja).

7.8.3 Ako zadani administrativni računi nisu onemogućeni ili uklonjeni, zahtijevati korištenje privremenih lozinki, odjavnih ID-ova ili sličnih kontrola za pristup zadanom administrativnom računu.

7.8.4 Zahtijevati da se neaktivni redovni računi zaključaju ili deaktiviraju nakon 90 dana neaktivnosti.

7.8.5 Zabraniti pristup računu nakon više neuspješnih pokušaja pristupa.

7.8.6 Zahtijevati jedinstvene identifikatore i snažne lozinke koje uključuju, najmanje, sljedeće: minimalan broj od 8 znakova; moraju se mijenjati svakih 90 dana; i imati zahtjeve složenosti.

7.8.7 Zabraniti zaposlenicima da dijele ili zapisuju lozinke.

7.9 Kontrole za nenadzirane sustave. Iron Mountain će koristiti čuvar zaslona zaštićen lozinkom za sve sustave koji su ostavljeni bez nadzora i nisu bili aktivni 30 minuta.

8. RAZVOJ I ODRŽAVANJE AKVIZICIJE INFORMACIJSKIH SUSTAVA

8.1 Sigurnost razvoja sustava. Iron Mountain će osigurati da sigurnost bude dio razvoja svih informacijskih sustava i operacija te će objaviti i pridržavati se internih sigurnih metodologija šifriranja temeljenih na sigurnosnim standardima razvoja aplikacija.

8.2 Upravljanje sigurnošću softvera. Informacijski sustavi tvrtke Iron Mountain (uključujući operativne sustave, infrastrukturu, poslovne aplikacije, usluge i aplikacije koje su razvili korisnici) bit će dizajnirani da budu u skladu sa standardima informacijske sigurnosti.

8.3 Mrežni dijagrami. Iron Mountain će razviti, dokumentirati i održavati fizičke i logičke dijagrame mrežnih uređaja i prometa.

8.4 Procjena ranjivosti aplikacije/etičko hakiranje. Iron Mountain će, najmanje jednom godišnje, izvršiti procjenu ranjivosti aplikacija u svojim hostiranim okruženjima koja se koriste za pružanje usluga koje obrađuju Osobne podatke korisnika. Detaljni rezultati povjerljive su i zaštićene informacije tvrtke Iron Mountain i neće biti dostavljeni.

8.5 Promjena - testiranje i pregled. Iron Mountain će pregledati i testirati promjene aplikacija i operativnih sustava prije implementacije kako bi osigurao da nema negativnih učinaka na Osobne podatke korisnika ili sustave.

9. OPORAVAK OD KATASTROFE

Iron Mountain će održavati plan oporavka od katastrofe, uključujući replikaciju sustava i elektroničkih podataka koji se koriste za podršku uslugama u rezervni podatkovni centar. Replikacija sustava i elektroničkih podataka ne uključuje Osobne podatke korisnika koji su fizički pohranjeni u objektu Iron Mountaina. Iron Mountain će održavati plan kontinuiteta poslovanja za obnovu ključnih poslovnih funkcija. Iron Mountain će obavljati testiranje oporavka od katastrofe najmanje jednom svakih dvanaest (12) mjeseci.

10. VANJSKE REVIZIJE I OCJENE

Sigurnosni protokoli tvrtke Iron Mountain osmišljeni su tako da budu u skladu s industrijskim standardima. Iron Mountain će Korisniku dostaviti sva neovisna izvješća o reviziji treće strane koje je naručio (npr. PCI, ISO27001, SOC2, itd.) relevantna za Usluge u regiji u kojoj se te Usluge pružaju ("Izvješće o reviziji"). Iron Mountain će pružiti sva takva izvješća koja su naručena s namjerom da budu suočena s klijentima, bez obzira na rezultate izvješća. Iron Mountain neće morati dostaviti rezultate interne revizije ili rezultate drugih neovisnih procjena koje su naručene s namjerom da budu povjerljive Iron Mountainu. Korisniku i njegovim vanjskim revizorima bit će dostavljene kopije Revizijsko izvješće na zahtjev. Svako izvješće o reviziji ili drugi rezultat dobiven testovima ili revizijama koje zahtijeva ovaj odjeljak smatrat će se povjerljivim informacijama tvrtke Iron Mountain. Korisnik će imati pravo dostaviti kopiju takvog izvješća o reviziji svim primjenjivim klijentima ili regulatorima Korisnika, podložno restriktivnim odredbama o povjerljivosti kao što su one ovdje. Na zahtjev Korisnika, Iron Mountain će pismeno potvrditi da nije bilo promjena u relevantnim politikama, procedurama i internim kontrolama od završetka bilo kojeg takvog izvješća o reviziji, a ne više od tri mjeseca od kraja razdoblja izvješćivanja izvješća o reviziji. .

DODATAK 3

Međunarodni prijenos podataka

1. DEFINICIJE

”**Standardne ugovorne klauzule EU-a iz 2021**” znači standardne ugovorne klauzule za prijenos Osobnih podataka u treće zemlje u skladu s GDPR-om, koje je usvojila Europska komisija prema Provedbenoj odluci Komisije (EU) 2021/914, dostupne ovdje[3].

“**Dodatak za UK iz 2022**” znači predložak dodatka B.1.0 koji je izdao Ured povjerenika za informiranje Ujedinjenog Kraljevstva i izložio Parlamentu u skladu sa člankom 119A Zakona o zaštiti podataka iz 2018. 2. veljače 2022., budući da se može revidirati prema njegovom odjeljku 18, dostupan ovdje[4].

“**Osobni podaci korisnika u EU**” znači obrada Osobnih podataka korisnika na koju su zakoni o zaštiti podataka Europske unije ili države članice Europske unije ili Europskog gospodarskog prostora bili primjenjivi prije obrade od strane Iron Mountaina;

“**Zaštićeno područje**" sredstva:

i. u slučaju Osobnih podataka korisnika iz EU-a, države članice Europske unije i Europskog gospodarskog prostora te bilo koja država, teritorij, sektor ili međunarodna organizacija u odnosu na koju je na snazi odluka o primjerenosti prema članku 45. GDPR-a;

ii. u slučaju Osobnih podataka korisnika u Ujedinjenom Kraljevstvu, Ujedinjeno Kraljevstvo i bilo koja država, teritorij, sektor ili međunarodna organizacija u odnosu na koje je na snazi odluka o primjerenosti prema propisima Ujedinjenog Kraljevstva o primjerenosti;

iii. u slučaju osobnih podataka švicarskih korisnika, bilo koja država, teritorij, sektor ili međunarodna organizacija koja je priznata kao odgovarajuća prema zakonima Švicarske;

iv. u slučaju bilo kojih drugih osobnih podataka korisnika koji se prenose izvan jurisdikcije koja nudi sličnu zaštitu kao i osobni podaci korisnika u EU, UK-u ili Švicarskoj, bilo koja država, teritorij, sektor ili međunarodna organizacija koja je priznata kao odgovarajuća prema zakonima takve jurisdikcije;

“**Standardne ugovorne klauzule**” zajedno znači Standardne ugovorne klauzule EU-a iz 2021. i Dodatak za UK iz 2022.

“**Osobni podaci švicarskih korisnika**” znači obrada Osobnih podataka korisnika na koju su bili primjenjivi zakoni o zaštiti podataka Švicarske prije obrade od strane Iron Mountaina;

“**Osobni podaci korisnika u UK**” znači obrada Osobnih podataka korisnika na koju su bili primjenjivi zakoni o zaštiti podataka Ujedinjenog Kraljevstva prije obrade od strane Iron Mountaina;

2. RAZNO

2.1 Ovaj Prilog 3 uključuje sljedeće dijelove: (i) Dio A – Prijenosi osobnih podataka korisnika iz EU-a; (ii) Dio B – Prijenosi osobnih podataka korisnika u Švicarskoj; (iii) Dio C – Prijenos osobnih podataka korisnika u UK, koji će se primjenjivati kao relevantan za prijenos Osobnih podataka korisnika od strane Iron Mountaina u vezi sa svojim Uslugama.

2.2 Standardne ugovorne klauzule primjenjivat će se na Iron Mountain i njegove podružnicama kao “uvoznicima podataka” te Korisniku i njegovim podružnicama kao "izvoznicima podataka".

2.3 Potpis i datiranje Ugovora predstavljat će sve potrebne potpise i datume za Standardne ugovorne klauzule.

2.4 U slučaju da stranke prenesu osobne podatke korisnika iz EU-a, UK-a ili Švicarske izvan Zaštićenog područja i smatra se da je relevantna odluka Europske komisije ili druga važeća metoda primjerenosti prema primjenjivim zakonima o zaštiti podataka na koje se Iron Mountain oslonio za prijenos podataka nevažeće, ili da bilo koje nadzorno tijelo zahtijeva obustavu prijenosa osobnih podataka izvršenih u skladu s takvom odlukom, tada će stranke surađivati i olakšati korištenje alternativnog mehanizma prijenosa. Stranke su također suglasne da odgovarajuće zaštitne mjere koje se koriste za olakšavanje međunarodnih prijenosa u ovom Prilogu 3. nisu isključive i da stranke mogu slijediti dodatne mehanizme prijenosa, kao što je EU-SAD Okvir za privatnost podataka.

DIO A – PRIJENOSI OSOBNIH PODATAKA KORISNIKA IZ EU

Ako i u mjeri u kojoj Korisnik ili njegova povezana društva prenesu osobne podatke korisnika iz EU izvan Zaštićenog područja tvrtki Iron Mountain ili njegovim povezanim društvima u vezi s uslugama Iron Mountaina prema Ugovoru, primjenjivat će se ovaj Dio A Dodatka 3, a stranke se slažu kako slijedi:

[3] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[4] https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

1. **Standardne ugovorne klauzule - odabiri.** Tekst iz MODUL DVA Standardnih ugovornih klauzula EU-a iz 2021. primjenjivat će se ako je Korisnik ili bilo koje od njegovih povezanih društava Voditelj obrade podataka, a Iron Mountain ili bilo koje od njegovih povezanih društava Izvršitelj obrade; tekst iz MODUL TRI Standardnih ugovornih klauzula EU-a iz 2021. primjenjivat će se ako je Korisnik ili bilo koje od njegovih povezanih društava izvršitelj obrade, a Iron Mountain ili bilo koje od njegovih povezanih društava Podizvršitelj obrade. Relevantne odredbe sadržane u standardnim ugovornim klauzulama EU-a iz 2021. uključene su referencom u ovaj DPA i sastavni su dio ovog DPA. Neće se primjenjivati nikakvi drugi moduli ili bilo koje klauzule označene kao izborne u standardnim ugovornim klauzulama EU-a iz 2021. Podaci potrebni za potrebe dodataka Standardnim ugovornim klauzulama EU-a iz 2021. navedeni su u Dodatku 1 – Opis obrade/prijenosa, Dodatku 2 – Tehničke i organizacijske mjere i Članku 6.2 DPA – Popis Podizvršitelja obrade.

2. **Korištenje Podizvršitelja obrade.**U svrhe klauzule 9 Standardnih ugovornih klauzula EU-a iz 2021., primjenjivat će se opcija 2 (Opće pisano ovlaštenje) za korištenje Podizvršitelja obrade za izvođenje Usluga. Korisnik potvrđuje i slaže se da Iron Mountain može angažirati nove podizvršitelje obrade putem mehanizma dogovorenog u klauzuli 6 ovog DPA i da će vremenski period za podnošenje zahtjeva za promjene Podizvršiteljima obrade biti petnaest (15) dana.

3. **Primjenjivo pravo i rješavanje sporova.** U svrhe klauzule 17 Standardnih ugovornih klauzula EU-a iz 2021. (Mjerodavno pravo), primjenjivat će se mjerodavno pravo opcije 2, a ove će klauzule biti uređene pravom države članice EU-a u kojoj izvoznik podataka ima poslovni nastan, u mjeri u kojoj dopušta prava korisnika treće strane. Za potrebe članka 18 Standardnih ugovornih klauzula EU-a iz 2021. (izbor foruma i nadležnosti) to su sudovi države članice EU-a u kojoj izvoznik podataka ima poslovni nastan.

4. **Potvrda o brisanju.** Za potrebe klauzule 8.5 i 16(d) standardnih ugovornih klauzula EU-a iz 2021., Iron Mountain će korisniku dostaviti potvrdu o brisanju osobnih podataka samo na pismeni zahtjev Korisnika.

5. **Zaštita osobnih podataka.** Za potrebe članka 8.6(c) Standardnih ugovornih klauzula EU-a iz 2021., s povredama osobnih podataka postupat će se u skladu s mehanizmom dogovorenim u članku 7 DPA.

6. **Revizije.**Za potrebe klauzule 8.9 Standardnih ugovornih klauzula EU-a iz 2021., revizije ovih klauzula provodit će se u skladu s mehanizmom revizije dogovorenim u Ugovoru.

7. **Pritužbe.** U svrhe klauzule 11 Standardnih ugovornih klauzula EU-a iz 2021., Iron Mountain će obavijestiti Korisnika ako primi pritužbu od Ispitanika u vezi s Osobnim podacima korisnika u EU-u i priopćit će pritužbu Korisniku u skladu s dogovorenim mehanizmom u Ugovoru.

8. **Nadzorno tijelo.** Za Standardne ugovorne klauzule EU-a iz 2022. relevantno nadležno nadzorno tijelo određuje se u skladu s klauzulom 13 Standardnih ugovornih klauzula EU-a.

DIO B – PRIJENOSI OSOBNIH PODATAKA KORISNIKA U ŠVICARSKOJ

Ako i u mjeri u kojoj Korisnik ili njegova povezana društva prenesu Osobne podatke švicarskih korisnika izvan Zaštićenog područja tvrtki Iron Mountain ili njezinim povezanim društvima u vezi s uslugama Iron Mountaina prema Ugovoru, primjenjivat će se ovaj Dio B Dodatka 3, a stranke se slažu kako slijedi:

1. **Standardne ugovorne klauzule - odabiri.** Standardne ugovorne klauzule EU-a iz 2021. i relevantne odredbe u Dijelu A primjenjivat će se kada je Korisnik ili bilo koje od njegovih povezanih društava Voditelj obrade podataka, a Iron Mountain ili bilo koje od njegovih povezanih društava je Izvršitelj obrade, i/ili Korisnik ili bilo koje od njegovih povezanih društava je Izvršitelj obrade, a Iron Mountain ili bilo koje od njegovih povezanih društava je Podizvršitelj obrade, osim ako:

   a. nadležno nadzorno tijelo prema klauzuli 13 Standardnih ugovornih klauzula EU-a iz 2021. je Švicarska savezna komisija za zaštitu podataka i informacije;

   b. mjerodavno pravo za ugovorna potraživanja prema klauzuli 17 Standardnih ugovornih klauzula EU iz 2021. je švicarsko pravo, a mjesto nadležnosti za radnje između stranaka u skladu s klauzulom 18 (b) su švicarski sudovi.

2. Upućivanja na EU GDPR u standardnim ugovornim klauzulama EU-a iz 2021. treba shvatiti kao upućivanja na FADP.

3. Izraz "država članica" u standardnim ugovornim klauzulama EU-a iz 2021. ne smije se tumačiti na način da se subjekti podataka u Švicarskoj isključuju iz mogućnosti traženja prava u mjestu njihovog uobičajenog boravišta (Švicarska) u skladu s klauzulom 18 (c) Standardnih ugovornih klauzula EU-a iz 2021.

DIO C – PRIJENOSI OSOBNIH PODATAKA KORISNIKA U UK

Ako i u mjeri u kojoj Korisnik ili njegova povezana društva prenesu Osobne podatke korisnika iz UK izvan Zaštićenog područja tvrtki Iron Mountain ili njezinim povezanim društvima u vezi s uslugama Iron Mountaina prema Ugovoru, primjenjivat će se ovaj Dio A Dodatka 3, a stranke se slažu kako slijedi:

1. **Standardne ugovorne klauzule - odabiri.** Standardne ugovorne klauzule EU-a iz 2021., relevantne odredbe u Dijelu A i Dodatak za UK iz 2022. primjenjivat će se kada je Korisnik ili bilo koje od njegovih povezanih društava Voditelj obrade podataka, a Iron Mountain ili bilo koje od njegovih povezanih društava Izvršitelj obrade, i/ili Korisnik ili bilo koje od njegovih povezanih društava je Izvršitelj, a Iron Mountain ili bilo koje od njegovih povezanih društava je Podizvršitelj obrade.

2. **1. dio: Tablica 1 - 3 Dodatka za UK iz 2022.:** Podaci o strankama - Tablica 1; Odabrani SCC-ovi, moduli i odabrane klauzule; i Dodatak Informacije, uključujući Dodatak 1A: Popis stranaka, Dodatak 1B: Opis prijenosa i Dodatak 1C: Tehničke i organizacijske mjere za osiguranje sigurnosti podataka - Tablica 3, smatrat će se dovršenima pozivanjem na ovaj Dodatak 3, uključujući Dio A. Tablica 4 Dodatka za UK: Korisnik i Iron Mountain potvrđuju i suglasni su da bilo koja stranka može raskinuti Dodatak za UK.

3. **2. dio:**Obvezne klauzule Dodatka za UK: Korisnik i Iron Mountain prihvaćaju i slažu se s obveznim klauzulama Dodatka za UK.

4. **Nadzorno tijelo.** Ured povjerenika za informacije UK-a djelovat će kao nadležno nadzorno tijelo.

DIO D – PRIJENOSI DRUGIH OSOBNIH PODATAKA KORISNIKA

Ako i u mjeri u kojoj Korisnik ili njegova povezana društva prenose Osobne podatke korisnika koji nisu obuhvaćeni DIJELOM A-C tvrtki Iron Mountain ili njezinim povezanim društvima u vezi s uslugama Iron Mountaina prema Ugovoru, Dio A Dodatka 3 primjenjivat će se u mjeri relevantnoj i primjenjivoj prema važećim propisima o zaštiti podataka. Inače, u mjeri u kojoj su potrebne bilo kakve zamjenske ili dodatne odgovarajuće zaštite ili mehanizmi prijenosa prema zakonodavstvu o zaštiti podataka za prijenos Osobnih podataka korisnika u zemlju koja ne pruža odgovarajuću razinu zaštite osobnih podataka iz perspektive izvoznika podataka, stranke se slažu da će isti implementirati što je prije moguće i dokumentirati takve zahtjeve za implementaciju u prilogu ovog DPA.

DODATAK 4

HIPAA – Ugovor o poslovnoj suradnji ("BAA")

Ovaj BAA nadopunjuje i izmjenjuje bilo koji i sve sadašnje ili buduće ugovore sklopljene između Iron Mountaina i njegovih podružnica te Korisnika i njegovih podružnica prema kojima Iron Mountain ili njegove podružnice pružaju određene Usluge za Korisnika ili njegove podružnice, a koje usluge moraju koristiti poslovni suradnici i/ili otkriti ZZP u ime Pokrivenog entiteta. Osim u mjeri izmijenjenoj u ovom BAA, svi uvjeti i odredbe navedeni u Ugovoru ostat će na snazi i učinku i regulirat će Usluge koje Iron Mountain pruža Korisniku.

Iron Mountain i Korisnik sklapaju ovaj BAA kako bi obje stranke ispunile svoje obveze nakon što postanu učinkovite i obvezujuće za stranke u skladu s HIPAA pravilima o privatnosti, sigurnosti i obavješćivanju o kršenju, zajedno sa svim provedbenim propisima uključujući one koji se provode kao dio Omnibus pravila (zajedničkim nazivom "HIPAA pravila") prema kojem su Korisnik i njegova povezana društva "Pokriveni entitet" ili "Poslovni suradnik", a Iron Mountain i njegova povezana društva "Poslovni suradnik" Korisnika. Za potrebe ovog Ugovora, sve reference u daljnjem tekstu na poslovnog suradnika smatrat će se referencama na Iron Mountain ili njegovo primjenjivo povezano društvo.

1. DEFINICIJE

Pojmovi pisani velikim početnim slovom koji se koriste, ali nisu drugačije definirani u ovom BAA, imat će isto značenje koje je pripisano tim pojmovima u HIPAA pravilima ili u Ugovoru, kako je primjenjivo.

"**Pravilo obavijesti o kršenju**" znači pravilo Obavijesti o kršenju za nezaštićene zaštićene zdravstvene podatke u 45 CFR §164 Pododjeljak D.

"**Poslovni suradnik**" znači gore navedeni entitet poslovnog suradnika u onoj mjeri u kojoj prima, održava ili prenosi Zaštićene zdravstvene podatke prilikom pružanja Usluga korisnicima.

"**HIPAA**" znači Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja iz 1996.

"**HITECH zakon**" znači primjenjive odredbe Zakona o zdravstvenoj informacijskoj tehnologiji za gospodarstvo i kliničko zdravlje, kao što je uključeno u Američki zakon o oporavku i ponovnom ulaganju iz 2009., uključujući sve provedbene propise.

"**Pravilo o privatnosti**" znači Standarde za privatnost zdravstvenih podataka koji se mogu identificirati u 45 CFR §160 i §164, poddijelovi A i E.

"**Zaštićeni zdravstveni podaci**" ili "**ZZP**" imat će isto značenje kao izraz „zaštićeni zdravstveni podaci" u 45 CFR §160.103 i bit će ograničen na ZZP koje je kreirao poslovni suradnik u ime Korisnika ili ih je primio od ili u ime Korisnika u skladu s Ugovorom.

"**Sigurnosno pravilo**" znači Sigurnosni standardi za zaštitu elektroničkih zaštićenih zdravstvenih podataka u 45 CFR §160 i §164, poddijelovi A i C.

2. OBVEZE I AKTIVNOSTI POSLOVNOG SURADNIKA

2.1. Poslovni suradnik se slaže da neće koristiti ili dalje otkrivati ZZP osim kako je dopušteno ili zahtijevano ovim BAA ili kako je propisano zakonom.

2.2. Poslovni suradnik pristaje koristiti odgovarajuće zaštitne mjere i pridržavati se, prema potrebi, pododjeljka C 45 CFR §164 u vezi s elektroničkim ZZP, kako bi spriječio Korištenje ili otkrivanje ZZP drugačije nego što je predviđeno ovim BAA ili Ugovorom; međutim, stranke potvrđuju i slažu se da će biti odgovornost Korisnika, a ne Poslovnog suradnika, da se pridržava zahtjeva prema 45 CFR §164.312 za implementaciju mehanizama šifriranja ili dešifriranja za elektroničke ZZP koji se održavaju na fizičkim medijima (npr. vrpce) koje pohranjuje Korisnik s poslovnim suradnikom.

2.3. Poslovni suradnik se slaže odmah prijaviti Korisniku svaki sigurnosni incident, kršenje ili drugu upotrebu ili otkrivanje ZZP za koje sazna da nisu dopušteni ili zahtijevani ovim BAA ili Ugovorom. U slučaju Kršenja, takva obavijest bit će poslana u skladu s HIPAA pravilima i prema zahtjevima Poslovnog suradnika, uključujući bez ograničenja prema 45 CFR 164.410, ali ni u kojem slučaju više od tri (3) radna dana nakon što je Poslovni suradnik dovršio internu istragu i potvrdio da se kršenje dogodilo. Poslovni suradnik će pružiti razumnu pomoć i suradnju u istrazi svakog takvog kršenja i dokumentirati određene depozite koji su bili ugroženi, identitet bilo koje neovlaštene treće strane koja je mogla pristupiti ili primiti ZZP, ako je poznata, i sve radnje koje su poduzete od strane poslovnog suradnika kako bi se ublažili učinci takvog kršenja.

2.4. Poslovni suradnik će, u skladu s 45 CFR 164.502(e)(1)(ii) i 164.308(b)(2), kako je primjenjivo, osigurati da svaki poslovni suradnik koji je podizvođač koji stvara, prima, održava ili prenosi ZZP u ime Poslovnog suradnika u svrhu pomoći u pružanju Usluga u skladu s Ugovorom, pristaje na ista ograničenja, uvjete i zahtjeve koji se primjenjuju na Poslovnog suradnika u vezi s takvim ZZP kroz ovaj BAA.

2.5. Ako Poslovni suradnik ima skrbništvo nad ZZP u Određenom skupu zapisa u odnosu na pojedince, i ako Korisnik to zatraži, Poslovni suradnik pristaje omogućiti pristup takvim ZZP Korisniku preuzimanjem i

isporukom takvih ZZP u skladu s odredbama i uvjetima Ugovora, tako da Korisnik može odgovoriti pojedincu kako bi ispunio zahtjeve 45 CFR §164.524.

2.6. Poslovni suradnik je suglasan da će, ako je potrebna izmjena ZZP u Određenom skupu zapisa koje čuva Poslovni suradnik, i ako Korisnik uputi Poslovnog suradnika da pronađe takve ZZP u skladu s Ugovorom, Poslovni suradnik će izvršiti takvu uslugu kako bi Korisnik mogao učiniti bilo koju izmjenu takvih ZZP koju može zahtijevati ili Korisnik ili Pojedinac u skladu s 45 CFR §164.526.

2.7. Poslovni suradnik pristaje dokumentirati i učiniti dostupnim Korisniku informacije potrebne za pružanje izvješća o objavljivanju ZZP, pod uvjetom da je Korisnik Poslovnom suradniku pružio informacije dovoljne da mu se omogući odrediti koje je zapise ili podatke primio od ili u ime Korisnika koji sadrže ZZP. Dokumentacija o objavljivanjima sadržavat će informacije koje bi bile potrebne Korisniku da odgovori na zahtjev pojedinca za izvješća o objavljivanju ZZP u skladu s 45 CFR §164.528 ili drugim odredbama HIPAA pravila.

2.8. Osim ako nije drugačije izričito dogovoreno u Ugovoru, Poslovni suradnik će odmah obavijestiti Korisnika o svim zahtjevima pojedinaca za pristup, saznavanje ili ispravak ZZP, bez odgovara na takve zahtjeve, a Korisnik će biti odgovoran za primanje i odgovore na sve takve zahtjeve pojedinca.

2.9. U onoj mjeri u kojoj Poslovni suradnik treba izvršiti jednu ili više kupčevih obveza prema pododjeljku E 45 CFR §164, Poslovni suradnik će se pridržavati zahtjeva pododjeljka E koji se odnose na Korisnika u izvršavanju takve obveze(a).

2.10. Poslovni suradnik pristaje staviti svoje interne prakse, knjige i zapise na raspolaganje tajniku u svrhu utvrđivanja usklađenosti s HIPAA pravilima.

3. DOPUŠTENA UPOTREBA I OTKRIVANJE OD STRANE POSLOVNOG SURADNIKA

3.1. Poslovni suradnik može koristiti ili otkriti ZZP prema potrebi za obavljanje usluga navedenih u Ugovoru.

3.2. Poslovni suradnik može koristiti ili otkriti ZZP u skladu sa zakonom.

3.3. Poslovni suradnik pristaje uložiti razumne napore da ograniči ZZP na minimum koji je neophodan za postizanje predviđene svrhe Korištenja, objavljivanja ili zahtjeva.

3.4. Poslovni suradnik ne smije koristiti ili otkriti ZZP na način koji bi prekršio pododjeljak E 45 CFR §164 ako to učini Korisnik.

3.5. Poslovni suradnik može otkriti ZZP za svoje pravilno upravljanje i administraciju ili za izvršavanje svojih zakonskih odgovornosti, pod uvjetom da je otkrivanje potrebno po zakonu, ili ako Poslovni suradnik dobije razumna jamstva od osobe kojoj su podaci otkriveni da će podaci ostati povjerljivi i koristiti se ili dalje otkrivati samo kako je propisano zakonom ili u svrhe za koje su otkriveni osobi, a osoba obavještava Poslovnog suradnika o svim slučajevima za koje je svjesna da je povjerljivost podataka bila ugrožena.

4. OBVEZE KORISNIKA

4.1. Korisnik neće uputiti Poslovnog suradnika da djeluje na način koji nije u skladu s HIPAA pravilima.

4.2. Korisnik će obavijestiti Poslovnog suradnika o svim ograničenjima u svojoj obavijesti o praksi privatnosti Korisnika u skladu s 45 CFR §164.520, u mjeri u kojoj takvo ograničenje može utjecati na korištenje ili otkrivanje ZZP od strane Poslovnog suradnika.

4.3. Korisnik će obavijestiti Poslovnog suradnika o svim promjenama ili opozivu dopuštenja pojedinca za korištenje ili otkrivanje njegovih ZZP, u mjeri u kojoj takve promjene mogu utjecati na korištenje ili otkrivanje ZZP od strane Poslovnog suradnika.

4.4. Korisnik će pisanim putem obavijestiti Poslovnog suradnika o bilo kakvom ograničenju upotrebe ili otkrivanja ZZP na koje je Korisnik pristao u skladu s 45 CFR §164.522, u mjeri u kojoj takvo ograničenje može utjecati na korištenje ili otkrivanje ZZP od strane Poslovnog suradnika.

5. VALJANOST I PRESTANAK VAŽENJA

5.1. Trajanje ovog BAA počinje od Datuma stupanja na snagu i automatski prestaje nakon (i) isteka Ugovora, ili (ii) kada se svi ZZP koji je Korisnik dao Poslovnom suradniku unište ili vrate Korisniku.

5.2. Nakon saznanja stranke o suštinskom kršenju BAA od strane druge stranke, stranka koja ne krši ugovor mora pružiti priliku stranci koja krši ugovor da ispravi kršenje. Ako stranka koja je prekršila ne ispravi kršenje u roku od trideset (30) dana, nakon što je stranka koja je prekršila primila pisanu obavijest od stranke koja nije prekršila u kojoj se navode pojedinosti o takvom suštinskom kršenju, tada će stranka koja je prekršila imati pravo raskinuti ovaj BAA i Ugovor u skladu s uvjetima Ugovora ili, ako raskid nije izvediv, prijavit će problem tajniku ili bilo kojem drugom nadležnom tijelu.

5.3. Učinak raskida:

5.3.1.1. Osim kako je navedeno u 5.3.2 u nastavku, po raskidu ovog BAA iz bilo kojeg razloga, Poslovni suradnik će vratiti ili uništiti sve ZZP primljene od Korisnika u skladu s Ugovorom. Ova se odredba primjenjuje na ZZP koji je u posjedu podizvođača ili agenata Poslovnog suradnika. Poslovni suradnik neće zadržati kopije ZZP.

5.3.1.2. U slučaju da Poslovni suradnik utvrdi da je vraćanje ili uništavanje ZZP neizvodljivo, Poslovni suradnik će Korisniku dostaviti obavijest o uvjetima koji čine vraćanje ili uništenje neizvedivim. Nakon obavijesti Korisnika, Poslovni suradnik će proširiti zaštitu ovog BAA na takve ZZP i ograničiti daljnju upotrebu i otkrivanje takvih ZZP na one svrhe koje čine povrat ili uništenje neizvedivim, sve dok Poslovni suradnik održava takve ZZP u skladu s uvjetima Ugovora.

6. RAZNO

6.1. Naknada štete. Poslovni suradnik se slaže da će obeštetiti Korisnika od bilo kakvih (novčanih) kazni nametnutih Korisniku kao rezultat bilo kojeg ovršnog postupka koji je pokrenuo tajnik ili bilo koje građanske tužbe koju je pokrenuo glavni državni odvjetnik protiv Korisnika, a koji postupak ili radnja proizlaze izravno i isključivo iz bilo kojeg čina ili propusta od strane Poslovnog suradnika koji je ili kršenje HIPAA pravila ili suštinsko kršenje ovog BAA ("Potraživanje"). Poslovni suradnik neće biti obvezan nadoknaditi Korisniku bilo koji dio takvih (novčanih) kazni koje proizlaze iz (i) Korisnikovog kršenja HIPAA pravila ili ovog BAA, ili (ii) nemara ili namjernih radnji ili propusta Korisnika. Gore navedena obveza obeštećenja izričito je uvjetovana time da Korisnik Poslovnom suradniku dodijeli pravo, po izboru i trošku Poslovnog suradnika, te uz savjetnika po vlastitom izboru, da kontrolira ili sudjeluje u obrani bilo kojeg takvog Potraživanja, međutim, pod uvjetom da u mjeri u kojoj bilo koje takvo Potraživanje bude dio većeg postupka ili radnje, pravo Poslovnog suradnika na kontrolu ili sudjelovanje bit će ograničeno na Potraživanje, a ne na širi postupak ili radnju. U slučaju da Poslovni suradnik iskoristi svoju opciju kontrole obrane, tada (i) Poslovni suradnik neće rješavati bilo kakva potraživanja koja zahtijevaju bilo kakvo priznanje krivnje od strane Korisnika bez njegovog prethodnog pismenog pristanka, (ii) Korisnik će imati pravo sudjelovanja, o vlastitom trošku, u potraživanju ili tužbi i (iii) Korisnik će surađivati s Poslovnim suradnikom na razuman zahtjev. Prethodno navodi Korisnikov jedini i isključivi pravni lijek i isključivu odgovornost Poslovnog suradnika za bilo kakav gubitak, štetu, trošak ili odgovornost Korisnika za bilo koje Potraživanja u vezi s ovim BAA.

6.2. Pravna zabrana. Poslovni suradnik prihvaća da svako neovlašteno korištenje ili otkrivanje ZZP od strane Poslovnog suradnika može prouzročiti nepopravljivu štetu Korisniku za koju će Korisnik imati pravo, ako tako odluči, tražiti zabranu ili drugu pravnu zaštitu.

6.3. Regulatorne reference. Upućivanje u ovom BAA na odjeljak HIPAA pravila znači onaj odjeljak HIPAA, Pravila o privatnosti, Sigurnosnog pravila, HITECH ACT-a ili konačna Omnibus pravila kako su izmijenjena i na snazi, i za koja se zahtijeva usklađenost.

6.4. Izmjene i dopune. Stranke su suglasne da će u dobroj vjeri pregovarati o svim izmjenama i dopunama ovog BAA koje bi mogle biti potrebne s vremena na vrijeme, a koje su potrebne za Korisnika ili Poslovnog suradnika u skladu sa zahtjevima HIPAA pravila. Ako stranke ne mogu postići međusobni dogovor o uvjetima bilo koje takve izmjene i dopune u roku od šezdeset (60) dana od datuma primitka bilo kojeg takvog pisanog zahtjeva koji je Korisnik uputio Poslovnom suradniku, tada će bilo koja stranka imati pravo raskinuti ovaj BAA i Ugovor uz davanje pismene obavijesti drugoj stranci najmanje trideset (30) dana.

6.5. Bez korisnika treće strane. Ništa izraženo ili implicirano u ovom BAA nema namjeru dodijeliti, niti će bilo što ovdje navedeno dodijeliti, bilo kojoj osobi osim Korisniku, Poslovnom suradniku i njihovim nasljednicima ili opunomoćenicima, bilo kakva prava, pravne lijekove, obveze ili odgovornosti.

6.6. Neovisni ugovaratelj. Poslovni suradnik, uključujući njegove direktore, službenike, zaposlenike i agente, neovisni je ugovaratelj, a ne agent (kako je definirano u saveznom običajnom pravu zastupanja) Korisnika ili član njegove radne snage. Bez ograničavanja općenitosti gore navedenog, Korisnik neće imati pravo kontrolirati, usmjeravati ili na drugi način utjecati na ponašanje Poslovnog suradnika tijekom obavljanja usluga, osim kroz provedbu ovog BAA ili Ugovora, ili međusobne izmjene i dopune istih.

6.7. Prethodni ugovori, Cjelokupan ugovor. Sve nejasnoće u ovom BAA će se riješiti kako bi se strankama omogućilo pridržavanje HIPAA pravila. Ovaj BAA predstavlja cjelokupan ugovor između stranaka u vezi s predmetom ovog Ugovora i zamjenjuje sve prethodne komunikacije, izjave, sporazume i dogovore koji se odnose na HIPAA pravila, uključujući sve prethodne ugovore o poslovnoj suradnji između stranaka.