AMERICAN EXPRESS

Polityka operacyjna ochrony danych (DSOP)

Paski zmiany

Ważne aktualizacje są wymienione w Tabeli podsumowania zmian, a także wskazane w DSOP za pomocą paska zmiany. Paski zmiany to pionowe linie na lewym marginesie, które wskazują na zmieniony, dodany lub usunięty tekst. Wszystkie zmiany w DSOP są wskazane za pomocą paska zmiany, jak pokazano tutaj.

Tabela podsumowania zmian

Ważne aktualizacje są wymienione w poniższej tabeli, a także wskazane w *DSOP* za pomocą paska zmiany.

Dział/Podrozdział	Opis zmiany
W tym wydaniu nie wprowadzono żadnych zmian.	

Co robić w przypadku wystąpienia Incydentu dotyczącego Danych?

Po stwierdzeniu wystąpienia Incydentu dotyczącego Danych w Państwa firmie należy podjąć następujące kroki.

Krok 1:

Wypełnić Formularz Wstępnego Zawiadomienia o Incydencie Dotyczącym Danych Sprzedawcy i przesłać go drogą elektroniczną na adres EIRP@aexp.com w ciągu 72 godzin od stwierdzenia Incydentu dotyczącego Danych.

Krok 2:

Przeprowadzić dokładne dochodzenie; może to wymagać zatrudnienia Inspektora Sądowego branży kart płatniczych (PCI).

Krok 3:

Niezwłocznie przekazać nam numery wszystkich zagrożonych Kart American Express®.

Krok 4:

Współpracować z nami, aby wyjaśnić wszelkie kwestie związane z Incydentem dotyczącym Danych.

Więcej szczegółów dotyczących Obowiązków w zakresie Zarządzaniem Incydentami dotyczącymi Danych przedstawiono w Dziale 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych".

Mają Państwo pytania?

USA: (888) 732-3750 (numer bezpłatny)

Numer międzynarodowy: +1 (602) 537-3021

EIRP@aexp.com

Celem strategicznym American Express, lidera w dziedzinie ochrony konsumentów, od dawna jest ochrona Informacji o Posiadaczach Kart i Wrażliwych Danych Uwierzytelniających i dbanie o ich bezpieczeństwo.

Naruszenie bezpieczeństwa danych negatywnie wpływa na konsumentów, Sprzedawców, Dostawców Usług i wydawców kart. Nawet jeden incydent może poważnie zaszkodzić reputacji firmy i osłabić jej zdolność do skutecznego prowadzenia działalności. Przeciwdziałanie temu zagrożeniu poprzez wdrożenie Polityki operacyjnej ochrony danych danych może zwiększyć zaufanie klienta, podnieść rentowność i poprawić reputację firmy.

American Express wie, że Sprzedawcy i Dostawcy Usług (łącznie zwani Państwo) podzielają nasze obawy i wymaga, aby w ramach Państwa obowiązków przestrzegali **Państwo** postanowień dotyczących ochrony danych w ramach **Umowy** o akceptację (w przypadku Sprzedawców) lub przetwarzanie (w przypadku Dostawców Usług) Karty American Express® (zwanych z osobna Umową) oraz niniejszej Polityki operacyjnej ochrony danych z uwzględnieniem jej późniejszych zmian. Wymogi te odnoszą się do wszystkich Państwa urządzeń, systemów i sieci (oraz ich komponentów), w których przechowywane, przetwarzane lub przekazywane są klucze szyfrujące, Dane Posiadaczy Kart lub Wrażliwe Dane Uwierzytelniające (lub ich kombinacja).

Terminy pisane wielką literą, których nie zdefiniowano w niniejszym dokumencie, posiadają znaczenia nadane im w słowniczku na końcu niniejszej Polityki.

Dział 1 Program Analizy Ukierunkowanej (TAP)

Naruszenia danych Posiadaczy Kart mogą być spowodowane przez luki w zabezpieczeniach danych Środowiska Danych Posiadaczy Kart (CDE).

Przykłady naruszenia Danych Posiadaczy Kart obejmują między innymi:

- **Wspólny Punkt Zakupu (CPP):** Posiadacze kart American Express zgłaszają oszukańcze Transakcje na swoich kontach Kart i są one identyfikowane i ustalane jest, że pochodzą z dokonywania zakupów w Państwa Placówkach.
- **Znalezione Dane Kart:** Dane Kart i Posiadaczy Kart American Express znalezione w sieci WWW powiązane z Transakcjami w Państwa Placówkach.
- **Podejrzenie działania złośliwego oprogramowania:** American Express podejrzewa, że używają Państwo oprogramowania zainfekowanego lub podatnego na złośliwy kod.

Program TAP ma na celu identyfikację potencjalnych naruszeń danych Posiadaczy Kart.

Po powiadomieniu przez American Express o potencjalnym naruszeniu danych Posiadacza Karty, należy i trzeba sprawić, aby Uwzględnione Strony spełniły następujące wymagania.

- Muszą Państwo niezwłocznie przejrzeć swoje CDE pod kątem luk w zabezpieczeniach danych i usunąć wszelkie wykryte.
  - W przypadku outsourcingu muszą Państwo skłonić swojego zewnętrznego dostawcę (dostawców) do przeprowadzenia dokładnego dochodzenia w sprawie Państwa CDE.
- Muszą Państwo przedstawić podsumowanie działań podjętych lub planowanych po przeglądzie, ocenie i/lub działaniach naprawczych po otrzymaniu powiadomienia od American Express.
- Muszą Państwo dostarczyć zaktualizowane dokumenty walidacyjne PCI DSS zgodnie z Działem 5, „Ważna okresowa walidacja Państwa systemów”.
- W stosownych przypadkach muszą Państwo zaangażować wykwalifikowanego Inspektora Sądowego PCI (PFI) do zbadania Państwa CDE, jeśli Państwo lub Uwzględniona strona:
  - Nie można rozwiązać problemu naruszenia danych Posiadacza Karty w rozsądnym terminie określonym przez American Express, lub
  - Prosimy o potwierdzenie, że doszło do Incydentu Dotyczącego Danych i zastosowanie się do wymagań określonych w Dziale 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych”.

Tabela A-1: Opłata za niezgodność z TAP

Opis	Sprzedawca poziomu 1 lub Dostawca usług poziomu 1	Sprzedawca poziomu 2 lub Dostawca usług poziomu 2	Sprzedawca poziomu 3 lub poziomu 4
Opłata za niezgodność może zostać naliczona, gdy zobowiązania TAP nie zostaną wypełnione przed upływem pierwszego terminu.	25 000 USD	5 000 USD	1 000 USD
Opłata za niezgodność może zostać naliczona, gdy zobowiązania TAP nie zostaną wypełnione przed upływem drugiego terminu.	35 000 USD	10 000 USD	2 500 USD
Opłata za niezgodność może zostać naliczona, gdy zobowiązania TAP nie zostaną wypełnione przed upływem trzeciego terminu. **UWAGA:** *Opłaty za niezgodność mogą być nadal naliczane do czasu wywiązania się ze zobowiązań lub rozwiązania problemu z TAP.*	45 000 USD	15 000 USD	5 000 USD

Jeśli Państwa zobowiązania TAP nie zostaną spełnione, American Express ma prawo do nałożenia opłat za niezgodność łącznie, wstrzymania płatności i/lub rozwiązania Umowy.

Dział 2 Standardy w zakresie ochrony Kluczy Szyfrujących, Danych Posiadaczy Kart i Wrażliwych Danych Uwierzytelniających

Muszą Państwo spełnić następujące warunki oraz dopilnować, aby spełniły je Uwzględnione Strony:

- przechowywać Dane Posiadaczy Kart wyłącznie w celu umożliwienia Transakcji Kartą American Express zgodnie z wymogami Umowy.
- przestrzegać obowiązujących wymogów PCI DSS i innych wymogów PCI SSC mających zastosowanie do przetwarzania, przechowywania lub przesyłania Danych Posiadacza Karty lub Wrażliwych Danych Uwierzytelniających nie później niż w dniu wejścia w życie danej wersji stosownego wymogu.
- podczas wdrażania nowych i/lub wymiany starych Urządzeń do wprowadzania kodu PIN lub Aplikacji Płatniczych wykorzystywać wyłącznie te, które zostały zatwierdzone przez PCI.

Muszą Państwo chronić wszystkie przechowywane na podstawie Umowy Rachunki obciążeniowe i Rachunki uznaniowe American Express zgodnie z niniejszymi postanowieniami dotyczącymi ochrony danych; mogą Państwo wykorzystywać te Rachunki wyłącznie w celach wynikających z Umowy oraz zapewnić im odpowiednią ochronę. Ponoszą Państwo odpowiedzialność finansową i prawną wobec American Express w zakresie zapewnienia przestrzegania przez Uwzględnione Strony niniejszych postanowień dotyczących ochrony danych (poza wykazaniem, że Uwzględnione Strony przestrzegają niniejszej Polityki zgodnie z Działem 5, „Ważna okresowa walidacja Państwa systemów”, z wyjątkiem sytuacji określonych w niniejszym dziale).

Dział 3 Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych

O Incydencie dotyczącym Danych muszą Państwo powiadomić American Express niezwłocznie, a najpóźniej w ciągu siedemdziesięciu dwóch (72) godzin od jego wykrycia.

Aby powiadomić American Express, należy skontaktować się z Programem Reagowania na Incydenty Dotyczące Przedsiębiorstwa (Enterprise Incident Response Programme, *EIRP*) American Express pod numerem +1 (602) 537-3021 (+ oznacza międzynarodowy numer kierunkowy „IDD", obowiązują opłaty za połączenia międzynarodowe) lub przez e-mail pod adresem EIRP@aexp.com. Muszą Państwo wyznaczyć osobę, która będzie Państwa osobą do kontaktu w sprawach związanych z Incydentami dotyczącymi Danych. Ponadto:

- Należy przeprowadzić dokładne dochodzenie sądowe w sprawie każdego Incydentu dotyczącego Danych.
- W przypadku Incydentów dotyczących Danych obejmujących 10 000 lub więcej unikalnych Numerów Kart, muszą Państwo zaangażować Inspektora Sądowego PCI (PFI) w celu przeprowadzenia takiego dochodzenia w ciągu pięciu (5) dni po wykryciu Incydentu dotyczącego Danych.
- Należy dostarczyć American Express raport z dochodzenia sądowego bez wprowadzonych zmian w ciągu dziesięciu (10) dni roboczych od daty jego ukończenia.
- Muszą Państwo niezwłocznie przekazać American Express wszystkie Naruszone Numery Kart. American Express zastrzega sobie prawo do przeprowadzenia własnej wewnętrznej analizy w celu identyfikacji Numerów Kart dotkniętych przez Incydent dotyczący Danych.

Raporty z dochodzeń sądowych muszą być sporządzane przy użyciu aktualnego Formularza Raportu Końcowego dot. Incydentu Sądowego dostępnego w dziale PCI. Taki raport musi zawierać ekspertyzy sądowe, raporty dotyczące zgodności oraz wszelkie inne informacje związane z Incydentem dotyczącym Danych, identyfikować przyczynę Incydentu dotyczącego Danych, potwierdzać, czy w czasie Incydentu dotyczącego Danych przestrzegany był standard PCI DSS, a także weryfikować Państwa możliwości zapobiegania przyszłym Incydentem dotyczącym Danych poprzez (i) dostarczenie planu usunięcia wszystkich wad standardu PCI DSS oraz (ii) uczestnictwo w programie zgodności American Express (jak opisano poniżej). Na żądanie American Express muszą Państwo przedstawić potwierdzenie wystawione przez Wykwalifikowanego Rzeczoznawcę ds. Bezpieczeństwa (QSA), że takie wady zostały usunięte.

Niezależnie od powyższych punktów niniejszego Działu 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych":

- American Express może, według własnego uznania, zażądać zaangażowania PFI w celu przeprowadzenia dochodzenia w sprawie Incydentu dotyczącego Danych obejmującego mniej niż 10 000 unikalnych numerów kart. Każde takie dochodzenie musi spełniać wymagania określone powyżej w niniejszym Dziale 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych" i musi zostać zakończone w terminie wymaganym przez American Express.
- American Express może, według własnego uznania, osobno zaangażować PFI w celu przeprowadzenia dochodzenia w sprawie dowolnego Incydentu dotyczącego Danych i może obciążyć Państwa kosztami takiego dochodzenia.

Muszą Państwo współpracować z American Express w celu skorygowania wszelkich problemów wynikających z Incydentu dotyczącego Danych, w tym poprzez konsultowanie z American Express Państwa komunikacji z Posiadaczami Kart, których dotknął Incydent dotyczący Danych oraz poprzez podanie (oraz uzyskanie wszelkich wymaganych w tym celu zezwoleń) wszelkich istotnych informacji w celu weryfikacji Państwa możliwości zapobiegania przyszłym Incydentom dotyczącym Danych w sposób zgodny z Umową.

Niezależnie od wszelkich przeciwnych zobowiązań dotyczących zachowania poufności zawartych w Umowie, American Express ma prawo do ujawniania informacji dotyczących wszelkich Incydentów dotyczących Danych Posiadaczom Kart, wystawcom, innym uczestnikom sieci American Express oraz do ich podania do wiadomości publicznej zgodnie z wymogami obowiązującego prawa; drogą nakazu sądowego, administracyjnego lub regulacyjnego, dekretu, wezwania do stawiennictwa w sądzie, prośby lub innego środka prawnego w celu zmniejszenia ryzyka oszustwa lub innej szkody w zakresie wymaganym do obsługi sieci American Express.

Dział 4 Zobowiązania odszkodowawcze w związku z Incydentem dotyczącym Danych

Państwa zobowiązania odszkodowawcze wobec American Express, wynikające z niniejszej Umowy w związku z Incydentami dotyczącymi Danych, podlegają postanowieniom niniejszego Działu 4, „Zobowiązania odszkodowawcze w związku z Incydentem dotyczącym Danych" bez wyłączenia innych praw i środków prawnych przysługujących American Express. Oprócz Państwa zobowiązań odszkodowawczych (jeśli istnieją), mogą Państwo podlegać opłatom za nieprzestrzeganie zasad w zakresie Incydentu dotyczącego Danych, jak opisano poniżej w niniejszym Dziale 4, „Zobowiązania odszkodowawcze w związku z Incydentem dotyczącym Danych".

W przypadku Incydentów dotyczących Danych, które obejmują:

- 10 000 lub więcej Numerów Kart American Express oraz jedną z poniższych opcji:
  - Wrażliwe Dane Uwierzytelniające lub
  - Termin ważności

  zapłacą Państwo odszkodowanie na rzecz American Express w wysokości 5 USD za każdy numer konta.

Jednak American Express nie będzie ubiegać się o odszkodowanie w przypadku Incydentu dotyczącego Danych, który obejmuje:

- mniej niż 10 000 Numerów Kart American Express lub
- ponad 10 000 Numerów Kart American Express, w przypadku spełnienia następujących warunków:
  - powiadomią Państwo American Express o Incydencie dotyczącym Danych zgodnie z Działe 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych",
  - w momencie wystąpienia Incydentu dotyczącego Danych przestrzegali Państwo zasad PCI DSS (zgodnie z ustaleniami dochodzenia PFI w sprawie Incydentu dotyczącego Danych) oraz
  - Incydent dotyczący Danych nie został spowodowany niewłaściwym postępowaniem Państwa lub Uwzględnionych Stron.

Niezależnie od powyższych punktów niniejszego Działu 4, „Zobowiązania odszkodowawcze w związku z Incydentem dotyczącym Danych", za jakiekolwiek Incydent dotyczący Danych, niezależnie od liczby Numerów Kart American Express, uiszczą Państwo opłatę na rzecz American Express za nieprzestrzeganie zasad dotyczących Incydentu dotyczącego Danych w wysokości nieprzekraczającej 100 000 USD za każdy Incydent dotyczący Danych (według uznania American Express) w przypadku niewypełnienia któregokolwiek ze zobowiązań określonych w Dziale 3, „Obowiązki w zakresie Zarządzania Incydentami dotyczącymi Danych". Aby uniknąć wątpliwości, łączna opłata za nieprzestrzeganie zasad dotyczących Incydentu dotyczącego Danych oszacowana dla pojedynczego Incydentu dotyczącego Danych nie może przekroczyć 100 000 USD.

American Express wyłączy z obliczeń jakiekolwiek Numery Kont Kart American Express ujęte we wcześniejszym zgłoszonym roszczeniu odszkodowawczym za Incydent dotyczący Danych w ciągu dwunastu (12) miesięcy przed terminem powiadomienia. Wszystkie obliczenia dokonane przez American Express zgodne z tą metodologią są ostateczne.

American Express może obciążyć Państwa pełną kwotą zobowiązań odszkodowawczych za Incydenty dotyczące Danych lub odliczyć kwotę z płatności American Express na Państwa rachunek (lub odpowiednio obciążyć Konto Bankowe) zgodnie z Umową.

Państwa zobowiązania odszkodowawcze z tytułu Incydentów dotyczących Danych w ramach niniejszej Umowy nie będą obejmować odszkodowań przypadkowych, pośrednich, spekulacyjnych, wtórnych, specjalnych, karnych lub przykładowych w ramach niniejszej Umowy, pod warunkiem, że takie zobowiązania nie obejmują szkód związanych z utraconymi zyskami lub przychodami, utratą wartości firmy lub utratą możliwości biznesowych.

American Express może według własnego uznania zmniejszyć zobowiązanie odszkodowawcze Sprzedawców wyłącznie w odniesieniu do Incydentów dotyczących Danych spełniających każde z poniższych kryteriów:

- Przed wystąpieniem Incydentu dotyczącego Danych i na cały czas trwania Okna Incydentu dotyczącego Danych wykorzystywane były Odpowiednie Technologie Ograniczania Ryzyka,
- Zakończono szczegółowe dochodzenie w ramach programu PFI (chyba że wcześniej uzgodniono inaczej na piśmie),

- W raporcie sądowym wyraźnie stwierdzono, że Technologie Ograniczania Ryzyka były wykorzystywane do przetwarzania, przechowywania i/lub przesyłania danych w momencie wystąpienia Incydentu dotyczącego Danych, oraz
- nie przechowywano (również w czasie wystąpienia Okna Incydentu Dotyczącego Danych) żadnych Wrażliwych Danych Uwierzytelniających lub jakichkolwiek Danych Posiadacza Karty, które nie zostały zmienione na nieczytelne.

W przypadku gdy możliwe jest zmniejszenie zobowiązania odszkodowawczego, zostanie ono określone z wyłączeniem należnych opłat za niezachowanie zgodności w następujący sposób:

Tabela A-2: Wymagane kryteria redukcji zobowiązania odszkodowawczego

Redukcja Zobowiązania Odszkodowawczego	Wymagane Kryteria
Redukcja Standardowa: 50%	>75% wszystkich Transakcji przetworzonych na Urządzeniach obsługujących Chipy[1] LUB
	Technologie Ograniczania Ryzyka stosowane w >75% placówkach Sprzedawców[2]
Redukcja Rozszerzona: 75% do 100%	>75% wszystkich Transakcji przetwarzanych na Urządzeniach obsługujących Chipy[1] ORAZ inne Technologie Ograniczania Ryzyka stosowane w >75% placówkach Sprzedawców[2]

[1] Zgodnie z wewnętrzną analizą American Express

[2] Zgodnie z ustaleniami dochodzenia PFI

- Redukcja Rozszerzona (75% do 100%) zostanie określona na podstawie niższej wartości procentowej Transakcji z wykorzystaniem Urządzeń obsługujących Chipy ORAZ placówek Sprzedawców stosujących inne Technologie Ograniczania Ryzyka. Poniższe przykłady ilustrują sposób obliczania zmniejszonego zobowiązania odszkodowawczego.
- Aby zakwalifikować się jako podmiot wykorzystujący Technologię Ograniczania Ryzyka, należy wykazać jej skuteczność wykorzystania zgodnie z jej projektem i przeznaczeniem. Na przykład, wdrażanie Urządzeń obsługujących Chipy i przetwarzanie Kart z Chipami z Paskiem Magnetycznym lub wpisywanie Kodu Autoryzacyjnego, NIE są sposobami efektywnego wykorzystania takiej technologii.
- Odsetek placówek, które korzystają z Technologii Ograniczania Ryzyka, jest określany w ramach dochodzenia PFI.
- Zmniejszenie zobowiązania odszkodowawczego nie ma zastosowania do żadnych opłat za niezachowanie zgodności, które są płatne w związku z Incydentem dotyczącym Danych.

Tabela A-3: Rozszerzona Redukcja Zobowiązania Odszkodowawczego

Przy-kład	Technologia Ograniczania Ryzyka w praktyce	Odszkodowawczego	Redukcja
1	80% Transakcji na Urządzeniach obsługujących Chipy	Nie	50%: Redukcja Standardowa (mniejsze niż 75% wykorzystanie Technologii Ograniczania Ryzyka nie kwalifikuje się do Redukcji Rozszerzonej)[1]
	0% placówek korzysta z innych Technologii Ograniczania Ryzyka		

Przy-kład	Technologia Ograniczania Ryzyka w praktyce	Odszkodowawczego	Redukcja
2	80% Transakcji na Urządzeniach obsługujących Chipy 77% placówek korzysta z innych Technologii Ograniczania Ryzyka	Tak	77%: Redukcja Rozszerzona (w oparciu o 77% wykorzystanie Technologii Ograniczania Ryzyka)
3	93% Transakcji na Urządzeniach obsługujących Chipy 100% placówek korzysta z innych Technologii Ograniczania Ryzyka	Tak	93%: Redukcja Rozszerzona (w oparciu o 93% Transakcji na Urządzeniach obsługujących Chipy)
4	40% Transakcji na Urządzeniach obsługujących Chipy 90% placówek korzysta z innych Technologii Ograniczania Ryzyka	Nie	50%: Redukcja Standardowa (mniej niż 75% Transakcji na Urządzeniach obsługujących Chipy nie kwalifikuje się do Redukcji Rozszerzonej)

[1] Incydent dotyczący Danych obejmujący 10 000 Kont Kart American Express, przy stawce 5 USD na numer konta (10 000 x 5 USD = 50 000 USD), może kwalifikować się do obniżenia o 50%, co zmniejszy Zobowiązania odszkodowawcze z 50 000 USD do 25 000 USD, z wyłączeniem wszelkich opłat za niezachowanie zgodności.

Dział 5 Ważna okresowa walidacja Państwa systemów

Muszą Państwo podjąć następujące czynności w celu dokonania walidacji raz na rok i raz na 90 dni, zgodnie z PCI DSS oraz poniższym opisem, stanu urządzeń Państwa i Franczyzobiorców, systemów i/lub sieci (oraz ich elementów), w których przechowywane, przetwarzane lub przekazywane są Dane Posiadaczy Kart oraz Wrażliwe Dane Uwierzytelniające.

W celu przeprowadzenia walidacji należy wykonać cztery następujące czynności:

Akcja 1: Uczestniczenie w programie przestrzegania zasad zgodności PCI American Express („Program") zgodnie z niniejszą polityką.

Akcja 2: Zapoznanie się z Wymogami dotyczącymi Poziomu Sprzedawców i Poziomu Walidacji.

Akcja 3: Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wysłać do American Express.

Akcja 4: Przesłanie Dokumentacji Walidacyjnej do American Express w wyznaczonym terminie.

Akcja 1: Uczestniczenie w Programie Przestrzegania Zasad Zgodności American Express zgodnie z niniejszą Polityką

Sprzedawcy Poziomu 1, Sprzedawcy Poziomu 2 oraz wszyscy Usługodawcy, jak opisano poniżej, muszą uczestniczyć w Programie zgodnie z niniejszą Polityką. American Express może wyznaczyć, według własnego uznania, określonych Sprzedawców Poziomu 3 i Poziomu 4 do uczestnictwa w Programie zgodnie z niniejszą Polityką.

Sprzedawcy i Dostawcy Usług zobowiązani do uczestnictwa w Programie muszą w wyznaczonych terminach zapisać się na Portalu udostępnionym przez Administratora Programu wybranego przez American Express.

- Muszą Państwo zaakceptować wszystkie uzasadnione warunki związane z korzystaniem z Portalu.
- Muszą Państwo przypisać i podać dokładne informacje dla co najmniej jednej osoby kontaktowej ds. bezpieczeństwa danych w ramach Portalu. Wymagane elementy danych obejmują:
  - imię i nazwisko

  - adres e-mail
  - numer telefonu
  - adres do korespondencji
- W przypadku zmiany informacji należy podać aktualne lub nowe dane osoby kontaktowej ds. bezpieczeństwa danych w ramach Portalu.
- Muszą Państwo zadbać o aktualizację swoich systemów, aby umożliwić komunikację serwisową z wyznaczonej domeny Portalu.

Brak podania lub zadbania o aktualizację informacji kontaktowych dotyczących bezpieczeństwa danych lub umożliwienia komunikacji e-mailowej nie będzie miał wpływu na nasze prawa do naliczania opłat.

Akcja 2: Zapoznanie się z Wymogami dotyczącymi Poziomu Sprzedawców i Poziomu Walidacji

Istnieją cztery Poziomy dotyczące Sprzedawców i dwa Poziomy dotyczące Dostawców Usług oparte na liczbie Transakcji dokonanych przy użyciu Karty American Express.

- W przypadku Sprzedawców jest to liczba Transakcji przekazana przez ich placówki, która sięga najwyższego poziomu konta American Express dla Sprzedawców.*
- W przypadku Dostawców usług jest to suma liczby Transakcji przekazanych przez Dostawcę usług oraz Podmioty, którym Dostawcy usług świadczą usługi.

Transakcje Inicjowane przez Kupującego (BIP) nie są uwzględniane w wolumenie Transakcji przy użyciu Karty American Express w celu określenia poziomu Sprzedawcy i weryfikacji wymogów dotyczących walidacji. Będą Państwo należeć do jednego z Poziomów Sprzedawcy określonych w poniższych tabelach Sprzedawców i Dostawcy Usług.

* W przypadku Franczyzodawców obejmuje to również wolumen transakcji dokonywanych w placówkach Franczyzobiorców. Franczyzodawcy, którzy upoważniają swoich Franczyzobiorców do korzystania z określonego Systemu Sprzedażowego (POS) lub Dostawcy Usług, muszą również dostarczyć dokumentację dotyczącą walidacji zainteresowanym Franczyzobiorcom.

Wymogi dotyczące Dokumentacji Walidacyjnej Sprzedawcy

Sprzedawcom (nie Dostawcom Usług) przysługują cztery możliwe klasyfikacje Poziomu Sprzedawcy. Po określeniu poziomu Sprzedawcy na podstawie poniższej listy, należy zapoznać się z Tabela A-4: Dokumentacja Walidacyjna Sprzedawcy, aby określić wymagania dotyczące Dokumentacji Walidacyjnej.

- **Sprzedawca Poziomu 1** — 2,5 mln lub więcej Transakcji realizowanych przy użyciu Kart American Express rocznie; lub jakikolwiek Sprzedawca, któremu American Express w inny sposób i według własnego uznania przydziela Poziom 1.
- **Sprzedawca Poziomu 2** — od 50 000 do 2,5 mln Transakcji realizowanych przy użyciu Kart American Express rocznie.
- **Sprzedawca Poziomu 3** — od 10 000 do 50 000 Transakcji realizowanych przy użyciu Kart American Express rocznie.
- **Sprzedawca Poziomu 4** — mniej niż 10 000 Transakcji realizowanych przy użyciu Kart American Express rocznie.

Tabela A-4: Dokumentacja Walidacyjna Sprzedawcy

Poziom Sprzedawcy/ Roczne Transakcje American Express	Raport dotyczący zgodności Poświadczenia Zgodności (ROC AOC)	Kwestionariusz dotyczący Poświadczenia Zgodności (SAQ AOC) i Kwartalnego skanowania podatności sieci zewnętrznej (Skanowanie)	Poświadczenie STEP dla uprawnionych Sprzedawców
Poziom 1/ 2,5 miliona lub więcej	Obowiązkowe	Nie dotyczy	Opcjonalnie za zgodą American Express (zastępuje ROC)
Poziom 2/ 50 000 do 2,5 miliona	Opcjonalne	SAQ AOC obowiązkowe, (w przypadku braku przedłożenia ROC AOC Onsite Assessment); skanowanie obowiązkowe w przypadku niektórych typów SAQ	Opcjonalne (zastępuje SAQ i skanowanie sieci lub ROC)
Poziom 3/ 10 000 do 50 000	Opcjonalne	SAQ AOC opcjonalne (obowiązkowe, jeśli wymaga tego American Express); skanowanie obowiązkowe w przypadku niektórych typów SAQ	Opcjonalne (zastępuje SAQ i skanowanie sieci lub ROC)
Poziom 4/ 10 000 lub mniej	Opcjonalne	SAQ AOC opcjonalne (obowiązkowe, jeśli wymaga tego American Express); skanowanie obowiązkowe w przypadku niektórych typów SAQ	Opcjonalne (zastępuje SAQ i skanowanie sieci lub ROC)

* W celu uniknięcia wątpliwości, Sprzedawcy Poziomu 3 i 4 nie są zobowiązani do przedkładania Dokumentacji Walidacyjnej, chyba że jest to wymagane według uznania American Express, niemniej jednak muszą stosować się do wszystkich innych postanowień niniejszej Polityki operacyjnej w zakresie bezpieczeństwa danych i podlegają odpowiedzialności z tego tytułu.

American Express zastrzega sobie prawo do sprawdzenia kompletności, dokładności i kompletności, dokładności i adekwatności Dokumentacji Walidacyjnej PCI. American Express może w tym celu zażądać od Państwa dostarczenia dodatkowych dokumentów potwierdzających ocenę. Ponadto American Express ma prawo wymagać od Państwa zaangażowania zatwierdzonego QSA lub PFI przez działającą z ramienia PCI Radę Standardów Bezpieczeństwa.

Program Ulepszania Technologii Bezpieczeństwa (STEP)

Sprzedawcy, którzy spełniają wymagania standardu PCI DSS, mogą również, według uznania American Express, zakwalifikować się do programu STEP American Express, jeśli wdrożą pewne dodatkowe technologie zabezpieczeń w swoich środowiskach przetwarzania kart. Program STEP ma zastosowanie tylko wtedy, gdy Sprzedawca nie doświadczył Incydentu Dotyczącego Danych w ciągu ostatnich 12 miesięcy i gdy 75% wszystkich Transakcji Sprzedawcy przy użyciu Kart jest wykonywanych z wykorzystaniem kombinacji następujących ulepszonych opcji bezpieczeństwa:

- **Specyfikacja EMV, EMV Zbliżeniowe lub Portfel Cyfrowy** – na aktywnym Urządzeniu obsługującym Chipy, posiadającym ważne i aktualne zatwierdzenie/certyfikację EMVCo (www.emvco.com) oraz mogącym przetwarzać Transakcje przy użyciu Kart z Chipem zgodnych ze standardami AEIPS. (Sprzedawcy amerykańscy muszą uwzględnić Zbliżeniowe)
- **Szyfrowanie Point-to-Point (P2PE)** – komunikacja z procesorami Sprzedawców za pomocą systemu Szyfrowania Point-to-Point zatwierdzonego przez PCI SSC lub zatwierdzonego przez QSA
- **Tokenizacja** – wdrożone rozwiązanie tokenizacji musi:

- spełniać specyfikacje EMVCo,
- być zabezpieczone, przetwarzane, przechowywane, przekazywane i w całości zarządzane przez zewnętrznego dostawcę usług przestrzegającego zasad zgodności PCI oraz
- Token nie może być odwrócony w celu ujawnienia niezamaskowanych Głównych numerów rachunków (PAN) Sprzedawcy.

Sprzedawcy kwalifikujący się do programu STEP mają zmniejszone wymagania dotyczące Dokumentacji Walidacji PCI, co opisano szerzej w Akcji 3: „Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wysłać do American Express" poniżej.

Wymagania dotyczące Dostawców usług

Dostawcy usług (nie Sprzedawcy) mają dwie możliwe Poziomy klasyfikacje. Po ustaleniu poziomu Dostawcy Usług zgodnie z poniższą listą należy zapoznać się z Tabela A-5: Dokumentacja Dostawcy Usług, aby określić wymagania dotyczące Dokumentacji Walidacyjnej.

Dostawca usług poziomu 1 — 2,5 mln Transakcji dokonanych Kartą American Express lub więcej w skali roku; lub jakikolwiek Dostawca usług, którego American Express uzna za Dostawcę usług poziomu 1.

Dostawca usług poziomu 2 — mniej niż 2,5 mln Transakcji dokonanych Kartą American Express rocznie; lub jakikolwiek Dostawca usług, którego American Express nie uzna za Dostawcę usług poziomu 1.

Dostawcy usług nie kwalifikują się do programu STEP.

Tabela A-5: Dokumentacja Dostawcy Usług

Poziom	Dokumentacja Walidacyjna	Wymóg
1	Roczny raport dotyczący zgodności Poświadczenia Zgodności (ROC AOC)	Obowiązkowe
2	Roczne SAQ D (Dostawca usług) i kwartalne skanowanie sieci lub roczny raport dotyczący zgodności Poświadczenia Zgodności (ROC AOC), jeśli będzie to opcja preferowana	Obowiązkowe

Zaleca się, aby Dostawcy Usług przestrzegali również Dodatkowej Walidacji Podmiotów określonej przez PCI.

Akcja 3: Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wysłać do American Express

Poniższe dokumenty są wymagane dla różnych poziomów Sprzedawców i Dostawców usług, zgodnie z Tabelą Sprzedawców oraz Tabelą Dostawców Usług, które zostały przedstawione powyżej.

Muszą Państwo dostarczyć Poświadczenie Zgodności (AOC) dla odpowiedniego typu oceny. AOC jest deklaracją statusu zgodności i jako taka musi być podpisana i opatrzona datą przez odpowiedni szczebel kierownictwa w organizacji.

Oprócz AOC American Express może zażądać od Państwa dostarczenia kopii pełnej oceny oraz, według naszego uznania, dodatkowych dokumentów potwierdzających zgodność z wymogami PCI DSS. Dokumentacja Walidacyjna jest wypełniana na Państwa koszt.

Raport dotyczący zgodności Poświadczenia Zgodności (ROC AOC) - (wymóg roczny) – Raport dotyczący Zgodność dokumentuje wyniki szczegółowego miejscowego badania sprzętu, systemów i sieci (i ich elementów), w których przechowywane, przetwarzane lub przekazywane są Dane Posiadacza Karty lub Wrażliwe Dane Uwierzytelniające (lub oba te elementy). Istnieją dwie wersje: jedna dla Sprzedawców i druga dla Dostawców usług. Raport dotyczący Zgodności musi być wykonany przez:

- QSA lub
- Państwa i poświadczony przez dyrektora generalnego, dyrektora finansowego, dyrektora ds. bezpieczeństwa informacji lub głównego zarządzającego

AOC musi być podpisany i opatrzony datą przez QSA lub Wewnętrznego Inspektora Bezpieczeństwa (ISA) oraz uprawniony szczebel kierownictwa w Państwa organizacji dostarczony do American Express przynajmniej raz w roku.

Kwestionariusz Samooceny dotyczący Potwierdzenia Zgodności (SAQ AOC) - (wymóg roczny) – Kwestionariusz Samooceny pozwala na samodzielne sprawdzenie Państwa urządzeń, systemów i sieci (oraz ich elementów) gdzie przechowywane, przetwarzane lub przekazywane są dane Posiadacza Karty lub Wrażliwe Dane Uwierzytelniające (lub oba te elementy). Istnieje wiele wersji SAQ. Mogą Państwo wybrać jedną lub więcej wersji w oparciu o swoje Środowisko Danych Posiadacza Karty.

SAQ może być wypełniony przez pracowników Państwa Firmy, którzy posiadają kwalifikacje do udzielenia dokładnych i wyczerpujących odpowiedzi na pytania lub mogą Państwo zaangażować QSA do pomocy. AOC musi być podpisane i datowane przez upoważniony szczebel kierownictwa w Państwa organizacji i przynajmniej raz w roku dostarczane do American Express.

Podsumowanie skanowania podatności sieci zewnętrznej przez autoryzowanego sprzedawcę usług skanowania (Skanowanie ASV) - (wymóg 90 dni) – Zewnętrzne skanowanie podatności jest zdalnym testem, który pomaga zidentyfikować potencjalne słabe strony, zagrożenia i błędne konfiguracje komponentów internetowych środowiska danych posiadaczy kart (np. stron internetowych, aplikacji, serwerów internetowych, serwerów pocztowych, domen publicznych lub hostów).

Skanowanie ASV powinno zostać przeprowadzone przez Autoryzowanego sprzedawcę usług skanowania (ASV).

Jeśli jest to wymagane przez SAQ, Raport skanowania ASV poświadczający zgodność skanowania (AOSC) lub streszczenie zawierające liczbę zeskanowanych celów, poświadczenie, że wyniki spełniają procedury skanowania PCI DSS, oraz status zgodności wypełniony przez ASV, muszą być przekazywane do American Express przynajmniej raz na 90 dni.

ROC AOC lub STEP nie są zobowiązani do dostarczenia streszczenia AOSC lub Skanu ASV, chyba że zostanie to wyraźnie zażądane. Dla uniknięcia wątpliwości Skany są obowiązkowe, jeśli wymaga tego odpowiedni SAQ.

Dla uniknięcia wątpliwości, ASV są obowiązkowe, jeśli wymaga tego odpowiedni SAQ.

Dokumentacja Walidacyjna Poświadczenia STEP (STEP) - (roczny wymóg) – STEP jest tylko dostępny dla Sprzedawców. którzy spełniają kryteria wymienione w Akcja 2: „Zapoznanie się z Wymogami dotyczącymi Poziomu Sprzedawców i Poziomu Walidacji" opisanymi powyżej. Jeśli Państwa firma kwalifikuje się do programu, muszą Państwo wypełnić i corocznie przesłać do American Express formularz Poświadczenia STEP. Coroczny formularz Poświadczenia STEP jest dostępny do pobrania z Portalu.

Brak zgodności z PCI DSS - (Wymóg roczny, 90-dniowy lub doraźny) – Jeśli nie spełniają Państwo zasad zgodności z PCI DSS, to muszą Państwo przedłożyć jeden z następujących dokumentów:

- Poświadczenie zgodności (AOC) zawierające „Akcja 4. Plan działania w przypadku statusu niezgodności" (dostępne do pobrania za pośrednictwem strony internetowej Rady Standardów Bezpieczeństwa PCI)
- Podsumowanie narzędzia podejścia priorytetowego PCI (dostępne do pobrania za pośrednictwem Rady Standardów Bezpieczeństwa PCI)
- Szablon planu projektu (dostępny do pobrania z Portalu). Plan Projektu może być złożony w miejsce rocznego poświadczenia (SAQ/ROC) i/lub w miejsce wymogu skanowania.

Każdy z powyższych dokumentów musi mieć wyznaczoną datę naprawczą, nie dłuższą niż dwanaście (12) miesięcy od daty zakończenia dokumentu w celu osiągnięcia zgodności. Są Państwo zobowiązani do okresowego informowania American Express o postępach w usuwaniu skutków Statusu Niezgodności (Sprzedawcy Poziomu 1, Poziomu 2, Poziomu 3 i Poziomu 4; wszyscy Dostawcy Usług). Działania naprawcze niezbędne do osiągnięcia zgodności z PCI DSS mają być zrealizowane na Państwa koszt.

Działania naprawcze niezbędne do osiągnięcia zgodności z PCI DSS mają być zrealizowane na Państwa koszt.

American Express nie nałoży na Państwa opłat za brak walidacji (opisanych poniżej) ze względu na niezachowanie zgodności przed datą dokonania poprawek, jednak pozostają Państwo odpowiedzialni wobec American Express za wszelkie zobowiązania z tytułu odpowiedzialności odszkodowawczej za Incydenty dotyczące Danych oraz podlegają Państwo wszystkim innym przepisom określonym w niniejszej Polityce.

W celu uniknięcia jakichkolwiek wątpliwości, Sprzedawcy, którzy nie wykazują zgodności ze standardami PCI DSS nie kwalifikują się do udziału w programie STEP.

Akcja 4: Przesyłanie Dokumentacji walidacyjnej do American Express

Wszyscy Sprzedawcy i Dostawcy Usług, od których wymaga się udziału w Programie zgodności z PCI American Express muszą przedłożyć American Express Dokumentację Walidacyjną oznaczoną jako „obowiązkową" w tabelach w Akcji 2: „Zapoznanie się z Wymogami dotyczącymi Poziomu Sprzedawców i Poziomu Walidacji" w obowiązujących terminach.

Muszą Państwo złożyć Dokumentację Walidacyjną do American Express za pomocą Portalu udostępnionego przez Administratora Programu wybranego przez American Express. Składając Dokumentację Walidacyjną, oświadczają Państwo i gwarantują American Express, że poniższe informacje są prawdziwe (zgodnie z Państwa najlepszą wiedzą):

- Twoja ocena była kompletna i dokładna;
- Status PCI DSS jest dokładnie przedstawiony w momencie zakończenia prac jako zgodny lub niezgodny;
- Są Państwo upoważnieni do ujawnienia informacji zawartych w Dokumentacji Walidacyjnej i przekazują ją firmie American Express bez naruszania jakichkolwiek praw innych stron.

Opłaty za brak walidacji i wypowiedzenie Umowy

American Express ma prawo nałożyć kary umowne za brak walidacji i wypowiedzieć Umowę, jeśli nie spełnią Państwo tych wymagań lub nie przedstawią American Express obowiązkowej Dokumentacji Walidacyjnej w obowiązującym terminie. American Express powiadomi Państwa osobno o terminie obowiązującym dla każdego rocznego i kwartalnego okresu sprawozdawczego.

Tabela A-6: Opłaty za brak walidacji

Opis*	Sprzedawca poziomu 1 lub Dostawca usług poziomu 1	Sprzedawca poziomu 2 lub Dostawca usług poziomu 2	Sprzedawca poziomu 3 lub poziomu 4
Za brak walidacji zostanie nałożona opłata, jeżeli Dokumentacja Walidacyjna nie zostanie złożona w pierwszym terminie.	25 000 USD	5 000 USD	50 USD
Za brak walidacji zostanie nałożona dodatkowa opłata, jeżeli Dokumentacja Walidacyjna nie zostanie złożona w drugim terminie.	35 000 USD	10 000 USD	100 USD
Za brak walidacji zostanie nałożona dodatkowa opłata, jeżeli Dokumentacja Walidacyjna nie zostanie złożona w trzecim terminie. **UWAGA:** Opłaty za brak walidacji będą stosowane do czasu, gdy Dokumentacja Walidacyjna zostanie złożona.	45 000 USD	15 000 USD	250 USD

* Opłaty za brak walidacji zostaną naliczone w równowartości w walucie lokalnej.

* Nie dotyczy Argentyny.

Jeśli Państwa obowiązki związane z Dokumentacją Walidacyjną PCI DSS nie zostaną spełnione, wówczas American Express ma prawo nałożyć opłaty za brak walidacji w sposób kumulatywny, wstrzymać płatności i/lub rozwiązać Umowę.

Dział 6 Poufność

American Express podejmie rozsądne kroki, by zachować poufność (i narzucić zachowanie poufności swoim agentom i podwykonawcom, w tym dostawcy Portalu) Państwa raportów dotyczących zgodności, w tym Dokumentacji walidacyjnej, a także aby nie ujawniać Dokumentacji walidacyjnej osobom trzecim (innym niż spółki stowarzyszone, agenci, przedstawiciele, Dostawcy usług i podwykonawcy American Express) przez okres trzech lat od daty otrzymania, przy czym obowiązek zachowania poufności nie dotyczy Dokumentacji walidacyjnej, która:

a. była już znana American Express przed ujawnieniem;

b. jest lub stanie się dostępna publicznie w sposób niestanowiący naruszenia niniejszego postanowienia przez American Express;

c. została otrzymana przez American Express zgodnie z prawem od osoby trzeciej bez zobowiązania do zachowania poufności;

d. została niezależnie opracowana przez American Express; lub

e. jej ujawnienie jest wymagane przez nakaz sądu, organu administracyjnego lub rządowego lub prawo, regulamin lub rozporządzenie albo wezwanie do okazania, przedprocesowy wymóg okazania dowodów, wezwanie lub w ramach innej procedury administracyjnej lub prawnej, albo w toku formalnego lub nieformalnego zapytania lub dochodzenia prowadzonego przez dowolny organ rządowy (w tym przez urząd nadzoru, inspektorat, biegłego lub organy ścigania).

Dział 7 Wyłączenie odpowiedzialności

AMERICAN EXPRESS NINIEJSZYM OŚWIADCZA, ŻE NIE PONOSI ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK OŚWIADCZENIA, GWARANCJE I ZOBOWIĄZANIA W ODNIESIENIU DO NINIEJSZEJ POLITYKI OPERACYJNEJ OCHRONY DANYCH, PCI DSS, SPECYFIKACJI EMV ORAZ WYZNACZANIA I WYKONYWANIA OBOWIĄZKÓW PRZEZ QSA, ASV, LUB PFI (LUB KTÓREGOKOLWIEK Z NICH), NIEZALEŻNIE OD TEGO CZY WYRAŹNYCH, DOROZUMIANYCH, USTAWOWYCH LUB INNYCH, W TYM GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU. WYSTAWCY KART AMERICAN EXPRESS NIE SĄ BENEFICJENTAMI STRON TRZECICH W RAMACH NINIEJSZEJ POLITYKI.

Przydatne strony internetowe

Bezpieczeństwo danych American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Słowniczek

Na potrzeby wyłącznie niniejszej Polityki operacyjnej ochrony danych (DSOP) obowiązują następujące definicje, które są nadrzędne w przypadku konfliktu pojęć znajdujących się w *Regulamin dla Sprzedawców*.

Aplikacja płatnicza ma znaczenie nadane jej w obowiązującym Glosariuszu Standardu bezpiecznego oprogramowania i Standardu cyklu życia bezpiecznego oprogramowania, dostępnym pod adresem www.pcisecuritystandards.org.

Atest zgodności (Attestation of Compliance, AOC) oznacza deklarację stanu Państwa zgodności ze standardami PCI DSS, w postaci przekazanej przez Payment Card Industry Security Standards Council, LLC.

Atest zgodności skanowania (Attestation of Scan Compliance, AOSC) oznacza deklarację stanu Państwa zgodności ze standardami PCI DSS, na podstawie skanowania sieci, w postaci przekazanej przez Payment Card Industry Security Standards Council, LLC.

Autoryzowany sprzedawca usług skanowania (Approved Scanning Vendor, ASV) oznacza podmiot, który został zakwalifikowany przez Payment Card Industry Security Standards Council, LLC do weryfikowania przestrzegania niektórych wymagań PCI DSS poprzez wykonywanie skanów narażenia środowisk mających kontakt z Internetem.

Chip oznacza wbudowany w Kartę mikroprocesor zawierający informacje o Posiadaczu Karty i rachunku Karty.

Dane Posiadacza Karty mają znaczenie zgodne z definicją obowiązującego Glosariusza pojęć PCI DSS.

Data powiadomienia oznacza datę, z którą American Express przekazuje emitentom ostateczne powiadomienie o Incydencie dotyczącym Danych. Data ta jest uzależniona od otrzymania przez American Express końcowego raportu sądowego lub analizy wewnętrznej i zostanie ustalona według wyłącznego uznania American Express.

Dokumentacja walidacyjna oznacza AOC wydane w związku z Coroczną Oceną Bezpieczeństwa na miejscu lub SAQ, AOSC i podsumowania ustaleń wydane w związku z Kwartalnymi Skanami Sieci lub Atestacją Rocznego Programu Ulepszania Technologii Bezpieczeństwa.

Dostawcy usług oznaczają uprawnione podmioty przetwarzające, zewnętrzne podmioty przetwarzające, dostawców systemów POS i wszelkich innych dostawców systemów POS i innych rozwiązań albo usług związanych z przetwarzaniem płatności dla Sprzedawcy.

Dostawca usług poziomu 1 oznacza Dostawcę Usług, który obsługuje 2,5 mln Transakcji realizowanych przy użyciu Kart American Express lub więcej rocznie; lub jakikolwiek Dostawca usług, którego American Express uzna za Dostawcę usług poziomu 1.

Dostawca usług poziomu 2 oznacza Dostawcę Usług, który obsługuje mniej niż 2,5 mln Transakcji realizowanych przy użyciu Kart American Express rocznie; lub jakikolwiek Dostawca usług, którego American Express nie uzna za Dostawcę usług poziomu 1.

Franczyzobiorca oznacza niezależnie posiadaną i obsługiwaną stronę trzecią (w tym franczyzobiorcę, licencjobiorcę lub oddział) inną niż Partner, która jest licencjonowana przez Franczyzodawcę na prowadzenie franczyzy i która zawarła pisemną umowę z Franczyzodawcą, zgodnie z którą konsekwentnie wyświetla zewnętrzną identyfikację, w widoczny sposób identyfikuje się ze Znakami Franczyzodawcy lub ujawnia się publicznie jako członek grupy spółek Franczyzodawcy.

Franczyzodawca oznacza podmiot prowadzący działalność, który udziela licencji osobom lub Podmiotom (Franczyzobiorcom) na dystrybucję towarów i/lub usług w ramach znaku towarowego lub na prowadzenie działalności przy użyciu Znaku Towarowego tego Podmiotu; udziela pomocy Franczyzobiorcom w prowadzeniu działalności lub wpływa na sposób prowadzenia działalności przez Franczyzobiorcę; oraz wymaga uiszczenia opłaty przez Franczyzobiorców.

Główny numer rachunku (Primary Account Number, PAN) ma znaczenie nadane mu w obowiązującym wówczas Słowniku terminów dla PCI DSS.

Incydent dotyczący Danych jest związany z naruszeniem lub podejrzewanym naruszeniem kluczy szyfrujących American Express lub co najmniej jednego numeru Konta American Express, w wyniku którego nastąpił:

- nieautoryzowany dostęp lub wykorzystanie Kluczy Szyfrujących, Danych Posiadacza Karty lub Poufnych Danych Uwierzytelniających (lub ich kombinacji), które są przechowywane, przetwarzane lub przesyłane przez Państwa sprzęt, systemy i/lub sieci (lub ich komponenty) lub których wykorzystanie jest przez Państwo upoważnione, dostarczane lub udostępniane;
- wykorzystanie takich Kluczy Szyfrujących, Danych Posiadacza Karty lub Poufnych Danych Uwierzytelniających (lub ich kombinacji) w sposób inny niż zgodny z Umową; i/lub
- podejrzenie lub potwierdzenie utraty, kradzieży lub przywłaszczenia za pomocą dowolnych środków przekazu, materiałów, zapisów lub informacji zawierających takie Klucze Szyfrujące, Dane Posiadacza Karty lub Wrażliwe Dane Uwierzytelniające (ich połączenie).

Informacje o posiadaczu karty oznaczają informacje o posiadaczach kart American Express i transakcjach kartowych, w tym imiona i nazwiska, adresy, numery kont kart i numery identyfikacyjne karty (CID).

Inspektor Sądowy PCI (PFI) oznacza podmiot, który został upoważniony przez Payment Card Industry Security Standards Council, LLC do przeprowadzania śledztw dotyczących naruszenia danych kart płatniczych.

Karta American Express lub **Karta** oznacza każdą kartę, urządzenie umożliwiające dostęp do rachunku lub urządzenie płatnicze albo usługę płatniczą opatrzone nazwą, logo, znakiem towarowym, znakiem usługowym, nazwą handlową lub innym zastrzeżonym wzorem lub określeniem należącym do American Express lub spółki stowarzyszonej i wydane przez wystawcę lub numer rachunku karty.

Karta chipowa oznacza Kartę wyposażoną w Chip, która może wymagać podania kodu PIN w celu weryfikacji tożsamości Posiadacza Karty lub danych o rachunku zawartych na Chipie albo obu tych elementów jednocześnie (czasem nazywana w naszych materiałach „kartą inteligentną", „kartą EMV" albo „ICC" lub „kartą z układem scalonym").

Klucz szyfrujący (Klucz szyfrujący American Express) oznacza wszystkie klucze wykorzystywane do przetwarzania, generowania, ładowania i/lub ochrony danych rachunku. Pojęcie to obejmuje między innymi:

- Klucze szyfrowania kluczy: klucze Zone Master Keys (ZMK) i klucze Zone Pin Keys (ZPK)
- Klucze główne wykorzystywane w bezpiecznych urządzeniach szyfrujących: Local Master Keys (LMKs)
- Klucze Card Security Code Keys (CSCK)
- Klucze PIN: klucze Base Derivation Keys (BDK), PIN Encryption Key (PEK) i ZPK

Kredyt oznacza kwotę Obciążenia, która jest zwracana przez Państwa Posiadaczom Kart za zakupy lub płatności dokonywane przy użyciu Karty.

Kwestionariusz samooceny (Self-Assessment Questionnaire, SAQ) oznacza narzędzie służące do samooceny opracowane przez Payment Card Industry Security Standards Council, LLC, którego celem jest ocena i potwierdzenie przestrzegania standardów PCI DSS.

Naruszony numer karty oznacza numer rachunku Karty American Express związany z Incydentem dotyczącym Danych.

Numer Karty oznacza niepowtarzalny numer identyfikacyjny, który Wydawca nadaje Karcie w momencie jej wydania.

Obciążenie oznacza płatność lub zakup dokonane przy użyciu Karty.

Okno Incydentu dotyczącego Danych oznacza okno czasowe włamania (lub podobnie określony okres) podane w końcowym raporcie kryminalistycznym (np. raporcie PFI) lub, jeśli nie jest znane, do 365 dni przed ostatnią Datą Powiadomienia o potencjalnie Naruszonych Numerach Kart objętych Naruszeniem Danych, które zostały do nas zgłoszone.

Payment Card Industry Data Security Standard (PCI DSS) oznacza Standard bezpieczeństwa danych stosowany w branży kart płatniczych dostępny pod adresem www.pcisecuritystandards.org.

PCI DSS oznacza Standard bezpieczeństwa danych stosowany w branży kart płatniczych dostępny pod adresem www.pcisecuritystandards.org.

Podmiot przetwarzający dane oznacza dostawcę usług działającego na rzecz Akceptantów, który ułatwia przetwarzanie autoryzacji i zgłoszeń w sieci American Express.

Portal oznacza system raportowania dostarczony przez wybranego przez American Express administratora Programu PCI. Sprzedawcy i Dostawcy Usług są zobowiązani do korzystania z Portalu w celu przekazania Dokumentacji Walidacyjnej PCI do American Express.

Posiadacz Karty oznacza osobę fizyczną lub podmiot, (i) którzy zawarli z wystawcą umowę otwarcia rachunku Karty lub (ii) których nazwisko/nazwa znajduje się na Karcie.

Poziom Sprzedawcy to oznaczenie, które przypisujemy Sprzedawcom w związku z ich zobowiązaniami dotyczącymi walidacji zgodności z PCI DSS, jak opisano w Dział 5, „Ważna okresowa walidacja Państwa systemów".

Program oznacza Program Zgodności PCI American Express.

Program Analizy Ukierunkowanej oznacza program, który zapewnia wczesną identyfikację potencjalnego naruszenia danych Posiadacza Karty w Środowisku Danych Posiadaczy Kart (CDE). Patrz Dział 1, „Program Analizy Ukierunkowanej (TAP)".

Program Ulepszania Technologii Bezpieczeństwa (Security Technology Enhancement Programme, STEP) oznacza program American Express, w ramach którego Sprzedawcy są zachęcani do wdrażania technologii poprawiających bezpieczeństwo danych.

Rzeczoznawca ds. bezpieczeństwa (Qualified Security Assessor, QSA) oznacza podmiot, który został zakwalifikowany przez Payment Card Industry Security Standards Council, LLC do weryfikowania przestrzegania standardów PCI DSS.

Specyfikacje EMV oznaczają specyfikacje wydane przez EMVCo, LLC, które są dostępne pod adresem www.emvco.com.

Sprzedawca oznacza sprzedawcę i wszystkie jego filie, które akceptują Karty American Express w ramach umowy z American Express lub jego filiami.

Sprzedawca Poziomu 1 oznacza Sprzedawcę, który obsługuje 2,5 mln Transakcji realizowanych przy użyciu Kart American Express lub więcej rocznie; lub jakiegokolwiek Sprzedawcę, którego American Express uzna za Sprzedawcę poziomu 1.

Sprzedawca Poziomu 2 oznacza Sprzedawcę, który obsługuje od 50 000 do 2,5 mln Transakcji realizowanych przy użyciu Kart American Express rocznie.

Sprzedawca Poziomu 3 oznacza Sprzedawcę, który obsługuje od 10 000 do 50 000 Transakcji realizowanych przy użyciu Kart American Express rocznie.

Sprzedawca Poziomu 4 oznacza Sprzedawcę, który obsługuje mniej niż 10 000 Transakcji realizowanych przy użyciu Kart American Express rocznie.

System sprzedażowy (POS) oznacza system lub wyposażenie przetwarzające informacje, w tym terminal, komputer, kasę elektroniczną, czytnik bezdotykowy lub mechanizm albo proces płatności wykorzystywany przez Sprzedawcę w celu uzyskiwania autoryzacji lub pobierania danych Transakcji albo obu tych czynności jednocześnie.

Szyfrowanie Point-to-Point (P2PE) oznacza rozwiązanie, które kryptograficznie chroni dane konta od punktu, w którym sprzedawca akceptuje kartę płatniczą do bezpiecznego punktu odszyfrowania.

Środowisko Danych Posiadaczy Kart (Cardholder Data Environment, CDE) oznacza osoby, procesy i technologie, które przechowują, przetwarzają lub przesyłają dane posiadacza karty lub wrażliwe dane uwierzytelniające.

Technologia Ograniczania Ryzyka oznacza rozwiązania technologiczne zwiększające bezpieczeństwo Danych Posiadaczy Kart American Express oraz Wrażliwych Danych Uwierzytelniających, określone przez American Express. Aby móc zakwalifikować daną technologię się jako Technologię Ograniczania Ryzyka, należy wykazać jej skuteczność wykorzystania zgodnie z jej projektem i przeznaczeniem. Przykłady obejmują między innymi: EMV, szyfrowanie Point-to-Point i tokenizacja.

Transakcja oznacza Obciążenie lub Uznanie dokonane za pomocą Karty.

Transakcja EMV oznacza Transakcję dokonaną za pomocą karty z układem scalonym (czasem nazywaną „kartą IC", „kartą chipową", „kartą inteligentną", „kartą EMV" lub „ICC") w znajdującym się w punkcie sprzedaży (POS) terminalu obsługującym karty IC i posiadającym ważną homologację EMV. Homologacje EMV są dostępne pod adresem www.emvco.com.

Transakcje Inicjowane przez Kupującego (Buyer Initiated Payment, BIP) oznaczają Transakcje płatnicze aktywowane poprzez plik instrukcji płatniczych przetwarzany za pośrednictwem BIP.

Token oznacza token kryptograficzny, który zastępuje PAN, na podstawie danego indeksu na nieprzewidywalną wartość.

Urządzenie do wprowadzania kodu PIN ma znaczenie nadane jej w obowiązującym Glosariuszu pojęć związanych z Wymaganiami dotyczącymi bezpieczeństwa Transakcji z kodem PIN (PTS), bezpieczeństwa punktów interakcji (POI) oraz bezpieczeństwa modułowego, który jest dostępny pod adresem www.pcisecuritystandards.org.

Urządzenie obsługujące transakcje z użyciem kart chipowych oznacza urządzenie znajdujące się w punkcie sprzedaży posiadające ważną autoryzację/świadectwo EMVCo (www.emvco.com), które przetwarza transakcje z użyciem kart chipowych zgodne ze standardem AEIPS.

Uwzględnione Strony oznaczają któregokolwiek lub wszystkich pracowników, agentów, przedstawicieli, podwykonawców, Procesorów, Dostawców Usług, dostawców sprzętu w punktach sprzedaży (POS) lub systemów lub rozwiązań w zakresie przetwarzania płatności, podmioty powiązane z kontem Sprzedawcy American Express oraz wszelkie inne strony, którym mogą Państwo zapewnić dostęp do Informacji o Posiadaczu Karty zgodnie z niniejszą Umową.

Wydawca oznacza dowolny Podmiot (w tym American Express i jego Podmioty Stowarzyszone), któremu licencję wydał American Express lub Podmiot Stowarzyszony American Express do wydawania Kart i angażowania się w działalność związaną z wydawaniem Kart.

Wymagania bezpieczeństwa PCI PIN oznaczają Wymagania bezpieczeństwa PIN stosowane w branży kart płatniczych dostępne pod adresem www.pcisecuritystandards.org.

Wymagania Payment Card Industry Security Standards Council (PCI SSC) oznaczają zbiór standardów i wymagań związanych z zabezpieczaniem i ochroną danych kart płatniczych, w tym PCI DSS i PA DSS, dostępnych pod adresem www.pcisecuritystandards.org.

Wrażliwe dane uwierzytelniające mają znaczenie zgodne z definicją obowiązującego Glosariusza pojęć PCI DSS.

Wzór raportu końcowego z incydentu kryminalistycznego oznacza szablon udostępniony przez PCI Security Standards Council, który jest dostępny pod adresem www.pcisecuritystandards.org.

Zatwierdzone przez PCI oznacza, że Urządzenie do wprowadzania kodu PIN lub Aplikacja płatnicza (lub oba) pojawiają się w chwili uruchomienia na liście zatwierdzonych spółek i dostawców prowadzonej przez PCI Security Standards Council, LLC, dostępnej pod adresem www.pcisecuritystandards.org.

Zatwierdzone Rozwiązanie Szyfrowania Point-to-Point (P2PE), zawarte na liście sprawdzonych rozwiązań PCI SSC lub zatwierdzone przez Wykwalifikowanego Rzeczoznawcę ds. Bezpieczeństwa (QSA) PCI SSC P2PE.