UMOWA PRZETWARZANIA DANYCH

CEL I KOLEJNOŚĆ PIERWSZEŃSTWA

Niniejsza Umowa Przetwarzania Danych, wraz z aneksami i wszelkimi dokumentami, do których się wyraźnie odwołuje („UPD"), jest uważana za część umowy świadczenia usług zawartej pomiędzy Iron Mountain i Klientem („Umowa"). Warunki i zasady Umowy mają zastosowanie oraz regulują prawa i obowiązki stron na mocy UPD.

Jeżeli jakiekolwiek warunki i zasady zawarte w niniejszej UPD będą sprzeczne z zasadami i warunkami określonymi w Umowie, warunki zasady określone w niniejszej UPD będą miały znaczenie rozstrzygające w odniesieniu do przedmiotu tej UPD. Niniejsza UPD jest nadrzędna i zastępuje wszystkie wcześniejsze umowy przetwarzania danych lub klauzule ochrony danych bądź prywatności zawarte przez strony w odniesieniu do Usług świadczonych na mocy Umowy.

WARUNKI OGÓLNE

1. DEFINICJE

Wszystkie określenia pisane wielką literą będą miały takie same znaczenia jak przypisane im w Umowie, chyba że zostały konkretnie zdefiniowane w niniejszej umowie.
„Administrator" oznacza osobę fizyczną lub prawną, urząd, agencję lub innego rodzaju organ publiczny, który samodzielnie lub wraz z innymi określa cele i środki Przetwarzania Danych Osobowych;
„Dane Osobowe Klientów" oznacza Dane Osobowe należące lub zebrane przez Klienta lub jego podmioty powiązane Przetwarzane w ramach Usług;
„Podmiot Danych" oznacza osobę fizyczną zidentyfikowaną lub możliwą do identyfikacji.
„Ustawodawstwo o Ochronie Danych" oznacza wszystkie obowiązujące prawa i przepisy dotyczące Przetwarzania Danych Osobowych, które mogą istnieć pod danymi jurysdykcjami, w tym między innymi RODO UE (Rozporządzenie (UE) 2016/679), RODO brytyjskie (RODO obowiązujące w ramach prawa krajowego Wielkiej Brytanii na mocy ustępu 3 Ustawy o (Wycofaniu się z) Unii Europejskiej z 2018 r. ze zmianami na mocy Rozporządzeń o Ochronie Danych, Prywatności i Komunikacji Elektronicznej (Poprawki itp.) (Wyjście z UE) z 2019 r. (ze zmianami)), Ustawy o Ochronie Danych z 2018 r., FADP (szwajcarska Federalna Ustawa o Ochronie Danych), Stanowe Prawa o Prywatności USA , LGPD (brazylijska Ustawa Ogólna o Ochronie Danych), PIPL (Ustawa o Ochronie Informacji Osobowych Chińskiej Republiki Ludowej) oraz wszelkie inne ustawy i/lub rozporządzenia wprowadzające je w życie lub wydane na ich mocy, lub zmieniające, zastępujące, nowelizujące lub konsolidujące którekolwiek z nich, włącznie, tam gdzie ma to zastosowanie, z wytycznymi i kodeksami praktyk wydanymi przez organy nadzorujące.
„Dane Osobowe" oznacza wszelkie informacje dotyczące Podmiotu Danych;
„Przetwarzający" oznacza osobę fizyczną lub prawną, urząd, agencję lub innego rodzaju organ publiczny, który Przetwarza Dane Osobowe w imieniu Administratora.

„Przetwarzanie” oznacza wszelkie działanie lub serię działań wykonywanych na Danych Osobowych lub zbiorach Danych Osobowych, środkami automatycznymi lub nie, takie jak zbieranie, utrwalanie, organizacja, strukturyzowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultacja, wykorzystanie, ujawnienie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, przyrównywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
„Naruszenie Bezpieczeństwa Danych” oznacza wszelkie uszkodzenie, zniszczenie, utratę, zmianę, lub nieuprawnione ujawnienie lub udostępnienie Danych Osobowych Klienta Przetwarzanych przez Iron Mountain lub jej podwykonawców w ramach świadczenia Usług, dokonane przypadkowo lub niezgodnie z prawem.
„Usługi” oznacza wszelkie usługi świadczone przez Iron Mountain lub jej podmioty powiązane na rzecz Klienta lub jego podmiotów powiązanych na mocy Umowy.
„Stanowe Ustawy o Prywatności USA” oznacza wszystkie stanowe ustawy o prywatności i ochronie danych w Stanach Zjednoczonych mające zastosowanie do Przetwarzania Danych Osobowych na mocy Umowy, w tym między innymi z każdorazowymi zmianami, wprowadzeniem mocy nadrzędnej lub zastąpieniem (1) Ustawy o Prywatności Konsumenckiej stanu Kalifornia zmienionej na mocy Ustawy o Prawach do Prywatności stanu Kalifornia, oraz wszelkie dotyczące ich rozporządzenia wykonawcze (łącznie „CCPA”), (2) Ustawy o Prywatności stanu Kolorado (CPA), (3) Ustawy o Ochronie Danych Konsumenckich stanu Wirginia („CDPA”), (4) Ustawy o Ochronie Danych Konsumenckich stanu Utah („UCPA”) oraz (5) ustawy o Prywatności Danych stanu Connecticut („CTDPA”).

2. ZAKRES I INFORMACJE DOTYCZĄCE PRZETWARZANIA DANYCH

2.1 Niniejsza UPD ma zastosowanie do Danych Osobowych Klienta Przetwarzanych przez Iron Mountain jako Przetwarzającego w ramach świadczenia Usług na mocy Umowy w imieniu Klienta.

2.2 Iron Mountain może zbierać i Przetwarzać Dane Osobowe pracowników Klienta oraz jego podmiotów powiązanych jako Administrator dla uzasadnionych celów biznesowych, takich jak zarządzanie kontraktami i stosunkami z klientami, oraz zgodnie z Ustawodawstwem o Ochronie Danych oraz powiadomieniem o prywatności Iron Mountain dostępnym na stronach internetowych Iron Mountain, oraz innymi obowiązującymi politykami prywatności. Zobowiązania Iron Mountain określone w niniejszej UPD nie będą miały zastosowania do przetwarzania takich Danych Osobowych.

2.3 Przedmiotem Przetwarzania Danych Osobowych jest świadczenie Usług. Prawa i obowiązki Klienta oraz Iron Mountain zostały określone w niniejszej UPD. Aneks 1 do UPD określa charakter, czas trwania oraz cel Przetwarzania, rodzaje Danych Osobowych Klienta Przetwarzanych przez Iron Mountain oraz kategorie Podmiotów Danych, których Dane Osobowe są Przetwarzane.

2.4 W trakcie Przetwarzania Danych Osobowych Klienta przez Iron Mountain w ramach świadczenia Usług Iron Mountain zobowiązana jest:

2.4.1 przetwarzać Dane Osobowe Klienta tylko zgodnie z udokumentowanymi instrukcjami Klienta. Jeżeli Iron Mountain będzie zobowiązana do Przetwarzania Danych Osobowych Klienta w jakimkolwiek innym celu na mocy przepisów prawa, którym Iron Mountain podlega, Iron Mountain wcześniej poinformuje Klient o takim wymogu, chyba że przepis(y) taki(e) zabrania(ją) tego na gruncie ważnego interesu publicznego; oraz

2.4.2 zawsze przestrzegać Ustawodawstwa od Ochronie Danych i powiadamiać Klienta niezwłocznie jeżeli zdaniem Iron Mountain instrukcje dotyczące Przetwarzania Danych Osobowych Klienta przez niego przekazane naruszają obowiązujące Ustawodawstwo o Ochronie Danych.

2.5 Instrukcje Klienta będą obowiązujące dla Iron Mountain, chyba że wykonanie tych instrukcji będzie wymagało wykonania usługi na mocy Umowy a Klient nie wyraża zgody na zapłacenie należności za taką usługę.

2.6 Iron Mountain zapewni, że personel, który będzie musiał mieć dostęp do Danych Osobowych Klienta podlega zobowiązaniu do zachowania poufności w odniesieniu do takich Danych Osobowych Klienta oraz podejmie wszelkie kroki w celu zapewnienia wiarygodności i kompetencji personelu Iron Mountain, który będzie miał dostęp do Danych Osobowych Klienta.

3. OBSŁUGA KLIENTA

3.1 Iron Mountain zapewni Klientowi obsługę i pomoc, zawsze z uwzględnieniem charakteru Przetwarzania:

3.1.1 przy pomocy odpowiednich środków technicznych i organizacyjnych oraz w miarę możliwości w odniesieniu do spełniania przez Klienta zobowiązania do udzielenia odpowiedzi na wnioski Podmiotów Danych wykonujących swoje prawa;

3.1.2 w zakresie przestrzegania zobowiązań Klienta (takich jak bezpieczeństwo Przetwarzania, powiadamianie organu nadzorującego o naruszeniu bezpieczeństwa Danych Osobowych, przekazaniu informacji o naruszeniu bezpieczeństwa Danych Osobowych Podmiotowi Danych, oceny wpływu na ochronę danych oraz uprzednich konsultacji z organami nadzorującymi w przypadkach, gdy Przetwarzanie mogłoby prowadzić do wysokiego ryzyka przy braku środków podjętych przez Administratora w celu ograniczenia takiego ryzyka), z uwzględnieniem informacji dostępnych Iron Mountain, oraz

3.1.3 przez udostępnienie Klientowi wszystkich informacji, których Klient zasadnie zażąda aby umożliwić Klientowi wykazanie, że jego zobowiązania w zakresie wyboru i powołania Iron Mountain zostały spełnione.

4. ZABEZPIECZENIA

4.1 Uwzględniając normalne procedury operacyjne, koszty ich wdrożenia oraz charakter, zakres, kontekst i cel Przetwarzania, Iron Mountain będzie stosował odpowiednie i zasadne środki techniczne i organizacyjne, których celem będzie ochrona poufności, integralności i dostępności Danych Osobowych Klienta oraz ochrona Danych Osobowych Klienta przed nieuprawnionym lub bezprawnym Przetwarzaniem oraz przypadkową utratą, zniszczeniem, uszkodzeniem, zmianą lub ujawnieniem. Standardy bezpieczeństwa Iron Mountain zostały opisane w Aneksie 2 do niniejszej UPD.

4.2 Klient ponosi wyłączną odpowiedzialność za ocenę, czy te środki techniczne i organizacyjne spełniają wymagania Klienta.

5. PRZESTRZEGANIE PRAWA

Klient i jego podmioty powiązane zobowiązane są: (i) Przetwarzać Dane Osobowe Klienta zgodnie z Ustawodawstwem o Ochronie Danych; (ii) być uprawnieni do wydawania pisemnych instrukcji Iron Mountain w zakresie Przetwarzania Danych Osobowych Klienta w związku z Usługami (w tym w imieniu ewentualnego podmiotu trzeciego będącego Administratorem Danych Osobowych Klienta); oraz (iii) zawsze zachowywać kontrolę i uprawnienia dotyczące Danych Osobowych Klienta w odniesieniu do Przetwarzania.

6. ZLECENIE PRZETWARZANIA

6.1 Klient przyjmuje do wiadomości i wyraża zgodę by, Iron Mountain zaangażowała swój podmiot macierzysty, podmioty powiązane i innych zewnętrznych Podwykonawców Przetwarzania (w tym zewnętrznych Podwykonawców Przetwarzania zatrudnionych przez podmioty powiązane Iron Mountain lub podmiot macierzysty) w celu Przetwarzania Danych Osobowych Klienta na mocy niniejszej UPD z zastrzeżeniem punktu 6.2 poniżej.

6.2 Lista Podwykonawców Przetwarzania zatwierdzona przez Klienta w dniu zawarcia niniejszej UPD jest dostępna tutaj[1]. Iron Mountain może w dowolnym czasie zastąpić lub powołać nowego Podwykonawcę Przetwarzania pod warunkiem, że Klient otrzyma pisemne powiadomienie z piętnastodniowym (15) wyprzedzeniem i w tym terminie nie zgłosi sprzeciwu wobec takich zmian na z solidnym uzasadnieniem związanym z ochroną danych. Aby otrzymać takie powiadomienia mailem Klient zasubskrybuje i będzie utrzymywał ewentualną dotychczasową subskrypcję serwisu powiadomień Iron Mountain za pośrednictwem niniejszej strony www,[2]

6.3 Jeżeli Klient nie dokona subskrypcji serwisu powiadomień Iron Mountain nie będzie ponosiła odpowiedzialności za niepowiadomienie o Podwykonawcy Przetwarzania i wszystkie takie powołania będą uważane za zaakceptowane przez Klienta. Jeżeli Klient wniesie sprzeciw na piśmie na solidnych podstawach związanych z ochroną danych na powołanie lub wymianę lub na nowego Podwykonawcę Przetwarzania w terminie piętnastu (15) dni od uprzedniego pisemnego powiadomienia wówczas Iron Mountain dołoży wszelkich starań by udostępnić Klientowi zmianę w Usługach lub zaleci zmianę w konfiguracji lub korzystaniu z Usług przez Klienta, w każdym przypadku w celu uniknięcia Przetwarzania Danych Osobowych Klienta przez Podwykonawcę Przetwarzania, na którego Klient wyraził sprzeciw, w celu rozważenia i zatwierdzenia przez Klienta. Jeżeli Klient nie wyrazi zgody na zmiany zaproponowane przez Iron Mountain w terminie piętnastu (15) dni Iron Mountain będzie miała prawo, przez wystosowanie pisemnego powiadomienia do Klienta, do niezwłocznego wypowiedzenia Usługi lub części Usługi, która nie może być wykonana przez Iron Mountain bez udziału oprotestowanego Podwykonawcy Przetwarzania. Wypowiedzenie takie nastąpi bez uszczerbku dla jakichkolwiek nabytych praw i zobowiązań stron, z zastrzeżeniem, że Iron Mountain oraz podmioty zależne Iron Mountain nie będą zobowiązane do zapłaty żadnych opłat z tytułu wypowiedzenia, kosztów ani rekompensat w związku z takim wypowiedzeniem, a Klient niezwłocznie przejmie we władanie wszelkie aktywa, które udostępnił Iron Mountain w ramach wypowiedzianych Usług, z zastrzeżeniem warunków Umowy oraz na koszt i rachunek własny Klienta.

6.4 Iron Mountain zapewni, że każda umowa z Podwykonawcami Przetwarzania dotycząca zakresu niniejszej UPD będzie zawierała postanowienia takie same we wszystkich istotnych aspektach jak postanowienia niniejszej UPD i zgodne z wymogami obowiązującego Ustawodawstwa o Ochronie Danych. Jeżeli Podwykonawca Przetwarzania Iron Mountain doprowadzi do naruszenia przez Iron Mountain jej zobowiązań na mocy niniejszej UPD lub obowiązującego Ustawodawstwa o Ochronie Danych, Iron Mountain będzie ponosiła całkowitą odpowiedzialność wobec Klienta za wypełnienie swoich zobowiązań zgodnie z tymi wymogami.

7. NARUSZENIE BEZPIECZEŃSTWA DANYCH

[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=JTlzF2zjI-gYEq5GmWmZcbgd--hqyVuIeEIP9Eu7Nvw&m=NB4wIISphmYGgqvrtYNU-28S8AaU6-YibdZ3Yg_2F68&s=xNzeKIzw6XbGZ_loyLbqEap2144HRDTflVtNiXKr6M4&e=

7.1 W przypadku podejrzenia Naruszenia Bezpieczeństwa Danych Iron Mountain:

7.1.1. niezwłocznie podejmie działania w celu zbadania podejrzeń Naruszenia Bezpieczeństwa Danych oraz zidentyfikowania, zapobieżenia, ograniczenia skutków podejrzanego Naruszenia Bezpieczeństwa Danych oraz naprawienia szkód spowodowanych Naruszeniem;

7.1.2. po powzięciu odpowiedniego stopnia pewności co do zaistnienia Naruszenia Bezpieczeństwa Danych bez zbędnej zwłoki powiadomi o tym Klienta oraz dostarczy mu szczegółowy opis Naruszenia Bezpieczeństwa Danych, włącznie z informacjami, które będą Klientowi niezbędne w celu wypełnienia jego obowiązków na mocy Ustawodawstwa o Ochronie Danych;

7.2. Klient wyraża zgodę na to, by Iron Mountain dostarczała informacje wymienione w punkcie 7.1.2. etapami. W takich przypadkach, gdy Iron Mountain nie będzie miała dostępu lub nie będzie mogła dostarczyć Klientowi określonych informacji wymienionych w punkcie 7.1.2. Iron Mountain poinformuje o tym Klienta i nie będzie ponosiła odpowiedzialności za niedostarczenie takich informacji.

8. AUDYTY

Iron Mountain pozwoli Klientowi i jego audytorom lub upoważnionym agentom, po wystosowaniu do Iron Mountain powiadomienia z wyprzedzeniem przynajmniej dziesięciu (10) dni roboczych, na przeprowadzenie audytów lub kontroli w okresie obowiązywania Umowy, z zastrzeżeniem, że Iron Mountain nie będzie musiała dostarczyć lub zapewnić dostępu do informacji dotyczących: (i) innych klientów Iron Mountain, (ii) jakichkolwiek raportów zewnętrznych Iron Mountain niepodanych do publicznej wiadomości, oraz (iii) raportów wewnętrznych sporządzonych przez działy audytu wewnętrznego lub przestrzegania prawa Iron Mountain. Cele audytu lub kontroli przeprowadzanych na mocy niniejszego akapitu będą ograniczały się do weryfikacji czy Iron Mountain dokonuje Przetwarzania Danych Osobowych Klienta zgodnie ze zobowiązaniami określonymi w niniejszej UPD. Jeżeli nie wystąpiło Naruszenie Bezpieczeństwa Danych będzie można przeprowadzić nie więcej niż jeden taki audyt w ciągu każdego okresu dwunastu (12) miesięcy.

9. MIĘDZYNARODOWE PRZEKAZYWANIE DANYCH (TRANSFER ORGANICZONY)

9.1. W stosownym zakresie Klient wyraża zgodę i zezwala na międzynarodowe przekazywanie Danych Osobowych Klienta na rzecz podmiotów określonych w punkcie 6.2 i zgodnie z Aneksem 3 w celu świadczenia Usług, przy czym Klient i Iron Mountain zobowiązują się i oświadczają:

9.1.1. przestrzegać obowiązującego Ustawodawstwa o Ochronie Danych w odniesieniu do takich transferów;

9.1.2 że, z uwzględnieniem między innymi (i) kategorii Danych Osobowych Klienta, (ii) krajów, których przepisy prawa krajowego nie zapewniają odpowiedniego poziomu ochrony Danych Osobowych o porównywalnym zakresie do obowiązującego w UE/Wlk. Brytanii („Państwa Trzecie"), (iii) odpowiednich środków technicznych i organizacyjnych wymienionych w artykule 7, oraz (iv) odpowiednich stron uczestniczących w przetwarzaniu takich Danych Osobowych Klienta, przeprowadzić ocenę zasadności danego mechanizmu przekazania przyjętego na mocy niniejszej Umowy jeżeli przepisy prawa tego wymagały i ustalić, że taki mechanizm przekazania jest adekwatnie zorganizowany aby zapewnić, że przekazanie Danych Osobowych odbywa się w zgodzie z postanowieniami UPD i zapewnia poziom ochrony w kraju docelowym zasadniczo równorzędny do poziomu zagwarantowanego na mocy Ustawodawstwa o Ochronie Danych.

10. ODPOWIEDZIALNOŚĆ I ODSZKODOWANIA

10.1 Niezależnie od wszelkich innych postanowień niniejszej Umowy, w przypadku Naruszenia Bezpieczeństwa Danych spowodowanego bezpośrednio przez niewykonanie przez Iron Mountain swoich obowiązków na mocy niniejszej UPD, Iron Mountain zwróci Klientowi, w zakresie dozwolonym przez obowiązujące przepisy prawa, bezpośrednie, udowodnione, konieczne i zasadnie poniesione koszty na rzecz stron trzecich poniesione w związku z (a) badaniem takiego Naruszenia Bezpieczeństwa Danych, (b) przygotowania wysyłania powiadomień do Podmiotów Danych oraz organów regulacyjnych zgodnie z wymogami Ustawodawstwa o Ochronie Danych, (c) świadczeniem usług monitorowania kredytu a rzecz osób zgodnie z wymogami prawa na okres nieprzekraczający dwanaście (12) miesięcy, oraz (d) wypłatą części grzywien, kar lub sankcji regulacyjnych nałożonych przez organ nadzorujący, za które według organu nadzorującego Iron Mountain ponosi bezpośrednią odpowiedzialność.

10.2 W przypadku wysunięcia roszczenia przez Podmiot Danych przeciwko którejkolwiek lub obu stronom z tytułu naruszenia Ustawodawstwa o Ochronie Danych („Roszczenia Podmiotów Danych") jeżeli takie są dozwolone, każda ze stron będzie kontrolowała swoją własną obronę przeciwko takiemu roszczeniu (lub swoją część obrony) i ponosiła wyłączną odpowiedzialność za swoje koszty, wydatki i zobowiązania z tym związane w tym honoraria prawnicze oraz wszelkie kwoty zasądzone od niej przez sąd lub należne w ramach ugody, z zastrzeżeniem jednak, że tam gdzie każda ze stron ponosi odpowiedzialność za część lub każda ze stron odpowiada za pełną kwotę szkody poniesionej przez Podmiot Danych za ten samy incydent lub serię incydentów a Podmiot Danych uzyskał pełną rekompensatę tylko od jednej strony („Strona Kompensująca"), wówczas Strona Kompensująca będzie miała prawo do dochodzenia od drugiej strony części rekompensaty odpowiadającej szkodzie wyrządzonej przez tę drugą stronę. Strona Kompensująca może wnosić roszczenie przeciwko drugiej stronie w ciągu 12 miesięcy po incydencie w zakresie dozwolonym przez obowiązujące przepisy prawa.

10.3 W najszerszym zakresie dozwolonym przez obowiązujące przepisy prawa ograniczenia odpowiedzialności oraz ewentualne wyłączenia odszkodowań określone w Umowie będą miały zastosowanie do łącznej odpowiedzialności z tytułu wszelkich roszczeń Klienta przeciwko Iron Mountain wynikających lub związanych z niniejszą UPD i/lub Umową. Tego rodzaju ograniczenia odpowiedzialności oraz wyłączenia odszkodowań mają zastosowanie do wszelkich roszczeń, niezależnie od tego czy powstały na gruncie umowy, deliktu czy innej teorii odpowiedzialności, oraz wszelkie odniesienia do odpowiedzialności Iron Mountain oznaczają łączną odpowiedzialność Iron Mountain i wszystkich podmiotów powiązanych Iron Mountain łącznie z tytułu roszczeń Klienta i wszystkich innych podmiotów powiązanych Klienta. W zakresie wymaganym przez obowiązujące przepisy prawa celem niniejszego punktu nie jest (i) zmodyfikowanie ani ograniczenie odpowiedzialności stron z tytułu roszczeń Podmiotów Danych przeciwko stronie jeżeli istnieje odpowiedzialność łączna i solidarna, ani (ii) ograniczenie odpowiedzialności którejkolwiek ze stron z tytułu zapłacenia kar nałożonych na tę stronę przez organ nadzorujący.

10.4. Punkty 10.1 do 10.3 określają indywidualne i wyłączne środki zadośćuczynienia każdej ze stron oraz indywidualną odpowiedzialność każdej ze stron z tytułu straty, szkody, kosztów lub zobowiązań związanych z niniejszą UPD.

11. ŻĄDANIA WŁADZ PUBLICZNYCH

11.1 W zakresie prawnie dozwolonym oraz z zastrzeżeniem punktów 11.2 do 11.5 poniżej Iron Mountain zobowiązuje się powiadomić Klienta jeżeli:

11.1.1 otrzyma prawnie obowiązujące żądanie od organu władzy publicznej, w tym od organów sądowych, na mocy prawa kraju docelowego, ujawnienia Danych Osobowych Klienta przekazanych na mocy niniejszej Umowy; oraz

11.1.2 poweźmie wiadomość o bezpośrednim dostępie władz publicznych do Danych Osobowych Klienta przekazanych na mocy Umowy zgodnie z prawem kraju docelowego;

11.2. Jeżeli powiadomienie Klienta przez Iron Mountain jest zabronione na mocy prawa kraju docelowego Iron Mountain zobowiązuje się dołożyć wszelkich starań by uzyskać uchylenie tego zakazu w celu przekazania możliwie największej ilości informacji możliwie jak najszybciej.

11.3. Iron Mountain zobowiązuje się zweryfikować zgodność z prawem takiego żądania ujawnienia, w szczególności tego czy znajduje się ono w granicach kompetencji żądającego organu władzy publicznej, oraz do zakwestionowania go jeżeli uzna, że istnieją uzasadnione podstawy by sądzić że żądanie jest niezgodne z prawem kraju docelowego. Iron Mountain nie dokona żądanego ujawnienia Danych Osobowych Klienta dopóki nie zostanie zobowiązana do tego na mocy obowiązujących przepisów postępowania.

11.4. Iron Mountain zobowiązuje się do przekazania minimalnej dozwolonej ilości informacji w ramach odpowiedzi na żądanie ujawnienia, w oparciu o zasadną interpretację takiego żądania.

11.5. Iron Mountain zobowiązuje się do przechowywania informacji na mocy niniejszego akapitu przez okres obowiązywania Umowy oraz do udostępniania ich na wniosek kompetentnych organów nadzorujących.

12. POSTANOWIENIA RÓŻNE

12.1 Z zastrzeżeniem charakteru Usług świadczonych przez Iron Mountain, po wypowiedzeniu/wygaśnięciu Umowy, w oparciu o konkretne instrukcje Klienta i zgodnie z postanowieniami Umowy, Iron Mountain albo usunie/zniszczy lub zwróci Klientowi lub stronie trzeciej wyznaczonej przez Klienta wszystkie Dane Osobowe Klienta. Wszelkie Dane Osobowe Klienta zawarte w aktywach Klienta przechowywanych przez Iron Mountain na rzecz Klienta zostaną zwrócone Klientowi zgodnie z ustalony planem wyjścia lub przejścia i zgodnie z ustalonymi kosztami, jak określono w Umowie lub innym obowiązującym dokumencie umownym. We wszystkich pozostałych przypadkach, jeżeli Umowa nie wypowiada się na temat usunięcia/zniszczenia lub zwrotu Danych Osobowych Klienta a Klient nie przekaże instrukcji dotyczących usunięcia/zniszczenia lub zwrotu Danych Osobowych Klienta w terminie piętnastu (15) dni od wypowiedzenia/wygaśnięcia Umowy, Iron Mountain wystosuje do Klienta pisemne powiadomienie z żądaniem przesłania w terminie piętnastu (15) dni konkretnych pisemnych instrukcji dotyczących tego czy usunąć/zniszczyć czy zwrócić Dane Osobowe Klienta, oraz informujące Klienta o wszystkich obowiązujących opłatach za bezpieczne zniszczenie lub innych należnych od Klienta. Gdyby Klient nie przedstawił pisemnych instrukcji w takim piętnastodniowym (15) terminie i nie zapłacił w tym terminie należnych opłat Klient niniejszym upoważnia Iron Mountain do dalszego Przetwarzania, usunięcia, zniszczenia wszystkich Danych Osobowych Klienta po wypowiedzeniu Umowy według uznania Iron Mountain i na koszt Klienta.

12.2 Niezależnie od postanowień punktu 12.1 Iron Mountain nie dopuści się naruszenia swoich zobowiązań w odniesieniu do usunięcia Danych Osobowych Klienta zachowanych na taśmach zapasowych jeżeli takie zapasowe awaryjne zostaną nadpisane (tym samym usuwając Dane Osobowe Klienta) w toku normalnej działalności.

12.3 Z wyjątkiem Standardowych Klauzul Umownych (zgodnie z definicją zawartą w Aneksie 3 do niniejszej UPD), prawem właściwym dla niniejszej UPD oraz ewentualnego sporu, roszczenia lub kontrowersji wynikającej lub związanej z niniejszą UPD, jej naruszeniem, wypowiedzeniem lub ważnością, jest prawo wybrane w stosownym postanowieniu Umowy; wszelkie spory, kontrowersje lub roszczenia wynikające lub związane z niniejszą UPD będą podlegały rozstrzygnięciu na drodze procedur rozstrzygania sporów określonej w Umowie.

12.4 Każda ze stron ma prawo każdorazowo powiadomić drugą stronę na piśmie o ewentualnych zmianach do niniejszej UPD, które strona ta zasadnie uznaje za konieczne w celu sprostania wymogom Ustawodawstwa o Ochronie Danych lub wszelkim postanowieniom organu nadzorującego lub właściwego sądu. Wszelkie tego rodzaju zmiany będą skuteczne tylko jeżeli i w takim zakresie, w jakim będą wprowadzone na mocy wspólnie uzgodnionej poprawki do niniejszej UPD sporządzonej przez obie strony z wyjątkiem, sytuacji gdy jedna strona informuje drugą o nowych wymogach prawnych i prześle taką poprawkę zawierającą tylko niezbędne zmiany, które mogą być przyjęte bez formalnych uzgodnień, tzn. przez niewniesienie sprzeciwu w określonym terminie, i tego rodzaju poprawki będą uznawane za uzgodnione wspólnie poprawki do UPD.

ANEKS 1

Informacje szczegółowe dotyczące Przetwarzania i Przekazywania Danych (jeżeli ma zastosowanie)

A. WYKAZ STRON:

Strony niniejszej UPD oraz role Eksportera Danych oraz Importera Danych zostały określone w Umowie i Aneksie 3 (Międzynarodowe Przekazanie Danych), jeżeli ma to zastosowanie.

B. OPIS PRZETWARZANIA/PRZEKAZANIA (jeżeli ma zastosowanie):

Kategorie Podmiotów Danych, których Dane Osobowe są przetwarzane/przekazywane:

W zależności od charakteru Usług Iron Mountain oraz działalności Klienta Klient może dostarczać Iron Mountain Dane Osobowe należące do różnych kategorii Podmiotów Danych, których zakres jest ustalany i kontrolowany przez Klienta według jego wyłącznego uznania. W związku z tym kategorie Podmiotów Danych mogą obejmować: aktualnych i byłych pracowników, aktualnych i byłych podwykonawców lub konsultantów, wykonawców i konsultantów poleconych przez agencje i osoby oddelegowane z zewnątrz, osoby aplikujące o pracę i kandydatów, studentów i wolontariuszy, osoby określone przez pracowników lub emerytów jako beneficjenci, małżonkowie, partnerzy domowi/cywilni, osoby na utrzymaniu oraz osoby kontaktowe w nagłych przypadkach, emerytów, aktualnych i byłych dyrektorów i członków kierownictwa, udziałowców/akcjonariuszy, obligatariuszy, posiadaczy kont, użytkowników końcowych/konsumentów (osoby dorosłe, dzieci), pacjentów (osoby dorosłe, dzieci), przechodniów (kamery CCTV) oraz użytkowników stron internetowych.

Kategorie przetwarzanych/przekazywanych Danych Osobowych:

W zależności od charakteru Usług Iron Mountain oraz działalności Klienta Klient może dostarczać Iron Mountain Dane Osobowe należące do różnych kategorii Podmiotów Danych, których zakres jest ustalany i kontrolowany przez Klienta według jego wyłącznego uznania. W związku z tym kategorie mogą obejmować dane osobowe dotyczące Klienta i/lub jego własnych klientów, pracowników itp.

Przekazywanie danych wrażliwych (jeżeli ma zastosowanie)

W zależności od charakteru Usług Iron Mountain oraz działalności Klienta Klient może dostarczać Iron Mountain dane wrażliwe, których zakres jest ustalany i kontrolowany przez Klienta według jego wyłącznego uznania.

Jeżeli ma to zastosowanie, częstotliwość przekazywania (np. czy dane są przekazywane jednorazowo czy w sposób ciągły)

Przekazywanie odbywa się w sposób ciągły.

Charakter Przetwarzania:

Zbieranie, utrwalanie, organizowanie, strukturyzowanie, przechowywanie, adaptacja lub zmiana, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie na drodze transmisji, rozpowszechniania lub innych sposobów udostępniania, przyrównywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Cele Przetwarzania/Przekazywania danych (jeżeli ma zastosowanie) i dalszego Przetwarzania:

Świadczenie Usług jak określono w Umowie.

Utrzymywanie Danych:

Dane Osobowe będą utrzymywane przez Iron Mountain przez okres świadczenia Usług na rzecz Klienta i do momentu zwrotu lub zniszczenia Danych Osobowych zgodnie z postanowieniami punktu 12.1 niniejszej UPD.

Jeżeli ma to zastosowanie, w przypadku przekazywania Przetwarzającym (Podwykonawcom Przetwarzania) określić przedmiot, charakter i czas Przetwarzania:

W okresie obowiązywania Umowy z Klientem Podwykonawcy Przetwarzania dostarczają między innymi usług informatycznych (IT) i doradczych, w tym globalnego wsparcia IT, raportowania o zdarzeniach oraz usług zarządzania.

WŁAŚCIWY ORGAN NADZORUJĄCY

Określony w Załączniku 3 (Międzynarodowe Przekazywanie Danych), jeżeli ma zastosowanie.

ANEKS 2
ŚRODKI TECHNICZNE I ORGANIZACYJNE („ZABEZPIECZENIA")

1. PROGRAM I POLITYKA BEZPIECZEŃSTWA INFORMACJI

Iron Mountain zobowiązana jest do posiadania programu bezpieczeństwa informacji z odpowiednimi fizycznymi, technicznymi i administracyjnymi środkami kontroli spełniającymi standardy branży. Program bezpieczeństwa informacji będzie obejmował:

1.1. Dokumentację, publikacje wewnętrzne oraz komunikowanie informacji na temat wewnętrznych zasad bezpieczeństwa, standardów i procedur Iron Mountain;

1.2. Udokumentowany, wyraźny przydział odpowiedzialności i uprawnień mający na celu ustanowienie i utrzymywanie programu bezpieczeństwa informacji;

1.3. Regularne testowanie kluczowych punktów kontrolnych, systemów i procedur programu bezpieczeństwa informacji;

1.4. Środki administracyjne, techniczne i operacyjne mające na celu ochronę wszystkich Danych Osobowych Klienta wykorzystujące praktyki, procedury i procesy opisane w niniejszym Aneksie dotyczącym bezpieczeństwa w takim zakresie, w jakim są one odpowiednie i mają zastosowanie do formatu, w jakim utrzymywane są Dane Osobowe Klienta.

2. OCENA RYZYKA

Iron Mountain zobowiązana jest utrzymywać program oceny ryzyka dla bezpieczeństwa mający na celu identyfikację i ocenę zasadnie przewidywalnego ryzyka wewnętrznego i zewnętrznego oraz słabych punktów, które mogą mieć wpływ na bezpieczeństwo, poufność i/lub integralność Danych Osobowych Klienta. Iron Mountain będzie oceniała i aktualizowała, w razie potrzeby oraz gdy jest to zasadne i odpowiednie, skuteczność aktualnego programu bezpieczeństwa informacji w celu ograniczania takiego ryzyka, co roku lub zawsze gdy nastąpi istotna zmiana w zakresie ryzyka lub słabych punktach dla Danych Osobowych Klienta.

3. ZARZĄDZANIE AKTYWAMI PRZETWARZANIA INFORMACJI I MEDIAMI FIZYCZNYMI

3.1. Zarządzanie Aktywami Przetwarzania Informacji. Iron Mountain prowadzi program zarządzania zbiorem aktywów w celu zarządzania fizycznymi, technicznymi i administracyjnymi środkami kontroli aktywów przetwarzania danych Iron Mountain (takimi jak komputery, serwery, urządzenia do przechowywania, sieci komunikacyjne, komputery osobiste, laptopy i urządzenia peryferyjne).

Program zarządzania zbiorem aktywów obejmuje następujące działania:

3.1.1. Udokumentowany przydział i przynależność aktywów do pracowników Iron Mountain w celu zapewnienia odpowiedniej klasyfikacji informacji, określenia ograniczeń dostępu oraz weryfikacji kontroli dostępu;

3.1.2. Sanityzacja aktywów przed ich utylizacją zgodnie z NIST 800-88;

3.1.3. Wymóg autoryzacji przez zarząd przed usunięciem sprzętu lub oprogramowania nie przydzielonego do konkretnej osoby z pomieszczeń Iron Mountain.

3.2. Środki kontroli. Środki kontroli Iron Mountain obejmują:

3.2.1. Procedury operacyjne i środki kontroli technicznej mające na celu ochronę dokumentów, mediów komputerowych, dane wchodzące/wychodzące/kopie zapasowe oraz dokumentacji systemu przed nieuprawnionym ujawnieniem, modyfikacją i zniszczeniem;

3.2.2. Procedury mające na celu bezpieczną utylizację mediów elektronicznych i fizycznych zawierających Dane Osobowe Klienta;

3.2.3. Ustalony proces śledzenia wszystkich fizycznych mediów Klienta od przejęcia pieczy nad nimi przez Iron Mountain do stałego wycofania lub zniszczenia.

ZABEZPIECZENIA DOTYCZĄCE PRACOWNIKÓW

4.1. Poufność. Iron Mountain będzie zasadnie wymagać by wszyscy pracownicy, w tym pracownicy tymczasowi i zakontraktowani zobowiązali się do zachowania poufności Danych Osobowych Klienta oraz przestrzegali wewnętrznych zasad bezpieczeństwa informacji i przyjętych wymogów dotyczących ich wykorzystania.

4.2 Polityka Badania Przeszłości. Iron Mountain posiada politykę badania przeszłości oraz politykę badania na obecność narkotyków (tylko USA) wobec swoich pracowników. Iron Mountain będzie utrzymywała takie polityki przez cały okres obowiązywania Umowy. Wymogi tych polityk obejmują między innymi testy na obecność narkotyków (tylko USA), weryfikację tożsamości pracowników, badanie przeszłości kryminalnej, weryfikację zatrudnienia, przeszukiwanie państwowych list rządowych/terrorystycznych oraz weryfikację wykształcenia w przypadku niektórych pracowników, a także historii posiadania prawa jazdy i wykroczeń w przypadku kandydatów na kierowców i już pracujących kierowców. W przypadku sprawdzenia przeszłości jeżeli ujawnione zostaną informacje niekorzystne Iron Mountain dokonuje indywidualnej oceny zgodnie z obowiązującym prawem pracy i zasadami dobrej praktyki.

4.3 Praca z Podwykonawcami. Iron Mountain wymaga, by podwykonawcy wykonujący Usługi na mocy Umowy przestrzegali podobnych ograniczeń do tych określonych w niniejszym akapicie, w odniesieniu do wszystkich pracowników podwykonawców wykonujących Usługi na mocy Umowy, które obejmują Przetwarzanie Danych Osobowych Klienta.

4.4 Szkolenie z Wiedzy o Bezpieczeństwie. Przynajmniej raz do roku Iron Mountain przeprowadza ogólne szkolenie z wiedzy o bezpieczeństwie oraz specjalistyczne szkolenie uzależnione od funkcji dla wszystkich pracowników Iron Mountain, którzy mają dostęp do Danych Osobowych Klienta. Iron Mountain prowadzi dokumentację z nazwiskami uczestniczących pracowników Iron Mountain oraz datami każdego takiego szkolenia. Iron Mountain regularnie weryfikuje i aktualizuje swój program szkolenia z wiedzy o bezpieczeństwie.

4.5 Zwalnianie Pracowników Iron Mountain. Iron Mountain posiada procedurę dyscyplinarną stosowaną wobec tych swoich pracowników, którzy winni są naruszenia określonych tutaj zasad bezpieczeństwa.

4.6 Zamknięcie Dostępus po Wypowiedzeniu/Przeniesieniu. Z chwilą zwolnienia lub przeniesienia na funkcję niewymagającą dostępu do Danych Osobowych Klienta dostęp pracownika Iron Mountain do Danych Osobowych Klienta zostanie niezwłocznie anulowany.

5. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

5.1 Fizyczne środki kontroli bezpieczeństwa. Obiekty Iron Mountain wyposażone są w fizyczne środki kontroli, które odpowiednio ograniczają dostęp do Danych Osobowych Klienta w sposób, jaki Iron Mountain uważa za stosowny: protokoły kontroli dostępu, bariery fizyczne takie jak zamykanie obiektów i obszarów, identyfikatory dostępu dla pracowników, rejestry gości, identyfikatory dostępu dla gości, czytniki kart, wideo-kamery monitoringu oraz alarmy wykrywające wtargnięcie. Wszyscy goście muszą się zarejestrować i poruszać się z osobą eskortującą.

5.2 Wsparcie mediów. Iron Mountain stosuje środki mające na celu ochronę obiektów zawierających Dane Osobowe Klienta oraz systemy przed awariami energii elektrycznej, telekomunikacji, dostaw wody, odprowadzenia ścieków, wentylacji i klimatyzacji, w zależności od sytuacji.

5.3 Zabezpieczenie systemów transmisji. Iron Mountain stosuje środki mające na celu ochronę fizycznego bezpieczeństwa sieci infrastruktury oraz systemów telekomunikacyjnych przed przechwyceniem i uszkodzeniem.

5.4 Sprzęt poza terenem. W przypadku stosowania przez Iron Mountain outsourcingu wymagającego korzystania ze sprzętu poza terenem w celu wspierania świadczonych usług wszelki sprzęt znajdujący się poza terenem na którym przechowywane są Dane Osobowe Klienta jest chroniony przez zabezpieczenia równoważne z tymi stosowanymi dla sprzętu będącego na terenie i wykorzystywanego w tym samym celu.

5.5 Fizyczny dostęp do Aktywów Przetwarzania Danych. Iron MOuntain przechowuje dokumentację pracowników Iron Mountain upoważnionych do fizycznego dostępu do środowisk(a) komputerowych(ego) kontrolowanego(ych) przez Iron Mountain i wykorzystywanego przez Iron Mountain do świadczenia Usług przez okres jednego roku, i na wniosek Klienta związany z Naruszeniem Bezpieczeństwa Danych oraz z zastrzeżeniem polityki bezpieczeństwa Iron Mountain przekaże Klientowi dostęp do podlegającej kontroli dokumentacji takich pracowników Iron Mountain.

5.6 Ograniczenie dostępu fizycznego. Iron Mountain ogranicza dostęp fizyczny do kontrolowanych przez siebie obiektów w których wykonywane jest Przetwarzanie Danych Osobowych Klienta do tych pracowników Iron Mountain i upoważnionych osób, które mają potrzebę biznesową takiego dostępu. Iron Mountain stosuje procedurę zezwoleń w celu autoryzacji i śledzenia wniosków o dostęp fizyczny do takich obiektów.

5.7 Naprawy i modyfikacje. Iron Mountain odnotowuje wszystkie naprawy związane z bezpieczeństwem oraz modyfikacje wszelkich komponentów fizycznych takich jak sprzęt, ściany, drzwi oraz zamki do zabezpieczonych obszarów w obiektach, w których przechowywane są Dane Osobowe Klienta.

5.8 Dokumentacja. Firma przechowuje dokumentację ruchu sprzętowego i mediów elektronicznych a także wszelkich osób za nie odpowiedzialnych.

6. KOMUNIKACJA I ZARZĄDZANIE OPERACJAMI PRZETWARZANIA INFORMACJI

6.1 Standardy konfiguracji urządzeń. Iron Mountain stworzy, wdroży i będzie utrzymywać procedury administracji systemu spełniające standardy branży, w tym między innymi hardening systemu oraz łatki *[patching]* urządzeń (system operacyjny i aplikacje) oraz odpowiednie instalacje antywirusowe i ich aktualizacje.

6.2 Zmiana kontroli nad systemami przetwarzania informacji. Iron Mountain zobowiązana jest posiadać wewnętrzne formalne procedury zarządzania wnioskami o zmianę w odniesieniu do systemów przetwarzania informacji i sieci komunikacyjnych, i wnioski i zmianę Iron Mountain będą udokumentowane, przetestowane i zatwierdzone przed wdrożeniem jakichkolwiek nowych możliwości przetwarzania informacji lub sieci komunikacyjnych, łatek systemu lub zmian w dotychczasowych systemach.

6.3 Segregacja obowiązków. Iron Mountain będzie segregowała obowiązki i zakresy obowiązków w taki sposób, aby żadna pojedyncza osoba nie miała możliwości modyfikowania systemów przetwarzania informacji, które mają dostęp do Danych Osobowych Klienta.

6.4 Oddzielenie środowiska rozwoju i produkcji. Środowiska rozwoju, testowania i produkcji Iron Mountain dla potrzeb systemów przetwarzania informacji muszą być logicznie i fizycznie rozdzielone.

6.5 Zarządzanie architekturą techniczną. Iron Mountain ustanowi proces zarządzania konfiguracją, który będzie definiował, zarządzał i kontrolował komponenty systemu przetwarzania informacji wykorzystywane do świadczenia Usług oraz infrastrukturę techniczną takich komponentów.

6.6 Wykrywanie wtargnięcia. Iron Mountain będzie przez cały czas prowadziła monitoring systemów i procesów komputerowych pod kątem prób lub faktycznych zakłóceń lub naruszeń bezpieczeństwa i będzie powiadamiać Klienta o każdym nieautoryzowanym dostępie do Danych Osobowych Klienta.

6.7 Bezpieczeństwo sieci. Iron Mountain zapewni stosowanie następujących środków:

6.7.1. W odniesieniu do środowisk(a) wykorzystywanego do świadczenia Usług, którego hostem jest Iron Mountain - system wykrywania wtargnięcia („IDS" – Intrusion Detection System) oraz czujniki zapobiegania wtargnięciu („IPS"- Intrusion Prevension Sensors), które alarmują o zarejestrowanych zdarzeniach, przy czym generowane są codzienne raporty do kontroli (łącznie zwane „IDS/IPS").

6.7.2. W odniesieniu do środowisk(a) wykorzystywanego do świadczenia Usług, którego hostem jest Iron Mountain, IDS/IPD aktualizowane nie rzadziej niż raz w tygodniu ale tak szybko jak to praktycznie możliwe po otrzymaniu aktualizacji, i niezwłoczne wdrożenie najnowszych sygnatur lub zasad zagrożeń.

6.7.3 Porty wysokiego ryzyka na systemach skierowanych na zewnątrz nie są dostępne przez internet.

6.7.4 Łącza sieciowe Iron Mountain są zalogowane i dokumentowane w plikach logowania.

6.7.5. Rozmieszczenie ścian ogniowych *[firewall]* mających na celu ochronę i kontrolę całego wchodzącego i wychodzącego ruchu obsługi pomiędzy określonymi punktami sieci.

6.7.6. Polityka hardeningu w celu zdefiniowania portów wejściowych i wyjściowych sieci lub ruchu obsługi dla wszystkich systemów należących lub zarządzanych przez Iron Mountain, które są udokumentowane i uwierzytelnione w ramach programu bezpieczeństwa informacji.

6.7.7. Porty sieciowe i diagnostyczne odpowiednio zabezpieczone; oraz

6.7.8. Polityki, procedury i środki kontroli technicznej mające na celu zapobieganie, wykrywanie i usuwanie kodów złośliwych lub znanych ataków na systemy informatyczne Iron Mountain.

6.8. Szyfrowane dane uwierzytelniające. Iron MOuntain zapewni, że dane uwierzytelniające przekazywane przy pomocy urządzeń sieciowych Iron Mountain będą po drodze zaszyfrowane.

6.9. Bezpieczna administracja sieci. Sieci Iron Mountain będą odpowiednio zarządzane i kontrolowane aby chronić je przed znanymi zagrożeniami oraz zachować bezpieczeństwo wszystkich aplikacji zarządzanych przez Iron Mountain a także danych w sieci oraz przepływających przez sieć. Wdrażane będą środki kontroli technicznej i bezpieczne protokoły komunikacji aby zapobiec nienadzorowanym połączeniom z sieciami niezaufanymi lub publicznie dostępnymi serwerami.

6.10. Ochrona przed wirusami. Iron Mountain wdroży i będzie utrzymywał program zarządzania antywirusowego, w tym ochronę przed złośliwym oprogramowaniem, aktualne pliki podpisu lub inne środki ochrony przed pojawiającymi się zagrożeniami, łatkami i definicjami wirusów, dla serwerów i stanowisk roboczych zarządzanych przez Iron Mountain wykorzystywanych do przechowywania lub dostępu do Danych Osobowych Klienta.

6.11. Strona internetowa – szyfrowanie Klienta. Iron Mountain zapewni bezpieczny dostęp do internetu przy pomocy Secure Sockets Layering (SSL) i ważnego certyfikatu SSL wymagającego kontroli poufności, uwierzytelniania oraz autoryzacji.

6.12. Kopie zapasowe informacji. Iron Mountain utworzy odpowiednie kopie zapasowe plików systemowych. Oprócz tego Iron Mountain opracuje i będzie utrzymywać procedury odzyskiwania danych na wypadek katastrofy, więcej szczegółów patrz „Odzyskiwanie danych w przypadku katastrofy".

6.13. Tranzyt informacji elektronicznych. Iron Mountain będzie wykorzystywać szyfrowanie przy pomocy algorytmu o standardzie odpowiednim w branży o minimalnej długości klucza 12 bitów w celu ochrony Danych Osobowych Klienta przekazywanych przez sieci publiczne jeżeli będą one rozpoczynały przepływ na infrastrukturze, której hostem jest Iron Mountain.

6.14. Kontrole kryptograficzne. Iron Mountain będzie przestrzegała udokumentowanej polityki dotyczącej korzystania z kontroli kryptograficznych. Kontrole kryptograficzne Iron Mountain będą:

6.14.1. miały na celu zasadną ochronę poufności i integralności Danych Osobowych Klienta przetwarzanych, przesyłanych lub przechowywanych przez Iron Mountain w jakimkolwiek wspólnym środowisku sieciowym zgodnie z postanowieniami Umowy;

6.14.2. stosowane w środowisku(ach) którego(ych) hostem jest Iron Mountain i wykorzystywanych do świadczenia usług, do Danych Osobowych Klienta przepływających przez „niezaufane" sieci (tzn. sieci których Iron Mountain zgodnie z prawem nie kontroluje), w tym używanych do przesyłu danych do sieci korporacyjnej Klienta z sieci Iron Mountain, w każdym wypadku z zastrzeżeniem współpracy Klienta w zakresie zarządzania kluczami szyfrowania koniecznymi do rozszyfrowania transmisji otrzymanych przez Klienta, oraz

6.14.3. obejmowały udokumentowane praktyki zarządzania kluczami szyfrowania w celu wspierania bezpieczeństwa technologii szyfrowania;

6.14.4. obejmowały szyfrowanie wszystkich Danych Osobowych Klienta na laptopach i innych urządzeniach przenośnych.

6.15. Wymogi rejestrowania: Iron Mountain zapewni jak następuje:

6.15.1. Istotne wydarzenia z zakresu bezpieczeństwa i systemów są rejestrowane i weryfikowane.

6.15.2. Rejestry audytów są przechowywane przez minimum rok dla systemów w środowiskach, których hostem jest Iron Mountain wykorzystywanych do świadczenia usług;

6.15.3. Rejestry audytów systemu są weryfikowane pod kątem anomalii, oraz

6.15.4. Urządzenia rejestrów i informacje o systemach są odpowiednio chronione przed manipulacją i nieuprawnionym dostępem.

6.16. Synchronizacja czasu sieci. Iron Mountain zapewni synchronizację zegarów systemowych wszystkich systemów przetwarzania informacji korzystając z autorytatywnego źródła czasu.

6.17. Rozdział sieci. Iron Mountain dokona odpowiedniej segregacji powiązanych grup usług informatycznych, użytkowników oraz systemów informatycznych na sieciach.

7. KONTROLA DOSTĘPU

7.1. Polityka kontroli dostępu. Iron Mountain stosuje politykę kontroli dostępu w odniesieniu do aktywów przetwarzania informacji, które podlegają formalnemu zatwierdzeniu przez Iron Mountain, publikacji i wdrożeniu.

7.2. Logiczna autoryzacja dostępu. Iron Mountain posiada zatwierdzoną procedurę dla wniosków o dostęp logiczny do Danych Osobowych Klienta i wniosków o dostęp do systemów Iron Mountain przeznaczonych do wykonywania Usług.

7.3. Kontrola dostępu i weryfikacja dostępu. Iron Mountain udzieli dostępu do Danych Osobowych Klienta tylko aktywnym pracownikom Iron Mountain, w tym pracownikom tymczasowym i na kontraktach, a także aktywnym użytkownikom kont którym taki dostęp jest potrzebny w celu wykonywania obowiązków służbowych. Wszelki uprzywilejowany dostęp musi zostać zweryfikowany i potwierdzony jako zgodny z aktualną funkcją służbową oraz udokumentowany przynajmniej raz na kwartał,

7.4. Kontrola dostępu osób trzecich. Przed udzieleniem dostępu stronom zewnętrznym do systemów informatycznych Iron Mountain mających dostęp do Danych Osobowych Klienta Iron Mountain zobowiązana jest zapewnić odpowiednie środki kontroli.

7.5. Kontrola dostępu do systemów operacyjnych. Iron Mountain zobowiązana jest kontrolować dostęp do systemów operacyjnych (zarówno opartych na sprzęcie jak i oprogramowaniu) przez wymaganie procedury logowania, która przeprowadza dokładną identyfikację osoby mającej dostęp do systemu operacyjnego.

7.6. Mobilne urządzenia komputerowe. Iron Mountain zobowiązana jest stosować politykę lub procedurę mającą na celu ochronę mobilnych urządzeń komputerowych Iron Mountain przed nieuprawnionym dostępem. Tego rodzaju polityka lub procedury będą obejmowały ochronę fizyczną, kontrolę dostępu oraz kontrolę bezpieczeństwa taką jak szyfrowanie, ochrona przeciwwirusowa oraz kopie zapasowe urządzenia.

7.7. Izolacja systemów Klienta. W ramach środowisk(a), w których Iron Mountain jest hostem wykorzystywanych do świadczenia Usług Iron Mountain zobowiązana jest utrzymać logiczny rozdział i segregację Danych Osobowych Klienta od wszelkich innych informacji.

7.8. Konta. W odniesieniu do kont Iron Mountain zobowiązana jest:

7.8.1. Wymagać uwierzytelnienia tożsamości każdego pracownika Iron Mountain ubiegającego się o dostęp do systemów Iron Mountain które Przetwarzają Dane Osobowe Klienta oraz zakazać używania wspólnych kont o generycznych danych referencyjnych (np. ID) w celu uzyskania dostępu do Danych Osobowych Klienta lub systemów.

7.8.2. Wymagać, aby wszystkie ID użytkowników, w tym konta uprzywilejowane, były powiązane bezpośrednio z osobą (a nie ze stanowiskiem).

7.6.3. Jeżeli domyślne konta administracyjne nie są wyłączone lub usunięte, wymagać korzystania z tymczasowych haseł, ID wylogowania lub temu podobnych środków kontroli w celu dostępu do domyślnych kont administracyjnych.

7.8.4. Wymagać, by nieaktywne regularne konta były zablokowane lub wyłączone po 90 dniach braku aktywności.

7.8.5. Zakazać dostępu kontu po kilku nieudanych próbach dostępu.
7.8.6. Wymagać unikalnych identyfikatorów i silnych haseł zawierających przynajmniej: najmniejsza liczba znaków 8; obowiązkowa zmiana co 90 dni; wymogi stopnia skomplikowania.
7.8.7. Zakaz udostępniania lub zapisywania haseł.

7.9. Kontrola systemów pozostających bez nadzoru. Iron Mountain będzie korzystać z wygaszacza ekranu chronionego hasłem dla wszystkich systemów pozostawionych bez nadzoru i nie działających przez 30 minut.

8. NABYWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW INFORMATYCZNYCH

8.1. Bezpieczeństwo rozwoju systemów. Iron Mountain zapewni by bezpieczeństwo było częścią rozwoju wszystkich systemów informatycznych i operacyjnych oraz będzie publikować i przestrzegać wewnętrznych bezpiecznych metodologii kodowania opartych na standardach bezpieczeństwa opracowywania aplikacji.

8.2. Zarządzanie bezpieczeństwem oprogramowania. Systemy informatyczne Iron Mountain (w tym systemy operacyjne, infrastruktura, aplikacje biznesowe, usługi oraz aplikacje opracowane po stronie użytkownika) będą zaprojektowane w sposób zgodny ze standardami bezpieczeństwa informatycznego.

8.3. Wykresy sieci. Iron Mountain opracuje, udokumentuje i będzie utrzymywać fizyczne i logiczne diagramy urządzeń sieciowych i ruchu.

8.4. Ocena słabości aplikacji/Etyczny hacking. Co najmniej raz do roku Iron Mountain przeprowadzi ocenę słabości aplikacji w środowisku(ach), w których jest hostem a wykorzystywanych do świadczenia usług Przetwarzania Danych Osobowych Klienta. Szczegółowe wyniki będą stanowiły informacje własne i poufne Iron Mountain i nie będą udostępniane.

8.5. Testowanie i weryfikacja zmian. Iron Mountain będzie weryfikowała i testowała zmiany w aplikacjach i systemach operacyjnych przed ich wdrożeniem aby zapewnić, że nie mają negatywnych skutków dla Danych Osobowych Klienta lub systemów.

9. ODZYSKIWANIE DANYCH PO KATASTROFACH

Iron Mountain zobowiązana jest posiadać plan odzyskania danych po katastrofie, obejmujący odtworzenie systemów i danych elektronicznych wykorzystywanych do świadczenia Usług w zapasowym centrum danych. Odtworzenie systemów i danych elektronicznych nie obejmuje Danych Osobowych Klienta fizycznie przechowywanych w obiekcie Iron Mountain. Iron Mountain będzie też utrzymywała plan zapewnienia ciągłości działania mający na celu przywrócenie krytycznych funkcji biznesowych. Iron Mountain zobowiązana jest przeprowadzać testy odzyskiwania danych po katastrofie nie rzadziej niż co dwanaście 1(12) miesięcy).

10. AUDYTY I OCENY ZEWNĘTRZNE

Protokoły bezpieczeństwa Iron Mountain są zbudowane w sposób zgodny ze standardami branży. Iron Mountain będzie przedstawiała Klientowi zlecone przez siebie raporty niezależnych zewnętrznych audytorów (np. PCI, ISO27001, SOC2 itp.) stosownie do Usług w regionie, gdzie takie Usługi są świadczone („Raport z Audytu”). Iron Mountain dostarczy wszystkie takie raporty zlecone na potrzeby klientów niezależnie od wyników tych raportów. Iron Mountain nie będzie zobowiązana do przedstawiania wyników audytów wewnętrznych ani wyników innych niezależnych ocen zleconych z

założeniem, że będą one poufne dla Iron Mountain. Klient oraz jego audytorzy zewnętrzni będą otrzymywali kopie Raportu z Audytu na życzenie. Wszelkie Raporty z Audytów lub inne wyniki generowane w wyniku testów lub audytów opisanych w niniejszym akapicie będą uważane za Informacje Poufne Iron Mountain. Klient będzie miał prawo przekazać egzemplarz takiego Raportu z Audytu ewentualnym klientom lub regulatorom Klienta z zastrzeżeniem zobowiązania do zachowania poufności tak restrykcyjnym, jak zobowiązanie określone w niniejszym dokumencie. Na wniosek Klienta Iron Mountain potwierdzi na piśmie, że nie wprowadzono żadnych zmian do odpowiednich polityk, procedur ani środków kontroli wewnętrznej od zakończenia Raportu z Audytu, które nie może obejmować dłuższego okresu czasu niż trzy miesiące od końca okresu sprawozdawczego opisanego w Raporcie z Audytu.

ANEKS 3
Międzynarodowe przekazywanie danych

1. DEFINICJE

„Standardowe klauzule umowne UE 2021" oznacza standardowe klauzule umowne dotyczące transferu Danych Osobowych do państw trzecich na mocy RODO, przyjęte przez Komisję Europejską na mocy Postanowienia Wykonawczego Komisji (UE) 2021/914 dostępnego tutaj[3].

„Dodatek UK 2022" oznacza szablon Dodatek B.1.0 wydany przez Urząd Komisarza ds. Informacji Wielkiej Brytanii i przedłożony Parlamentowi zgodnie z s119A Ustawo o Ochronie Danych z 2018 r. w dniu 2 lutego 2022 r., z ewentualnymi zmianami na mocy ustępu 18 tej ustawy, dostępny tutaj[4].

„Dane Osobowe Klienta UE" oznacza Przetwarzanie Danych Osobowych Klienta, do których miały zastosowanie przepisy prawa o ochronie danych Unii Europejskiej lub Państwa Członkowskiego Unii Europejskiej lub Europejskiego Obszaru Gospodarczego przed ich przetwarzaniem przez Iron Mountain.

„Obszar Chroniony" oznacza:

i. w przypadku Danych Osobowych Klienta UE członków państw Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego oraz dowolny kraj, terytorium, sektor lub organizację międzynarodową, w odniesieniu do których obowiązuje postanowienie o adekwatności na mocy Art. 45 RODO;

ii. w przypadku Danych Osobowych Klienta UK, Wielką Brytanię oraz dowolny kraj, terytorium, sektor lub organizację międzynarodową w odniesieniu do których obowiązuje postanowienie o adekwatności na mocy brytyjskich przepisów o adekwatności;

iii. w przypadku szwajcarskich Danych Osobowych Klienta, Wielką Brytanię oraz dowolny kraj, terytorium, sektor lub organizację międzynarodową uznane za adekwatne na mocy przepisów prawa szwajcarskiego;

iv. w przypadku wszystkich innych Danych Osobowych Klienta przekazanych poza jurysdykcję zapewniającą podobną ochronę do ochrony Danych Osobowych Klienta UE, UK lub Szwajcarii, dowolny kraj, terytorium, sektor lub organizację międzynarodową uznane za adekwatne na mocy przepisów prawa takiej jurysdykcji;

„Standardowe Klauzule Umowne" oznacza łącznie Standardowe Klauzule Umowne UE 2021 oraz Dodatek UK 2022.

„Szwajcarskie Dane Osobowe Klienta" oznacza Przetwarzanie Danych Osobowych Klient, do których zastosowanie miały szwajcarskie przepisy prawa o ochronnie danych przed ich przetwarzaniem przez Iron Mountain.

„Dane Osobowe Klienta UK" oznacza Przetwarzanie Danych Osobowych Klient, do których zastosowanie miały szwajcarskie przepisy prawa o ochronnie danych przed ich przetwarzaniem przez Iron Mountain.

2. POSTANOWIENIA RÓŻNE

[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

2.1. Niniejszy Aneks 3 obejmuje następujące Części: (i) Część A – Przekazanie Danych Osobowych Klienta UE, (ii) Część B – Przekazanie Szwajcarskich Danych Osobowych Klienta, (iii) Część C – Przekazanie Danych Osobowych Klienta UK, które mają zastosowanie odpowiednio do przekazania Danych Osobowych Klienta przez Iron MOuntain w związku ze świadczeniem przez nią Usług.

2.2. Standardowe Klauzule Umowne będą miały zastosowanie do Iron Mountain oraz jej podmiotów powiązanych jako „Importerów Danych" oraz do Klienta i jego podmiotów powiązanych jako „Eksporterów Danych".

2.3. Podpis oraz datowanie Umowy będzie stanowiło całość wymaganych podpisów i dat na potrzeby Standardowych Klauzul Umownych.

2.4. W przypadku, gdyby strony dokonywały przekazania Danych Osobowych UE, UK lub szwajcarskich poza Obszar Chroniony i w przypadku, gdyby odpowiednie postanowienie Komisji Europejskiej lub inna obowiązująca metoda określania adekwatności na mocy obowiązującego Ustawodawstwa o Ochronie Danych, na którą Iron Mountain powoływała się dokonując przekazania danych, zostałyby uznane za nieważne, lub gdyby jakikolwiek organ nadzorujący wymagał aby przekazywanie Danych Osobowych na mocy takiego postanowienia został wstrzymany, wówczas strony będą współpracowały i ułatwią wykorzystanie alternatywnego mechanizmu przekazania. Stron postanawiają także, że odpowiednie środki ochrony wykorzystane do dokonywania transferów międzynarodowych na mocy niniejszego Aneksu 3 nie są wyłączne i że mogą posłużyć się dodatkowymi mechanizmami przekazania takimi jak Ramy Prywatności Danych UE-USA.

CZĘŚĆ A – PRZEKAZYWANIE DANYCH OSOBOWYCH KLIENTA UE

Jeżeli w takim zakresie, w jakim Klient lub jego podmioty powiązane dokonują przekazania Danych Osobowych Klienta UE poza Obszar Chroniony na rzecz Iron Mountain i jej podmiotów powiązanych w związku z Usługami świadczonymi przez Iron Mountain na mocy Umowy, zastosowanie ma niniejsza Część A Aneksu 3 a strony postanawiają co następuje:

1. **Wybór Standardowych Klauzul Umownych.** Tekst MODUŁU DRUGIEGO Standardowych Klauzul Umownych UE 2021 ma zastosowanie jeżeli Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Administrator a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Przetwarzający; tekst MODUŁU TRZECIEGO Standardowych Klauzul Umownych UE 2021 ma zastosowanie jeżeli Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Przetwarzający a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Podwykonawca Przetwarzania. Odpowiednie postanowienia Standardowych Klauzul Umownych UE 2021 zostały włączone do niniejszej UPD przez odniesienie i stanowią jej integralną część. Żadne inne moduły ani klauzule oznaczone jako opcjonalne w Standardowych Klauzulach Umownych UE 2021 nie będą miały zastosowania. Informacja wymagana dla celów Załączników do Standardowych Klauzulach Umownych UE 2021 znajduje sięw Załączniku 1 – Opis Przetwarzania/Przekazywania, Aneks 2 – Środki techniczne i organizacyjne, oraz punkcie 6.2 UPD – Lista Podwykonawców Przetwarzania.

2. **Korzystanie z Podwykonawców Przetwarzania.** Dla celów punktu 9 Standardowych Klauzul Umownych UE 2021 zastosowanie ma opcja 2 (Ogólna Autoryzacja Pisemna) dotycząca wykorzystania Podwykonawców Przetwarzania w świadczeniu Usług. Klient uznaje i wyraża zgodę, by Iron Mountain zatrudniała nowych Podwykonawców Przetwarzania przy pomocy mechanizmu określonego w punkcie 6 niniejszej UPD, oraz by okres czasu na składanie wniosku o zmiany podwykonawców przetwarzania wynosił piętnaście (15) dni.

3. **Prawo właściwe i wybór forum.** Dla celów punktu 17 Standardowych Klauzul Umownych UE 2021 (Prawo Właściwe) opcja 2 prawa właściwego będzie miała zastosowanie, a prawem właściwym dla tych punktów będzie prawo Państwa Członkowskiego UE, w którym siedzibę ma eksporter danych, pod warunkiem że dopuszcza ono prawa beneficjenta zewnętrznego. Dla celów punktu 18 Standardowych Klauzul Umownych UE 2021 (Wybór Forum i Jurysdykcji) będą to sądy Państwa Członkowskiego UE, w którym siedzibę ma eksporter danych.

4. **Certyfikacja usunięcia.** Dla celów punktu 8.5 i 16(d) Standardowych Klauzul Umownych UE 2021 certyfikat usunięcia Danych Osobowych będzie przedstawiany Klientowi przez Iron Mountain tylko na pisemne żądanie Klienta.

5. **Naruszenie bezpieczeństwa danych osobowych.** Dla celów punktu 8.6(c) Standardowych Klauzul Umownych UE 2021 naruszenie bezpieczeństwa Danych Osobowych będzie traktowane zgodnie z mechanizmem określonym w akapicie 7 UPD.

6. **Audyty.** Dla celów akapitu 9 Standardowych Klauzul Umownych UE 2021 audyty tych klauzul będą przeprowadzane zgodnie z mechanizmem audytów określonym w Umowie.

7. **Skargi.** Dla celów akapitu 11 Standardowych Klauzul Umownych UE 2021 Iron Mountain poinformuje Klienta jeżeli otrzyma skargę od Podmiotu Danych w odniesieniu do Danych Osobowych Klienta i przekaże skargę Klientowi zgodnie z mechanizmem określonym w Umowie.

8. **Organ nadzorujący.** W odniesieniu do Standardowych Klauzul Umownych UE 2022 odpowiedni właściwy organ nadzorujący zostanie określony zgodnie z akapitem 13 Standardowych Klauzul Umownych UE.

CZĘŚĆ B – PRZEKAZANIE SZWAJCARSKICH DANYCH OSOBOWYCH.

Jeżeli w takim zakresie w jakim Klient lub jego podmioty powiązane dokonują przekazania Szwajcarskich Danych Osobowych Klienta poza Obszar Chroniony na rzecz Iron Mountain i jej podmiotów powiązanych w związku z Usługami świadczonymi przez Iron Mountain na mocy Umowy, zastosowanie ma niniejsza Część B Aneksu 3, a strony postanawiają co następuje:

1. **Wybór Standardowych Klauzul Umownych.** Standardowe Klauzule Umownej UE 2021 i odpowiednie postanowienia Części A mają zastosowanie jeżeli Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Administrator, a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Przetwarzający; oraz/lub Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Przetwarzający a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Podwykonawca Przetwarzania, z zastrzeżeniem, że:

    a. właściwym organem nadzorującym na mocy klauzuli 12 Standardowych Klauzul Umownych UE 2021 jest Szwajcarska Federalna Komisja ds. Ochrony Danych i Informacji.
    b. prawem właściwym dla skarg umownych na mocy akapitu 17 Standardowych Klauzul Umownych UE 2021 jest prawo szwajcarskie, a sądy szwajcarskie będą posiadały właściwość miejscową dla powództw pomiędzy stronami na mocy punktu 18(b).

2. Odniesienia do RODO UE w Standardowych Klauzul Umownych UE 2021 winny być rozumiane jako odniesienia do FADP *[szwajcarska Federalna Ustawa o Ochronie Danych].*

3. Określenie „państwo członkowskie” w Standardowych Klauzul Umownych UE 2021 nie będzie interpretowane w sposób wyłączający Podmiotom Danych w Szwajcarii możliwość dochodzenia swoich praw w miejscu ich normalnego zamieszkania (Szwajcaria) zgodnie z punktem 18(c) Standardowych Klauzul Umownych UE 2021.

CZĘŚĆ C – PRZEKAZYWANIE DANYCH OSOBOWYCH UK

Jeżeli i w takim zakresie, w jakim Klient lub jego podmioty powiązane będą przekazywały Dane Osobowe UK poza Obszar Chroniony na rzecz Iron Mountain lub jej podmiotów powiązanych w związku z Usługami świadczonymi przez Iron Mountain na mocy Umowy, zastosowanie ma niniejsza Część C Aneksu 3, a strony postanawiają jak następuje:

1. **Wybór Standardowych Klauzul Umownych.** Standardowe Klauzule Umownej UE 2021, odpowiednie postanowienia Części A oraz Dodatek UK 2022 mają zastosowanie jeżeli Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Administrator, a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Przetwarzający; oraz/lub Klient lub którykolwiek z jego podmiotów powiązanych występuje jako Przetwarzający a Iron Mountain lub którykolwiek z jej podmiotów powiązanych jako Podwykonawca Przetwarzania.

2. **Część 1: Tabela 1 – 3 Dodatku UK 2022:** Informacja o Stronach – Tabela 1; Wybrane Moduły SCC oraz Wybrane Klauzule; oraz Załącznik Informacje, w tym Aneks 1A: Wykaz Stron, Aneks 1B: Opis Przekazywania oraz Aneks 1C: Środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa danych – Tabela 3, będą uważane za wypełnione przez odniesienie do niniejszego Aneksu 3, w tym Części A. Tabela 4 Dodatku UK: Klient i Iron Mountain uznają i postanawiają, że Dodatek UK może ulec wypowiedzeniu przez którąkolwiek ze stron.

3. **Część 2:** Klauzule Obowiązkowe Dodatku UK: Klient i Iron Mountain uznają i wyrażają zgodę na Klauzule Obowiązkowe Dodatku UK.

4. **Organ nadzorujący:** Właściwym organem nadzorującym będzie Brytyjski Urząd Komisarza ds. Informacji.

CZĘŚĆ D – PRZEKAZYWANIE INNYCH DANYCH OSOBOWYCH KLIENTA

Jeżeli i w takim zakresie, w jakim Klient lub jego podmioty powiązane będą przekazywały Dane Osobowe nieobjęte CZĘŚCIAMI A – C na rzecz Iron Mountain lub jej podmiotów powiązanych w związku z Usługami świadczonymi przez Iron Mountain na mocy Umowy, zastosowanie ma CZĘŚĆ A Aneksu 3 w takim zakresie, w jakim jest odpowiednia i obowiązuje na gruncie Ustawodawstwa o Ochronie Danych. W pozostałych przypadkach, jeżeli jakiekolwiek zastępcze lub dodatkowe zabezpieczenia lub stosowne mechanizmy przekazania na mocy Ustawodawstwa o Ochronie Danych wymagane są w celu przekazania Danych Osobowych Klienta do państwa, które nie zapewnia odpowiedniego poziomu ochrony Danych Osobowych z perspektywy eksportera danych, strony postanawiają je zastosować tak szybko jak będzie to praktycznie możliwe i udokumentować takie wymogi zastosowania w załączniku do niniejszej UPD.