AMERICAN EXPRESS

Allgemeine Datensicherheitsrichtlinien (Data Security Operating Policy, DSOP)

Änderungsbalken

Wichtige Aktualisierungen sind in der Tabelle „Zusammenfassung der Änderungen“ aufgeführt und in den DSOP mit einem Änderungsbalken gekennzeichnet. Änderungsbalken sind senkrechte Linien am linken Rand, die überarbeiteten, hinzugefügten oder entfernten Text kennzeichnen. Alle Änderungen in den DSOP sind, wie folgt dargestellt, mit einem Änderungsbalken gekennzeichnet.

Tabelle „Zusammenfassung der Änderungen“

Wichtige Aktualisierungen sind in der folgenden Tabelle aufgeführt und in den *DSOP* mit einem Änderungsbalken gekennzeichnet.

Abschnitt/Unterabschnitt	Beschreibung der Änderung
Für diese Version gibt es keine Änderungen.	

Verfahrensweise bei einem Datenvorfall

Bitte führen Sie die folgenden Schritte aus, wenn Sie in Ihrem Unternehmen einen Datenvorfall festgestellt haben.

Schritt 1:

Füllen Sie das Erstmitteilungsformular für Datenvorfälle bei Akzeptanzpartnern aus und senden Sie dieses per E-Mail an EIRP@aexp.com. Diese E-Mail muss innerhalb von 72 Stunden nach Feststellung des Datenvorfalls versandt werden.

Schritt 2:

Führen Sie eine gründliche Untersuchung durch, wofür gegebenenfalls die Verpflichtung eines forensischen Ermittlers der Zahlungskartenindustrie (Payment Card Industry, PCI) erforderlich ist.

Schritt 3:

Informieren Sie uns unverzüglich über alle kompromittierten American Express®-Kartennummern.

Schritt 4:

Arbeiten Sie mit uns zusammen, um aus dem Datenvorfall gegebenenfalls hervorgehende Probleme zu beheben.

Lesen Sie Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall“, in dem Sie nähere Einzelheiten zu Ihren Verpflichtungen und Vorgehensweisen bei einem Datenvorfall finden.

Noch Fragen?

USA: (888) 732-3750 (gebührenfrei)

International: +1 (602) 537-3021

EIRP@aexp.com

Im Sinne des Verbraucherschutzes verpflichtet sich American Express schon seit vielen Jahren dem Schutz der Daten seiner Karteninhaber und vertraulichen Authentifizierungsdaten, um höchste Sicherheit zu gewährleisten.

Die Kompromittierung von Daten wirkt sich negativ auf Verbraucher, Akzeptanzpartner, Dienstleister und Kartenherausgeber aus. Ein einziger Datenvorfall kann den Ruf eines Unternehmens stark schädigen und die effiziente Abwicklung seiner Geschäfte beeinträchtigen. Die Einführung von Datensicherheitsrichtlinien als Antwort auf diese Bedrohung kann dazu beitragen, das Vertrauen der Kunden zu stärken, die Rentabilität zu steigern und die Reputation eines Unternehmens zu verbessern.

Bei American Express wissen wir, dass Akzeptanzpartner und Dienstleister (zusammenfassend als Sie bezeichnet) unser Anliegen teilen. Wir setzen daher als Teil Ihrer Verantwortung voraus, dass **Sie** die Datensicherheitsbestimmungen Ihres **Vertrags** und diese Allgemeinen Datensicherheitsrichtlinien, die wir von Zeit zu Zeit überarbeiten, einhalten. Im Fall der Akzeptanzpartner gilt dies für die Akzeptanz und im Fall der Dienstleister für die Verarbeitung der American Express® Kartentransaktion (jeweils nach Maßgabe des Vertrags). Diese Anforderungen gelten für alle Geräte, Systeme und Netzwerke (und deren Komponenten), in denen Verschlüsselungscodes, Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder eine Kombination daraus) gespeichert, verarbeitet oder übertragen werden.

In diesem Dokument verwendete, aber nicht definierte großgeschriebene Begriffe haben die ihnen im Glossar am Ende dieser Richtlinie zugewiesene Bedeutung.

Abschnitt 1 Programm für gezielte Analysen (Targeted Analysis Program, TAP)

Eine Kompromittierung von Karteninhaberdaten kann von Datensicherheitslücken in Ihrer Karteninhaberdatenumgebung (Cardholder Data Environment, CDE) verursacht werden.

Beispiele für eine Kompromittierung von Karteninhaberdaten sind unter anderem:

- **Gemeinsame Verkaufsstelle (Common Point of Purchase, CPP):** American Express-Kartenmitglieder melden betrügerische Transaktionen auf ihren Kartenkonten und es wird festgestellt, dass sie aus Einkäufen in Ihren Akzeptanzstellen stammen.
- **Gefundene Kartendaten:** Daten von American Express Karten und Karteninhabern, die im Internet gefunden wurden und mit Transaktionen in Ihren Akzeptanzstellen verknüpft sind.
- **Vermutete Malware:** American Express vermutet, dass Sie Software verwenden, die mit bösartigem Code infiziert oder für diesen anfällig ist.

Das TAP dient der Identifizierung möglicher Kompromittierungen von Karteninhaberdaten.

Sie sind verpflichtet – und müssen die von Ihnen Eingeschalteten Dritten ebenfalls dazu verpflichten –, bei Benachrichtigung seitens American Express über eine potenzielle Kompromittierung von Karteninhaberdaten die folgenden Anforderungen zu erfüllen.

- Sie müssen Ihre CDE unverzüglich auf Datensicherheitslücken überprüfen und festgestellte Probleme beheben.
  - Sie müssen Ihre Drittanbieter veranlassen, eine gründliche Untersuchung Ihrer CDE durchzuführen, wenn diese ausgelagert wird.
- Sie müssen nach Benachrichtigung durch American Express eine Zusammenfassung der ergriffenen oder für die Zeit nach Ihren Überprüfungs-, Bewertungs- und/oder Korrekturmaßnahmen geplanten Maßnahmen vorlegen.
- Sie müssen aktualisierte PCI-DSS-Validierungsdokumente gemäß Abschnitt 5, „Wichtige periodische Validierung Ihrer Systeme“.
- Gegebenenfalls müssen Sie einen qualifizierten forensischen Ermittler der Zahlungskartenindustrie (PCI Forensic Investigator, PFI) beauftragen, um Ihre CDE zu untersuchen, wenn Sie oder Ihre Drittanbieter:
  - nicht in der Lage sind, die Kompromittierung der Karteninhaberdaten innerhalb eines angemessenen, von American Express festgelegten Zeitraums zu lösen, oder
  - bestätigen, dass ein Datenvorfall stattgefunden hat, und die Anforderungen in Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall“.

Tabelle A-1: Strafgebühren wegen Nichteinhaltung des TAP

Beschreibung	Akzeptanzpartner oder Dienstleister, Stufe 1	Akzeptanzpartner oder Dienstleister, Stufe 2	Akzeptanzpartner, Stufe 3 oder 4
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird veranschlagt, wenn TAP-Verpflichtungen nicht innerhalb der ersten Frist erfüllt werden.	USD 25.000	USD 5.000	USD 1.000
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird veranschlagt, wenn TAP-Verpflichtungen nicht innerhalb der zweiten Frist erfüllt werden.	USD 35.000	USD 10.000	USD 2.500
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird veranschlagt, wenn TAP-Verpflichtungen nicht innerhalb der dritten Frist erfüllt werden. **HINWEIS:** *Strafgebühren wegen Nichteinhaltung von Vorschriften können weiterhin monatlich erhoben werden, bis die Verpflichtungen erfüllt sind oder der TAP-Verstoß abgestellt ist.*	USD 45.000	USD 15.000	USD 5.000

Wenn Ihre TAP-Verpflichtungen nicht erfüllt werden, hat American Express das Recht, die Strafgebühren wegen Nichteinhaltung von Vorschriften kumulativ zu erheben, Zahlungen zurückzuhalten und/oder den Vertrag zu kündigen.

Abschnitt 2 Standards für den Schutz von Verschlüsselungscodes, Karteninhaber- und vertraulichen Authentifizierungsdaten

Sie sind verpflichtet – und müssen die von Ihnen Eingeschalteten Dritten ebenfalls dazu verpflichten:

- Daten von Karteninhabern nur zu speichern, um die Abwicklung von American Express Kartentransaktionen in Übereinstimmung mit den im Vertrag geregelten Bedingungen zu ermöglichen,
- die aktuellen, für Ihre Verarbeitung, Speicherung oder Übertragung von Karteninhaber- oder vertraulichen Authentifizierungsdaten geltenden PCI-DSS- und PCI-SSC-Anforderungen spätestens ab dem Stichtag für die Implementierung dieser Fassung der anwendbaren Anforderungen einzuhalten sowie
- bei der Bereitstellung von Neu- oder Ersatzgeräten für die PIN-Eingabe oder von Zahlungssoftware (oder beidem) nur solche zu verwenden, die PCI-zugelassen sind.

Sie sind verpflichtet, sämtliche nach Maßgabe des Vertrags aufzubewahrenden American Express Belastungs- und Gutschriftsbelege gemäß diesen Datensicherheitsbestimmungen zu schützen; die Belege dürfen lediglich im Rahmen der Zweckbestimmung des Vertrags verwendet werden und sind entsprechend zu sichern. Sie sind American Express gegenüber für die Einhaltung dieser Datensicherheitsrichtlinien durch die von Ihnen Eingeschalteten Dritten haftbar. (Sie haften jedoch nicht für den Nachweis der Einhaltung dieser Richtlinie durch die von Ihnen Eingeschalteten Dritten gemäß Abschnitt 5, „Wichtige periodische Validierung Ihrer Systeme“, sofern nicht anderweitig dort angegeben.)

Abschnitt 3 Verpflichtungen und Vorgehen bei einem Datenvorfall

Sie müssen American Express sofort, in keinem Fall aber später als zweiundsiebzig (72) Stunden nach der Entdeckung eines Datenvorfalls benachrichtigen.

Um American Express zu informieren, wenden Sie sich bitte an das American Express Enterprise Incident Response Programme (*EIRP*) unter der Rufnummer +1 (602) 537-3021 (+ steht für die internationale Direktwahl, es fallen Gebühren für internationale Anrufe an) oder schreiben Sie eine E-Mail an EIRP@aexp.com. Sie müssen jemanden ernennen, der als Kontaktperson für einen solchen Datenvorfall zuständig ist. Darüber hinaus gilt:

- Sie müssen für jeden einzelnen Datenvorfall eine gründliche forensische Untersuchung durchführen.
- Bei Datenvorfällen mit 10.000 oder mehr individuellen Karten- oder Kontennummern müssen Sie binnen fünf (5) Tagen nach der Entdeckung des jeweiligen Datenvorfalls für diese Untersuchung einen forensischen Ermittler der Zahlungskartenindustrie (PFI) hinzuziehen.
- Der unveränderte forensische Ermittlungsbericht muss American Express innerhalb von zehn (10) Werktagen nach Fertigstellung vorliegen.
- Sie sind verpflichtet, American Express unverzüglich alle kompromittierten Karten- und Kontonummern zur Verfügung zu stellen. American Express behält sich das Recht vor, eigene interne Untersuchungen durchzuführen, um an dem Datenvorfall beteiligte Karten- oder Kontennummern zu identifizieren.

Die forensischen Ermittlungsberichte sind anhand der aktuellen Vorlage für forensische Abschlussberichte zu Datenvorfällen anzufertigen, die von PCI erhältlich ist. Diese Berichte müssen forensische Überprüfungen, Berichte über die Einhaltung der Bestimmungen und alle anderen Informationen zu dem Datenvorfall beinhalten; sie müssen die Ursache des Datenvorfalls aufzeigen, bestätigen, ob Sie zum Zeitpunkt des Datenvorfalls den PCI-DSS eingehalten haben, und überprüfen, ob Sie (i) durch Vorlage eines Plans zur Beseitigung aller PCI-DSS-Mängel und (ii) durch Teilnahme am (weiter unten beschriebenen) American Express Compliance-Programm in der Lage sind, zukünftige Datenvorfälle zu verhindern. Auf Wunsch von American Express ist eine Validierung durch einen Qualified Security Assessor (QSA) vorzulegen, dass die Mängel behoben wurden.

Ungeachtet der vorstehenden Absätze in diesem Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall“:

- American Express kann nach eigenen Ermessen verlangen, dass Sie einen PFI verpflichten, der eine Untersuchung eines Datenvorfalls durchführt, der weniger als 10.000 eindeutige Karten- oder Kontennummern betrifft. Alle Untersuchungen dieser Art müssen die oben in diesem Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall“, genannten Anforderungen erfüllen und innerhalb des von American Express vorgeschriebenen zeitlichen Rahmens durchgeführt werden.
- American Express kann nach eigenem Ermessen separat einen PFI verpflichten, der eine Untersuchung eines Datenvorfalls durchführt, und Ihnen die Kosten dieser Untersuchung in Rechnung stellen.

Sie erklären sich bereit, in Zusammenarbeit mit American Express alle aus dem Datenvorfall hervorgehenden Probleme zu beheben. Dazu gehören Konsultationen mit American Express über Ihre Kommunikation mit von dem Datenvorfall betroffenen Karteninhabern und die Zurverfügungstellung aller relevanten Informationen an American Express (sowie die Einholung gegebenenfalls erforderlicher Verzichtserklärungen für die Zurverfügungstellung dieser Informationen), damit überprüft werden kann, ob Sie in der Lage sind, zukünftigen Datenvorfällen im Einklang mit dem Vertrag vorzubeugen.

Ungeachtet einer gegenteiligen, im Vertrag geregelten Geheimhaltungspflicht hat American Express das Recht, Karteninhaber, Kartenherausgeber, andere am American Express Netzwerk Beteiligte und die allgemeine Öffentlichkeit gemäß dem Anwendbaren Recht über jeden Datenvorfall zu informieren. Ferner ist American Express zur Offenlegung von Datenvorfällen auf Anordnung eines Gerichts, einer Verwaltungs- oder Aufsichtsbehörde, eines Erlasses, einer Vorladung, eines Antrags oder eines anderen Verfahrens berechtigt, um das Risiko von Betrug oder anderen Schäden zu mindern oder insofern, als dies zum Betrieb des American Express Netzwerks angezeigt ist.

Abschnitt 4 Schadensersatzverpflichtungen für einen Datenvorfall

In diesem Abschnitt 4, „Schadensersatzverpflichtungen für einen Datenvorfall" sind unter Vorbehalt der Geltendmachung weiterer Rechte und Rechtsmittel durch American Express Ihre im Vertrag geregelten Schadensersatzverpflichtungen gegenüber American Express bei einem Datenvorfall festgelegt. Zusätzlich zu Ihren (evtl. bestehenden) Schadensersatzverpflichtungen unterliegen Sie gegebenenfalls einer Strafgebühr für die Nichteinhaltung von Vorschriften, die weiter unten in diesem Abschnitt 4, „Schadensersatzverpflichtungen für einen Datenvorfall", beschrieben sind.

Bei Datenvorfällen, die:

- 10.000 oder mehr American Express Karten- oder Kontonummern mit
  - vertraulichen Authentifizierungsdaten oder
  - dem Verfallsdatum betreffen,

  sind Sie American Express gegenüber zur Zahlung eines pauschalierten Schadenersatzes in Höhe von 5 USD pro Kartennummer verpflichtet.

American Express fordert jedoch keinen Schadensersatz von Ihnen für einen Datenvorfall, von dem

- weniger als 10.000 American Express Karten- oder Kontennummern oder
- mehr als 10.000 American Express Karten- oder Kontennummern betroffen sind, wenn Sie die folgenden Bedingungen erfüllen:
  - Sie haben American Express den Datenvorfall gemäß diesem Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall", gemeldet;
  - Sie haben zum Zeitpunkt des Datenvorfalls den PCI-DSS (wie bei der Untersuchung des Datenvorfalls durch den PFI bestimmt) eingehalten und
  - der Datenvorfall ist nicht auf ein Fehlverhalten Ihrerseits oder seitens der von Ihnen Eingeschalteten Dritten zurückzuführen.

Ungeachtet der vorstehenden Absätze in diesem Abschnitt 4, „Schadensersatzverpflichtungen für einen Datenvorfall", sind Sie unabhängig von der Anzahl der betroffenen American Express Karten- oder Kontennummern verpflichtet, American Express für jeden (von American Express nach eigenem Ermessen zu bestimmenden) Datenvorfall einen Schadensersatz wegen Nichteinhaltung von Vorschriften von maximal 100.000 USD für den Fall zu zahlen, dass Sie Ihren in Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall", beschriebenen Verpflichtungen nicht nachkommen. Zur Klarstellung: Die für jeden einzelnen Datenvorfall bemessene Strafgebühr wegen Nichteinhaltung von Vorschriften wird auf 100.000 USD begrenzt.

American Express schließt aus seiner Berechnung alle American Express Karten- oder Kontennummern aus, die in einem vorherigen Datenvorfall-Schadensersatzanspruch eingeschlossen waren, der innerhalb von zwölf (12) Monaten vor dem Benachrichtigungsdatum geltend gemacht wurde. Sämtliche von American Express mit dieser Methode vorgenommenen Berechnungen sind endgültig.

American Express kann Ihnen den vollständigen Betrag Ihrer Schadensersatzverpflichtungen für Datenvorfälle in Rechnung stellen oder den Betrag von den für Sie bestimmten Zahlungen durch American Express abziehen (bzw. Ihr Bankkonto entsprechend belasten).

Ihre hier festgestellten Schadensersatzverpflichtungen für Datenvorfälle sind gemäß diesem Vertrag nicht als Verpflichtung zum Ersatz beiläufig entstandener, indirekter oder zukünftiger Schäden, Folgeschäden, besonderer Schadensfolgen oder zu Strafschadensersatz zu erachten, vorausgesetzt, dass diese Verpflichtungen keinen Schadensersatz in Bezug auf entgangene Gewinne oder Einnahmen, einen Verlust des Firmenwerts oder entgangene Geschäftsmöglichkeiten oder in diesem Sinne beinhalten.

American Express kann nach eigenem Ermessen die Schadensersatzverpflichtung von Akzeptanzpartnern ausschließlich für Datenvorfälle reduzieren, wenn der Akzeptanzparnter folgende Kriterien kumulativ erfüllt:

- Geeignete Technologien zur Risikominderung wurden vor dem Datenvorfall angewendet und waren während des gesamten Datenvorfall-Zeitfensters aktiv;
- eine umfassende Untersuchung in Übereinstimmung mit dem PFI-Programm wurde durchgeführt (sofern nicht vorher anderweitig schriftlich vereinbart);

- der forensische Bericht beschreibt eindeutig die Technologien zur Risikominderung, die zum Zeitpunkt des Datenvorfalls für die Verarbeitung, Speicherung und/oder Übermittlung der Daten angewendet wurden, und
- Sie speichern keine vertraulichen Authentifizierungsdaten und auch keine Karteninhaberdaten, die nicht unlesbar gemacht wurden (und haben solche Daten auch während des Datenvorfall-Zeitfensters nicht gespeichert).

Wenn eine Reduzierung der Schadensersatzverpflichtung in Betracht kommt (ausschließlich eventuell zu zahlender Strafgebühren wegen Nichteinhaltung von Vorschriften), wird diese wie folgt ermittelt:

Tabelle A-2: Kriterien für eine Reduzierung der Schadensersatzverpflichtung

Reduzierung der Schadensersatzverpflichtung	Erforderliche Kriterien
Standardreduzierung: 50 %	> 75 % der gesamten Transaktionen werden auf chipfähigen Geräten verarbeitet[1] ODER
	an > 75 % der Standorte der Akzeptanzpartner werden Technologien zur Risikominderung eingesetzt[2]
Erweiterte Reduzierung: 75 % bis 100 %	> 75 % der gesamten Transaktionen werden auf chipfähigen Geräten verarbeitet[1] UND an > 75 % der Standorte der Akzeptanzpartner werden Technologien zur Risikominderung eingesetzt[2]

[1] gemäß internen Analysen von American Express

[2] gemäß PFI-Untersuchung

- Die erweiterte Reduzierung (75 % bis 100 %) errechnet sich aus dem Prozentsatz der Transaktionen, die über chipfähige Geräte erfolgten, UND der Standorte der Akzeptanzpartner, an denen eine andere Technologie zur Risikominderung eingesetzt wurde, wobei der niedrigere Prozentsatz maßgeblich ist. Die folgenden Beispiele veranschaulichen die Berechnung der Reduzierung der Schadensersatzverpflichtung.
- Damit die Nutzung einer Technologie zur Risikominderung geltend gemacht werden kann, müssen Sie eine effektive Nutzung derselben in Übereinstimmung mit ihrer Gestaltung und Zweckbestimmung nachweisen. Beispielsweise ist nach einer Implementierung von chipfähigen Geräten die Verarbeitung von Chipkartentransaktionen auf manuellem Weg oder über Magnetstreifen KEINE effektive Nutzung dieser Technologie.
- Der Prozentsatz der Standorte, die eine Technologie zur Risikominderung einsetzen, wird anhand der PFI-Untersuchung ermittelt.
- Die Reduzierung der Schadensersatzverpflichtung gilt nicht für möglichen Schadensersatz wegen Nichteinhaltung von Vorschriften, die in Verbindung mit dem Datenvorfall zu zahlen sind.

Tabelle A-3: Erweiterte Reduzierung der Schadensersatzverpflichtung

Bsp.	Einsatz von Technologien zur Risikominderung	Erfüllt	Reduzierung
1	80 % der Transaktionen erfolgen über chipfähige Geräte	Nein	50 %: Standardreduzierung (wird bei weniger als 75 % der Transaktionen eine Technologie zur Risikominderung eingesetzt, sind die Voraussetzungen für eine erweiterte Reduzierung nicht gegeben)[1]
	0 % der Standorte verwenden eine andere Technologie zur Risikominderung		

Bsp.	Einsatz von Technologien zur Risikominderung	Erfüllt	Reduzierung
2	80 % der Transaktionen erfolgen über chipfähige Geräte 77 % der Standorte verwendet eine andere Technologie zur Risikominderung	Ja	77 %: erweiterte Reduzierung (da bei 77 % der Transaktionen eine Technologie zur Risikominderung eingesetzt wurde)
3	93 % der Transaktionen erfolgen über chipfähige Geräte 100 % der Standorte verwenden eine andere Technologie zur Risikominderung	Ja	93 %: erweiterte Reduzierung (da 93 % der Transaktionen über chipfähige Geräte erfolgten)
4	40 % der Transaktionen erfolgen über chipfähige Geräte 90 % der Standorte verwenden eine andere Technologie zur Risikominderung	Nein	50 %: Standardreduzierung (erfolgen weniger als 75 % der Transaktionen über chipfähige Geräte, sind die Voraussetzungen für eine erweiterte Reduzierung nicht gegeben)

[1] Bei einem Datenvorfall mit 10.000 betroffenen American Express Kartenkonten in Höhe von 5 USD je Kontonummer (10.000 x 5 USD = 50.000 USD) kann eine Reduzierung von 50 % infrage kommen. Damit würde die Schadensersatzverpflichtung von 50.000 USD auf 25.000 USD sinken, ausschließlich eines eventuell anfallenden Schadensersatzes wegen Nichteinhaltung von Vorschriften.

Abschnitt 5 Wichtige periodische Validierung Ihrer Systeme

Sie müssen – wie nachfolgend beschrieben – jährlich und alle 90 Tage die folgenden Maßnahmen ausführen, um den Status der von Ihnen und Ihren Franchisenehmern verwendeten Geräte, Systeme und/oder Netzwerke (und der zugehörigen Komponenten), in denen Karteninhaber- oder vertrauliche Authentifizierungsdaten gespeichert, verarbeitet oder übertragen werden, gemäß dem PCI-DSS zu validieren.

Für die Validierung sind die vier folgenden Maßnahmen erforderlich:

Maßnahme 1: Teilnahme am PCI-Compliance-Programm von American Express (dem „Programm“) im Rahmen dieser Richtlinie

Maßnahme 2: Einstufung als Akzeptanzpartner und Bestimmung der Validierungsanforderungen

Maßnahme 3: Ausfüllen der bei American Express einzureichenden Validierungsdokumentation

Maßnahme 4: Übermittlung der Validierungsdokumentation an American Express innerhalb des dafür vorgesehenen zeitlichen Rahmens

Maßnahme 1: Teilnahme am American Express Compliance-Programm im Rahmen dieser Richtlinie

Akzeptanzpartner der Stufe 1 und 2 und alle Dienstleister, wie unten beschrieben, müssen im Rahmen dieser Richtlinie an dem Programm teilnehmen. Unter Umständen kann American Express nach eigenem Ermessen bestimmte Akzeptanzpartner der Stufen 3 und 4 gemäß dieser Richtlinie zur Teilnahme an dem Programm anweisen.

Zur Teilnahme an dem Programm verpflichtete Akzeptanzpartner und Dienstleister müssen sich innerhalb der vorgeschriebenen Frist auf dem Portal anmelden, das von dem von American Express ausgewählten Programmadministrator zur Verfügung gestellt wird.

- Sie müssen alle angemessenen Geschäftsbedingungen in Verbindung mit der Nutzung des Portals akzeptieren.
- Sie müssen korrekte Informationen für mindestens einen Ansprechpartner für die Datensicherheit auf dem Portal zuweisen und angeben. Die folgenden Datenelemente sind erforderlich:
  - Vor- und Nachname
  - E-Mail-Adresse
  - Telefonnummer
  - physische Anschrift
- Wenn sich diese Informationen ändern, müssen Sie aktualisierte oder neue Kontaktdaten für den zugewiesenen Ansprechpartner für die Datensicherheit auf dem Portal bereitstellen.
- Sie müssen sicherstellen, dass Ihre Systeme aktualisiert werden, um Dienstmitteilungen von der dem Portal zugewiesenen Domäne zuzulassen.

Wenn Sie keine aktuellen Informationen über Ihren Ansprechpartner für die Datensicherheit bereitstellen oder pflegen oder keine E-Mail-Mitteilungen aktivieren, hat dies keine Auswirkungen auf unsere Rechte, Gebühren zu veranschlagen.

Maßnahme 2: Einstufung als Akzeptanzpartner und Bestimmung der Validierungsanforderungen

Es gibt vier Stufen für Akzeptanzpartner und zwei Stufen für Dienstleister. Die Einteilung der Stufen richtet sich nach dem Umfang Ihrer mit American Express Karten abgewickelten Transaktionen.

- Für Akzeptanzpartner ist dies das von ihren Akzeptanzstellen übermittelte Volumen an Transaktionen, das für das Erreichen der höchsten Akzeptanzpartner-Stufe bei American Express maßgeblich ist.*
- Für Dienstleister ist dies der Gesamtbetrag des von den Dienstleistern und Unternehmensdienstleistern, für die Sie Dienstleistungen erbringen, übermittelten Volumens an Transaktionen.

Buyer-Initiated-Payments(BIP)-Transaktionen sind nicht im Umfang der American Express Kartentransaktionen enthalten, die der Bestimmung der Akzeptanzpartnerstufe und der Validierungsanforderungen dienen.
Die Zuordnung erfolgt gemäß einer der in den folgenden Tabellen angegebenen Stufen für Akzeptanzpartner und Dienstleister.

* Im Fall von Franchisegebern ist hierin der Umsatz aus den Franchisebetrieben enthalten. Franchisegeber, die ihren Franchisenehmern die Nutzung eines bestimmten Point-of-Sale(POS)-Systems oder Dienstleisters vorschreiben, müssen die Validierungsdokumentation auch für die betroffenen Franchisenehmer einreichen.

Anforderungen an die Akzeptanzpartner-Validierungsdokumentation

Für Akzeptanzpartner (nicht für Dienstleister) gibt es vier mögliche Akzeptanzpartner-Einstufungen. Nach Bestimmung der Akzeptanzpartner-Stufe anhand der folgenden Liste können Sie die entsprechenden Anforderungen für die Validierungsdokumentation Tabelle A-4: Akzeptanzpartner-Validierungsdokumentation entnehmen.

- **Akzeptanzpartner Stufe 1** – mindestens 2,5 Millionen American Express Kartentransaktionen pro Jahr oder jeder andere Akzeptanzpartner, den American Express nach eigenem Ermessen der Stufe 1 zuordnet.
- **Akzeptanzpartner Stufe 2** – 50.000 bis 2,5 Millionen American Express Kartentransaktionen pro Jahr.
- **Akzeptanzpartner Stufe 3** – 10.000 bis 50.000 American Express Kartentransaktionen pro Jahr.
- **Akzeptanzpartner Stufe 4** – weniger als 10.000 American Express Kartentransaktionen pro Jahr.

Tabelle A-4: Akzeptanzpartner-Validierungsdokumentation

Akzeptanzpartner-Stufe/Jährliche American Express Transaktionen	Compliance-Bericht – Compliance-Bescheinigung (ROC AOC)	Fragebogen zur Compliance-Bescheinigung (SAQ AOC) UND vierteljährlicher externer Netzwerk-Schwachstellenscan (Scan)	STEP-Nachweis für qualifizierte Akzeptanzpartner
Stufe 1/ 2,5 Mio. oder mehr	Obligatorisch	Nicht zutreffend	Optional mit Genehmigung durch American Express (ersetzt ROC)
Stufe 2/ 50.000 bis 2,5 Mio.	Optional	SAQ AOC obligatorisch (außer bei Einreichung eines/einer ROC AOC); Scan bei bestimmten Arten von SAQ obligatorisch	Optional (ersetzt SAQ und Netzwerkscan oder ROC)
Stufe 3/ 10.000 bis 50.000	Optional	SAQ AOC optional (obligatorisch, falls von American Express gefordert); Scan bei bestimmten Arten von SAQ obligatorisch	Optional (ersetzt SAQ und Netzwerkscan oder ROC)
Stufe 4/ 10.000 oder weniger	Optional	SAQ AOC optional (obligatorisch, falls von American Express gefordert); Scan bei bestimmten Arten von SAQ obligatorisch	Optional (ersetzt SAQ und Netzwerkscan oder ROC)

* Zur Klarstellung: Akzeptanzpartner der Stufen 3 und 4 brauchen keine Validierungsdokumentation einzureichen, sofern dies nicht von American Express anderweitig vorgeschrieben wird. Sie unterliegen aber dennoch einer Haftungsverpflichtung gemäß allen anderen Bestimmungen dieser Allgemeinen Datensicherheitsrichtlinien.

American Express behält sich das Recht vor, die Vollständigkeit, Richtigkeit und Angemessenheit Ihrer PCI-Validierungsdokumentation zu überprüfen. American Express verpflichtet Sie gegebenenfalls, zusätzliche stützende Unterlagen zur Auswertung für diesen Zweck vorzulegen. Des Weiteren ist American Express berechtigt, von Ihnen zu verlangen, dass Sie einen vom PCI Security Standards Council (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) genehmigten QSA oder PFI verpflichten.

Security Technology Enhancement Programme (STEP)

Akzeptanzpartner, die den PCI-DSS einhalten, sind im Ermessen von American Express zur Teilnahme am American Express STEP-Programm berechtigt, wenn sie während der gesamten Kartenverarbeitungsprozesse bestimmte zusätzliche Sicherheitstechnologien einsetzen. Für das STEP-Programm kommen nur Akzeptanzpartner in Frage, bei denen in den letzten 12 Monaten kein Datenvorfall aufgetreten ist und die 75 % aller Akzeptanzpartner-Kartentransaktionen unter Verwendung einer Kombination der folgenden erweiterten Sicherheitsoptionen abgewickelt haben:

- **EMV-Technologie, EMV-Kontaktlos-Technologie oder Digital Wallet** – auf einem aktiven chipfähigen Gerät mit einer gültigen und aktuellen EMVCo-Zulassung/-Zertifizierung (www.emvco.com), das AEIPS-konforme Chipkartentransaktionen verarbeiten kann. (US-Akzeptanzpartner müssen auch eine kontaktlose Zahlung anbieten.)
- **Point-to-Point-Verschlüsselung (P2PE)** – über ein vom PCI SSC zugelassenes oder durch einen QSA genehmigtes Point-to-Point-Verschlüsselungssystem an den Processor des Akzeptanzpartners übermittelt
- **Tokenisiert** – Die implementierte Tokenisierungslösung muss die folgenden Voraussetzungen erfüllen:
  - Sie muss die EMVCo-Spezifikationen erfüllen;
  - sie muss von einem PCI-konformen externen Dienstleister gesichert, verarbeitet, übertragen und zu hundert Prozent verwaltet werden, und
  - das Token kann nicht aufgelöst werden, um dem Akzeptanzpartner nicht maskierte Kartennummern (PANs) anzuzeigen.

Für Akzeptanzpartner, die die Voraussetzungen für das STEP-Programm erfüllen, gelten geringere Anforderungen bezüglich der PCI-Validierungsdokumentation, wie weiter unten in Maßnahme 3: „Ausfüllen der bei American Express einzureichenden Validierungsdokumentation“ näher beschrieben.

Dienstleister-Anforderungen

Für Dienstleister (nicht für Akzeptanzpartner) gibt es zwei mögliche Einstufungen. Nach Bestimmung der Dienstleister-Stufe anhand der folgenden Liste können Sie die entsprechenden Anforderungen für die Validierungsdokumente Tabelle A-5: Dienstleisterdokumentation entnehmen.

Dienstleister Stufe 1 – mindestens 2,5 Millionen American Express Kartentransaktionen pro Jahr oder jeder andere Dienstleister, den American Express der Stufe 1 zuordnet.

Dienstleister Stufe 2 – weniger als 2,5 Millionen American Express Kartentransaktionen pro Jahr oder Dienstleister, die American Express nicht der Stufe 1 zuordnet.

Dienstleister können nicht am STEP-Programm teilnehmen.

Tabelle A-5: Dienstleisterdokumentation

Stufe	Validierungsdokumentation	Anforderung
1	Jährlicher Compliance-Bericht – Compliance-Bescheinigung (ROC AOC)	Obligatorisch
2	Jährlicher SAQ D (Dienstleister) und vierteljährlicher Netzwerkscan oder Jährlicher Compliance-Bericht – Compliance-Bescheinigung (ROC AOC) (falls bevorzugt)	Obligatorisch

Für Dienstleister wird empfohlen, auch die ergänzenden PCI-Validierungsanforderungen für designierte Unternehmen zu erfüllen.

Maßnahme 3: Ausfüllen der bei American Express einzureichenden Validierungsdokumentation

Folgende Dokumente sind für die verschiedenen Akzeptanzpartner- und Dienstleister-Stufen erforderlich (siehe oben in den Tabellen „Akzeptanzpartner“ und „Dienstleister“).

Sie müssen die Compliance-Bescheinigung (AOC) für die jeweilige Bewertungsart bereitstellen. Die AOC ist eine Erklärung Ihres Compliance-Status und muss somit von der zuständigen Führungsebene Ihres Unternehmens unterzeichnet und datiert werden.

Zusätzlich zu dieser AOC kann American Express von Ihnen verlangen, dass Sie eine Kopie der vollständigen Bewertung und, nach unserem Ermessen, weitere stützende Unterlagen vorlegen, aus denen die Erfüllung der PCI-DSS-Anforderungen hervorgeht. Diese Validierungsdokumentation wird auf Ihre Kosten ausgefüllt.

Compliance-Bericht – Compliance-Bescheinigung (ROC AOC) – (jährliche Anforderung) – Der Compliance-Bericht dokumentiert die Ergebnisse einer detaillierten Vor-Ort-Sicherheitsprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), in denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden. Es gibt zwei Versionen: eine für Akzeptanzpartner und eine andere für Dienstleister. Der Compliance-Bericht muss angefertigt werden von:

- einem QSA oder
- von Ihnen selbst, und er muss von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Hauptverantwortlichen bescheinigt werden.

Die AOC muss von einem QSA oder einem Internal Security Assessor (ISA) sowie der bevollmächtigten Führungsebene Ihres Unternehmens unterzeichnet und datiert und American Express mindestens einmal jährlich zur Verfügung gestellt werden.

Fragebogen „Self-Assessment“ – Compliance-Bescheinigung (SAQ AOC) – (jährliche Anforderung) – Der Fragebogen „Self-Assessment“ ermöglicht eine Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), auf denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden. Es gibt mehrere Versionen des SAQ. Je nach Ihrer Karteninhaberdatenumgebung wählen Sie eine oder mehrere Versionen aus.

Der SAQ kann von Mitarbeitern Ihres Unternehmens ausgefüllt werden, die zur korrekten und sorgfältigen Beantwortung der Fragen qualifiziert sind, oder Sie können einen QSA hinzuziehen. Die AOC muss von der bevollmächtigten Führungsebene Ihres Unternehmens unterzeichnet und datiert und American Express mindestens einmal jährlich zur Verfügung gestellt werden.

Approved Scanning Vendor External Network Vulnerability Scan Summary – Zusammenfassung des externen Netzwerk-Schwachstellenscans (ASV-Scan) – (90-Tage-Anforderung) – Ein externer Schwachstellenscan ist ein Remote-Test zur Identifizierung potenzieller Sicherheitsrisiken, Schwachstellen und Fehlkonfigurationen von das Internet nutzenden Komponenten Ihrer Karteninhaberdatenumgebung (z. B. Websites, Anwendungen, Webserver, E-Mail-Server, öffentliche Domänen oder Hosts).

Der ASV-Scan muss von einem Approved Scanning Vendor (ASV) durchgeführt werden.

Wenn der SAQ dies erfordert, müssen die Bescheinigung ASV Scan Report Attestation of Scan Compliance (AOSC) oder eine Zusammenfassung mit Angabe der Zahl der gescannten Ziele, eine Zertifizierung, dass die Ergebnisse den PCI-DSS-Scanverfahren entsprechen, und der vom ASV anzugebende Compliance-Status mindestens einmal alle 90 Tage bei American Express eingereicht werden.

ROC AOC oder STEP müssen keine AOSC und keinen ASV-Scan enthalten, außer wenn diese ausdrücklich angefordert werden. Zur Klarstellung: Scans sind vorgeschrieben, wenn sie in dem jeweiligen SAQ angefordert werden.

Validierungsdokumentation im Rahmen des STEP-Nachweises (STEP) – (jährliche Anforderung) – Das STEP steht nur Akzeptanzpartnern zur Verfügung, die die in Maßnahme 2: „Einstufung als Akzeptanzpartner und Bestimmung der Validierungsanforderungen“ weiter oben angegebenen Kriterien erfüllen. Wenn Ihr Unternehmen die geltenden Qualifizierungsanforderungen erfüllt, müssen Sie das STEP-Nachweisformular ausfüllen und jährlich bei American Express einreichen. Das Formular für den jährlichen STEP-Nachweis steht auf dem Portal zum Download zur Verfügung.

Nichteinhaltung des PCI-DSS – (jährlich, 90 Tage und/oder Ad-Hoc-Anforderung) – Wenn Sie den PCI-DSS nicht einhalten, müssen Sie eines der folgenden Dokumente einreichen:

- eine Compliance-Bescheinigung (AOC) einschl. „Teil 4. Maßnahmenplan für Nicht-Compliance-Status“ (Download über die Website des PCI Security Standards Council)
- eine „PCI Prioritised Approach Tool Summary“ (Download über die Website des PCI Security Standards Council)
- eine Projektplanvorlage (Download über das Portal). Ein Projektplan kann anstelle des jährlichen Nachweises (SAQ/ROC) und/oder anstelle der Scananforderung eingereicht werden.

Jedes der oben genannten Dokumente muss ein Datum für eine entsprechende Korrektur angeben, das innerhalb von zwölf (12) Monaten ab dem Fertigstellungsdatum des Dokuments liegt, damit die Einhaltung der Vorschriften sichergestellt ist. Sie müssen American Express regelmäßig über Ihre aktuellen Fortschritte bei der Korrektur Ihres „Non-Compliant Status“ informieren (Akzeptanzpartner der Stufen 1, 2, 3 und 4; alle Dienstleister).

Alle zur Herbeiführung der Compliance mit dem PCI-DSS erforderlichen Maßnahmen werden auf Ihre Kosten ausgeführt.

American Express erhebt für die Nichteinhaltung vor dem angegebenen Korrekturdatum keine Vertragsstrafen für eine Nichtvalidierung (Beschreibung siehe unten), was Sie jedoch nicht von jeglichen Schadensersatzverpflichtungen für einen Datenvorfall gegenüber American Express befreit; weiterhin unterliegen Sie allen anderen Bestimmungen dieser Richtlinien.

Zur Klarstellung: Akzeptanzpartner, die den PCI-DSS nicht einhalten, können nicht am STEP-Programm teilnehmen.

Maßnahme 4: Übermittlung der Validierungsdokumentation an American Express

Alle Akzeptanzpartner und Dienstleister, die zur Teilnahme am American Express PCI-Complianceprogramm verpflichtet sind, müssen die in den Tabellen in Maßnahme 2: „Einstufung als Akzeptanzpartner und Bestimmung der Validierungsanforderungen“ als „obligatorisch“ gekennzeichnete Validierungsdokumentation innerhalb der geltenden Frist bei American Express einreichen.

Sie müssen Ihre Validierungsdokumentation über das Portal bei American Express einreichen, das von dem von American Express ausgewählten Programmadministrator zur Verfügung gestellt wird. Mit dem Einreichen der Validierungsdokumentation erklären und versichern Sie gegenüber American Express (soweit Ihnen das möglich ist), dass Folgendes zutrifft:

- Ihre Beurteilung war vollständig und wurde sorgfältig durchgeführt;
- der PCI-DSS-Status wurde zum Zeitpunkt der Anfertigung der Dokumentation korrekt als Compliance-Status oder Nicht-Compliance-Status angegeben;
- Sie sind berechtigt, die darin enthaltenen Informationen offenzulegen und stellen die Validierungsdokumentation American Express zur Verfügung, ohne damit die Rechte anderer zu verletzen.

Vertragsstrafen bei Nichtvalidierung und Kündigung des Vertrags

American Express hat das Recht, Vertragsstrafen für eine Nichtvalidierung zu erheben und den Vertrag zu kündigen, wenn Sie diese Anforderungen nicht einhalten oder die obligatorische Validierungsdokumentation nicht innerhalb der gültigen Frist bei American Express einreichen. Sie werden von American Express über die jeweils geltenden Fristen für jeden Jahres- und Quartalsberichtszeitraum gesondert informiert.

Tabelle A-6: Vertragsstrafe für eine Nichtvalidierung

Beschreibung*	Akzeptanzpartner oder Dienstleister, Stufe 1	Akzeptanzpartner oder Dienstleister, Stufe 2	Akzeptanzpartner, Stufe 3 oder 4
Wenn die Validierungsdokumentation nicht innerhalb der ersten Frist eingeht, wird eine entsprechende Vertragsstrafe erhoben.	USD 25.000	USD 5.000	USD 50
Wenn die Validierungsdokumentation nicht innerhalb der zweiten Frist eingeht, wird eine zusätzliche Vertragsstrafe erhoben.	USD 35.000	USD 10.000	USD 100
Wenn die Validierungsdokumentation nicht innerhalb der dritten Frist eingeht, wird eine zusätzliche Vertragsstrafe erhoben. **HINWEIS:** Vertragsstrafen für eine Nichtvalidierung werden so lange erhoben, bis die Validierungsdokumentation eingereicht wird.	USD 45.000	USD 15.000	USD 250

* Vertragsstrafen für Nichtvalidierung werden in der entsprechenden Landeswährung festgesetzt.

* Gilt nicht in Argentinien.

Wenn Ihre Verpflichtungen bezüglich der Validierungsdokumentation nach dem PCI-DSS nicht erfüllt werden, ist American Express berechtigt, die Vertragsstrafen für eine Nichtvalidierung kumulativ zu erheben, Zahlungen zurückzuhalten und/oder den Vertrag zu kündigen.

Abschnitt 6 Vertraulichkeit

American Express wird angemessene Maßnahmen treffen (und seine Agenten und Subunternehmer, einschließlich des Portalanbieters, entsprechend anweisen), um die von Ihnen eingereichten Complianceberichte, einschließlich der Validierungsdokumentation, vertraulich zu behandeln, und die Validierungsdokumentation für einen Zeitraum von drei Jahren ab dem Datum des Eingangs der Dokumente nicht an Dritte (die nicht zu den American Express Verbundenen Unternehmen, Bevollmächtigten, Agenten, Dienstleistern und Subunternehmern gehören) weiterzugeben. Diese Vertraulichkeitsverpflichtung gilt jedoch nicht für Validierungsdokumente, die:

a. American Express bereits vor der Offenlegung durch Sie bekannt waren;

b. ohne eine Verletzung der Bestimmungen dieses Absatzes durch American Express der Öffentlichkeit bereits zugänglich sind oder noch zugänglich gemacht werden;

c. American Express rechtmäßig von einem Dritten ohne eine Vertraulichkeitsverpflichtung erhalten hat;

d. American Express unabhängig entwickelt hat oder

e. auf Anordnung eines Gerichts, einer Verwaltungs- oder Regierungsbehörde oder aufgrund eines Gesetzes, einer Gesetzesbestimmung oder einer sonstigen Vorschrift oder aufgrund einer Zeugenvorladung, einer Aufforderung zur Urkundenvorlegung, einer Ladung oder eines sonstigen Verwaltungs- oder Rechtsverfahrens oder einer sonstigen formellen oder informellen Befragung oder Ermittlung seitens einer Regierungsstelle oder -behörde (einschließlich einer Aufsichtsbehörde, einer Kontrollstelle, einer Prüfstelle oder einer Vollstreckungsbehörde) offengelegt werden müssen.

Abschnitt 7 Haftungsausschluss

AMERICAN EXPRESS LEHNT HIERMIT ALLE AUSDRÜCKLICHEN, STILLSCHWEIGENDEN, GESETZLICHEN ODER ANDERWEITIGEN ZUSICHERUNGEN, GEWÄHRLEISTUNGEN UND HAFTUNGSVERPFLICHTUNGEN IN BEZUG AUF DIESE ALLGEMEINEN DATENSICHERHEITSRICHTLINIEN, DIE PCI-DSS, DIE EMV-SPEZIFIKATIONEN UND DIE ERNENNUNG UND LEISTUNG VON QSA, ASV ODER PFI (ODER EINER DIESER PERSONEN) AB, EINSCHLIESSLICH JEGLICHER GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT ODER DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK. HERAUSGEBER VON AMERICAN EXPRESS KARTEN SIND KEINE DRITTBEGÜNSTIGTEN GEMÄSS DIESEN RICHTLINIEN.

Hilfreiche Websites

American Express Data Security: www.americanexpress.com/datasecurity

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

Glossar

Die folgenden Begriffsdefinitionen gelten ausschließlich im Rahmen dieser Allgemeine Datensicherheitsrichtlinien (Data Security Operating Policy, DSOP) und sind im Falle von Widersprüchen zu den Begriffen in den *Regularien für Akzeptanzpartner* maßgebend

American Express Karte oder **Karte** bezeichnet jede Karte, jedes Kontozugriffsgerät bzw. alle Zahlungsgeräte und -dienste, die den Namen, das Logo, die Marke, die Dienstleistungsmarke, den Handelsnamen oder andere urheberrechtlich geschützte Bezeichnungen oder Gestaltungsmerkmale von American Express bzw. einem seiner Verbundenen Unternehmen oder eine Kontonummer aufweisen und die von einem Kartenherausgeber ausgestellt wurden, oder eine Kartenkontonummer.

Genehmigte Point-to-Point-Verschlüsselungs(P2PE)-Lösung ist auf der PCI-SSC-Liste validierter Lösungen enthalten oder wurde von einem „PCI SSC Qualified Security Assessor P2PE"-Unternehmen validiert.

Approved Scanning Vendor (ASV) bezeichnet ein vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) zugelassenes Unternehmen, das die Einhaltung bestimmter PCI-DSS-Anforderungen validiert, indem es Umgebungen mit Internetanschluss auf potenzielle Schwachstellen überprüft.

Compliance-Bescheinigung (AOC) ist die Konformitätsbescheinigung für die Statuserklärung zur Einhaltung des PCI-DSS in der vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) zur Verfügung gestellten Form.

Attestation of Scan Compliance (AOSC) ist eine Compliance-Bescheinigung für die Statuserklärung zur Einhaltung des PCI-DSS basierend auf einem Netzwerkscan und in der vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) zur Verfügung gestellten Form.

Buyer-Initiated-Payment(BIP)-Transaktionen sind Zahlungstransaktionen, die über eine über BIP verarbeitete Zahlungsanweisungsdatei ermöglicht werden.

Karteninhaberdaten ist im jeweils geltenden Begriffsglossar für den PCI-DSS definiert.

Karteninhaberdatenumgebung (CDE) bezeichnet die Personen, Prozesse und Technologien zur Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten oder vertraulichen Authentifizierungsdaten.

Karteninhaber bezeichnet eine natürliche oder juristische Person, (i) die mit einem Kartenherausgeber einen Vertrag zur Einrichtung eines Kartenkontos abgeschlossen hat oder (ii) deren Name auf der Karte erscheint.

Karteninhaberinformationen sind Informationen über American Express Karteninhaber und Kartentransaktionen, einschließlich Namen, Adressen, Kartennummern und Kartenprüfziffern (CID).

Kartennummer bezeichnet die eindeutige Identifikationsnummer, die der Kartenherausgeber bei der Ausstellung zuweist.

Belastung bezeichnet eine unter Verwendung der Karte vorgenommene Zahlung für eine Leistung.

Chip bezeichnet einen in eine Karte integrierten Mikrochip, der bestimmte Karteninhaber- und Kontodaten enthält.

Chipkarte bezeichnet eine Karte mit Chip, bei der die Eingabe einer PIN zwecks Überprüfung der Identität des Karteninhabers oder der auf dem Chip gespeicherten Kontoinformationen (oder beides) erforderlich sein kann; wird in unseren Materialien manchmal auch als „Smart-Karte“, „EMV-Karte“ oder „ICC-Karte“ („Integrated Circuit Card“) bezeichnet.

Chipfähiges Gerät bezeichnet ein POS-Gerät mit einer gültigen und aktuellen EMVCo-Zulassung/-Zertifizierung (siehe www.emvco.com), das AEIPS-konforme Chipkartentransaktionen verarbeiten kann.

Kompromittierte Kartennummer bezeichnet eine American Express Kontonummer, die in einen Datenvorfall involviert ist.

Eingeschaltete Dritte bezeichnet Ihre Mitarbeiter, Bevollmächtigten, Agenten, Subunternehmer, Processor, Dienstleister, Anbieter Ihrer POS-Geräte oder -Systeme oder Zahlungsabwicklungslösungen, mit Ihrem American Express Akzeptanzpartnerkonto verbundene Einrichtungen sowie jede sonstige Partei, der Sie nach Maßgabe des Vertrags Zugang zu Karteninhaberinformationen gewähren.

Gutschrift ist der Betrag der Belastung, den Sie Karteninhabern für mit der Karte abgewickelte Einkäufe oder Zahlungen im Fall der Rückabwicklung des Einkaufs oder der Zahlung erstatten.

Datenvorfall bezeichnet einen vermuteten oder tatsächlichen Zwischenfall, bei dem die American Express Verschlüsselungscodes oder eine oder mehrere Karten- oder Kontennummern von American Express Karten kompromittiert wurden. Als Datenvorfall gilt:

- der nicht autorisierte Zugriff auf oder die nicht autorisierte Verwendung von Verschlüsselungscodes, Karteninhaber- und/oder vertraulichen Authentifizierungsdaten (oder eine Kombination daraus), die auf den von Ihnen oder auf Ihre Anweisung hin genutzten Geräten, Systemen und/oder Netzwerken (bzw. den zugehörigen Komponenten) gespeichert, verarbeitet oder übertragen werden;
- die Nutzung der Verschlüsselungscodes, Karteninhaber- bzw. vertraulichen Authentifizierungsdaten (oder einer Kombination daraus) entgegen den Vertragsbedingungen und/oder
- der vermutete oder bestätigte Verlust oder Diebstahl oder jegliche widerrechtliche Verwendung von Medien, Materialien, Datensätzen oder Informationen, die solche Verschlüsselungscodes oder Karteninhaber- bzw. vertraulichen Authentifizierungsdaten (oder eine Kombination daraus) beinhalten.

Datenvorfall-Zeitfenster bezeichnet den Zeitraum des unbefugten Zugriffs (oder einen auf ähnliche Weise definierten Zeitraum), der im forensischen Abschlussbericht (z. B. dem PFI-Bericht) festgelegt ist. Wenn dieser Zeitraum nicht bekannt ist, bezieht sich der Begriff auf einen Zeitraum von bis zu 365 Tagen vor dem letzten Datum der Benachrichtigung über potenziell Kompromittierte Kartennummern, die an einer uns gemeldeten Datenkompromittierung beteiligt waren.

EMV-Spezifikationen sind die von EMVCo, LLC, herausgegebenen Spezifikationen, die unter www.emvco.com abgerufen werden können.

EMV-Transaktion bezeichnet eine Transaktion, die mit einer „Integrated Circuit Card" (manchmal auch als „IC-Karte", „Chipkarte", „Smart-Karte", „EMV-Karte" oder „ICC" bezeichnet) an einem POS-Terminal mit IC-Kartenunterstützung und mit einer gültigen und aktuellen EMV-Typzulassung abgewickelt wurde. EMV-Typzulassungen sind verfügbar unter www.emvco.com.

Verschlüsselungscode (American Express Verschlüsselungscode) bezieht sich auf alle beim Verarbeiten, Generieren, Laden und/oder Schützen von Kontodaten verwendeten Codes. Dazu gehören u. a. die folgenden Codes:

- Hauptverschlüsselungscodes: Zone Master Keys (ZMKs) und Zone Pin Keys (ZPKs)
- auf sicheren Verschlüsselungsgeräten verwendete Hauptcodes: Local Master Keys (LMKs)
- Kreditkarten-Sicherheitscodeschlüssel (Card Security Code Keys, CSCKs)
- PIN-Schlüssel: Base Derivation Keys (BDKs), PIN Encryption Keys (PEKs) und ZPKs

Vorlage für forensische Abschlussberichte zu Datenvorfällen bezeichnet die vom PCI Security Standards Council verfügbare Vorlage, die auf www.pcisecuritystandards.org zu finden ist.

Franchisenehmer bezeichnet einen eigenständigen und unabhängig betriebenen Dritten (einschließlich eines Franchisenehmers, Lizenznehmers oder einer Untergruppe), der kein Verbundenes Unternehmen ist und der von einem Franchisegeber zum Betreiben eines Franchise lizenziert ist und der eine schriftliche Vereinbarung mit dem Franchisegeber getroffen hat, wonach er durchweg eine externe Identifikation wiedergibt, die sich deutlich mit den Marken des Franchisegebers identifiziert oder sich in der Öffentlichkeit als Mitglied der Unternehmensgruppe des Franchisegebers präsentiert.

Franchisegeber bezeichnet den Betreiber eines Unternehmens, das Personen oder Rechtspersonen (Franchisenehmer) zum Vertrieb von Waren und/oder Dienstleistungen oder zur Geschäftstätigkeit unter Verwendung der Marke des Betreibers lizenziert. Franchisegeber unterstützen ihre Franchisenehmer, von denen sie eine bestimmte Gebühr verlangen, bei der Ausübung ihrer Geschäfte bzw. haben Einfluss auf deren Geschäftsbetrieb.

Kartenherausgeber bezeichnet jede juristische Person (einschließlich American Express und seiner Verbundenen Unternehmen), die von American Express oder einem Verbundenen Unternehmen von American Express zur Ausstellung von Karten und zur Ausübung des Kartenausstellungsgeschäfts lizenziert wurde.

Akzeptanzpartner der Stufe 1 bezeichnet einen Akzeptanzpartner mit mindestens 2,5 Millionen American Express Kartentransaktionen pro Jahr oder jeden anderen Akzeptanzpartner, den American Express der Stufe 1 zuordnet.

Akzeptanzpartner der Stufe 2 bezeichnet einen Akzeptanzpartner mit 50.000 bis 2,5 Millionen American Express Kartentransaktionen pro Jahr.

Akzeptanzpartner der Stufe 3 bezeichnet einen Akzeptanzpartner mit 10.000 bis 50.000 American Express Kartentransaktionen pro Jahr.

Akzeptanzpartner der Stufe 4 bezeichnet einen Akzeptanzpartner mit weniger als 10.000 American Express Kartentransaktionen pro Jahr.

Dienstleister der Stufe 1 bezeichnet einen Dienstleister mit mindestens 2,5 Millionen American Express Kartentransaktionen pro Jahr oder jeden anderen Dienstleister, den American Express der Stufe 1 zuordnet.

Dienstleister der Stufe 2 bezeichnet einen Dienstleister mit weniger als 2,5 Millionen American Express Kartentransaktionen pro Jahr oder Dienstleister, die American Express nicht der Stufe 1 zuordnet.

Akzeptanzpartner bezeichnet den Akzeptanzpartner und alle seine Verbundenen Unternehmen, die American Express Karten im Rahmen eines Vertrags mit American Express oder seinen Verbundenen Unternehmen akzeptieren.

Akzeptanzpartner-Stufe ist die Bezeichnung, die wir Akzeptanzpartnern hinsichtlich ihrer Validierungsverpflichtungen zur Sicherstellung ihrer Compliance mit dem PCI-DSS zuweisen – siehe die Beschreibung in Abschnitt 5, „Wichtige periodische Validierung Ihrer Systeme“.

Benachrichtigungsdatum bezeichnet das Datum, an dem American Express den Kartenherausgebern eine abschließende Mitteilung über einen Datenvorfall sendet. Dieses Datum hängt vom Erhalt des endgültigen forensischen Berichts oder der internen Analyse durch American Express ab und wird nach alleinigem Ermessen von American Express bestimmt.

Zahlungsanwendung ist im jeweils aktuellen Glossar für den Secure Software Standard und den Secure Software Life Cycle Standard definiert – siehe www.pcisecuritystandards.org.

Payment Card Industry Data Security Standard (PCI DSS) ist der Datensicherheitsstandard der Zahlungskartenindustrie, verfügbar unter www.pcisecuritystandards.org.

Payment Card Industry Security Standards Council(PCI SSC)-Anforderungen bezeichnen den Satz von Standards und Anforderungen in Bezug auf die Sicherung und den Schutz von Zahlungskartendaten, einschließlich der PCI DSS und PA DSS, verfügbar unter www.pcisecuritystandards.org.

PCI-zugelassen bedeutet, dass ein PIN-Eingabegerät oder eine Zahlungsanwendung (oder beides) zum Zeitpunkt der Bereitstellung auf der Liste der vom PCI Security Standards Council, LLC zugelassenen Unternehmen und Anbieter erscheint, verfügbar unter www.pcisecuritystandards.org.

PCI DSS steht für Payment Card Industry Data Security Standard (Datensicherheitsstandard der Zahlungskartenindustrie), verfügbar unter www.pcisecuritystandards.org.

Forensischer Ermittler der Zahlungskartenindustrie (PFI) bezeichnet eine Organisation, die vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) zugelassen ist, um forensische Untersuchungen von Datensicherheitsverstößen oder der Kompromittierung von Zahlungskartendaten durchzuführen.

PCI-PIN-Sicherheitsanforderungen beziehen sich auf die Sicherheitsanforderungen gemäß Payment Card Industry PIN Security Requirements (PIN-Sicherheitsanforderungen der Zahlungskartenindustrie), verfügbar unter www.pcisecuritystandards.org.

PIN-Eingabegerät ist im aktuellen Begriffsglossar für die Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, definiert – verfügbar unter www.pcisecuritystandards.org.

Point-of-Sale(POS)-System bezeichnet ein Informationsverarbeitungssystem oder -gerät (darunter ein Terminal, ein PC, eine elektronische Registrierkasse, ein berührungsloses Lesegerät oder eine(n) Zahlungsmaschine/-prozess), das von einem Akzeptanzpartner genutzt wird, um Genehmigungen zu erhalten oder Transaktionsdaten zu erfassen (oder beides).

Point-to-Point-Verschlüsselung (P2PE) bezeichnet eine Lösung, die Kontodaten durch Verschlüsselung ab dem Punkt schützt, an dem ein Akzeptanzpartner die Zahlungskarte entgegennimmt, bis zum sicheren Punkt der Entschlüsselung.

Das **Portal** ist das Berichterstattungssystem, das von dem von American Express ausgewählten American Express PCI-Programmadministrator bereitgestellt wird. Akzeptanzpartner und Dienstleister müssen zum Einreichen ihrer PCI-Validierungsdokumentation bei American Express das Portal verwenden.

Kartennummer (Primary Account Number – PAN) hat die Bedeutung, mit der dieser Begriff im jeweils aktuellen Begriffsglossar für den PCI-DSS versehen ist.

Processor bezeichnet einen Dienstleister für Akzeptanzpartner zur Verarbeitung der Genehmigung und Übermittlung an das American Express Netzwerk.

Das **Programm** ist das American Express PCI-Compliance-Programm.

Qualified Security Assessor (QSA) bezeichnet eine vom Payment Card Industry Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenbranche) qualifizierte Organisation, die die Einhaltung des PCI-DSS validiert.

Technologien zur Risikominderung sind Technologielösungen zur Verbesserung der Sicherheit von American Express Karteninhaberdaten und vertraulichen Authentifizierungsdaten gemäß Vorgaben von American Express. Damit eine Technologie zur Risikominderung geltend gemacht werden kann, müssen Sie eine effektive Nutzung derselben in Übereinstimmung mit ihrer Gestaltung und Zweckbestimmung nachweisen. Beispiele sind u. a.: EMV, Point-to-Point-Verschlüsselung und Tokenisierung.

Security Technology Enhancement Programme (STEP) bezeichnet ein Programm von American Express, das Akzeptanzpartner zum Einsatz von Technologien zur Verbesserung der Datensicherheit anregen soll.

Fragebogen „Self-Assessment" (SAQ) ist ein vom Payment Card Industry Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenindustrie) entwickeltes Selbstbeurteilungsinstrument zum Zweck der Bewertung und Bestätigung der Einhaltung des PCI-DSS.

Vertrauliche Authentifizierungsdaten sind im jeweils geltenden Begriffsglossar für den PCI-DSS definiert.

Dienstleister sind autorisierte Processor, Fremd-Processor, Gateway-Anbieter, Integratoren von POS-Systemen und alle anderen Anbieter, die Akzeptanzpartnern POS-Systeme oder andere Zahlungsverarbeitungslösungen oder Dienstleistungen zur Verfügung stellen.

Programm für gezielte Analysen (Targeted Analysis Program, TAP) bezeichnet ein Programm, das die frühzeitige Identifizierung einer potenziellen Kompromittierung von Karteninhaberdaten in Ihrer Karteninhaberdatenumgebung (CDE) ermöglicht. Siehe Abschnitt 1, „Programm für gezielte Analysen (Targeted Analysis Program, TAP)".

Token ist das kryptografische Token, das die PAN ersetzt. Es basiert auf einem bestimmten Index für einen unvorhersagbaren Wert.

Transaktion bezeichnet eine mit einer Karte abgewickelte Belastung oder Gutschrift.

Validierungsdokumentation bezeichnet die eingereichte AOC-Bescheinigung in Verbindung mit einem Annual Onsite Security Assessment (Jährliche Vor-Ort-Sicherheitsprüfung) oder einem SAQ, der AOSC-Bescheinigung sowie Zusammenfassungen der in Verbindung mit vierteljährlichen Netzwerkscans oder dem jährlichen STEP-Nachweis eingereichten Ergebnisse.