STRONY I KONTEKST

(A) Klient („Klient") zawarł umowę z Clerk, Inc. („Clerk") (każda ze Stron zwana dalej „Stroną", a łącznie „Stronami"), na mocy której Clerk zgodził się świadczyć Usługi zgodnie z taką umową („Umowa"). Niniejsze Uzupełnienie dotyczące Przetwarzania Danych („DPA") jest włączone do Umowy i stanowi jej część oraz wchodzi w życie z dniem wejścia w życie Umowy.

(B) W zakresie, w jakim Clerk przetwarza jakiekolwiek Dane Osobowe Klienta (zgodnie z definicją poniżej) w imieniu Klienta (lub, w stosownych przypadkach, użytkownika końcowego Klienta zdefiniowanego jako „Użytkownik Końcowy Klienta") w związku ze świadczeniem Usług, Strony uzgodniły, że będzie się to odbywało na warunkach określonych w niniejszym DPA.

Należy pamiętać, że Umowa o zachowaniu poufności Clerk została zmodyfikowana w celu odzwierciedlenia certyfikacji Clerk zgodnie z Ramami Prywatności Danych UE-USA. Ramy prywatności danych (w tym szwajcarsko-amerykańskie ramy prywatności i brytyjskie rozszerzenie DPF) zostały formalnie zatwierdzone przez Departament Handlu Stanów Zjednoczonych i Komisję Europejską, a Komisja Europejska wydała decyzję stwierdzającą odpowiedni stopień ochrony na rzecz DPF. Oznacza to, że dane osobowe z Unii Europejskiej (UE), Szwajcarii i Wielkiej Brytanii (UK) mogą być bezpiecznie przesyłane z tych lokalizacji przez klientów Clerk do Clerk w Stanach Zjednoczonych (USA). DPF zastępuje Tarczę Prywatności i, podobnie jak Tarcza Prywatności, dane osobowe mogą być przekazywane do firm w USA, które są certyfikowane w ramach DPF

DEFINICJE

1.1 Terminy pisane wielką literą, które nie zostały zdefiniowane w niniejszej Umowie DPA, mają znaczenie określone w Umowie. Następujące terminy pisane wielką literą w niniejszej Umowie DPA będą definiowane w następujący sposób:

„Informacje o Koncie" oznaczają informacje Klienta, w tym Dane Osobowe Klienta i Użytkowników Końcowych Klienta, przekazane w celu utworzenia konta, dostępu, administrowania i utrzymania, i mogą obejmować imiona i nazwiska, nazwy użytkownika, dane logowania, numery telefonów, adresy e-mail i informacje rozliczeniowe powiązane z kontem Clerk;

„Australijskie Przepisy o Ochronie Danych" oznaczają Australijską Ustawę o Prywatności z 1988 r. oraz Australijskie Zasady Prywatności zawarte w Załączniku 1 do Australijskiej Ustawy o Prywatności z 1988 r.

„Użytkownik Końcowy" lub »Użytkownik Końcowy Klienta« oznacza podmiot, który jest użytkownikiem usług Klienta;

„Obowiązujące Przepisy o Ochronie Danych" oznaczają wszystkie obowiązujące przepisy prawa, zasady, regulacje i wymogi rządowe dotyczące prywatności, poufności lub

bezpieczeństwa Danych Osobowych, które mogą być okresowo zmieniane lub w inny sposób aktualizowane;

„Zatwierdzone Uzupełnienie" oznacza wzór uzupełnienia w wersji B.1.0 wydany przez brytyjskiego Komisarza ds. Informacji na mocy S119A(1) Ustawy o ochronie danych z 2018 r. i przedłożony Parlamentowi Zjednoczonego Królestwa w dniu 2 lutego 2022 r., który może zostać zmieniony zgodnie z sekcją 18 Klauzul Obowiązkowych;

„Dane Osobowe Klienta" oznaczają Dane Osobowe przetwarzane przez Clerk w imieniu Klienta lub Użytkownika Końcowego Klienta w związku ze świadczeniem Usług, z wyłączeniem Danych Osobowych zawartych w Informacjach o Koncie;

„DPF" lub »Ramy Prywatności Danych« oznaczają Ramy Prywatności Danych UE-USA lub, w stosownych przypadkach, brytyjskie rozszerzenie Ram Prywatności Danych UE-USA i szwajcarsko-amerykańskie ramy prywatności danych;

„EOG" oznacza Europejski Obszar Gospodarczy;

„RODO„ oznacza Rozporządzenie (UE) 2016/679 ("RODO UE") lub, w stosownych przypadkach, »RODO Wielkiej Brytanii« zgodnie z definicją w sekcji 3 Ustawy o ochronie danych z 2018 r;

„LGPD" oznacza brazylijską ogólną ustawę o ochronie danych (Lei Gerai de Proteção de Dados Pessoais);

„Klauzule Obowiązkowe" oznaczają »Część 2: Klauzule Obowiązkowe« Zatwierdzonego Uzupełnienia;

„Państwo Członkowskie" oznacza państwo członkowskie EOG, będące państwem członkowskim Unii Europejskiej, Islandii, Norwegii lub Liechtensteinu;

„Dane Osobowe" oznaczają wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej lub urządzenia, lub są inaczej »danymi osobowymi«, »informacjami osobowymi«, »informacjami umożliwiającymi identyfikację osoby« i podobnymi terminami, a takie terminy mają takie samo znaczenie, jak zdefiniowane w Obowiązujących Przepisach o Ochronie Danych;

„Incydent Bezpieczeństwa" oznacza naruszenie bezpieczeństwa informacji lub sieci prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych Klienta;

„Standardowe Klauzule Umowne" lub »SCC« oznaczają Moduł Drugi (administrator-podmiot przetwarzający) i/lub Moduł Trzeci (podmiot przetwarzający-podmiot

przetwarzający) Standardowych Klauzul Umownych załączonych do Decyzji Wykonawczej Komisji (UE) 2021/914;

„Podprzetwarzający" oznacza zewnętrzne podmioty przetwarzające wyznaczone przez Clerk do przetwarzania Danych Osobowych Klienta;

„Zjednoczone Królestwo" oznacza Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej; oraz

„Amerykańskie Przepisy o Ochronie Danych" oznaczają, w stosownym zakresie, przepisy federalne i stanowe dotyczące ochrony danych, Przetwarzania Danych Osobowych, prywatności i/lub ochrony danych obowiązujące od czasu do czasu w Stanach Zjednoczonych.

1.2 Terminy „administrator", „podmiot przetwarzający", „osoba, której dane dotyczą", „przetwarzanie", „organ nadzorczy", „sprzedaż" i „usługodawca" mają takie samo znaczenie, jak określone w Obowiązujących przepisach o ochronie danych.

INTERAKCJA Z UMOWĄ

2.1 Niniejsze DPA uzupełnia i (w przypadku sprzeczności) zastępuje Umowę w odniesieniu do przetwarzania Danych Osobowych Klienta.

2.2 W odniesieniu do Użytkowników Końcowych Klienta, zawierając Umowę, Klient gwarantuje, że jest należycie upoważniony do zawarcia niniejszego DPA w imieniu i na rzecz takich Użytkowników Końcowych Klienta oraz, z zastrzeżeniem punktu 2.3, każdy Użytkownik Końcowy Klienta będzie związany warunkami niniejszego DPA tak, jakby był Klientem.

2.3 Klient gwarantuje, że jest należycie upoważniony przez Użytkowników Końcowych Klienta, w imieniu których Clerk przetwarza Dane Osobowe Klienta zgodnie z niniejszą Umową DPA, do (a) egzekwowania warunków niniejszej Umowy DPA w imieniu Użytkowników Końcowych Klienta oraz do działania w imieniu Użytkowników Końcowych Klienta w zakresie administrowania i prowadzenia wszelkich roszczeń powstałych w związku z niniejszą Umową DPA; oraz (b) otrzymywania i odpowiadania na wszelkie powiadomienia lub komunikaty w ramach niniejszej Umowy DPA w imieniu Użytkowników Końcowych Klienta.

2.4 Strony uzgadniają, że wszelkie powiadomienia lub komunikaty wysyłane przez Clerk do Klienta spełniają wszelkie zobowiązania do wysłania takiego powiadomienia lub komunikatu do Użytkownika Końcowego Klienta.

ROLA STRON

3.1 Strony przyjmują do wiadomości i zgadzają się, że:

(a) dla celów RODO, Clerk działa jako „podmiot przetwarzający" lub „podwykonawca przetwarzania". Funkcja Clerk jako podmiotu przetwarzającego lub podprzetwarzającego będzie określona przez funkcję Klienta:

(i) Ogólnie rzecz biorąc, Klient działa jako administrator danych, podczas gdy Clerk działa jako podmiot przetwarzający.

(ii) W niektórych przypadkach Klient działa jako podmiot przetwarzający w imieniu klientów Klienta, gdy Klient i klient Klienta zawarli umowę o przetwarzaniu danych w związku z przetwarzaniem Danych Osobowych klientów Klienta, a Pracownik jest podmiotem podprzetwarzającym; oraz

(iii) W odniesieniu do Informacji o Koncie, Clerk jest niezależnym administratorem, a nie współadministratorem z Klientem. Clerk będzie przetwarzać Informacje o Koncie jako administrator danych w celu zarządzania relacją z Klientem; prowadzenia podstawowej działalności biznesowej Clerk; przestrzegania obowiązków prawnych lub regulacyjnych mających zastosowanie do przetwarzania i przechowywania Informacji o Koncie; oraz w inny sposób dozwolony na mocy Obowiązujących Przepisów o Ochronie Danych, niniejszego DPA i Umowy. Clerk może również przetwarzać Informacje o Koncie jako administrator danych w celu świadczenia, optymalizacji i utrzymania Usług w zakresie dozwolonym przez Obowiązujące Przepisy o Ochronie Danych. Wszelkie przetwarzanie przez Clerk jako administratora danych będzie zgodne z Polityką Prywatności Clerk.

(b) Z wyjątkiem Informacji o koncie, dla celów amerykańskich przepisów o ochronie danych, Clerk będzie działać jako „usługodawca" lub „podmiot przetwarzający" (w zależności od przypadku) w ramach wykonywania swoich zobowiązań wynikających z Umowy.

SZCZEGÓŁY PRZETWARZANIA DANYCH

4.1 Szczegóły dotyczące przetwarzania danych (takie jak przedmiot, charakter i cel przetwarzania, kategorie Danych Osobowych i osoby, których dane dotyczą) zostały opisane w Umowie i Załączniku 1.

4.2 Dane Osobowe Klienta będą przetwarzane wyłącznie w imieniu i na polecenie Klienta oraz zgodnie z Obowiązującymi Przepisami o Ochronie Danych. Umowa i niniejsze DPA stanowią instrukcje Klienta dotyczące przetwarzania Danych Osobowych Klienta. Klient może wydawać dalsze pisemne instrukcje zgodnie z niniejszym DPA.

4.3 Jeśli instrukcje Klienta spowodują, że Clerk będzie przetwarzać Dane Osobowe Klienta z naruszeniem Obowiązujących Przepisów o Ochronie Danych lub poza zakresem Umowy lub DPA, Clerk niezwłocznie poinformuje o tym Klienta, chyba że zabraniają tego Obowiązujące Przepisy o Ochronie Danych (bez uszczerbku dla SCC).

4.4 Clerk może przechowywać i przetwarzać Dane Osobowe Klienta w dowolnym miejscu, w którym Clerk lub jego Podprzetwarzający posiadają swoje obiekty, z zastrzeżeniem punktu 5 niniejszego OOD.

PODPROCESORZY

5.1 Klient udziela Clerk ogólnego upoważnienia do angażowania Podprzetwarzających, z zastrzeżeniem punktu 5.2, z uzgodnionej listy, jak również aktualnych Podprzetwarzających Clerk wymienionych na stronie https://clerk.com/legal/subprocessors na Datę Wejścia w Życie.

5.2 Clerk (i) zawrze pisemną umowę z każdym Podprzetwarzającym nakładającą obowiązki w zakresie ochrony danych w stopniu nie mniejszym niż obowiązki Clerk wynikające z niniejszego DPA w zakresie mającym zastosowanie do charakteru usług świadczonych przez takiego Podprzetwarzającego; oraz (ii) pozostanie odpowiedzialny za przestrzeganie przez każdego Podprzetwarzającego obowiązków wynikających z niniejszego DPA.

5.3 Clerk powiadomi Klienta z co najmniej piętnastodniowym (15) wyprzedzeniem o wszelkich proponowanych zmianach Podprzetwarzających, z których korzysta w celu przetwarzania Danych Osobowych Klienta (w tym o dodaniu lub zastąpieniu Podprzetwarzających). Klient może w uzasadniony sposób sprzeciwić się korzystaniu przez Clerk z nowego Podprzetwarzającego (w tym korzystając z prawa do sprzeciwu na mocy klauzuli 9(a) SCC), przekazując Clerk pisemne powiadomienie o sprzeciwie w ciągu dziesięciu (10) dni od przekazania Klientowi przez Clerk powiadomienia o takiej proponowanej zmianie („Sprzeciw"). W przypadku, gdy Klient sprzeciwi się korzystaniu przez Clerk z nowego Podprzetwarzającego, Klient i Clerk będą współpracować w dobrej wierze w celu znalezienia wzajemnie akceptowalnego rozwiązania takiego sprzeciwu. Jeśli strony nie będą w stanie osiągnąć wzajemnie akceptowalnego rozwiązania w rozsądnym terminie, każda ze stron może, jako jedyny i wyłączny środek prawny, rozwiązać Umowę poprzez pisemne powiadomienie drugiej strony. W okresie takiego sprzeciwu Clerk może zawiesić daną część Usług.

ŻĄDANIA DOTYCZĄCE PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

6.1 W stosunkach między Stronami Klient ponosi wyłączną odpowiedzialność za reagowanie na prawa dochodzone przez dowolną osobę fizyczną w związku z Danymi Osobowymi Klienta („Żądanie Podmiotu Danych").

6.2 Clerk przekaże Klientowi bez zbędnej zwłoki wszelkie Wnioski Podmiotu Danych otrzymane przez Clerk lub Podprzetwarzającego od osoby fizycznej w związku z jej Danymi Osobowymi Klienta i może doradzić osobie fizycznej złożenie wniosku bezpośrednio do Klienta.

6.3 Clerk (biorąc pod uwagę charakter przetwarzania Danych Osobowych Klienta) zapewni Klientowi i jego Użytkownikom Końcowym możliwość korzystania z interfejsu programowania aplikacji (API) dla funkcji samoobsługowych za pośrednictwem Usług

lub innej uzasadnionej pomocy niezbędnej Klientowi do wypełnienia jego obowiązku wynikającego z Obowiązujących Przepisów o Ochronie Danych w zakresie odpowiadania na Wnioski Podmiotu Danych. Clerk może obciążyć Klienta, a Klient zwróci Clerk koszty takiej pomocy wykraczającej poza zapewnienie funkcji samoobsługowych w ramach Usług.

BEZPIECZEŃSTWO I AUDYTY

7.1 Clerk wdroży i będzie utrzymywać odpowiednie techniczne i organizacyjne środki ochrony i bezpieczeństwa danych w celu zapewnienia bezpieczeństwa Danych Osobowych Klienta, w tym, bez ograniczeń, ochrony przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem (w tym, bez ograniczeń, nieuprawnionym lub niezgodnym z prawem ujawnieniem, dostępem i/lub zmianą Danych Osobowych Klienta) oraz przed ich przypadkową utratą, zniszczeniem lub uszkodzeniem.

7.2 Clerk wdroży i będzie utrzymywać jako minimalny standard środki określone w Załączniku 2. Clerk może od czasu do czasu aktualizować lub modyfikować środki bezpieczeństwa określone w Załączniku 2, pod warunkiem, że takie aktualizacje i/lub modyfikacje nie zmniejszą ogólnego poziomu ochrony Danych Osobowych Klienta zapewnianego przez Clerk na mocy niniejszego DPA.

7.3 Klient lub jego niezależny audytor będący stroną trzecią, który może zostać zaakceptowany przez Clerk (co nie obejmuje audytorów, którzy nie są odpowiednio wykwalifikowani lub niezależni lub są konkurentami Clerk), może przeprowadzać audyt zgodności Clerk z jego zobowiązaniami wynikającymi z niniejszego DPA do jednego razu w roku lub częściej w przypadku wystąpienia Incydentu Bezpieczeństwa lub w zakresie wymaganym przez obowiązujące przepisy o ochronie danych, w tym w przypadku, gdy jest to wymagane przez organ regulacyjny lub rządowy Klienta.

7.4 Aby zażądać audytu, Klient musi przedłożyć Clerk szczegółowy proponowany plan audytu z co najmniej dwutygodniowym wyprzedzeniem przed proponowaną datą audytu. Clerk dokona przeglądu proponowanego planu audytu i będzie współpracować z Klientem w celu uzgodnienia ostatecznego planu audytu. Wszystkie takie audyty muszą być przeprowadzane w regularnych godzinach pracy, z zastrzeżeniem uzgodnionego ostatecznego planu audytu oraz zasad BHP lub innych odpowiednich zasad obowiązujących u Clerk, i nie mogą w nieuzasadniony sposób zakłócać działalności biznesowej Clerk. Żadne z postanowień niniejszego punktu 7.4 nie wymaga od Sprzedawcy naruszenia jakichkolwiek obowiązków zachowania poufności.

7.5 Jeśli żądany zakres audytu został uwzględniony w certyfikacie ISO 27001, raporcie SOC 2 Typ 2 lub podobnym raporcie z audytu przeprowadzonego przez wykwalifikowanego audytora zewnętrznego w ciągu dwunastu (12) miesięcy od żądania audytu przez Klienta, a Clerk potwierdzi brak znanych istotnych zmian w kontrolach poddanych audytowi, Klient zgadza się zaakceptować te ustalenia zamiast żądania audytu kontroli objętych raportem.

7.6 Klient niezwłocznie powiadomi Clerk o wszelkich niezgodnościach wykrytych w trakcie audytu i dostarczy Clerk wszelkie raporty z audytu wygenerowane w związku z audytem, chyba że jest to zabronione przez obowiązujące prawo lub w inny sposób nakazane przez organ regulacyjny lub rządowy. Klient może wykorzystywać raporty z audytu wyłącznie w celu spełnienia wymogów audytowych Klienta i/lub potwierdzenia zgodności z wymogami niniejszego DPA.

7.7 Wszelkie audyty przeprowadzane są na koszt Klienta. Klient zwróci Clerk czas poświęcony przez Clerk lub jego Podprzetwarzających w związku z takimi audytami.

7.8 Klient przyjmuje do wiadomości i zgadza się, że biorąc pod uwagę aktualny stan wiedzy, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko o różnym prawdopodobieństwie i wadze dla praw i wolności osób fizycznych, środki bezpieczeństwa określone w Załączniku 2 są odpowiednie do zapewnienia bezpieczeństwa Danych Osobowych Klienta.

INCYDENTY ZWIĄZANE Z BEZPIECZEŃSTWEM

Clerk niezwłocznie powiadomi Klienta na piśmie w przypadku jakiegokolwiek naruszenia niniejszej Umowy o partnerstwie, Obowiązujących przepisów o ochronie danych lub jakichkolwiek instrukcji Klienta w związku z przetwarzaniem Danych osobowych Klienta na mocy niniejszej Umowy o partnerstwie. Nie ograniczając ogólnego charakteru powyższego, Clerk powiadomi Klienta na piśmie bez zbędnej zwłoki po uzyskaniu informacji o jakimkolwiek Incydencie bezpieczeństwa i będzie w rozsądnym zakresie współpracować w dochodzeniu w sprawie takiego Incydentu bezpieczeństwa oraz wszelkich zobowiązań Klienta wynikających z Obowiązujących przepisów o ochronie danych do dokonywania jakichkolwiek powiadomień osób fizycznych, organów nadzorczych, rządowych lub innych organów regulacyjnych lub opinii publicznej w odniesieniu do takiego Incydentu bezpieczeństwa. Clerk podejmie uzasadnione kroki w celu powstrzymania, zbadania i złagodzenia wszelkich Incydentów Bezpieczeństwa i bez zbędnej zwłoki prześle Klientowi terminowe informacje o Incydencie Bezpieczeństwa, w tym między innymi o charakterze Incydentu Bezpieczeństwa, środkach podjętych w celu złagodzenia lub powstrzymania Incydentu Bezpieczeństwa oraz statusie dochodzenia. Powiadomienie lub reakcja Clerk na Incydent Bezpieczeństwa zgodnie z niniejszym punktem 8 nie będą interpretowane jako uznanie przez Clerk jakiejkolwiek winy lub odpowiedzialności w odniesieniu do Incydentu Bezpieczeństwa.

USUNIĘCIE I ZWROT

Clerk (a) na żądanie Klienta do dnia rozwiązania lub wygaśnięcia Umowy zwróci kopię wszystkich Danych Osobowych Klienta lub zapewni samoobsługową funkcję umożliwiającą Klientowi zrobienie tego samego; oraz (b) w ciągu 90 dni od rozwiązania lub wygaśnięcia Umowy usunie i dołoży wszelkich uzasadnionych starań, aby zapewnić usunięcie wszystkich innych kopii Danych Osobowych Klienta przetwarzanych przez Clerk lub jakichkolwiek Podprzetwarzających.

OKRES OBOWIĄZYWANIA UMOWY

Niniejsze DPA rozpocznie się w Dacie Wejścia w Życie i, niezależnie od rozwiązania Umowy, pozostanie w mocy do momentu usunięcia przez Clerk wszystkich Danych Osobowych Klienta zgodnie z opisem w niniejszym DPA i automatycznie wygaśnie.

TRANSGRANICZNE PRZEKAZYWANIE DANYCH

11.1 Standardowe klauzule umowne

Strony uzgadniają, że warunki Standardowych Klauzul Umownych Moduł Pierwszy (Administrator do Administratora), Moduł Drugi (Administrator do Podmiotu Przetwarzającego) i Moduł Trzeci (Podmiot Przetwarzający do Podmiotu Przetwarzającego), jak określono w Załączniku 3 do niniejszego DPA, zostają niniejszym włączone przez odniesienie i uznaje się je za wykonane przez Strony oraz mają zastosowanie do wszelkich transferów Danych Osobowych Klienta objętych zakresem RODO od Klienta (jako eksportera danych) do Clerk (jako importera danych) w zakresie i tak długo, jak Clerk nie może polegać na DPF zgodnie z klauzulą 11.2.

11.2 Ramy prywatności danych

Clerk jest certyfikowany zgodnie z DPF i przestrzega zasad prywatności danych w nim zawartych. W zakresie i tak długo, jak DPF jest uznawany za ważny mechanizm przekazywania danych w danym kraju/regionie, Dane Osobowe pochodzące z EOG, Wielkiej Brytanii lub Szwajcarii lub w inny sposób podlegające RODO będą przekazywane na podstawie DPF. Zobacz Politykę DPF Clerk tutaj.

11.3 Wsparcie dla transgranicznych transferów danych

Clerk zapewni Klientowi rozsądne wsparcie, aby umożliwić Klientowi spełnienie wymogów nałożonych na przekazywanie danych osobowych do państw trzecich w odniesieniu do osób, których dane dotyczą, znajdujących się w EOG, Szwajcarii i Wielkiej Brytanii. Na żądanie Klienta, Clerk dostarczy Klientowi informacje, które są niezbędne do przeprowadzenia przez Klienta oceny wpływu transferu („TIA"). Ponadto Clerk zgadza się wdrożyć dodatkowe środki uzgodnione i określone w Załączniku 4 do niniejszego DPA w celu umożliwienia Klientowi spełnienia wymogów nałożonych na przekazywanie danych osobowych do państw trzecich. Clerk może obciążyć Klienta, a Klient zwróci Clerk koszty wszelkiej pomocy świadczonej przez Clerk w odniesieniu do wszelkich TIA, ocen wpływu na ochronę danych lub konsultacji z jakimkolwiek organem nadzorczym Klienta.

DANE OSOBOWE KLIENTA PODLEGAJĄCE BRYTYJSKIM I SZWAJCARSKIM PRZEPISOM O OCHRONIE DANYCH OSOBOWYCH

W zakresie, w jakim przetwarzanie Danych Osobowych Klienta podlega brytyjskim lub szwajcarskim przepisom o ochronie danych, zastosowanie ma Załącznik brytyjski i/lub Załącznik szwajcarski (w zależności od przypadku) określone w Załączniku 5.

DANE OSOBOWE KLIENTA PODLEGAJĄCE NASZYM PRZEPISOM O OCHRONIE DANYCH OSOBOWYCH
W zakresie, w jakim przetwarzanie Danych Osobowych Klienta podlega amerykańskim Przepisom o Ochronie Danych Osobowych, zastosowanie ma Załącznik USA określony w Załączniku 6.

Klient rozumie i zgadza się, że jeśli korzysta z Usług w celu przechowywania lub przesyłania chronionych informacji zdrowotnych zgodnie z amerykańskimi przepisami o ochronie danych, musi osobno zawrzeć i podpisać Umowę Współpracownika Biznesowego („BAA"), jeśli Klient kwalifikuje się jako Podmiot Objęty Ochroną lub Współpracownik Biznesowy. W przypadku, gdy strony zawarły umowę BAA, umowa BAA ma pierwszeństwo przed niniejszą umową DPA w odniesieniu do wszelkich chronionych informacji zdrowotnych.

POSTANOWIENIA OGÓLNE
14.1 Strony niniejszym zaświadczają, że rozumieją wymogi zawarte w niniejszym DPA i będą ich przestrzegać.

14.2 Niniejsze DPA i Umowa określają całość porozumienia między Stronami w odniesieniu do przedmiotu niniejszego DPA.

Załącznik 1

SZCZEGÓŁY PRZETWARZANIA

Część 1
LISTA STRON

1. Eksporter danych

Klient i/lub Użytkownicy końcowi Klienta działający w krajach należących do Europejskiego Obszaru Gospodarczego, Wielkiej Brytanii i/lub Szwajcarii i/lub - w zakresie uzgodnionym przez Strony - Klient i/lub Użytkownicy końcowi Klienta w dowolnym innym kraju w zakresie, w jakim zastosowanie ma RODO lub odpowiednie prawo szwajcarskie.

Stanowisko i dane kontaktowe Klienta oraz Użytkownika Końcowego Klienta, a także (jeśli został wyznaczony) dane kontaktowe inspektora ochrony danych i (jeśli dotyczy) przedstawiciela zostaną przekazane Sprzedawcy przed rozpoczęciem przetwarzania danych osobowych za pośrednictwem poczty elektronicznej na adres privacy@clerk.dev lub formularza udostępnionego przez Sprzedawcę na koncie Klienta w Usługach.

Czynności związane z przekazywaniem danych na podstawie niniejszych klauzul są określone w Umowie oraz przez osobę przekazującą dane, która decyduje o zakresie przetwarzania danych osobowych w związku z Usługami opisanymi w niniejszym Załączniku 1 oraz w Umowie.

2. Importer danych

Clerk, Inc,
660 King Street
Unit 345
San Francisco, CA 94107
Stany Zjednoczone

Z osobą kontaktową importera danych można skontaktować się pod adresem privacy@clerk.dev. Z przedstawicielem importera danych w UE można również skontaktować się pod adresem
VeraSafe Ireland Ltd.
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Irlandia
https://verasafe.com/public-resources/contact-data-protection-representative
+420 228 881 031

Działania podmiotu odbierającego dane związane z przekazywaniem danych na mocy niniejszych klauzul są następujące: podmiot odbierający dane przetwarza dane osobowe przekazane przez podmiot przekazujący dane w imieniu podmiotu przekazującego dane w związku ze świadczeniem Usług na rzecz podmiotu przekazującego dane, jak określono w niniejszym Załączniku 1 i w Umowie.

Część 2
OPIS PRZEKAZANIA

1. Kategorie osób, których dane dotyczą

Kategorie osób, których dane dotyczą, których dane osobowe są przekazywane:

Klienci
Klienci Użytkownicy końcowi
Kontakty

2. Kategorie danych osobowych

Przekazywane kategorie danych osobowych to:

Określone przez konfigurację Usług przez Klienta i mogą obejmować imię i nazwisko, numer telefonu, adres e-mail, dane adresowe, adres IP, identyfikatory urządzeń, dane dotyczące użytkowania (takie jak interakcje między użytkownikiem a systemem online, stroną internetową lub pocztą elektroniczną Klienta, używana przeglądarka, używany system operacyjny, adres URL odsyłacza).

Ponadto Klient może uwzględnić dalsze dane osobowe osób, których dane dotyczą, w imieniu swoich Użytkowników Końcowych, jak określono powyżej (w szczególności w formie nieustrukturyzowanej) w związku z korzystaniem przez nich z Usług zgodnie z Umową.

3. Szczególne kategorie danych osobowych (jeśli dotyczy)

Przekazywane dane osobowe obejmują następujące szczególne kategorie danych: Nie dotyczy - Umowa Sprzedawcy zabrania Klientowi korzystania z Usług w celu pozyskiwania, wyświetlania, przechowywania, przetwarzania, wysyłania lub przekazywania szczególnych kategorii danych.

Zastosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi ryzyko, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp tylko dla pracowników, którzy przeszli specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania lub dodatkowe środki bezpieczeństwa: NIE DOTYCZY

4. Częstotliwość przekazywania danych

Częstotliwość przekazywania danych jest następująca: Transfer odbywa się w sposób ciągły i jest określany na podstawie konfiguracji Usług przez Klienta.

5. Przedmiot i charakter przetwarzania

Przedmiotem przetwarzania jest: zapewnienie Klientowi platformy automatyzacji uwierzytelniania.

6. Cel(e) przekazywania i dalszego przetwarzania danych

Celem/celami przekazywania i dalszego przetwarzania danych jest: świadczenie Usług na rzecz Klienta zgodnie z Umową, aby Klient mógł opracowywać procesy uwierzytelniania.

7. Czas trwania

Okres, przez który dane osobowe będą przechowywane, lub, jeśli nie jest to możliwe, kryteria stosowane do określenia tego okresu: czas trwania jest określony w klauzuli 10 RODO.

8. Podmiot podprzetwarzający (jeśli dotyczy)

W przypadku przekazywania danych podprzetwarzającym należy określić przedmiot, charakter i czas trwania przetwarzania: zgodnie z klauzulą 5.1 RODO. Podprzetwarzający mogą mieć dostęp do Danych Osobowych przez okres obowiązywania niniejszego DPA lub do momentu rozwiązania umowy o świadczenie usług z danym Podprzetwarzającym lub wyłączenia dostępu przez Podprzetwarzającego zgodnie z ustaleniami pomiędzy Clerk a Klientem.

Część 3
WŁAŚCIWY ORGAN NADZORCZY

Określenie właściwego organu nadzorczego zgodnie z klauzulą 13 SCC

Właściwym organem nadzorczym jest organ nadzorczy w Irlandii, a mianowicie Komisja Ochrony Danych (https://www.dataprotection.ie/).

Załącznik 2

ŚRODKI TECHNICZNE I ORGANIZACYJNE

Clerk wdrożył następujące środki techniczne i organizacyjne (w tym odpowiednie certyfikaty), aby zapewnić odpowiedni poziom bezpieczeństwa, biorąc pod uwagę charakter, zakres, kontekst i cel przetwarzania, a także ryzyko dla praw i wolności osób fizycznych:

1. Kierownictwo organizacyjne i dedykowany personel odpowiedzialny za opracowanie, wdrożenie i utrzymanie programu bezpieczeństwa informacji Clerk.

2. Procedury audytu i oceny ryzyka do celów okresowego przeglądu i oceny ryzyka dla organizacji Clerk, monitorowania i utrzymywania zgodności z politykami i procedurami Clerk oraz raportowania stanu bezpieczeństwa informacji i zgodności z wewnętrznym kierownictwem wyższego szczebla.

3. Wykorzystanie dostępnych na rynku i zgodnych ze standardami branżowymi technologii szyfrowania Danych Osobowych Klienta, które są:

(a) są przesyłane przez Clerk za pośrednictwem sieci publicznych (tj. Internetu) lub przesyłane bezprzewodowo; lub

(b) w stanie spoczynku.

4. Kontrole bezpieczeństwa danych, które obejmują co najmniej, ale nie wyłącznie, logiczną segregację danych, logiczne kontrole dostępu zaprojektowane w celu zarządzania elektronicznym dostępem do danych i funkcjonalności systemu w oparciu o poziomy uprawnień i funkcje zawodowe (np. przyznawanie dostępu w oparciu o zasadę ograniczonego dostępu i najmniejszych uprawnień, korzystanie z unikalnych identyfikatorów i haseł dla wszystkich użytkowników, okresowe przeglądy oraz niezwłoczne cofanie/zmienianie dostępu w przypadku zakończenia zatrudnienia lub zmiany funkcji zawodowych).

5. Kontrola haseł mająca na celu zarządzanie i kontrolowanie siły, wygaśnięcia i użycia haseł, w tym zakaz udostępniania haseł przez użytkowników i wymóg, aby hasła urzędnika, które są przypisane do jego pracowników: (i) miały długość co najmniej ośmiu (8) znaków, (ii) nie były przechowywane w formacie do odczytu w systemach komputerowych urzędnika; (iii) muszą mieć określoną złożoność; (iv) muszą mieć próg historii, aby zapobiec ponownemu użyciu ostatnich haseł; oraz (v) nowo wydane hasła muszą zostać zmienione po pierwszym użyciu.

6. Audyt systemu lub rejestrowanie zdarzeń i powiązane procedury monitorowania w celu proaktywnego rejestrowania dostępu pracownika biurowego i aktywności systemu w celu rutynowego przeglądu.

7. Clerk przechowuje dane osobowe głównie w centrach danych Google Cloud i Cloudflare, które uzyskały certyfikat zgodności z normą ISO 27001 i/lub SOC2. Więcej informacji na temat kontroli Google Cloud można znaleźć tutaj. Więcej informacji na temat kontroli Cloudfare można znaleźć tutaj.

8. Procedury operacyjne i kontrole zapewniające konfigurację, monitorowanie i konserwację technologii i systemów informatycznych zgodnie z określonymi wewnętrznymi i przyjętymi standardami branżowymi, w tym bezpieczne usuwanie systemów i nośników w celu uniemożliwienia odszyfrowania lub odzyskania wszystkich zawartych w nich informacji lub danych przed ostatecznym usunięciem lub zwolnieniem z posiadania Clerk.

9. Procedury zarządzania zmianami i mechanizmy śledzenia mające na celu testowanie, zatwierdzanie i monitorowanie wszystkich zmian w technologii i zasobach informacyjnych Urzędu.

10. Procedury zarządzania incydentami/problemami zaprojektowane w celu umożliwienia Urzędnikowi badania, reagowania, łagodzenia i powiadamiania o zdarzeniach związanych z technologią i zasobami informacyjnymi Urzędnika.

11. Kontrole bezpieczeństwa sieci, które przewidują stosowanie systemów zapór sieciowych, systemów wykrywania włamań oraz innych procedur korelacji ruchu i

zdarzeń mających na celu ochronę systemów przed włamaniami i ograniczenie zakresu każdego udanego ataku.

12. Ocena podatności, zarządzanie poprawkami i technologie ochrony przed zagrożeniami oraz zaplanowane procedury monitorowania mające na celu identyfikację, ocenę, łagodzenie i ochronę przed zidentyfikowanymi zagrożeniami bezpieczeństwa, wirusami i innym złośliwym kodem.

13. Odporność biznesowa/ciągłość działania i procedury odzyskiwania danych po awarii w celu utrzymania usług i/lub odzyskania danych po przewidywalnych sytuacjach awaryjnych lub katastrofach.

Załącznik 3
STANDARDOWE KLAUZULE UMOWNE

Dla celów Standardowych Klauzul Umownych:

1. Moduł Pierwszy (Administrator do Administratora) ma zastosowanie w przypadku przetwarzania zgodnie z klauzulą 3.1.(a)(iii) RODO. Moduł Drugi (Administrator do Podmiotu przetwarzającego) ma zastosowanie w przypadku przetwarzania na mocy klauzuli 3.1(a)(i) RODO, a Moduł Trzeci (Podmiot przetwarzający do Podmiotu podprzetwarzającego) ma zastosowanie w przypadku przetwarzania na mocy klauzuli 3.1(a)(ii) RODO. Dla każdego Modułu, w stosownych przypadkach, zastosowanie mają następujące postanowienia:

2. Klauzula 7 Standardowych Klauzul Umownych (Klauzula dokowania) nie ma zastosowania.

3. Wybrano klauzulę 9(a) Opcja 2 (Ogólne pisemne upoważnienie), a okres, który należy określić, określono w klauzuli 5.3 Umowy o partnerstwie.

4. Opcja w klauzuli 11(a) Standardowych Klauzul Umownych (Niezależny organ rozstrzygania sporów) nie ma zastosowania.

5. W odniesieniu do klauzuli 17 Standardowych Klauzul Umownych (Prawo właściwe) Strony uzgadniają, że zastosowanie ma opcja pierwsza. Strony uzgadniają, że prawem właściwym będzie prawo Republiki Irlandii.

6. W klauzuli 18 Standardowych Klauzul Umownych (Wybór sądu i jurysdykcji) Strony poddają się jurysdykcji sądów Republiki Irlandii.

7. Dla celów Załącznika I do Standardowych Klauzul Umownych, Załącznik 1 zawiera specyfikacje dotyczące stron, opis transferu oraz właściwy organ nadzorczy.

8. Dla celów Załącznika II do Standardowych Klauzul Umownych, Załącznik 2 zawiera środki techniczne i organizacyjne.

9. Specyfikacje dla Załącznika III do Standardowych Klauzul Umownych są określone w klauzuli 5.1 RODO. Imię i nazwisko, stanowisko i dane kontaktowe osoby kontaktowej Podprzetwarzającego zostaną dostarczone przez Clerk na żądanie.

Załącznik 4
DODATKOWE ŚRODKI UZUPEŁNIAJĄCE

Clerk zobowiązuje się ponadto do wdrożenia dodatkowych środków w oparciu o wytyczne organów nadzorczych UE w celu zwiększenia ochrony Danych Osobowych Klienta w związku z przetwarzaniem w państwie trzecim, jak opisano w niniejszym Załączniku 4.

1. Dodatkowe środki techniczne (szyfrowanie)

1.1 Dane osobowe są przesyłane (między Stronami i przez Clerk między centrami danych, a także do Podprzetwarzającego i z powrotem) przy użyciu silnego szyfrowania.

1.2 Dane osobowe w stanie spoczynku są przechowywane przez Sprzedawcę przy użyciu silnego szyfrowania.

2. Dodatkowe środki organizacyjne

2.1 Wewnętrzne polityki zarządzania przekazywaniem danych, w szczególności w odniesieniu do grup przedsiębiorstw

(a) Przyjęcie odpowiednich polityk wewnętrznych z jasnym podziałem obowiązków w zakresie przekazywania danych, kanałów sprawozdawczości i standardowych procedur operacyjnych w przypadkach formalnych lub nieformalnych wniosków organów publicznych o dostęp do danych.

(b) Opracowanie specjalnych procedur szkoleniowych dla personelu odpowiedzialnego za zarządzanie wnioskami o dostęp do danych osobowych od organów publicznych, które powinny być okresowo aktualizowane w celu odzwierciedlenia nowych zmian legislacyjnych i orzeczniczych w państwie trzecim i EOG.

2.2 Środki przejrzystości i rozliczalności

Regularna publikacja raportów przejrzystości lub podsumowań dotyczących rządowych wniosków o dostęp do danych i rodzaju udzielonej odpowiedzi, o ile publikacja jest dozwolona przez lokalne prawo.

2.3 Metody organizacyjne i środki minimalizacji danych

Opracowanie i wdrożenie najlepszych praktyk przez obie Strony w celu odpowiedniego i terminowego zaangażowania i zapewnienia dostępu do informacji odpowiednim inspektorom ochrony danych, jeśli istnieją, oraz ich służbom prawnym i audytu wewnętrznego w sprawach związanych z międzynarodowym przekazywaniem danych osobowych.

2.4 Inne

Przyjęcie i regularny przegląd przez Clerk wewnętrznych polityk w celu oceny adekwatności wdrożonych środków uzupełniających oraz zidentyfikowania i wdrożenia dodatkowych lub alternatywnych rozwiązań w razie potrzeby, aby zapewnić utrzymanie zasadniczo równoważnego poziomu ochrony przekazywanych danych osobowych do poziomu gwarantowanego w EOG.

3. Dodatkowe środki umowne

3.1 Zobowiązania w zakresie przejrzystości

(a) Clerk oświadcza, że (1) celowo nie stworzył backdoorów lub podobnego oprogramowania, które mogłoby zostać wykorzystane do uzyskania dostępu do systemu i/lub danych osobowych, (2) celowo nie stworzył lub nie zmienił swoich procesów biznesowych w sposób ułatwiający dostęp do danych osobowych lub systemów oraz (3) prawo krajowe lub polityka rządowa nie wymagają od Clerk tworzenia lub utrzymywania backdoorów lub ułatwiania dostępu do danych osobowych lub systemów ani posiadania lub przekazywania klucza szyfrowania przez Clerk.

(b) Clerk będzie regularnie weryfikować ważność informacji podanych w kwestionariuszu TIA i niezwłocznie powiadamiać Klienta o wszelkich zmianach. Punkt 14(e) SCC pozostaje bez zmian.

3.2 Obowiązek podjęcia określonych działań

W przypadku jakiegokolwiek nakazu ujawnienia lub udzielenia dostępu do danych osobowych, Clerk zobowiązuje się poinformować żądający organ publiczny o niezgodności nakazu z zabezpieczeniami zawartymi w art. 46 RODO i wynikającym z tego konflikcie obowiązków Clerk.

3.3 Umożliwienie osobom, których dane dotyczą, korzystania z przysługujących im praw

(a) Clerk zobowiązuje się do uczciwego zrekompensowania osobie, której dane dotyczą, wszelkich szkód materialnych i niematerialnych poniesionych z powodu ujawnienia jej danych osobowych przekazanych w ramach wybranego narzędzia transferu z naruszeniem zawartych w nim zobowiązań.

(b) Niezależnie od powyższego, Clerk nie ma obowiązku wypłaty odszkodowania osobie, której dane dotyczą, w zakresie, w jakim osoba ta otrzymała już odszkodowanie za tę samą szkodę.

(c) Odszkodowanie jest ograniczone do szkód materialnych i niematerialnych przewidzianych w RODO i wyklucza szkody następcze oraz wszelkie inne szkody niewynikające z naruszenia RODO przez Clerk.

4. Dodatkowe obowiązki w przypadku żądań lub dostępu ze strony organów publicznych

4.1 Sprzedawca niezwłocznie poinformuje Klienta:

(a) o wszelkich prawnie wiążących żądaniach organów ścigania lub innych organów rządowych („Organ publiczny") dotyczących ujawnienia danych osobowych udostępnionych przez Klienta („Przekazane dane osobowe"); takie powiadomienie będzie zawierać informacje o żądanych danych osobowych, organie żądającym, podstawie prawnej żądania i udzielonej odpowiedzi. Takie powiadomienie powinno nastąpić przed ujawnieniem jakichkolwiek danych osobowych w odpowiedzi na takie żądania.

(b) W przypadku uzyskania informacji o bezpośrednim dostępie organów publicznych do przekazywania danych osobowych zgodnie z prawem kraju docelowego, takie powiadomienie powinno zawierać wszystkie informacje dostępne dla Clerk.

(c) Jeśli Clerk nie może powiadomić Klienta i/lub osoby, której dane dotyczą, Clerk zgadza się dołożyć wszelkich starań, aby uzyskać zwolnienie z zakazu, w celu przekazania jak największej ilości informacji i tak szybko, jak to możliwe. Sprzedawca zgadza się udokumentować swoje starania, aby móc je wykazać na żądanie podmiotu przekazującego dane.

4.2 Clerk zgadza się zbadać, zgodnie z prawem kraju docelowego, legalność wniosku organu publicznego, w szczególności, czy pozostaje on w ramach uprawnień przyznanych wnioskującemu organowi publicznemu i wyczerpać wszystkie dostępne środki zaradcze w celu zakwestionowania wniosku, jeżeli po dokładnej ocenie Clerk dojdzie do wniosku, że istnieją ku temu podstawy zgodnie z prawem kraju docelowego. Obejmuje to wnioski na mocy sekcji 702 Sądu Nadzoru Wywiadu Zagranicznego Stanów Zjednoczonych lub rozporządzenia wykonawczego 12333. W przypadku zakwestionowania wniosku, Clerk będzie dążył do zastosowania środków tymczasowych w celu zawieszenia skutków wniosku do czasu podjęcia przez sąd decyzji co do istoty sprawy. Clerk nie ujawni ani nie zapewni dostępu do żądanych danych osobowych, dopóki nie będzie do tego zobowiązany zgodnie z obowiązującymi przepisami proceduralnymi, a w takim czasie dostarczy jedynie minimalną ilość informacji wymaganych do spełnienia żądania, w oparciu o rozsądną interpretację żądania.

4.3 Clerk zobowiązuje się przechowywać informacje wymagane do przestrzegania niniejszego Załącznika 4 przez okres obowiązywania Umowy i, o ile nie zabrania tego obowiązujące prawo, udostępniać je właściwemu organowi nadzorczemu na żądanie i gdy jest to wymagane przez obowiązujące prawo.

Załącznik 5
UZUPEŁNIENIE BRYTYJSKIE I SZWAJCARSKIE

1. ANEKS BRYTYJSKI

W odniesieniu do wszelkich transferów Danych Osobowych Klienta objętych zakresem brytyjskiego RODO od Klienta (jako eksportera danych) do Clerk (jako importera danych):

1.1 Zatwierdzone Uzupełnienie, jak określono dalej w niniejszym Załączniku 5, stanowi część niniejszej Umowy o zachowaniu poufności, a Standardowe Klauzule Umowne należy odczytywać i interpretować w świetle postanowień Zatwierdzonego Uzupełnienia, w niezbędnym zakresie zgodnie z klauzulą 12 Klauzul Obowiązkowych.

1.2 W odstępstwie od Tabeli 1 Zatwierdzonego Uzupełnienia i zgodnie z klauzulą 17 Klauzul Obowiązkowych, strony są dalej określone w Załączniku 1 Część 1 niniejszej Umowy DPA.

1.3 Wybrane Moduły i Klauzule, które mają zostać określone zgodnie z Tabelą 2 Zatwierdzonego Uzupełnienia, są dalej określone w Załączniku 3 do niniejszej Umowy DPA, zmienionej Klauzulami Obowiązkowymi.

1.4 Załączniki 1 A i B do Tabeli 3 do Zatwierdzonego Uzupełnienia są określone w Załączniku 1 do niniejszej Umowy DPA, Załącznik II do Zatwierdzonego Uzupełnienia jest określony w Załączniku 2 do niniejszej Umowy DPA, a Załącznik III do Zatwierdzonego Uzupełnienia jest określony w Załączniku 1 klauzula B.10 do niniejszej Umowy DPA.

1.5 Clerk (jako podmiot odbierający dane) może wypowiedzieć niniejszą Umowę o partnerstwie w zakresie, w jakim Zatwierdzone Uzupełnienie ma zastosowanie, zgodnie z klauzulą 19 Klauzul Obowiązkowych.

1.6 Klauzula 16 Klauzul Obowiązkowych nie ma zastosowania.

2. SZWAJCARSKIE UZUPEŁNIENIE

Zgodnie z klauzulą 13 RODO, niniejszy Szwajcarski Dodatek ma zastosowanie do każdego przetwarzania Danych Osobowych Klienta podlegającego szwajcarskiemu prawu o ochronie danych lub zarówno szwajcarskiemu prawu o ochronie danych, jak i RODO.

2.1 Interpretacja niniejszego Aneksu

(a) W przypadku, gdy w niniejszym Aneksie używane są terminy zdefiniowane w Standardowych Klauzulach Umownych, jak określono w Załączniku 3 do niniejszego DPA, terminy te mają takie samo znaczenie jak w Standardowych Klauzulach Umownych. Ponadto następujące terminy mają następujące znaczenie:

(i) „Niniejszy Dodatek" oznacza Niniejszy Dodatek do Klauzul.

(ii) „Klauzule" oznaczają Standardowe Klauzule Umowne określone w Załączniku 3 do niniejszej Umowy.

(iii) „Szwajcarskie Przepisy o Ochronie Danych" oznaczają Szwajcarską Ustawę Federalną o Ochronie Danych z dnia 19 czerwca 1992 r. oraz Szwajcarskie Rozporządzenie do Szwajcarskiej Ustawy Federalnej o Ochronie Danych z dnia 14 czerwca 1993 r., a także wszelkie nowe lub zmienione wersje tych przepisów, które mogą wejść w życie od czasu do czasu.

(b) Niniejszy Załącznik należy odczytywać i interpretować w świetle przepisów szwajcarskich przepisów o ochronie danych, tak aby spełniał on zamiar zapewnienia odpowiednich zabezpieczeń wymaganych przez art. 46 RODO i/lub art. 6(2)(a) szwajcarskich przepisów o ochronie danych, w zależności od przypadku.

(c) Niniejszy Załącznik nie może być interpretowany w sposób sprzeczny z prawami i obowiązkami przewidzianymi w szwajcarskich przepisach o ochronie danych.

(d) Wszelkie odniesienia do ustawodawstwa (lub konkretnych przepisów ustawodawstwa) oznaczają, że ustawodawstwo (lub konkretny przepis) może się zmieniać w czasie. Dotyczy to również sytuacji, w których ustawodawstwo (lub konkretny przepis) zostało skonsolidowane, ponownie uchwalone i/lub zastąpione po zawarciu niniejszego Aneksu.

2.2 Hierarchia

W przypadku konfliktu lub niespójności między niniejszym Aneksem a postanowieniami Klauzul lub innych powiązanych umów między Stronami, istniejących w momencie uzgodnienia niniejszego Aneksu lub zawartych później, pierwszeństwo mają postanowienia, które zapewniają największą ochronę osobom, których dane dotyczą.

2.3 Włączenie Klauzul

(a) W odniesieniu do przetwarzania danych osobowych podlegających szwajcarskim przepisom o ochronie danych lub zarówno szwajcarskim przepisom o ochronie danych, jak i RODO, niniejszy Aneks zmienia DPA, w tym jak określono w Załączniku 3 do niniejszego DPA, w zakresie niezbędnym do ich funkcjonowania:

(i) w przypadku przekazywania danych przez podmiot przekazujący dane podmiotowi odbierającemu dane, w zakresie, w jakim szwajcarskie przepisy o ochronie danych lub szwajcarskie przepisy o ochronie danych i RODO mają zastosowanie do przetwarzania danych przez podmiot przekazujący dane podczas przekazywania danych; oraz

(ii) zapewnienie odpowiednich zabezpieczeń dla przekazywania danych zgodnie z art. 46 RODO i/lub art. 6(2)(a) szwajcarskich przepisów o ochronie danych, w zależności od przypadku.

(b) W zakresie, w jakim przetwarzanie danych osobowych podlega wyłącznie szwajcarskim przepisom o ochronie danych, zmiany Umowy o partnerstwie biznesowym, w tym SCC, jak określono w Załączniku 3 do niniejszej Umowy o partnerstwie biznesowym i zgodnie z wymogami klauzuli 2.1 niniejszego Dodatku szwajcarskiego, obejmują (bez ograniczeń):

(i) Odniesienia do „Klauzul" lub „SCC" oznaczają niniejsze Szwajcarskie Uzupełnienie, ponieważ zmienia ono SCC oraz

(ii) Klauzula 6 Opis transferu(ów) otrzymuje brzmienie:
„Szczegóły dotyczące przekazywania danych, a w szczególności kategorie przekazywanych danych osobowych oraz cel(e), dla których są one przekazywane, są określone w Załączniku 1 do niniejszego DPA, w przypadku gdy szwajcarskie przepisy o ochronie danych mają zastosowanie do przetwarzania danych przez podmiot przekazujący dane podczas dokonywania tego przekazania."

(iii) Odniesienia do „rozporządzenia (UE) 2016/679" lub „tego rozporządzenia" lub „RODO" zastępuje się „szwajcarskimi przepisami o ochronie danych", a odniesienia do konkretnych artykułów „rozporządzenia (UE) 2016/679" lub „RODO" zastępuje się równoważnym artykułem lub sekcją szwajcarskich przepisów o ochronie danych w odpowiednim zakresie.

(iv) Usunięto odniesienia do rozporządzenia (UE) 2018/1725.

(v) Odniesienia do „Unii Europejskiej", „Unii", „UE" i „państwa członkowskiego UE" zastępuje się odniesieniem do „Szwajcarii".

(vi) Klauzula 13(a) i część C załącznika I nie są stosowane; „właściwym organem nadzorczym" jest Federalny Komisarz ds. Ochrony Danych i Informacji („FDPIC") w zakresie, w jakim przekazywanie danych podlega szwajcarskim przepisom o ochronie danych;

(vii) Klauzula 17 otrzymuje brzmienie:

„Niniejsze Klauzule podlegają prawu Szwajcarii w zakresie, w jakim transfery podlegają szwajcarskim przepisom o ochronie danych".

(viii) Klauzula 18 otrzymuje brzmienie:

„Wszelkie spory wynikające z niniejszych klauzul dotyczących szwajcarskich przepisów o ochronie danych będą rozstrzygane przez sądy szwajcarskie. Osoba, której dane dotyczą, może również wszcząć postępowanie sądowe przeciwko podmiotowi przekazującemu i/lub odbierającemu dane przed sądami szwajcarskimi, w których ma miejsce zwykłego pobytu. Strony zgadzają się poddać jurysdykcji takich sądów."

Do czasu wejścia w życie zmienionych szwajcarskich przepisów o ochronie danych osobowych, niniejsze klauzule będą również chronić dane osobowe osób prawnych, a osoby prawne otrzymają taką samą ochronę na mocy niniejszych klauzul jak osoby fizyczne.

2.4 W zakresie, w jakim jakiekolwiek przetwarzanie danych osobowych podlega zarówno szwajcarskim przepisom o ochronie danych, jak i RODO, RODO, w tym Klauzule, jak określono w Załączniku 3 do niniejszej Umowy, będą miały zastosowanie (i) w obecnej formie oraz (ii) dodatkowo, w zakresie, w jakim przekazanie podlega szwajcarskim przepisom o ochronie danych, zmienionym przez klauzule 2.1 i 2.3 niniejszego Dodatku Szwajcarskiego, z jedynym wyjątkiem, że klauzula 17 SCC nie zostanie zastąpiona zgodnie z klauzulą 2.3(b)(vii) niniejszego Dodatku Szwajcarskiego.

2.5 Klient gwarantuje, że on i/lub Użytkownicy Końcowi Klienta dokonali wszelkich zgłoszeń do FDPIC, które są wymagane na mocy szwajcarskich przepisów o ochronie danych.

Harmonogram 6
DODATEK USA

Zgodnie z klauzulą 14 DPA, niniejszy Dodatek USA ma zastosowanie do wszelkiego przetwarzania Danych Osobowych Klienta podlegającego Przepisom o Ochronie Danych USA.

W zakresie wymaganym przez amerykańskie przepisy o ochronie danych, Clerk nie może:

(a) sprzedaży Danych Osobowych Klienta lub innego udostępniania Danych Osobowych Klienta jakiejkolwiek stronie trzeciej za wynagrodzeniem pieniężnym lub innym wartościowym wynagrodzeniem;

(b) udostępniania Danych Osobowych Klienta jakimkolwiek stronom trzecim na potrzeby reklamy krzyżowej;

(c) przechowywanie, wykorzystywanie lub ujawnianie Danych Osobowych Klienta w jakimkolwiek celu innym niż cele biznesowe określone w Umowie lub w inny sposób dozwolony przez amerykańskie przepisy o ochronie danych;

(d) przechowywanie, wykorzystywanie lub ujawnianie Danych Osobowych Klienta poza bezpośrednimi relacjami biznesowymi między Stronami; oraz

(e) łączenie Danych Osobowych Klienta z Danymi Osobowymi, które Clerk otrzymuje od lub w imieniu innej osoby lub osób, lub które gromadzi w wyniku własnej interakcji z osobą, której dane dotyczą, chyba że amerykańskie przepisy o ochronie danych stanowią inaczej.

ZAŁĄCZNIK 7
ZAŁĄCZNIK AUSTRALIJSKI

Jeśli Klient przekazuje Clerk Dane Osobowe podlegające Australijskim Przepisom o Ochronie Danych, Klient przyjmuje do wiadomości, że postanowienia określone w niniejszej Umowie o Ochronie Danych chronią informacje w sposób zasadniczo podobny do Australijskich Zasad Prywatności (z wyjątkiem APP1).

ZAŁĄCZNIK 8
DODATEK JAPOŃSKI

W przypadku przekazania Danych Osobowych Klienta podlegających japońskiej Ustawie o Ochronie Danych Osobowych („APPI") do kraju uznanego za niezapewniający odpowiedniego poziomu ochrony prywatności, strony uzgadniają, że niniejsza Umowa o Ochronie Danych Osobowych i jej elementy mają zastosowanie jako uzasadnione środki dla takiego przekazania.

Strony zgadzają się powiadomić drugą stronę, jeśli po wyrażeniu zgody na DPA i w okresie obowiązywania Umowy, strona ma powody, by sądzić, że którakolwiek ze stron nie jest w stanie wywiązać się ze swoich zobowiązań wynikających z DPA lub DPA nie jest zgodna z postanowieniami APPI. W takim przypadku strony będą współpracować w dobrej wierze w celu określenia odpowiednich środków, które należy przyjąć. Jeśli nie będzie możliwe wdrożenie odpowiednich środków, strony będą współpracować w celu oceny, czy należy zawiesić przekazywanie Danych Osobowych Klienta.

Usługi nie są przeznaczone do obsługi określonych Danych Osobowych zdefiniowanych i podlegających japońskiej ustawie My Number Act (tj. ustawie o wykorzystaniu numerów do identyfikacji konkretnej osoby w ustawie o postępowaniu administracyjnym (ustawa nr 27 z 2013 r.), z ewentualnymi zmianami), chyba że Cl uzgodni inaczej.

ZAŁĄCZNIK 9
ZAŁĄCZNIK BRAZYLIA

W odniesieniu do danych osobowych brazylijskich osób, których dane dotyczą, Klient wyraża zgodę na przetwarzanie przez Clerk Danych Osobowych Klienta poza Brazylią oraz oświadcza i gwarantuje, że takie przekazywanie Danych Osobowych Klienta jest zgodne z LGPD.