AMERICAN EXPRESS

Allgemeine Datensicherheitsrichtlinien (DSOP)

Änderungssymbole

Wichtige Aktualisierungen sind in der Tabelle „Zusammenfassung der Änderungen“ aufgeführt und in den *DSOP* mit einem Änderungssymbol gekennzeichnet. Ein Änderungssymbol neben dem Titel eines Abschnitts oder Unterabschnitts kennzeichnet überarbeiteten, hinzugefügten oder entfernten Text aus dem Abschnitt oder Unterabschnitt. Änderungen in den *DSOP* werden wie hier gezeigt mit einem Änderungssymbol angezeigt.

Zusammenfassung der Änderungstabelle

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

Abschnitt/Unterabschnitt	Beschreibung der Änderung
Änderungssymbole	Sprache für Änderungssymbole hinzugefügt.
Zusammenfassung der Änderungstabelle	Zusammenfassung der Änderungstabelle hinzugefügt.
Abschnitt 1, „Kompromittierung von Karteninhaberdaten“	Programm bei Kompromittierung von Karteninhaberdaten hinzugefügt.
Abschnitt 3, „Verpflichtungen und Vorgehen bei einem Datenvorfall“	Der Zeitrahmen für die Benachrichtigung über Datenvorfälle wurde von 24 auf 72 Stunden erhöht.
Abschnitt 5, „Wichtige periodische Validierung Ihrer Systeme“	Tabelle der Vertragsstrafen aufgrund von Nichtvalidierung wurde aktualisiert. Vertragsstrafe für Akzeptanzpartner der Stufen 3 und 4 wurde erhöht, wenn die Validierungsdokumentation nicht fristgerecht eingeht.

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 unberechtigte Nutzung 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 besitzen die ihnen im Glossar am Ende dieser Richtlinie zugewiesene Bedeutung.

Abschnitt 1 Kompromittierung von Karteninhaberdaten

Sie sind verpflichtet – und müssen die von Ihnen eingeschalteten Dritten ebenfalls dazu verpflichten –, Datensicherheitslücken in Ihrer Karteninhaberdatenumgebung (Cardholder Data Environment, CDE) zu beurteilen und beheben, wenn American Express über eine mögliche Kompromittierung von Karteninhaberdaten informiert. 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 Einrichtungen stammen
- **Gefundene Kartendaten:** Daten von American Express Card und Karteninhabern, die im Internet gefunden wurden und mit Transaktionen in Ihren Einrichtungen verknüpft sind
- **Vermutete Malware:** American Express vermutet, dass Sie Software verwenden, die mit bösartigem Code infiziert oder für diesen anfällig ist

Ihre Verpflichtungen bei einer Kompromittierung von Karteninhaberdaten:

- 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 geplanten Maßnahmen Ihrer Überprüfungs-, Bewertungs- und/oder Korrekturmaßnahmen vorlegen
- Sie müssen aktualisierte PCI-DSS-Validierungsdokumente gemäß Abschnitt 5, „Wichtige periodische Validierung Ihrer Systeme“, Maßnahme 3: „Ausfüllen der bei American Express einzureichenden Validierungsdokumentation“ unten bereitstellen.
- Gegebenenfalls müssen Sie einen qualifizierten forensischen PCI-Ermittler (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.

American Express hat das Recht, Strafgebühren wegen Nichteinhaltung von Vorschriften zu erheben, Zahlungen zurückzuhalten und/oder den Vertrag zu kündigen, wenn Sie diesen Verpflichtungen nicht nachkommen.

Strafgebühren wegen Nichteinhaltung von Vorschriften bei einer Kompromittierung von Karteninhaberdaten

Beschreibung	Akzeptanzpartner oder Dienstleister, Stufe 1	Akzeptanzpartner oder Dienstleister, Stufe 2	Akzeptanzpartner, Stufe 3 oder Stufe 4
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird festgesetzt, wenn die Verpflichtungen bei einer Kompromittierung von Karteninhaberdaten nicht innerhalb von 45 Tagen ab dem Datum der Benachrichtigung erfüllt werden.	USD 25.000	USD 5.000	USD 1.000
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird festgesetzt, wenn die Verpflichtungen bei einer Kompromittierung von Karteninhaberdaten nicht innerhalb von 90 Tagen ab dem Datum der Benachrichtigung erfüllt werden.	USD 35.000	USD 10.000	USD 2.500
Die Strafgebühr wegen Nichteinhaltung von Vorschriften wird festgesetzt, wenn die Verpflichtungen bei einer Kompromittierung von Karteninhaberdaten nicht innerhalb von 120 Tagen ab dem Datum der Benachrichtigung erfüllt werden. **HINWEIS:** *Strafgebühren wegen Nichteinhaltung von Vorschriften können weiterhin monatlich erhoben werden, bis die Verpflichtungen erfüllt sind oder die* Kompromittierung von Karteninhaberdaten *behoben ist.*	USD 45.000	USD 15.000	USD 5.000

Wenn Ihre Verpflichtungen bei einer Kompromittierung von Karteninhaberdaten nicht innerhalb von 120 Tagen ab dem Datum der Benachrichtigung 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 vertraglich festgelegten 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) an unterstützten Standorten nur solche zu verwenden, die nach dem PCI-Standard 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 Kontonummern müssen Sie binnen fünf (5) Tagen nach der Entdeckung des jeweiligen Datenvorfalls für diese Untersuchung einen forensischen PCI-Ermittler (PFI) hinzuziehen.
- Der unveränderte forensische Ermittlungsbericht muss American Express innerhalb von zehn (10) Werktagen nach Fertigstellung vorliegen.
- Sie sind verpflichtet, American Express unverzüglich alle von einer unberechtigten Nutzung betroffenen Karten- oder Kontonummern zur Verfügung zu stellen. American Express behält sich das Recht vor, eigene interne Untersuchungen durchzuführen, um an dem Datenvorfall beteiligte Karten- oder Kontonummern 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-Standard 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“ gilt:

- 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 Kontonummern 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 das Zurverfügungstellen dieser Informationen), damit überprüft werden kann, ob Sie in der Lage sind, zukünftigen Datenvorfällen im Einklang mit dem Vertrag vorzubeugen.

Ungeachtet einer gegenteiligen vertraglichen Geheimhaltungspflicht hat American Express das Recht, American Express Karteninhaber, -herausgeber, andere am American Express Netzwerk Beteiligte und die allgemeine Öffentlichkeit gemäß den geltenden Gesetzen 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, sowie 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 Schadensersatzverpflichtungen gegenüber American Express bei einem Datenvorfall festgelegt.

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 Karten- oder Kontonummer verpflichtet.

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

- weniger als 10.000 American Express Karten- oder Kontonummern oder
- mehr als 10.000 American Express Karten- oder Kontonummern betroffen sind, wenn Sie die folgenden Bedingungen erfüllen:
  - Sie haben American Express den Datenvorfall gemäß diesem Abschnitt 4, „Schadensersatzverpflichtungen für einen Datenvorfall“, gemeldet;
  - Sie haben zum Zeitpunkt des Datenvorfalls den PCI-DSS-Standard (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 Kontonummern verpflichtet, American Express für jeden (von American Express nach eigenem Ermessen zu bestimmenden) Datenvorfall einen pauschalierten 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: Der für jeden einzelnen Datenvorfall bemessene pauschalierte Schadenersatz wegen Nichteinhaltung von Vorschriften wird auf 100.000 USD begrenzt.

American Express schließt aus seiner Berechnung alle American Express Karten- oder Kontonummern 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).

Bezüglich der pauschalierten Schadensersatzbeträge bleibt es Ihnen unbenommen, Nachweis dafür zu erbringen, dass American Express kein Schaden oder ein wesentlich geringerer Schaden als die Pauschale entstanden ist.

American Express kann nach eigenem Ermessen die Schadensersatzverpflichtung von Akzeptanzpartnern ausschließlich für Datenvorfälle reduzieren, wenn der Akzeptanzpartner 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:

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 eine 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 pauschalierten Schadensersatz wegen Nichteinhaltung von Vorschriften, der in Verbindung mit dem Datenvorfall zu zahlen ist.

Erweiterte Reduzierung der Schadensersatzverpflichtung

Bsp.	Einsatz von Technologien zur Risikominderung	Erfüllt	Reduzierung
1	80 % der Transaktionen erfolgen über chipfähige Geräte 0 % der Standorte verwendet eine andere Technologie zur Risikominderung	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]
2	80 % der Transaktionen erfolgen über chipfähige Geräte 77 % der Standorte verwenden 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 eventuell anfallenden pauschalierten Schadensersatz wegen Nichteinhaltung von Vorschriften.

Abschnitt 5 Wichtige periodische Validierung Ihrer Systeme

Sie müssen – wie nachfolgend beschrieben – jährlich und vierteljährlich 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 PCI-DSS-Standard zu validieren.

Für die Validierung sind die vier folgenden Maßnahmen erforderlich:

Maßnahme 1: Teilnahme am American Express Complianceprogramm im Rahmen dieser Richtlinie

Maßnahme 2: Einstufung Ihres Unternehmens 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 Complianceprogramm im Rahmen dieser Richtlinie

Akzeptanzpartner der Stufen 1 und 2 sowie alle Dienstleister, wie unten beschrieben, müssen im Rahmen dieser Richtlinie am PCI-Compliance-Programm von American Express teilnehmen und dabei den vollständigen Namen, die E-Mail-Adresse, Telefonnummer und Postanschrift einer Person angeben, die als ihr Ansprechpartner für die Datensicherheit fungieren wird. Sie müssen diese Informationen an SecureTrust, einer Division von Trustwave (https://portal.securetrust.com), den von American Express beauftragten Programmverwalter, übermitteln. Dazu ist eine der unten in Maßnahme 4: „Übermittlung der Validierungsdokumentation an American Express“ unten genannten Methoden an American Express zu übermitteln. Änderungen an diesen Informationen und ggf. aktualisierte Kontaktdaten sind SecureTrust mitzuteilen. Sollten Sie diese Kontaktdaten nicht zur Verfügung stellen, hat dies keine Auswirkungen auf unsere Rechte, gemäß den Angaben in der Tabelle Tabelle „Vertragsstrafen für Nichtvalidierung“ eine Gebühr für eine unterlassene Validierung zu veranschlagen.

Unter Umständen kann American Express nach eigenem Ermessen bestimmte Akzeptanzpartner der Stufen 3 und 4 schriftlich anweisen, gemäß dieser Richtlinie am Compliance-Programm von American Express teilzunehmen. Die betroffenen Akzeptanzpartner müssen sich spätestens 90 Tage nach Erhalt des Schreibens anmelden.

Maßnahme 2: Einstufung Ihres Unternehmens 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 Einrichtungen übermittelte Volumen an Transaktionen, das für das Erreichen der höchsten Akzeptanzpartner-Stufe bei American Express maßgeblich ist.* Die Zuordnung erfolgt gemäß einer der in den folgenden Tabellen angegebenen Stufen für Akzeptanzpartner und Dienstleister. Buyer-Initiated-Payments(BIP)-Transaktionen sind nicht im Umfang der American Express Kartentransaktionen enthalten, die der Bestimmung der Akzeptanzpartnerstufe und der Validierungsanforderungen dienen.

* 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.

Akzeptanzpartner-Anforderungen

Für Akzeptanzpartner (nicht Dienstleister) gibt es vier mögliche Einstufungen und Validierungsanforderungen. Nach Bestimmung der Akzeptanzpartner-Stufe anhand der folgenden Liste können Sie die entsprechenden Anforderungen für die Validierungsdokumente der unten stehenden Tabelle „Akzeptanzpartner“ 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 „Akzeptanzpartner“

	Validierungsdokumentation		
Akzeptanzpartner-Stufe/Jährliche American Express Transaktionen	Bericht über das Annual Onsite Assessment (ROC)	Fragebogen „Self-Assessment“ (SAQ) UND vierteljährlicher Netzwerkscan	STEP-Nachweis für qualifizierte Akzeptanzpartner
Stufe 1/ 2,5 Mio. oder mehr	Obligatorisch	Nicht zutreffend	Optional (ersetzt ROC)
Stufe 2/ 50.000 bis 2,5 Mio.	Optional	SAQ obligatorisch (außer bei Einreichung eines Onsite Assessment); Scan bei bestimmten Arten von SAQ obligatorisch	Optional (ersetzt SAQ und Netzwerkscan oder ROC)
Stufe 3/ 10.000 bis 50.000	Optional	SAQ 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 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 Richtigkeit und Angemessenheit der nach Bedarf bereitgestellten PCI-Validierungsdokumentation zu verifizieren, u. a. durch Verpflichtung eines QSA oder PFI auf Kosten und im Ermessen von American Express.

Security Technology Enhancement Programme (STEP)

Akzeptanzpartner, die den PCI-DSS-Standard 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 Kartentransaktionen folgendermaßen abgewickelt haben:

- **EMV-Technologie** – 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 Verarbeiter des Akzeptanzpartners übermittelt

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 Akzeptanzpartner) gibt es zwei mögliche Einstufungen und Validierungsanforderungen. Nach Bestimmung der Dienstleister-Stufe anhand der folgenden Liste können Sie die entsprechenden Anforderungen für die Validierungsdokumentationsanforderungen der Tabelle „Dienstleister“ 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 „Dienstleister“

Stufe	Validierungsdokumentation	Anforderung
1	Compliance-Bericht über das Annual Onsite Security Assessment	Obligatorisch
2	Jährlicher SAQ D (Dienstleister) und vierteljährlicher Netzwerkscan oder Compliance-Bericht über das Annual Onsite Security Assessment, falls gewünscht.	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“).

Annual Onsite Security Assessment – Bei dem Annual Onsite Security Assessment handelt es sich um eine detaillierte Vor-Ort-Sicherheitsprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), mit denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden. Die Sicherheitsprüfung muss durchgeführt werden von:

- einem QSA oder
- Ihnen selbst und muss anschließend von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Hauptverantwortlichen bestätigt und jährlich über die entsprechende Compliancebescheinigung (Attestation of Compliance, AOC) an American Express übermittelt werden.

Die AOC muss die Einhaltung sämtlicher Anforderungen des PCI-DSS-Standards bescheinigen; auf Verlangen sind Kopien des vollständigen Complianceberichts (Akzeptanzpartner und Dienstleister der Stufe 1) beizufügen.

Fragebogen „Annual Self-Assessment“ – Die jährliche Selbsteinschätzung ist ein Verfahren unter Verwendung des PCI-DSS-Fragebogens, das die Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), auf denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden, ermöglicht. Dieses Verfahren muss von Ihnen ausgeführt und von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Hauptverantwortlichen zertifiziert werden. Der AOC-Abschnitt des SAQ muss jährlich bei American Express eingereicht werden. Im AOC-Abschnitt des SAQ muss die Einhaltung aller PCI-DSS-Anforderungen bestätigt werden. Auf Anforderung sind vollständige Kopien des SAQ hinzuzufügen (für Akzeptanzpartner der Stufen 2, 3 und 4 sowie Dienstleister der Stufe 2).

Vierteljährlicher Netzwerkscan – Beim vierteljährlichen Netzwerkscan werden Ihre mit dem Internet verbundenen Computernetzwerke und Webserver online auf potenzielle Schwachstellen und Sicherheitslücken getestet. Er muss von einem Approved Scanning Vendor (**ASV**) durchgeführt werden. Die ausgefüllte Bescheinigung ASV Scan Report Attestation of Scan Compliance (**AOSC**) oder eine Zusammenfassung der Scanergebnisse (auf Verlangen auch Kopien des vollständigen Scans) muss (müssen) vierteljährlich bei American Express eingereicht werden. In der AOSC bzw. Zusammenfassung muss zertifiziert werden, dass die Ergebnisse den PCI-DSS-Scanverfahren entsprechen, dass keine mit hohen Risiken behafteten Probleme festgestellt wurden und dass der Scan standardkonform ist (alle Akzeptanzpartner mit Ausnahme derjenigen, die auch einen Onsite Security Assessment-Bericht einreichen, STEP-berechtigte Akzeptanzpartner und alle Dienstleister). Zur Klarstellung: Vierteljährliche Netzwerkscans sind vorgeschrieben, wenn sie in dem jeweiligen SAQ angefordert werden.

Validierungsdokumentation im Rahmen des STEP-Jahresnachweises – Der STEP-Qualifizierungs-Jahresnachweis von American Express („STEP-Nachweis“) steht nur Akzeptanzpartnern zur Verfügung, die alle in Maßnahme 2: „Einstufung Ihres Unternehmens und Bestimmung der Validierungsanforderungen“ oben aufgeführten Kriterien erfüllen. Der STEP-Nachweis beinhaltet ein auf den Anforderungen des PCI DSS basierendes Verfahren, das die Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), auf denen Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden, ermöglicht. Dieses Verfahren muss von Ihnen ausgeführt und von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Hauptverantwortlichen zertifiziert werden. Das STEP-Nachweisformular muss zum Abschluss des Verfahrens jährlich von Ihnen bei American Express eingereicht werden. (Nur STEP-berechtigte Akzeptanzpartner). Das Formular für den jährlichen STEP-Nachweis steht über das sichere Portal von SecureTrust zum Download bereit.

Nichteinhaltung des PCI-DSS-Standards – Wenn Sie den PCI-DSS-Standard nicht einhalten, müssen Sie eines der folgenden Dokumente einreichen:

- eine Compliancebescheinigung (AOC) einschl. „Teil 4. Maßnahmenplan für Nicht-Compliance-Status“
- eine „PCI Prioritised Approach Tool Summary and Attestation of Compliance“ (PASAOC)
- eine Projektplanvorlage (Download über das sichere Portal von SecureTrust)

Jedes der oben genannten Dokumente muss ein Datum für eine entsprechende Korrektur angeben, das innerhalb von zwölf Monaten ab dem Fertigstellungsdatum des Dokuments liegt, damit die Einhaltung der Vorschriften sichergestellt ist. Sie müssen das jeweilige Dokument anhand einer der in Maßnahme 4: „Übermittlung der Validierungsdokumentation an American Express“ unten genannten Methoden an American Express übermitteln. 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). Zur Klarstellung: Akzeptanzpartner, die den PCI-DSS-Standard nicht einhalten, können nicht am STEP-Programm teilnehmen. 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.

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 Ihres Unternehmens und Bestimmung der Validierungsanforderungen“ als „obligatorisch“ gekennzeichnete Validierungsdokumentation einreichen. Sie müssen Ihre Validierungsdokumentation anhand einer der folgenden Methoden an SecureTrust übermitteln:

- **Secure Portal:** Die Validierungsdokumentation kann über das sichere SecureTrust-Portal unter https://portal.securetrust.com übermittelt werden.

  Anweisungen zur Verwendung dieses Portals erhalten Sie von SecureTrust unter der für Ihr Land vorgesehenen Rufnummer bzw. per E-Mail an americanexpresscompliance@securetrust.com.
- **Secure Fax:** Die Validierungsdokumentation kann gefaxt werden an: +1 (312) 276-4019. (+ steht für die internationale Direktwahl; es fallen Gebühren für internationale Anrufe an).

  Geben Sie bitte Ihren Namen, den angemeldeten Namen Ihres Unternehmens, den Namen Ihres Ansprechpartners für Datensicherheit, Ihre Adresse und Telefonnummer und – nur für Akzeptanzpartner – Ihre 10-stellige American Express Akzeptanzpartnernummer an.

Wenn Sie allgemeine Fragen zum Programm oder zu den oben beschriebenen Verfahren haben, wenden Sie sich bitte an SecureTrust unter der Rufnummer +800 9000 1140 oder +1 (312) 267-3208 bzw. per E-Mail an americanexpresscompliance@securetrust.com.

Die Kosten für Compliance und Validierung sind von Ihnen zu tragen. Mit dem Einreichen der Validierungsdokumentation erklären und versichern Sie gegenüber American Express, dass Sie berechtigt sind, die darin enthaltenen Informationen weiterzugeben, und dass die Übermittlung der Validierungsdokumentation an American Express ohne jegliche Verletzung der Rechte Dritter erfolgt.

Märkte	SecureTrust-Telefonnummer
Argentinien	+ 800 9000 1140
Australien	+ 800 9000 1140
Bulgarien	+ 312 267 3208
Dänemark	+ 800 9000 1140
Deutschland	+ 800 9000 1140
Estland	+ 312 267 3208
Frankreich	+ 800 9000 1140
Griechenland	+ 312 267 3208
Hongkong	+ 800 9000 1140
IDC	+ 888 900 0114
Indien	+ 800 9000 1140
Irland	+ 800 9000 1140
Island	+ 800 9000 1140
Italien	+ 800 9000 1140
Japan	+ 312 267 3208
Kanada	1 866 659 9016
Kroatien	+ 312 267 3208
Lettland	+ 312 267 3208
Litauen	+ 312 267 3208
Malta	+ 312 267 3208
Mexiko	+ 888 900 0114
Neuseeland	+ 800 9000 1140
Niederlande	+ 312 267 3208
Norwegen	+ 800 9000 1140

Märkte	SecureTrust-Telefonnummer
Österreich	+ 800 9000 1140
Polen	+ 800 9000 1140
Portugal	+ 312 267 3208
Rumänien	+ 312 267 3208
Russland	+ 312 267 3208
Schweden	+ 800 9000 1140
Singapur	+ 800 9000 1140
Slowakei	+ 312 267 3208
Slowenien	+ 312 267 3208
Spanien	+ 800 9000 1140
Taiwan	+ 312 267 3208
Thailand	+ 800 9000 1140
Tschechische Republik	+ 800 144 316
Ungarn	+ 800 9000 1140
Vereinigte Staaten	1 866 659 9016
Vereinigtes Königreich	+ 800 9000 1140
Zypern	+ 800 9000 1140

+ steht für die internationale Direktwahl; es fallen Gebühren für internationale Anrufe an.

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.

Übermitteln Sie die Dokumentation innerhalb der geltenden Frist an American Express. Sie werden von American Express über die jeweils geltenden Fristen für jeden Jahres- und Quartalsberichtszeitraum gesondert informiert. Wenn Ihre obligatorische Validierungsdokumentation nicht innerhalb von 90 Tagen nach Ablauf der ersten Frist bei American Express eingeht, hat American Express das Recht, den Vertrag seinen Bestimmungen gemäß zu kündigen und darüber hinaus die aufgrund der Nichtvalidierung angefallenen Vertragsstrafen kumulativ von Ihnen einzufordern.

Tabelle „Vertragsstrafen für Nichtvalidierung“

Beschreibung*	Akzeptanzpartner oder Dienstleister, Stufe 1	Akzeptanzpartner oder Dienstleister, Stufe 2	Akzeptanzpartner, Stufe 3 oder Stufe 4
Wenn die Validierungsdokumentation nicht innerhalb der ersten Frist eingeht, wird eine entsprechende Vertragsstrafe erhoben.	USD 25.000	USD 5.000	USD 50
Eine weitere Vertragsstrafe wird erhoben, wenn die Validierungsdokumentation nicht binnen 60 Tagen nach Ablauf der ersten Frist eingeht.	USD 35.000	USD 10.000	USD 100
Eine weitere Vertragsstrafe wird erhoben, wenn die Validierungsdokumentation nicht binnen 90 Tagen nach Ablauf der ersten Frist und danach binnen 30 Tagen eingeht.	USD 45.000	USD 15.000	USD 250

* Vertragsstrafen für Nichtvalidierung werden in der entsprechenden Landeswährung festgesetzt.

** Gilt nicht in Argentinien.

Abschnitt 6 Vertraulichkeit

American Express wird angemessene Maßnahmen treffen (und seine Vertreter und Subunternehmer, einschließlich SecureTrust, 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 mit American Express verbundenen Gesellschaften, Bevollmächtigten, Vertretern, Dienstleistern und Subunternehmern gehören) weitergeben. 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 übernimmt keinerlei Haftung dafür, dass die in dem Vertrag, in diesen Richtlinien oder im PCI-Standard enthaltenen Maßnahmen dazu ausreichen oder dazu geeignet sind, Ihre etwaigen speziellen Daten und Interessen des Akzeptanzpartners zu schützen. American Express schließt jegliche Haftung dafür aus, dass es trotz der Einhaltung dieser Datensicherheitsrichtlinien und des PCI-Standards bei Ihnen zu einem Datenvorfall kommt und Sie aufgrund dessen von einem Dritten in Anspruch genommen werden.

Insbesondere übernimmt American Express keine Haftung in Bezug auf die EMV-Spezifikationen und die Einstufung der Akzeptanzpartner und Dienstleister. Ebenso übernimmt American Express keine Haftung für die ordnungsgemäße Ausführung der Tätigkeit eines Qualified Security Assessors (QSA), eines PCI Forensic Investigators (PFI) und/oder eines Approved Scanning Vendors (ASV).

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 (DSOP) und sind im Falle von Widersprüchen zu den Begriffen in den *Bestimmungen für Akzeptanzpartner* maßgeblich.

Akzeptanzpartner bezeichnet den Akzeptanzpartner und alle mit ihm verbundenen Unternehmen, die American Express Karten im Rahmen einer Vereinbarung mit American Express oder seinen verbundenen Unternehmen akzeptieren.

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.

American Express Karte oder **Karte** bezeichnet jede Karte, jedes Mittel zum Kontozugang bzw. alle Zahlungsmittel 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 Partnerunternehmen oder eine Kontonummer aufweisen und die von einem Kartenherausgeber ausgestellt wurden, oder eine Kartennummer.

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

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

Aussteller bezeichnet jedes Unternehmen (einschließlich American Express und seiner verbundenen Unternehmen), das von American Express oder einem verbundenen Unternehmen von American Express zur Ausstellung von Karten und zur Ausübung des Kartenausstellungsgeschäfts lizenziert wurde.

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

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.

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

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

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

Chipkarte bezeichnet eine Karte mit Chip, bei der die Eingabe einer PIN zwecks Überprüfung der Identität des Kartenmitglieds 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.

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

Datenvorfall bezeichnet einen vermuteten oder tatsächlichen Zwischenfall, bei dem die American Express Verschlüsselungscodes oder eine oder mehrere Karten- oder Kontonummern von American Express Karten unberechtigt genutzt werden oder unberechtigt darauf zugegriffen wurde. Als Datenvorfall gilt:

- der nicht autorisierte Zugriff auf oder die nicht autorisierte Verwendung von Verschlüsselungscodes, Karteninhaber- und/oder vertrauliche 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, der ab dem Zwischenfall (falls Datum bekannt) oder 365 Tage vor dem Benachrichtigungsdatum (falls Datum des Zwischenfalls nicht bekannt) beginnt. Das Zeitfenster des Datenvorfalls endet 30 Tage nach dem Benachrichtigungsdatum.

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

Dienstleister der Stufe 1 bezeichnet einen Dienstleister mit mindestens 1 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.

Eingeschaltete Dritte bezeichnet Ihre Mitarbeiter, Bevollmächtigten, Vertreter, Subunternehmer, Verarbeiter, 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.

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.

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

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.

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.

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.

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.

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 eingetragen ist.

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

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

Kartennummer bezeichnet die eindeutige Identifikationsnummer, die der Aussteller der Karte bei der Ausstellung zuweist.

Kontonummer ist die der American Express Karte zugeordnete Kartennummer, auch Primary Account Number (PAN) genannt.

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

PCI Forensic Investigator (PFI) bezeichnet eine Organisation, die vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenbranche) zugelassen ist, um forensische Untersuchungen von Datensicherheitsverstößen oder der unberechtigten Nutzung 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.

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.

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 Autorisierungen 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.

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-Standards validiert.

Risikomindernde Technologien 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: 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. Damit ein Akzeptanzpartner die Voraussetzungen für das STEP-Programm erfüllt, darf es bei ihm in den 12 Monaten vor Einreichung des STEP-Jahresnachweises keinen Datenvorfall gegeben haben, und es müssen mindestens 75 % seiner Transaktionen über Point-to-Point-Verschlüsselung oder als Face-to-Face-Transaktionen unter Verwendung von chipfähigen EMV-Geräten abgewickelt worden sein.

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 dem vierteljährlichen Netzwerkscan oder dem jährlichen STEP-Nachweis eingereichten Ergebnisse.

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

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

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

Von unberechtigter Nutzung betroffene Kontonummer bezeichnet eine American Express Kontonummer, die in einen Datenvorfall involviert ist.

Zahlungsanwendung ist im jeweils aktuellen Glossar zum Datensicherheitsstandard der Zahlungskartenindustrie (Payment Card Industry Data Security Standard, PCI DSS) definiert – siehe www.pcisecuritystandards.org.