

Polityka operacyjna ochrony danych (DSOP)

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 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 umów 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 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 w miejscach obsługiwanych 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 [Dział 4, „Ważna okresowa walidacja Państwa systemów”](#), z wyjątkiem sytuacji określonych w niniejszym dziale).

Dział 2

Obowiązki w zakresie zarządzania incydentami dotyczącymi danych

O Incydencie dotyczącym Danych muszą Państwo powiadomić American Express niezwłocznie, a najpóźniej w ciągu dwudziestu czterech (24) godzin od jego wykrycia.

Aby powiadomić American Express, należy skontaktować się z Programem Reagowania na Incydenty Dotyczące Przedsiębiorstwa (Enterprise Incident Response Program, *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 specjalistę ds. dochodzeń sądowych w zakresie 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 Incydemem 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 przyszłemu Incydemem 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 [Dział 2. „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 [Dział 2. „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 Incydemem 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 American Express, wystawcom, innym uczestnikom sieci American Express oraz do ich podania do wiadomości publicznej zgodnie z wymogami obowiązującego prawa; drogą nakazu sądowego, administracyjnego lub regulacyjnego, dekrety, wezwania do stawienia się w sądzie, prośby lub innego środka prawnego w celu zmniejszenia ryzyka oszustwa lub innej szkody w zakresie wymaganym do obsługi sieci American Express.

Dział 3

Zobowiązania odszkodowawcze w związku z Incydemem dotyczącym Danych

Państwa zobowiązania odszkodowawcze wobec American Express, wynikające z niniejszej Umowy w związku z Incydentami dotyczącymi Danych, podlegają postanowieniom niniejszego [Dział 3, „Zobowiązania odszkodowawcze w związku z Incydemem 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 Incydemu dotyczącego Danych, jak opisano poniżej w niniejszym [Dział 3, „Zobowiązania odszkodowawcze w związku z Incydemem dotyczącym Danych”](#).

W przypadku Incydemów 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 Incydemu 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 Incydemie dotyczącym Danych zgodnie z niniejszym [Dział 3, „Zobowiązania odszkodowawcze w związku z Incydemem dotyczącym Danych”](#),
 - w momencie wystąpienia Incydemu dotyczącego Danych przestrzegali Państwo zasad PCI DSS (zgodnie z ustaleniami dochodzenia PFI w sprawie Incydemu dotyczącego Danych) oraz
 - Incydem dotyczący Danych nie został spowodowany niewłaściwym postępowaniem Państwa lub Uwzględnionych Stron.

Niezależnie od powyższych punktów niniejszego [Dział 3, „Zobowiązania odszkodowawcze w związku z Incydemem dotyczącym Danych”](#), za jakiegokolwiek Incydemu dotyczący Danych, niezależnie od liczby Numerów Kart American Express, uiszcza Państwo opłatę na rzecz American Express za nieprzestrzeganie zasad dotyczących Incydemu dotyczącego Danych w wysokości nieprzekraczającej 100 000 USD za każdy Incydemu dotyczący Danych (według uznania American Express) w przypadku niewypełnienia któregokolwiek ze zobowiązań określonych w [Dział 2, „Obowiązki w zakresie zarządzania incydentami dotyczącymi danych”](#).

Aby uniknąć wątpliwości, łączna opłata za nieprzestrzeganie zasad dotyczących Incydemu dotyczącego Danych oszacowana dla pojedynczego Incydemu dotyczącego Danych nie może przekroczyć 100 000 USD.

American Express wyłącza z obliczeń jakiegokolwiek Numery Kont Kart American Express ujęte we wcześniejszym zgłoszonym roszczeniu odszkodowawczym za Incydemu dotyczący Danych w ciągu dwunastu (12) miesięcy przed terminem powiadomienia. Wszystkie obliczenia dokonane przez American Express zgodnie 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.

Zobowiązania odszkodowawcze Sprzedawców z tytułu Incydemów 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 Incydemów dotyczących Danych spełniających każde z poniższych kryteriów:

- Przed wystąpieniem Incydemu dotyczącego Danych i na cały czas trwania Okna Incydemu 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:

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 móc zakwalifikować daną technologię się jako 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.

Przy- kład	Technologia Ograniczania Ryzyka w praktyce	Czy kwalifikuje się do Rozszerzonej Redukcji Zobowiązania 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		

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

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 4

Ważna okresowa walidacja Państwa systemów

Muszą Państwo podjąć następujące czynności w celu dokonania rocznej i kwartalnej walidacji, 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:](#) Uczestnictwo w programie przestrzegania zasad zgodności American Express w ramach niniejszej Polityki.

[Akcja 2:](#) Zapoznanie się z Wymogami dotyczącymi Poziomu i Walidacji.

[Akcja 3:](#) Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wystać 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 i wszyscy Dostawcy usług, jak opisano poniżej, muszą uczestniczyć w programie przestrzegania zasad zgodności American Express w ramach niniejszej Polityki, podając swoje pełne imię i nazwisko, adres e-mail, numer telefonu i fizyczny adres pocztowy osoby fizycznej, która będzie pełnić funkcję osoby odpowiedzialnej za bezpieczeństwo danych. Należy przestać te informacje do SecureTrust, oddziału Trustwave (<https://portal.securetrust.com>), zarządzającego programem w imieniu American Express, za pomocą jednej z metod wymienionych w [Akcja 4: „Przesyłanie Dokumentacji walidacyjnej do American Express”](#) poniżej. Jeśli te informacje ulegną zmianie, muszą Państwo powiadomić firmę SecureTrust, dostarczając aktualnie informacje tam, gdzie ma to zastosowanie. Niepodanie takich danych kontaktowych nie wpłynie na nasze prawa do naliczania opłat za brak walidacji, jak określono w [Tabela opłat za brak walidacji](#).

American Express może według własnego uznania wyznaczyć określonych Sprzedawców Poziomu 3 i 4 do udziału w programie zgodności American Express na mocy niniejszej Polityki, poprzez wystanie im pisemnego powiadomienia. Sprzedawca musi dokonać rejestracji nie później niż 90 dni po otrzymaniu takiego powiadomienia.

Akcja 2: Zapoznanie się z Wymogami dotyczącymi Poziomu i 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 wolumen przesyłany przez ich placówki, który kwalifikuje je do najwyższego poziomu konta American Express dla Sprzedawców.* Zostaną Państwo przydzieleni do jednego z tych Poziomów określonych w poniższych tabelach dla Sprzedawców i Dostawców Usług. 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.

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

Wymagania dotyczące Sprzedawcy

Sprzedawcy (a nie Dostawcy Usług) podlegają czterem możliwym klasyfikacjom dotyczącym ich poziomu i wymogów w zakresie walidacji. Po określeniu poziomu Sprzedawcy na podstawie poniższej listy, należy zapoznać się z Tabelą Sprzedawcy, aby określić wymagania dotyczące dokumentacji walidacji.

- **Sprzedawca Poziomu 1** — 2,5 miliona 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 Sprzedawców

Poziom Sprzedawcy/ Roczne transakcje American Express	Dokumentacja Walidacyjna		
	Sprawozdanie z oceny zgodności na miejscu (ROC)	Kwestionariusz samooceny (SAQ) ORAZ kwartalne skanowanie sieci	Poświadczenie STEP dla uprawnionych Sprzedawców
Poziom 1/ 2,5 miliona lub więcej	Obowiązkowe	Nie dotyczy	Opcjonalne (zastępuje ROC)
Poziom 2/ 50 000 do 2,5 miliona	Opcjonalne	SAQ obowiązkowe (chyba że przedłożono Sprawozdanie z Oceny Zgodności na Miejsce); obowiązkowe skanowanie w przypadku niektórych typów SAQ	Opcjonalne (zastępuje SAQ i skanowanie sieci lub ROC)
Poziom 3/ 10 000 do 50 000	Opcjonalne	SAQ 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 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 ochrony danych i podlegają odpowiedzialności z tego tytułu.

American Express zastrzega sobie prawo do weryfikacji w razie potrzeby dokładności i stosowności dostarczonej dokumentacji walidacji PCI, w tym poprzez zaangażowanie, na koszt American Express, wybranego przez siebie QSA lub PFI.

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:

- **Specyfikacji EMV** – 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 Płatności Zbliżeniowe)
- **Szyfrowania Point to Point (P2PE)** – komunikacji z procesorami Sprzedawców za pomocą systemu Szyfrowania Point to Point zatwierdzonego przez PCI-SSC lub zatwierdzonego przez QSA

Sprzedawcy kwalifikujący się do programu STEP mają zmniejszone wymagania dotyczące Dokumentacji Walidacji PCI, co opisano szerzej w [Akcja 3: „Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wystać do American Express”](#) poniżej.

Wymagania dotyczące Dostawców usług

Dostawcy usług (nie Sprzedawcy) są klasyfikowani na dwa sposoby w odniesieniu do ich poziomu i wymagań walidacyjnych. Po ustaleniu poziomu Dostawcy Usług zgodnie z poniższą listą należy zapoznać się z Tabelą Dostawców 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 Dostawców Usług

Poziom	Dokumentacja Walidacyjna	Wymóg
1	Roczne Sprawozdanie z Oceny Bezpieczeństwa na miejscu	Obowiązkowe
2	Roczny SAQ D (Dostawca Usług) i Kwartalne Skanowanie Sieci lub Roczne Sprawozdanie z Oceny Bezpieczeństwa na miejscu, dotyczące zgodności z przepisami, w razie potrzeby.	Obowiązkowe

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

Akcja 3: Wypełnienie Dokumentacji Walidacyjnej, którą muszą Państwo wystać 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.

Roczna ocena poziomu bezpieczeństwa na miejscu — Roczna ocena poziomu bezpieczeństwa na miejscu to przeprowadzane na miejscu szczegółowe badanie Państwa urządzeń, systemów i sieci (oraz ich części składowych), w których przechowywane, przetwarzane lub przekazywane są Dane Posiadaczy Kart lub Wrażliwe Dane Uwierzytelniające (lub oba rodzaje danych). Powinna zostać przeprowadzona przez:

- QSA lub
- Państwo oraz zatwierdzona przez dyrektora generalnego, dyrektora finansowego, dyrektora ds. bezpieczeństwa informacji lub zlecniodawcę i corocznie dostarczana do American Express w formie stosownego Atestu zgodności (AOC).

AOC powinien potwierdzać zgodność ze wszystkimi wymaganiami PCI DSS oraz, na żądanie, zawierać kopie pełnego raportu dotyczącego zgodności (Sprzedawcy poziomu 1 i Dostawcy usług poziomu 1).

Roczny kwestionariusz samooceny — Roczny kwestionariusz samooceny to procedura wykorzystująca Kwestionariusz samooceny stanu wdrożenia PCI DSS SAQ, który pozwala na przeprowadzenie samodzielnego badania Państwa urządzeń, systemów i sieci (oraz ich części składowych), w których przechowywane, przetwarzane lub przekazywane są Dane Posiadaczy Kart lub Wrażliwe Dane Uwierzytelniające (lub oba rodzaje danych). Powinna zostać przeprowadzona przez Państwo oraz zatwierdzona przez dyrektora generalnego, dyrektora finansowego, dyrektora ds. bezpieczeństwa informacji lub osobę odpowiedzialną. Część SAQ zawierająca AOC powinna być corocznie dostarczana do American Express. Część SAQ zawierająca AOC powinna potwierdzać zgodność ze wszystkimi wymaganiami standardów PCI DSS oraz, na żądanie, zawierać kopie kompletnego SAQ (Sprzedawcy Poziomu 1, Poziomu 2, Poziomu 3 i Poziomu 4; Dostawcy usług poziomu 2).

Kwartalne skanowanie sieci — Kwartalne skanowanie sieci to procedura, która zdalnie sprawdza Państwa sieci komputerowe i serwery webowe podłączone do internetu pod kątem potencjalnych słabych punktów i zagrożeń. Powinna zostać przeprowadzona przez autoryzowanego sprzedawcę usług skanowania (**ASV**). Są Państwo zobowiązani raz na kwartał wypełniać i dostarczać do American Express Atest zgodności skanowania (**AOSC**) z Raportu skanowania przeprowadzonego przez ASV lub podsumowanie wyników przeprowadzonego skanowania (a na żądanie: kopie pełnego skanowania). AOSC lub podsumowanie powinny potwierdzać, że wyniki spełniają wymagania procedur skanowania PCI DSS, że nie zidentyfikowano żadnych problemów wysokiego ryzyka, oraz że skanowanie ma charakter wystarczający lub zgodny (wszyscy Sprzedawcy z wyjątkiem tych, którzy również przedkładają Sprawozdanie z Oceny Bezpieczeństwa na miejscu, Sprzedawcy kwalifikujący się do programu STEP oraz wszyscy Dostawcy Usług). Dla uniknięcia wątpliwości, Kwartalne Skanowanie Sieci jest obowiązkowe, jeśli wymaga tego odpowiedni SAQ.

Dokumentacja weryfikacyjna poświadczenia rocznego programu STEP — Coroczny Certyfikat Kwalifikacji STEP („Poświadczenie STEP”) jest dostępny tylko dla Sprzedawców, którzy spełniają kryteria wymienione w [Akcia 2: „Zapoznanie się z Wymogami dotyczącymi Poziomu i Walidacji”](#) powyżej. Poświadczenie STEP obejmuje proces wykorzystujący wymagania standardów PCI DSS, który pozwala na samodzielną ocenę sprzętu, systemów i sieci (i ich komponentów), w których Dane Posiadacza Karty lub Wrażliwe Dane Uwierzytelniające (lub oba te elementy) są przechowywane, przetwarzane lub przesyłane. Powinna zostać przeprowadzona przez Państwo oraz zatwierdzona przez dyrektora generalnego, dyrektora finansowego, dyrektora ds. bezpieczeństwa informacji lub osobę odpowiedzialną. Proces ten muszą Państwo zakończyć poprzez coroczne przesyłanie Formularza Poświadczenia STEP do American Express. (Wyłącznie Sprzedawcy kwalifikujący się do programu STEP). Formularz poświadczenia rocznego programu STEP jest dostępny do pobrania za pośrednictwem bezpiecznego portalu SecureTrust.

Podsumowanie Zgodności — SOC to dokument, za pomocą którego Francyzodawca lub Dostawca Usług może zgłosić status zgodności PCI swoich Francyzobiorców. Szablon SOC jest dostępny do pobrania za pośrednictwem bezpiecznego portalu SecureTrust.

Niezgodność ze Standardami PCI DSS — Jeśli nie przestrzegają Państwo standardów PCI DSS, muszą Państwo dostarczyć jeden z poniższych dokumentów:

- Poświadczenie Zgodności (AOC) zawierające „Część 4. Plan Działania dotyczący Statusu Niezgodności”
- Podsumowanie Narzędzia Podejścia Priorytetowego PCI i Poświadczenie Zgodności (PASAOC)
- Szablon Planu Projektu (dostępny do pobrania za pośrednictwem bezpiecznego portalu SecureTrust)

Każdy z powyższych dokumentów musi mieć wyznaczoną datę naprawczą, nie dłuższą niż 12 miesięcy od daty zakończenia dokumentu w celu osiągnięcia zgodności. Należy dostarczyć odpowiedni dokument do American Express za pomocą jednej z metod wymienionych w [Akcia 4: „Przesyłanie Dokumentacji walidacyjnej do American Express”](#) poniżej. 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). W celu uniknięcia jakichkolwiek wątpliwości, Sprzedawcy, którzy nie wykazują zgodności ze standardami PCI DSS nie kwalifikują się do udziału w programie STEP. 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.

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 Dokumentację walidacyjną oznaczoną jako „obowiązkową” w tabelach w [Akcia 2: „Zapoznanie się z Wymogami dotyczącymi Poziomu i Walidacji”](#). Należy przekazać SecureTrust Dokumentację walidacyjną za pośrednictwem jednej z poniższych metod:

- **Bezpieczny portal:** Dokumentację walidacyjną można przesłać za pośrednictwem bezpiecznego portalu SecureTrust pod adresem: <https://portal.securetrust.com>.
Należy skontaktować się z SecureTrust pod numerem telefonu dla danego kraju lub poprzez e-mail pod adresem americanexpresscompliance@securetrust.com, aby uzyskać instrukcje na temat korzystania z tego portalu.
- **Bezpieczny faks:** Dokumentację walidacyjną można przesłać faksem pod numer: +1 (312) 276-4019. (+ oznacza międzynarodowy numer kierunkowy „IDD”, obowiązują opłaty za połączenia międzynarodowe).
Proszę podać firmę, nazwę spółki, imię i nazwisko osoby kontaktowej ds. bezpieczeństwa danych, swój adres i nr telefonu, a także (dotyczy wyłącznie Sprzedawców) dziesięciocyfrowy numer Sprzedawcy American Express.

W przypadku ogólnych pytań dotyczących programu lub powyższego procesu należy kontaktować się z SecureTrust pod numerem + 800 9000 1140 lub +1 (312) 267-3208 albo pod adresem e-mail americanexpresscompliance@securetrust.com.

Badanie zgodności i walidacja przeprowadzane są na Państwa koszt. Składając Dokumentację walidacyjną, oświadczają i zapewniają Państwo American Express, że są Państwo uprawnieni do ujawniania informacji w niej zawartych i przekazują Dokumentację walidacyjną American Express nie naruszając praw żadnych innych osób.

Rynki	Numer telefonu SecureTrust
Argentyna	+ 800 9000 1140
Australia	+ 800 9000 1140
Austria	+ 800 9000 1140
Bułgaria	+ 312 267 3208
Chorwacja	+ 312 267 3208
Cypr	+ 800 9000 1140
Dania	+ 800 9000 1140
Estonia	+ 312 267 3208
Francja	+ 800 9000 1140
Grecja	+ 312 267 3208
Hiszpania	+ 800 9000 1140
Holandia	+ 312 267 3208
Hongkong	+ 800 9000 1140
IDC	+ 888 900 0114
Indie	+ 800 9000 1140
Irlandia	+ 800 9000 1140
Islandia	+ 800 9000 1140
Japonia	+ 312 267 3208
Kanada	1 866 659 9016
Litwa	+ 312 267 3208
Łotwa	+ 312 267 3208

Rynki	Numer telefonu SecureTrust
Malta	+ 312 267 3208
Meksyk	+ 888 900 0114
Niemcy	+ 800 9000 1140
Nowa Zelandia	+ 800 9000 1140
Norwegia	+ 800 9000 1140
Polska	+ 800 9000 1140
Portugalia	+ 312 267 3208
Republika Czeska	+ 800 144 316
Rosyjski	+ 312 267 3208
Rumunia	+ 312 267 3208
Singapur	+ 800 9000 1140
Słowacja	+ 312 267 3208
Słowenia	+ 312 267 3208
Stany Zjednoczone	1 866 659 9016
Szwecja	+ 800 9000 1140
Tajwan	+ 312 267 3208
Tajlandia	+ 800 9000 1140
Węgry	+ 800 9000 1140
Włochy	+ 800 9000 1140
Zjednoczone Królestwo	+ 800 9000 1140

+ oznacza międzynarodowy numer kierunkowy „IDD”; obowiązują opłaty za połączenia międzynarodowe

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.

Dokumentację należy wystąpić do American Express w obowiązującym terminie. American Express powiadomi Państwa osobno o terminie obowiązującym dla każdego rocznego i kwartalnego okresu sprawozdawczego. Należy zapoznać się z poniższą tabelą Opłat za brak walidacji, aby dowiedzieć się o opłatach obowiązujących w Państwa kraju.

Opis	Sprzedawca poziomu 1 lub Dostawca usług poziomu 1	Sprzedawca poziomu 2, Dostawca usług poziomu 2 lub Sprzedawca STEP	Sprzedawca poziomu 3 lub poziomu 4
Za brak walidacji zostanie nałożona opłata, jeżeli Dokumentacja walidacyjna nie zostanie złożona w pierwszym terminie.	Opłata za 1. miesiąc dla Poziomu 1	Opłata za 1. miesiąc dla Poziomu 2	Opłata miesięczna
Za brak walidacji zostanie nałożona opłata, jeżeli Dokumentacja walidacyjna nie zostanie złożona w ciągu 30 dni od upływu pierwszego terminu.	Opłata za 2. miesiąc dla Poziomu 1	Opłata za 2. miesiąc dla Poziomu 2	
Za brak walidacji zostanie nałożona opłata, jeżeli Dokumentacja walidacyjna nie zostanie złożona w ciągu 60 dni od upływu pierwszego terminu.	Opłata za 3. miesiąc dla Poziomu 1	Opłata za 3. miesiąc dla Poziomu 3	

Jeżeli American Express nie otrzyma od Państwa obowiązkowej Dokumentacji walidacyjnej w ciągu 60 dni od upływu pierwszego terminu, wówczas American Express ma prawo wypowiedzieć Umowę zgodnie z jej postanowieniami, a także nałożyć łącznie powyższe kary umowne za brak walidacji.

Tabela opłat za brak walidacji

Rynek	Poziom	Typ	Waluta	Opłata za 1. miesiąc	Opłata za 2. miesiąc	Opłata za 3. miesiąc
Australia	Poziom 1	Sprzedawca lub Dostawca Usług	AUD	35 000	49 000	63 000
	Poziom 2	Sprzedawca lub Dostawca Usług	AUD	7 000	14 000	21 000
	Poziom 3 i Poziom 4	Sprzedawca	AUD	Opłata miesięczna: 20		
Bułgaria	Poziom 1	Sprzedawca lub Dostawca Usług	BGN	28 000	40 000	51 000
	Poziom 2	Sprzedawca lub Dostawca Usług	BGN	5 500	11 000	16 500
	Poziom 3 i Poziom 4	Sprzedawca	BGN	Opłata miesięczna: 33		

Rynek	Poziom	Typ	Waluta	Opłata za 1. miesiąc	Opłata za 2. miesiąc	Opłata za 3. miesiąc
Chorwacja	Poziom 1	Sprzedawca lub Dostawca Usług	HRK	105 000	152 000	195 000
	Poziom 2	Sprzedawca lub Dostawca Usług	HRK	21 000	42 000	63 000
	Poziom 3 i Poziom 4	Sprzedawca	HRK	Opłata miesięczna: 130		
Cypr, Estonia, Francja, Niemcy, Irlandia, Hiszpania, Łotwa, Litwa, Portugalia, Słowacja, Słowenia	Poziom 1	Sprzedawca lub Dostawca Usług	EUR	19 000	26 000	34 000
	Poziom 2	Sprzedawca lub Dostawca Usług	EUR	4 000	7 500	11 000
	Poziom 3 i Poziom 4	Sprzedawca	EUR	Opłata miesięczna: 15		
Dania	Poziom 1	Sprzedawca lub Dostawca Usług	DKK	110 000	156 000	200 000
	Poziom 2	Sprzedawca lub Dostawca Usług	DKK	22 000	42 000	65 000
	Poziom 3 i Poziom 4	Sprzedawca	DKK	Opłata miesięczna: 130		
Hongkong	Poziom 1	Sprzedawca lub Dostawca Usług	HKD	25 000	35 000	45 000
	Poziom 2	Sprzedawca lub Dostawca Usług	HKD	5 000	10 000	15 000
	Poziom 3 i Poziom 4	Sprzedawca	HKD	Opłata miesięczna: 150		
Islandia	Poziom 1	Sprzedawca lub Dostawca Usług	ISK	3 070 000	4 300 000	5 500 000
	Poziom 2	Sprzedawca lub Dostawca Usług	ISK	615 000	920 000	1 227 200
	Poziom 3 i Poziom 4	Sprzedawca	ISK	Opłata miesięczna: 2 400		
Nowa Zelandia	Poziom 1	Sprzedawca lub Dostawca Usług	NZD	35 000	49 000	63 000
	Poziom 2	Sprzedawca lub Dostawca Usług	NZD	7 000	14 000	21 000
	Poziom 3 i Poziom 4	Sprzedawca	NZD	Opłata miesięczna: 20		

Rynek	Poziom	Typ	Waluta	Opłata za 1. miesiąc	Opłata za 2. miesiąc	Opłata za 3. miesiąc
Norwegia	Poziom 1	Sprzedawca lub Dostawca Usług	NOK	135 000	195 000	249 000
	Poziom 2	Sprzedawca lub Dostawca Usług	NOK	27 000	54 000	81 000
	Poziom 3 i Poziom 4	Sprzedawca	NOK	Opłata miesięczna: 170		
Republika Czeska	Poziom 1	Sprzedawca lub Dostawca Usług	CZK	392 000	564 000	721 000
	Poziom 2	Sprzedawca lub Dostawca Usług	CZK	78 300	157 000	235 000
	Poziom 3 i Poziom 4	Sprzedawca	CZK	Opłata miesięczna: 440		
Singapur	Poziom 1	Sprzedawca lub Dostawca Usług	SGD	38 000	53 000	68 000
	Poziom 2	Sprzedawca lub Dostawca Usług	SGD	7 500	15 000	22 500
	Poziom 3 i Poziom 4	Sprzedawca	SGD	Opłata miesięczna: 25		
Szwecja	Poziom 1	Sprzedawca lub Dostawca Usług	SEK	175 000	245 000	315 000
	Poziom 2	Sprzedawca lub Dostawca Usług	SEK	35 000	70 000	105 000
	Poziom 3 i Poziom 4	Sprzedawca	SEK	Opłata miesięczna: 135		
Węgry	Poziom 1	Sprzedawca lub Dostawca Usług	HUF	4 650 000	6 700 000	8 600 000
	Poziom 2	Sprzedawca lub Dostawca Usług	HUF	930 000	1 860 000	2 800 000
	Poziom 3 i Poziom 4	Sprzedawca	HUF	Opłata miesięczna: 5 500		

Rynek	Poziom	Typ	Waluta	Opłata za 1. miesiąc	Opłata za 2. miesiąc	Opłata za 3. miesiąc
Zjednoczone Królestwo	Poziom 1	Sprzedawca lub Dostawca Usług	GBP	12 500	18 000	23 000
	Poziom 2	Sprzedawca lub Dostawca Usług	GBP	2 500	5 000	7 500
	Poziom 3 i Poziom 4	Sprzedawca	GBP	Opłata miesięczna: 15		

Dział 5

Poufność

American Express podejmie rozsądne kroki, by zachować poufność (i narzucić zachowanie poufności swoim agentom i podwykonawcom, w tym SecureTrust) 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 6

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 WYRAŻNYCH, 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 [Polityka operacyjna 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 standardów ochrony danych aplikacji stosowanym w branży kart płatniczych, 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 weryfikacyjna oznacza AOC wydane w związku z Coroczną Oceną Bezpieczeństwa na miejscu lub SAQ, podsumowania ustaleń wydanych w związku z Kwartalnymi Skanami Sieci lub Atestacją Roczno Programu Ulepszania Technologii Bezpieczeństwa.

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

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.

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.

Incydent dotyczący Danych jest związany z naruszeniem lub podejrzanym 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;
- 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).

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:

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 Incydem dotyczącym Danych.

Obciążenie oznacza płatność lub zakup dokonane przy użyciu Karty.

Okno Incydemu dotyczącego Danych oznacza okres rozpoczynający się w dniu zdarzenia naruszenia bezpieczeństwa danych, jeśli jest znany, lub 365 dni przed Datą Powiadomienia, jeśli faktyczna data takiego zdarzenia nie jest znana. Okno Zdarzenia Zagrożącego Bezpieczeństwu Danych kończy się 30 dni po Dacie Powiadomienia.

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.

Podsumowanie zgodności (Summary of Compliance, SOC) to dokument, za pomocą którego Francyzodawca lub Dostawca Usług może zgłosić status zgodności PCI swoich Francyzobiorców.

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.

Program Ulepszania Technologii Bezpieczeństwa (Security Technology Enhancement Program, STEP) oznacza program American Express, w ramach którego Sprzedawcy są zachęceni do wdrażania technologii poprawiających bezpieczeństwo danych. Aby zakwalifikować się do programu STEP, u Sprzedawcy nie może wystąpić Incydem dotyczący Danych w okresie 12 miesięcy poprzedzających złożenie poświadczenia rocznego programu STEP. Muszą też oni wykonać co najmniej 75% wszystkich transakcji przy użyciu szyfrowania Point to Point lub Transakcji bezpośrednich przy użyciu Urządzeń obsługujących transakcje z użyciem kart chipowych EMV.

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 sprzedaży (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.

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

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: 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.

- Klucze szyfrowania kluczy (Key Encrypting Keys): klucze Zone Master Keys (ZMK) i klucze Zone Pin Keys (ZPK)
- Klucze główne (Master Keys) wykorzystywane w bezpiecznych urządzeniach szyfrujących: lokalne klucze główne (Local Master Keys, LMK)
- klucze kodów bezpieczeństwa kart (Card Security Code Keys, CCK)
- Klucze PIN: klucze Base Derivation Keys (BDK), PIN Encryption Key (PEK) i ZPK

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

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 zgodnie ze standardem AEIPS.

Uwzględnione Strony oznaczają któregokolwiek lub wszystkich pracowników, agentów, przedstawicieli, podwykonawców, Procesorów, Dostawców Usług, dostawców sprzętu w punktach sprzedaży (POS) lub systemów POS 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.

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

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.

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 Rzecznawcę ds. Bezpieczeństwa (QSA) PCI SSC P2PE.