Umowa o przetwarzanie danych

Ostatnia aktualizacja: 15 grudnia 2023 r.

Niniejsza Umowa o Przetwarzaniu Danych („DPA”) podlega Umowie i stanowi jej część oraz reguluje Przetwarzanie Danych Osobowych przez Stripe i jej Podmioty Powiązane.

1. Struktura.
Jeśli Konto Stripe Użytkownika znajduje się w Ameryce Północnej lub Ameryce Południowej, Użytkownik zawiera niniejszą Umowę o partnerstwie ze Stripe, Inc. („SINC”). Jeśli konto Stripe użytkownika znajduje się w innym miejscu, użytkownik zawiera niniejszą Umowę o partnerstwie z firmą Stripe Payments Europe, Limited („SPEL”). W związku z tym odniesienia do „Stripe” w niniejszej Umowie DPA oznaczają odpowiednio SINC lub SPEL.

2. Stripe jako podmiot przetwarzający i administrator danych.
Role przetwarzania danych

Stripe jako podmiot przetwarzający dane	Gdy Stripe przetwarza dane osobowe jako podmiot przetwarzający dane, działa jako podmiot przetwarzający dane w imieniu użytkownika, administratora danych.
Stripe jako administrator danych	Gdy Stripe przetwarza dane osobowe jako administrator danych, to - ma jedyne i wyłączne prawo do określania celów i sposobów Przetwarzania Danych Osobowych, które otrzymuje od użytkownika lub za jego pośrednictwem; oraz - może zaangażować Podmiot Stowarzyszony Stripe do działania jako (a) Współadministrator w celu świadczenia Autoryzowanych Usług; oraz (b) Podmiot Przetwarzający Dane w celu świadczenia usług innych niż Autoryzowane Usługi.

Cele przetwarzania danych

Stripe jako podmiot przetwarzający dane	Cele przetwarzania danych osobowych przez Stripe w charakterze podmiotu przetwarzającego dane to: - obsługa platformy Stripe; oraz - dostarczanie i zapewnianie dostępu do produktów i usług Stripe.
Stripe jako administrator danych	Cele przetwarzania Danych Osobowych przez Stripe w charakterze Administratora Danych podczas dostarczania produktów i usług Stripe to: - określanie i wykorzystywanie stron trzecich (banków i dostawców metod płatności); - monitorowanie, zapobieganie i wykrywanie oszukańczych transakcji i innych oszukańczych działań na platformie Stripe - monitorowanie, zapobieganie i ograniczanie strat finansowych, zagrożeń bezpieczeństwa i innych szkód; - wdrażanie, utrzymywanie i wykonywanie wewnętrznych procesów, które umożliwiają Stripe dostarczanie produktów i usług, w tym zarządzanie relacjami, rozliczenia i fakturowanie; - przestrzegania przepisów prawa, w tym obowiązujących obowiązków w zakresie przeciwdziałania praniu pieniędzy i znajomości klienta, a także wymogów i żądań partnerów finansowych i organów rządowych; oraz - analizować i rozwijać produkty i usługi Stripe.

Kategorie osób, których dane dotyczą, i dane osobowe: Stripe jako podmiot przetwarzający i administrator danych

Podmioty danych	Stripe może przetwarzać dane osobowe Klientów, przedstawicieli i wszelkich osób fizycznych, które uzyskują dostęp do Konta Stripe lub z niego korzystają.
Dane osobowe	W stosownych przypadkach Stripe może przetwarzać dane konta płatniczego, dane konta bankowego, adres rozliczeniowy/ wysyłkowy, imię i nazwisko, opis zamówienia (w tym datę, godzinę, kwotę, opis produktu lub usługi), identyfikator urządzenia, adres e-mail, adres IP/lokalizację, identyfikator zamówienia, dane karty płatniczej, identyfikator podatkowy/status, unikalny identyfikator klienta, informacje o tożsamości, w tym dokumenty wydane przez rząd (np. dowody osobiste, prawa jazdy i paszporty).
Dane wrażliwe	W stosownych przypadkach Stripe może przetwarzać dane wrażliwe (np. dane rozpoznawania twarzy).

Czas trwania przetwarzania

Stripe jako podmiot przetwarzający dane	W Okresie Obowiązywania i w każdym okresie wymaganym do wykonania zobowiązań strony po rozwiązaniu umowy.

Bezpieczeństwo danych

Stripe jako podmiot przetwarzający dane i administrator danych	Stripe wdroży i będzie utrzymywać pisemny program bezpieczeństwa informacji obejmujący środki bezpieczeństwa danych określone w Załączniku do niniejszej Umowy o partnerstwie.

3. Obowiązki Stripe jako podmiotu przetwarzającego dane.

3.1 Obowiązki.

Gdy Stripe działa jako podmiot przetwarzający dane na rzecz użytkownika, Stripe będzie:

(a) Przetwarzać Dane Osobowe w imieniu Użytkownika i zgodnie z jego Instrukcjami. Stripe poinformuje użytkownika, jeśli jego zdaniem Instrukcje naruszają lub naruszają Prawo DP;

(b) zapewni, że wszystkie osoby upoważnione przez Stripe do Przetwarzania Danych Osobowych uzyskają dostęp do Danych Osobowych na zasadzie ograniczonego dostępu i będą zobowiązane do przestrzegania poufności tych Danych Osobowych;

(c) w zakresie wymaganym przez Ustawę o ochronie danych osobowych, informować użytkownika o każdym żądaniu otrzymanym przez Stripe od Podmiotów danych (w tym o „możliwych do zweryfikowania żądaniach konsumentów" zgodnie z definicją zawartą w CCPA) korzystających z przysługujących im na mocy Ustawy o ochronie danych osobowych praw do (i) dostępu (np. prawa do informacji zgodnie z CCPA) do swoich Danych osobowych; (ii) poprawienia lub usunięcia swoich Danych osobowych; (iii) ograniczenia lub sprzeciwu wobec Przetwarzania przez Stripe; lub (iv) przenoszenia danych (łącznie „Żądanie Podmiotu danych"). Poza żądaniem dalszych informacji, identyfikacji Podmiotu Danych oraz, w stosownych przypadkach, skierowania Podmiotu Danych do użytkownika jako Administratora Danych, Stripe nie odpowie na te żądania, chyba że użytkownik poinstruuje Stripe na piśmie, aby to zrobił. Biorąc pod uwagę charakter Przetwarzania, Stripe pomoże użytkownikowi za pomocą odpowiednich środków technicznych i organizacyjnych, o ile będzie to możliwe, w celu umożliwienia mu wywiązania się z obowiązku udzielenia odpowiedzi na Wniosek Podmiotu Danych;

(d) w zakresie wymaganym przez Prawo DP, informować użytkownika o każdym żądaniu organów ścigania otrzymanym przez Stripe od organu rządowego wymagającego od Stripe ujawnienia Danych Osobowych lub udziału w dochodzeniu wymagającym od Stripe ujawnienia Danych Osobowych, chyba że jest to zabronione przez Prawo;

(e) w zakresie wymaganym przez Prawo o ochronie danych osobowych, zapewnić użytkownikowi uzasadnioną pomoc, na jego pisemny wniosek, aby pomóc mu w wypełnieniu obowiązków wynikających z Prawa o ochronie danych osobowych oraz, biorąc pod uwagę charakter Przetwarzania i informacje dostępne dla Stripe, Stripe dostarczy

uzasadnione informacje, aby pomóc użytkownikowi w przeprowadzeniu oceny wpływu na ochronę danych lub skonsultować się z organem nadzorczym. Jeśli użytkownik zwróci się do Stripe o pomoc, która wykracza poza obowiązki Stripe wynikające z Ustawy o ochronie danych lub niniejszej Umowy, Stripe może naliczyć uzasadnioną opłatę;

(f) jeśli Stripe doświadczy Incydentu dotyczącego Danych, powiadomi użytkownika bez zbędnej zwłoki, co w przypadku Incydentów dotyczących Danych mających wpływ na Dane osobowe podlegające RODO lub brytyjskiemu RODO nastąpi nie później niż 48 godzin, w każdym przypadku po uzyskaniu informacji o Incydencie dotyczącym Danych. W zakresie znanym Stripe, powiadomienie użytkownika przez Stripe będzie opisywać w rozsądnych szczegółach (i) rodzaj Danych Osobowych, które były przedmiotem Incydentu dotyczącego Danych, (ii) kategorie i potencjalną liczbę osób lub rekordów, których dotyczy Incydent (w tym ich kraje) oraz (iii) status dochodzenia Stripe i bieżące lub planowane środki zaradcze. Po otrzymaniu powiadomienia Stripe dostarczy odpowiednie aktualizacje, aby pomóc użytkownikowi w wypełnianiu obowiązków wynikających z przepisów dotyczących ochrony danych;

(g) w zakresie wymaganym przez Prawo DP i na pisemny wniosek użytkownika, przyczyniać się do audytów lub inspekcji poprzez udostępnianie użytkownikowi raportów z audytów. Po otrzymaniu takiego żądania, nie częściej niż raz w roku, Stripe niezwłocznie dostarczy dokumentację lub wypełni pisemny kwestionariusz bezpieczeństwa danych o rozsądnym zakresie i czasie trwania dotyczący przetwarzania danych osobowych przez Stripe i jego podmioty stowarzyszone. Wszystkie dostarczone raporty i dokumentacja, w tym wszelkie odpowiedzi na kwestionariusz bezpieczeństwa, stanowią informacje poufne Stripe; oraz

(h) według wyboru użytkownika, usunąć lub zwrócić mu wszystkie Dane Osobowe przetwarzane w związku z Usługami oraz usunąć istniejące kopie po rozwiązaniu Umowy, z zastrzeżeniem, że Stripe nie będzie zobowiązany do usunięcia lub zwrotu tych Danych Osobowych ani usunięcia istniejących kopii w zakresie, w jakim przechowywanie przez Stripe tych Danych Osobowych lub tych kopii jest (i) wymagane przez Stripe w celu wykonywania jego praw i obowiązków wynikających z niniejszej Umowy; lub (ii) wymagane lub dozwolone przez Prawo DP przez dłuższy okres.

3.2 Podmioty przetwarzające dane.

(a) Stripe angażuje Podmioty Przetwarzające w zakresie niezbędnym do świadczenia Usług. Lista Podmiotów przetwarzających dane Stripe, która może również obejmować Podmioty stowarzyszone Stripe, znajduje się pod adresem stripe.com/service-providers/legal („Lista Podmiotów przetwarzających dane Stripe"). Użytkownik wyraża zgodę na korzystanie przez Stripe z istniejących Podprzetwarzających i udziela Stripe ogólnego pisemnego upoważnienia do angażowania Podprzetwarzających w zakresie niezbędnym do świadczenia Usług. Jeśli użytkownik subskrybuje powiadomienia e-mail na Liście Podprzetwarzających Stripe, Stripe powiadomi go pocztą elektroniczną, jeśli zamierza dodać jednego lub więcej Podprzetwarzających do tej listy co najmniej 30 dni przed wejściem zmian w życie. Użytkownik może w uzasadniony sposób sprzeciwić się zmianie z uzasadnionych przyczyn w ciągu 30 dni od otrzymania powiadomienia o zmianie. Użytkownik przyjmuje do wiadomości, że Podmioty przetwarzające dane Stripe są niezbędne do świadczenia Usług oraz że w przypadku wyrażenia przez użytkownika sprzeciwu wobec korzystania przez Stripe z Podmiotu przetwarzającego dane, niezależnie od odmiennych postanowień Umowy (w tym niniejszego dokumentu DPA), Stripe nie będzie zobowiązany do świadczenia użytkownikowi Usług, w odniesieniu do których Stripe korzysta z Podmiotu przetwarzającego dane.

(b) Stripe zawrze pisemną umowę z każdym Podprzetwarzającym, która nakłada na Podprzetwarzającego obowiązki porównywalne z obowiązkami nałożonymi na Stripe na mocy niniejszego DPA, w tym obowiązek wdrożenia odpowiednich Środków Bezpieczeństwa Danych. Jeśli Podprzetwarzający nie wypełni swoich zobowiązań w zakresie ochrony danych wynikających z tej umowy, Stripe pozostanie odpowiedzialny wobec użytkownika za działania i zaniechania swojego Podprzetwarzającego w takim samym zakresie, w jakim Stripe byłby odpowiedzialny, gdyby wykonywał odpowiednie Usługi bezpośrednio na podstawie niniejszego DPA.

3.3 CCPA.

Jeśli zastosowanie ma CCPA, a Stripe działa jako podmiot przetwarzający dane, Stripe nie będzie: (a) sprzedawać ani udostępniać (zgodnie z definicją zawartą w CCPA) Danych Osobowych; (b) przechowywać,

wykorzystywać ani ujawniać Danych Osobowych poza bezpośrednimi relacjami biznesowymi z użytkownikiem, z wyjątkiem dostarczania produktów i usług Stripe oraz w zakresie wymaganym przez prawo; oraz (c) łączyć Danych Osobowych otrzymanych od użytkownika lub za jego pośrednictwem z Danymi Osobowymi otrzymanymi od osoby fizycznej lub w jej imieniu lub zebranymi w wyniku własnych interakcji Stripe z daną osobą, z wyjątkiem dostarczania produktów i usług Stripe oraz w zakresie dozwolonym przez prawo. Stripe zaświadcza, że rozumie i będzie przestrzegać wymogów niniejszego DPA odnoszących się do CCPA i zapewni taki sam poziom ochrony prywatności danych osobowych, jaki jest wymagany przez CCPA. Stripe poinformuje użytkownika, jeśli stwierdzi, że nie może dłużej wypełniać swoich zobowiązań wynikających z CCPA i podejmie uzasadnione i odpowiednie kroki w celu zaradzenia wszelkiemu nieautoryzowanemu przetwarzaniu danych osobowych.

3.4 Wyłączenie odpowiedzialności.
Niezależnie od jakichkolwiek odmiennych postanowień Umowy, w tym niniejszego DPA, Stripe i jego podmioty stowarzyszone nie ponoszą odpowiedzialności za jakiekolwiek roszczenia zgłoszone przez osobę, której dane dotyczą, wynikające z działań lub zaniechań Stripe lub któregokolwiek z jego podmiotów stowarzyszonych lub z nimi związane, w zakresie, w jakim Stripe działał zgodnie z Instrukcjami użytkownika.

4. Obowiązki użytkownika działającego jako administrator danych.
Użytkownik musi:

(a) przekazywać Stripe wyłącznie Dyspozycje, które są zgodne z prawem;

(b) przestrzegać i wypełniać swoje obowiązki wynikające z prawa o ochronie danych, w tym w odniesieniu do praw osób, których dane dotyczą, bezpieczeństwa i poufności danych, a także zapewnić odpowiednią podstawę prawną do przetwarzania danych osobowych zgodnie z opisem w Umowie, w tym w niniejszym DPA; oraz

(c) dostarczać Podmiotom Danych wszelkich niezbędnych informacji (w tym poprzez oferowanie przejrzystej i łatwo dostępnej publicznej informacji o

ochronie prywatności) oraz, jeśli wymaga tego Prawo o ochronie danych, uzyskiwać wszelkie niezbędne zgody dotyczące Przetwarzania Danych Osobowych przez Stripe i użytkownika w celach opisanych w Umowie, w tym w niniejszym DPA.

5. Obowiązki Stripe jako administratora danych.
Podczas Przetwarzania Danych Osobowych Stripe musi przestrzegać i wypełniać swoje obowiązki wynikające z Ustawy o ochronie danych osobowych.

6. Przekazywanie danych.
6.1 Transgraniczne przekazywanie danych przez użytkownika.
Użytkownik przyjmuje do wiadomości, że w celu świadczenia Usług przez Stripe przekazuje Dane Osobowe do Stripe, Inc. („SINC") w Stanach Zjednoczonych. Jeśli transfer obejmuje Dane Osobowe, które wymagają Mechanizmu Transferu Danych, zastosowanie ma Załącznik dotyczący Transferu Danych, który jest włączony do niniejszego DPA.

6.2 Transgraniczne przekazywanie danych przez Stripe.
Stripe i jego Podmioty Stowarzyszone mogą przekazywać Dane Osobowe w skali globalnej w zakresie niezbędnym do świadczenia Usług. W szczególności Dane Osobowe mogą być przekazywane do SINC w Stanach Zjednoczonych oraz do Podmiotów Stowarzyszonych i Podprzetwarzających dane Stripe w innych jurysdykcjach.

7. Konflikt.
W przypadku konfliktu pomiędzy:

(a) postanowieniami niniejszej Umowy o partnerstwie i jakimkolwiek postanowieniem Umowy dotyczącym Przetwarzania Danych Osobowych, pierwszeństwo będą miały postanowienia niniejszej Umowy o partnerstwie; oraz

(b) postanowieniami niniejszej Umowy o partnerstwie i jakimkolwiek postanowieniem Uzupełnienia dotyczącego przekazywania danych, pierwszeństwo mają postanowienia Uzupełnienia dotyczącego przekazywania danych.

8. Definicje.
Terminy pisane wielką literą, które nie zostały zdefiniowane w niniejszym DPA, mają znaczenie nadane im w Umowie.

„Umowa" ma znaczenie nadane w umowie o świadczenie usług Stripe między użytkownikiem a Stripe, znajdującej się pod adresem www.stripe.com/[kod kraju]/legal/ssa, gdzie »[kod kraju]« oznacza dwuliterowy skrót kraju, w którym znajduje się konto Stripe użytkownika, lub w inny sposób uzgodniony przez strony.

„Autoryzowane Usługi" oznaczają Usługi, które są licencjonowane, autoryzowane lub regulowane przez organ rządowy.

„CCPA" oznacza California Consumer Privacy Act z 2018 r., Cal. Civ. Code Sections 1798.100-1798.199 oraz jej przepisy wykonawcze.

„Administrator Danych" oznacza podmiot, który samodzielnie lub wspólnie z innymi określa cele i sposoby Przetwarzania Danych Osobowych, co może obejmować, w stosownych przypadkach, »Przedsiębiorstwo« zgodnie z definicją zawartą w CCPA.

„Incydent dotyczący Danych" oznacza nieuprawnione lub niezgodne z prawem Przetwarzanie, wykorzystanie, dostęp, utratę, ujawnienie, zniszczenie lub zmianę Danych Osobowych znajdujących się w posiadaniu lub pod kontrolą strony lub jej Podmiotu Stowarzyszonego lub podwykonawcy, agenta lub przedstawiciela strony lub jej Podmiotu Stowarzyszonego.

„Ramy Prywatności Danych" oznaczają, odpowiednio, program samocertyfikacji Ram Prywatności Danych UE-USA, Szwajcaria-USA lub Wielka Brytania-USA prowadzony przez Departament Handlu USA.

„Podmiot Przetwarzający Dane" oznacza podmiot, który Przetwarza Dane Osobowe w imieniu Administratora Danych, co może obejmować, w stosownych przypadkach, »Dostawcę Usług« zgodnie z definicją zawartą w CCPA.

„Środki Bezpieczeństwa Danych" oznaczają środki techniczne i organizacyjne, które mają na celu zabezpieczenie Danych Osobowych do poziomu bezpieczeństwa odpowiedniego do ryzyka Przetwarzania.

„Podmiot Danych" oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której dotyczą Dane Osobowe.

„Mechanizm Przekazywania Danych" oznacza mechanizm przekazywania danych, który umożliwia zgodne z prawem transgraniczne przekazywanie Danych Osobowych zgodnie z Prawem Ochrony Danych, co obejmuje mechanizmy przekazywania danych wymagane zgodnie z Prawem Ochrony Danych w EOG, Szwajcarii i Wielkiej Brytanii, takie jak Ramy Prywatności Danych, SCC EOG, Uzupełnienie do Międzynarodowego Przekazywania Danych w Wielkiej Brytanii oraz wszelkie mechanizmy przekazywania danych dostępne zgodnie z Prawem Ochrony Danych, które zostały włączone do niniejszego DPA.

„Załącznik dotyczący przekazywania danych" oznacza załącznik dotyczący przekazywania danych znajdujący się pod adresem www.stripe.com/legal/dta.

„Prawo DP" oznacza prawo mające zastosowanie do Przetwarzania Danych Osobowych na mocy Umowy i niniejszego DPA, w tym prawo międzynarodowe, federalne, stanowe, prowincjonalne i lokalne odnoszące się w jakikolwiek sposób do prywatności, ochrony danych lub bezpieczeństwa danych.

„EOG" oznacza Europejski Obszar Gospodarczy.

„Standardowe klauzule umowne EOG" oznaczają Moduł 1 (Przekazanie: Administrator danych do Administratora danych) i Moduł 2 (Przekazanie: Administrator danych do Podmiotu przetwarzającego) standardowych klauzul umownych określonych w decyzji wykonawczej Komisji Europejskiej (UE) 2021/914 w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich zgodnie z RODO.

„RODO" oznacza ogólne rozporządzenie o ochronie danych (UE) 2016/679.

„Instrukcje” oznaczają wszelką komunikację lub dokumentację, w tym dokumentację, która może być dostarczana za pośrednictwem interfejsu API Stripe lub pulpitu Stripe, lub pisemne umowy między użytkownikiem a Stripe, za pośrednictwem których Administrator Danych instruuje Podmiot Przetwarzający Dane, aby wykonał określone Przetwarzanie Danych Osobowych dla tego Administratora Danych.

„Współadministrator” oznacza Administratora Danych, który wspólnie z co najmniej jednym Administratorem Danych określa cele i sposoby Przetwarzania Danych Osobowych.

„Dane Osobowe” oznaczają wszelkie informacje dotyczące możliwej do zidentyfikowania osoby fizycznej, które są Przetwarzane w związku z Usługami i obejmują »dane osobowe« zgodnie z definicją zawartą w RODO oraz »informacje osobowe« zgodnie z definicją zawartą w CCPA.

„Przetwarzanie” oznacza wykonywanie dowolnej operacji lub zestawu operacji na Danych Osobowych lub zestawach Danych Osobowych, takich jak gromadzenie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, dostosowywanie lub zmienianie, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, dostosowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, zgodnie z opisem w Ustawie o ochronie danych osobowych.

„Dane Wrażliwe” oznaczają, w zakresie, w jakim dane te są traktowane jako szczególna kategoria Danych Osobowych zgodnie z Ustawą o ochronie danych osobowych: (a) Dane Osobowe, które są danymi genetycznymi, danymi biometrycznymi, danymi dotyczącymi zdrowia, życia seksualnego lub orientacji seksualnej osoby fizycznej; (b) dane dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych lub przynależności do związków zawodowych; (c) dane geolokalizacyjne; lub (d) wrażliwe dane osobowe zgodnie z definicją zawartą w CCPA.

„Podprzetwarzający” oznacza podmiot, który Przetwarzający Dane angażuje do Przetwarzania Danych Osobowych w imieniu Przetwarzającego Dane w związku z Usługami.

„Organ Nadzorczy” oznacza niezależny organ publiczny, który jest (i) ustanowiony przez państwo członkowskie Unii Europejskiej zgodnie z art. 51 RODO; lub (ii) organ publiczny regulujący ochronę danych, który ma władzę nadzorczą i jurysdykcję nad użytkownikiem.

„RODO Wielkiej Brytanii” oznacza RODO transponowane do prawa krajowego Wielkiej Brytanii na mocy sekcji 3 Ustawy o wystąpieniu z Unii Europejskiej (European Union (Withdrawal) Act 2018) i zmienione Rozporządzeniem o ochronie danych, prywatności i łączności elektronicznej (zmiany itp.) (Wyjście z UE) z 2019 roku (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

„Dodatek dotyczący międzynarodowego przekazywania danych w Wielkiej Brytanii” oznacza dodatek dotyczący międzynarodowego przekazywania danych do standardowych klauzul umownych EOG wydany przez brytyjski urząd komisarza ds. informacji.

EKSPONAT: BEZPIECZEŃSTWO DANYCH STRIPE

Programy i zasady bezpieczeństwa	Stripe utrzymuje i egzekwuje program bezpieczeństwa, który dotyczy sposobu zarządzania bezpieczeństwem przez Stripe, w tym kontroli bezpieczeństwa. Program bezpieczeństwa obejmuje: - udokumentowane zasady, które Stripe formalnie zatwierdza, publikuje wewnętrznie, przekazuje odpowiednim pracownikom i przegląda co najmniej raz w roku; - udokumentowane, jasne przypisanie odpowiedzialności i uprawnień do działań związanych z programem bezpieczeństwa; - polityki obejmujące, w stosownych przypadkach, dopuszczalne użytkowanie komputera, klasyfikację danych, kontrole kryptograficzne, kontrolę dostępu, nośniki wymienne i dostęp zdalny; oraz - regularne testowanie kluczowych kontroli, systemów i procedur. Program ochrony prywatności. Stripe utrzymuje i egzekwuje program ochrony prywatności i powiązane polityki, które dotyczą sposobu gromadzenia, wykorzystywania i udostępniania Danych Osobowych.
Zarządzanie ryzykiem i aktywami	Stripe przeprowadza oceny ryzyka oraz wdraża i utrzymuje mechanizmy kontroli w zakresie identyfikacji, analizy, monitorowania, raportowania i działań naprawczych. Stripe utrzymuje i egzekwuje program zarządzania aktywami, który odpowiednio klasyfikuje i kontroluje zasoby sprzętowe i programowe przez cały cykl ich życia.

Edukacja i kontrola personelu	Wszyscy (a) pracownicy Stripe; oraz (b) niezależni wykonawcy Stripe, którzy mogą mieć dostęp do danych, w tym ci, którzy Przetwarzają Dane Osobowe ((a) i (b), łącznie „Personel") potwierdzają swoje obowiązki w zakresie bezpieczeństwa danych i prywatności zgodnie z zasadami Stripe. W przypadku Personelu, Stripe, samodzielnie lub za pośrednictwem strony trzeciej: - wdraża kontrole przeszłości i badania przesiewowe przed zatrudnieniem; - przeprowadza szkolenia w zakresie bezpieczeństwa i prywatności - wdraża procesy dyscyplinarne w przypadku naruszenia wymogów bezpieczeństwa danych lub prywatności; oraz - po rozwiązaniu umowy lub zmianie roli niezwłocznie usuwa lub aktualizuje prawa dostępu Personelu i wymaga od Personelu zwrotu lub zniszczenia Danych Osobowych. Uwierzytelnianie. Stripe uwierzytelnia tożsamość każdego Personelu za pomocą odpowiednich danych uwierzytelniających, takich jak silne hasła, tokeny lub dane biometryczne.
Szkolenie i świadomość	Coroczne szkolenie w zakresie bezpieczeństwa i prywatności. Pracownicy Stripe przechodzą coroczne szkolenie w zakresie bezpieczeństwa i prywatności dotyczące zasad i praktyk Stripe w zakresie bezpieczeństwa i poufności danych.

Zarządzanie siecią i operacjami	Zasady i procedury. Stripe wdraża zasady i procedury dotyczące zarządzania siecią i operacjami. Te zasady i procedury dotyczą utwardzania, kontroli zmian, podziału obowiązków, oddzielenia środowisk programistycznych i produkcyjnych, zarządzania architekturą techniczną, bezpieczeństwa sieci, ochrony przed złośliwym oprogramowaniem, ochrony danych w tranzycie i w spoczynku, integralności danych, szyfrowania, dzienników audytu i segregacji sieci. Oceny podatności. Stripe przeprowadza okresowe oceny podatności i testy penetracyjne swoich systemów i aplikacji, w tym tych, które przetwarzają dane osobowe. Podatności są zarządzane i naprawiane zgodnie ze standardem zarządzania podatnościami Stripe.

Techniczna kontrola dostępu	Kontrola dostępu. Stripe wdraża środki mające na celu zapobieganie wykorzystywaniu systemów przetwarzania danych przez osoby nieupoważnione, w tym następujące środki: - procedury identyfikacji i uwierzytelniania użytkowników; - procedury bezpieczeństwa identyfikatora/ hasła, w tym silniejsze środki uwierzytelniania cyfrowego oparte na NIST 800-63B, w tym MFA; - automatyczne blokowanie (np. hasło lub limit czasu); oraz - monitorowanie prób włamań. Kontrola dostępu do danych. Stripe wdraża środki mające na celu zapewnienie, że osoby uprawnione do korzystania z systemu przetwarzania danych uzyskują dostęp wyłącznie do Danych Osobowych dozwolonych dla ich praw dostępu oraz że Dane Osobowe nie mogą być odczytywane, kopiowane, modyfikowane ani usuwane bez upoważnienia, w tym: - wewnętrzne polityki i procedury; - schematy autoryzacji kontroli; - zróżnicowane prawa dostępu (profile, role, działania i obiekty); - monitorowanie i rejestrowanie dostępu; - raporty dostępu; - procedura dostępu; - procedura zmiany; oraz - procedura usuwania.

Fizyczna kontrola dostępu	Stripe korzysta z usług renomowanych zewnętrznych dostawców usług w celu hostowania swojej infrastruktury produkcyjnej. Stripe polega na tych osobach trzecich w zakresie zarządzania fizyczną kontrolą dostępu do zarządzanych przez nich centrów danych. Niektóre ze środków zapewnianych przez dostawców usług Stripe w celu uniemożliwienia osobom nieupoważnionym uzyskania fizycznego dostępu do systemów przetwarzania danych dostępnych w obiektach i obiektach (w tym baz danych, serwerów aplikacji i powiązanego sprzętu), w których przetwarzane są dane osobowe, obejmują: - fizyczny system kontroli dostępu i program wdrożony w siedzibie Stripe; - Globalne Centrum Operacyjne Bezpieczeństwa 24x7, które monitoruje systemy bezpieczeństwa fizycznego; - systemy wideo i alarmowe; - role kontroli dostępu i strefy obszarowe; - środki audytu kontroli dostępu; - elektroniczny program śledzenia i zarządzania kluczami; - proces autoryzacji dostępu dla pracowników i osób trzecich; - blokady drzwi (zamki elektryczne itp.); oraz - przeszkolony umundurowany personel ochrony. Stripe weryfikuje raporty z audytów stron trzecich w celu sprawdzenia, czy dostawcy usług Stripe utrzymują odpowiednią fizyczną kontrolę dostępu do zarządzanych centrów danych.

Kontrola dostępności	Stripe wdraża środki zapewniające możliwość przywrócenia dostępności i dostępu do Danych Osobowych w odpowiednim czasie w przypadku incydentu fizycznego lub technicznego, w tym: - replikację bazy danych; - procedury tworzenia kopii zapasowych; - redundancję sprzętu; oraz - plan odzyskiwania danych po awarii.
Kontrola ujawniania informacji	Stripe wdraża środki w celu zapewnienia, że dane osobowe (a) nie mogą być odczytywane, kopiowane, modyfikowane lub usuwane bez autoryzacji podczas transmisji elektronicznej, transportu lub przechowywania na nośnikach pamięci (ręcznych lub elektronicznych); oraz (b) można zweryfikować, którym firmom lub innym podmiotom prawnym ujawniane są dane osobowe, w tym rejestrowanie, bezpieczeństwo transportu i szyfrowanie.
Kontrola wejścia	Stripe wdraża środki w celu monitorowania, czy dane zostały wprowadzone, zmienione lub usunięte (usunięte) i przez kogo, z systemów przetwarzania danych, w tym systemów rejestrowania i raportowania oraz ścieżek audytu i dokumentacji.
Kontrola separacji	Stripe wdraża środki w celu zapewnienia, że Dane Osobowe gromadzone w różnych celach mogą być przetwarzane oddzielnie, w tym: - „najmniej uprzywilejowane” ograniczenie dostępu do danych przez służby wewnętrzne; - rozdzielenie funkcji (produkcja/testowanie); - procedury przechowywania, poprawiania, usuwania i przesyłania danych do różnych celów; oraz - procesy segmentacji logicznej w celu zarządzania separacją Danych Osobowych.

Certyfikaty i raporty	Zgodność z PCI. W zakresie mającym zastosowanie do Usług, Stripe jest odpowiedzialny za świadczenie Usług w sposób zgodny z najwyższym poziomem certyfikacji (PCI Level 1) przewidzianym przez wymagania PCI-DSS. Certyfikacja Stripe jest corocznie potwierdzana przez wykwalifikowanego rzeczoznawcę ds. bezpieczeństwa (QSA). Raporty SOC. Stripe stosuje standardy audytu Service Organization Controls („SOC") dla organizacji usługowych wydane przez AICPA. Raporty SOC 1 i 2 są sporządzane corocznie i będą dostarczane na żądanie. Stripe może dodać standardy lub certyfikaty w dowolnym momencie.

Szyfrowanie	Stripe stosuje mechanizmy szyfrowania danych w wielu punktach usługi Stripe w celu ograniczenia ryzyka nieautoryzowanego dostępu do danych Stripe w spoczynku i w tranzycie. Dostęp do materiałów klucza kryptograficznego Stripe jest ograniczony do ograniczonej liczby upoważnionych pracowników. Szyfrowanie w tranzycie. Aby chronić dane w tranzycie, Stripe wymaga, aby wszystkie przychodzące i wychodzące połączenia danych były szyfrowane przy użyciu protokołu TLS 1.2. W przypadku danych przechodzących przez wewnętrzne sieci produkcyjne Stripe, Stripe używa protokołu mTLS do szyfrowania połączeń między systemami produkcyjnymi. Szyfrowanie w spoczynku. Aby chronić dane w spoczynku, Stripe używa standardowego szyfrowania (AES-256) do szyfrowania wszystkich danych produkcyjnych przechowywanych w infrastrukturze serwerowej. Tokenizacja danych kart płatniczych i kont bankowych. Numery kart płatniczych i kont bankowych są oddzielnie szyfrowane przy użyciu standardowego szyfrowania przemysłowego (AES-256) na poziomie danych i przechowywane w oddzielnym sejfie danych, który jest wysoce ograniczony. Klucze deszyfrujące są przechowywane na oddzielnych maszynach. Tokeny są generowane w celu obsługi przetwarzania danych Stripe.
Zarządzanie incydentami związanymi z bezpieczeństwem danych i powiadamianie o nich	Stripe wdraża program zarządzania incydentami związanymi z bezpieczeństwem danych, który dotyczy sposobu zarządzania incydentami związanymi z danymi przez Stripe. Stripe powiadomi użytkowników Stripe i organy rządowe (w stosownych przypadkach) o incydentach związanych z danymi w odpowiednim czasie, zgodnie z wymogami prawa DP.

Przeglądy, raporty z audytów i kwestionariusze bezpieczeństwa	Na pisemny wniosek, nie częściej niż raz w roku, Stripe wypełni pisemny kwestionariusz bezpieczeństwa danych o rozsądnym zakresie i czasie trwania dotyczący praktyk biznesowych Stripe i środowiska technologii danych w odniesieniu do Przetwarzania Danych Osobowych. Odpowiedzi udzielone przez Stripe w kwestionariuszu bezpieczeństwa stanowią poufne dane Stripe.
Konfiguracja systemu	Stripe wdraża środki zapewniające konfigurację systemu, w tym domyślne środki konfiguracji dla wewnętrznego IT i zarządzania bezpieczeństwem IT. Stripe polega na narzędziach do automatyzacji wdrażania infrastruktury i konfiguracji systemu. Te narzędzia automatyzacji wykorzystują konfiguracje infrastruktury, które są zarządzane przez kod przepływający przez procesy kontroli zmian Stripe. Procesy zarządzania zmianami w Stripe wymagają formalnych przeglądów kodu i dwustronnych zatwierdzeń przed wydaniem do produkcji. Stripe wykorzystuje narzędzia monitorujące do monitorowania infrastruktury produkcyjnej pod kątem zmian w stosunku do znanych baz konfiguracyjnych.
Przenośność danych	Interfejs API Stripe umożliwia użytkownikom Stripe programowy dostęp do danych przechowywanych do transferu, z wyłączeniem danych objętych zakresem PCI. Proces przenoszenia danych PCI do innych procesorów płatności zgodnych z PCI-DSS Level 1 można znaleźć na stronie https://stripe.com/docs/security/data-migrations/exports.
Przechowywanie i usuwanie danych	Stripe wdraża i utrzymuje zasady i procedury przechowywania danych związane z Danymi Osobowymi oraz dokonuje przeglądu tych zasad i procedur w stosownych przypadkach.