ALLGEMEINE DATENSICHERHEITSRICHTLINIEN FÜR AKZEPTANZPARTNER – ÖSTERREICH

DSOP.AP_AT_202402

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Allgemeine Datensicherheitsrichtlinien für Akzeptanzpartner (Data Security Operating Policy) – Österreich

Im Sinne des Konsumentenschutzes hat sich American Express® schon seit vielen Jahren dem Schutz der Daten seiner Karteninhaber verpflichtet, um höchste Sicherheit zu gewährleisten.

Die unberechtigte Nutzung von Daten wirkt sich negativ auf Konsumenten, 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 erhöhen.

Bei American Express wissen wir, dass Akzeptanzpartner und Dienstleister (zusammenfassend nachfolgend auch „Sie" genannt) 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 Akzeptanz und im Fall der Dienstleister für die Verarbeitung der American Express Kartentransaktionen (jeweils nach Maßgabe des Vertrags). Diese Sicherheitsanforderungen 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.

Begriffe, die in den Richtlinien nicht definiert sind, werden im Glossar am Ende dieses Dokuments erläutert.

§ 1 – Standards für den Schutz von Verschlüsselungscodes, Karteninhaber- und vertraulichen Authentifizierungsdaten

Sie sind verpflichtet – und müssen die von Ihnen eingeschalteten Dritten ebenfalls dazu verpflichten –,

- Informationen in Bezug auf Karteninhaber nur zu speichern, um die Abwicklung von American Express Kartentransaktionen in Übereinstimmung mit den vertraglich festgelegten Bedingungen zu ermöglichen,
- die aktuelle Fassung des Datensicherheitsstandards der Zahlungskartenbranche (Payment Card Industry Data Security Standard, ***PCI DSS***) und der PCI-PIN-Sicherheitsanforderungen spätestens ab dem Stichtag zur Implementierung dieser Fassung einzuhalten sowie;
- bei der Bereitstellung von Neu- oder Ersatzgeräten für die PIN-Eingabe oder von Zahlungssoftware (oder beidem) an unterstützen Standorten nur solche zu verwenden, die nach PCI-Standard zugelassen sind.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Sie sind verpflichtet, sämtliche nach Maßgabe Ihres Vertrags aufzubewahrenden American Express Belastungs- und Gutschriftsbelege gemäß diesen Datensicherheitsbestimmungen zu schützen; die Belege dürfen lediglich im Rahmen der Zweckbestimmung und zur Abwicklung des Vertrags verwendet werden und sind entsprechend zu sichern. Sie stellen sicher, dass die von Ihnen eingeschalteten Dritten diese Datensicherheitsbestimmungen einhalten und verpflichten sich, diesen eine entsprechende Verpflichtung aufzuerlegen. Für etwaige Verstöße der von Ihnen eingeschalteten Dritten gegen diese Datensicherheitsbestimmungen (außer für den Nachweis der Einhaltung dieser Richtlinien durch die von Ihnen eingeschalteten Dritten nach § 4 unten, sofern nicht anderweitig dort angegeben) haften Sie.

§ 2 – Verpflichtungen und Vorgehen bei einem Datenvorfall

Sie müssen American Express sofort und in keinem Fall später als vierundzwanzig (24) Stunden nach der Entdeckung eines Datenvorfalls benachrichtigen. Um American Express zu informieren, wenden Sie sich bitte an das American Express Enterprise Incident Response Program (*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.

- Für jeden einzelnen Datenvorfall muss eine gründliche forensische Untersuchung vorgenommen werden. Bei Datenvorfällen mit 10.000 oder mehr individuellen American Express Kontonummern (oder ausdrücklich auf Wunsch von American Express) muss diese Untersuchung durch einen forensischen PCI-Ermittler (PCI Forensic Investigator, PFI) durchgeführt werden. Der unveränderte Bericht muss American Express innerhalb von 10 Werktagen nach Fertigstellung vorliegen.
- Sie sind verpflichtet, American Express unverzüglich alle von unberechtigter Nutzung betroffenen Kontonummern sowie den forensischen Untersuchungsbericht zum Datenvorfall zur Verfügung zu stellen. American Express behält sich das Recht vor, eigene interne Untersuchungen durchzuführen, um die an dem Datenvorfall beteiligten Kartennummern zu identifizieren.
- Sie müssen mit American Express zusammenarbeiten, um jegliche Probleme und Fragen im Zusammenhang mit dem Datenvorfall zu beheben bzw. zu klären; dies beinhaltet (1) die Beratung mit American Express über die Benachrichtigung der vom Datenvorfall betroffenen American Express Karteninhaber und (2) die Zurverfügungstellung aller relevanten Informationen an American Express (und die Einholung etwaiger erforderlicher Verzichts- und/oder Einwilligungserklärungen für das Zurverfügungstellen der Informationen), damit überprüft werden kann, ob Sie in der Lage sind, Datenvorfällen in Zukunft im Einklang mit dem Vertrag vorzubeugen.

Forensische Untersuchungsberichte müssen forensische Überprüfungen, Berichte über die Einhaltung der Bestimmungen und alle anderen Informationen zu dem Datenvorfall beinhalten; die Ursache des

Datenvorfalls aufzeigen; bestätigen, ob Sie zum Zeitpunkt des Datenvorfalls den PCI-DSS-Standard eingehalten haben oder nicht; und überprüfen, ob Sie durch Vorlage eines Plans zur Beseitigung aller PCI-DSS-Mängel in der Lage sind, zukünftige Datenvorfälle zu vermeiden. Auf Wunsch von American Express ist die Validierung durch einen Qualified Security Assessor ***(QSA)*** zur Verfügung zu stellen, um zu bestätigen, dass die Mängel behoben wurden.

Ungeachtet einer gegenteiligen vertraglichen Geheimhaltungspflicht hat American Express das Recht, American Express Karteninhaber, -aussteller, andere am American Express Netzwerk Beteiligte und die allgemeine Öffentlichkeit gemäß den geltenden Gesetzen über jeden Datenvorfall zu informieren und Datenvorfälle auf Anordnung eines Gerichts, einer Verwaltungs- oder Aufsichtsbehörde, eines Erlasses, einer Vorladung, eines Antrags oder eines anderen Verfahrens offenzulegen, um das Risiko von Betrug oder anderen Schäden zu mindern oder den Betrieb des American Express Netzwerks zu gewährleisten.

§3–Schadensersatzverpflichtungen für einen Datenvorfall

Nachfolgend sind, unter Vorbehalt der Geltendmachung weiterer Rechte und Rechtsmittel durch American Express, Ihre vertragsgemäßen Schadensersatzverpflichtungen gegenüber American Express bei einem Datenvorfall festgelegt.

(1) Vorbehaltlich des nachstehenden Absatzes (2) haften Sie für sämtliche Schäden im Zusammenhang mit einem von Ihnen zu vertretenden Datenvorfall wie folgt:

Für einen Datenvorfall, bei dem nur Kontonummern von American Express Karten betroffen sind, verlangt American Express einen Schadensersatz durch unverzügliche Zahlung eines pauschalierten Schadensersatzes von maximal 100.000 USD pro Datenvorfall. Für einen Datenvorfall, bei dem Kontonummern von American Express Karten einschließlich vertraulicher Authentifizierungsdaten betroffen sind, verlangt American Express unverzüglichen pauschalen Schadensersatz wie folgt:

- 5,00 USD pro Kartennummer
- pauschalierter Schadensersatz für die Nichteinhaltung der Vorschriften von maximal 100.000 USD pro Datenvorfall

American Express schließt aus der Berechnung der Kosten alle American Express Kartennummern aus, die in einen anderen Datenvorfall mit American Express Kartennummern mit vertraulichen Authentifizierungsdaten involviert waren, vorausgesetzt, dass dieser Datenvorfall American Express innerhalb von zwölf (12) Monaten vor dem Benachrichtigungsdatum mitgeteilt wurde. Sämtliche von American Express auf diese Methode vorgenommenen Berechnungen sind endgültig.

Bezüglich der pauschalierten Schadensersatzbeträge bleibt der Nachweis, dass American Express gar kein Schaden oder ein wesentlich geringerer Schaden als die Pauschale entstanden ist, unbenommen. Durch die Vereinbarung eines pauschalierten Schadensersatzes wird die Verpflichtung zur Erstattung eines ggf. weiteren konkreten Schadens nicht ausgeschlossen.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Für Datenvorfälle, die am oder nach dem 13. Oktober 2017 entdeckt wurden, gilt außerdem folgendes: American Express kann nach eigenem Ermessen die Schadensersatzverpflichtung für diejenigen Akzeptanzpartner reduzieren, die die folgenden Kriterien kumulativ erfüllen:

- Die anwendbaren Technologien zur Risikominderung wurden vor dem Datenvorfall angewendet und waren während des gesamten Datenvorfall-Zeitfensters aktiv;
- eine umfassende Untersuchung in Übereinstimmung mit dem Forensiker-Programm der Zahlungskartenindustrie (Payment Card Industry Forensic Investigator (PFI) program) 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 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 Ihrer 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 auf chipfähigen Geräten[1] verarbeitet ODER
	Technologie zur Risikominderung an >75 % der Standorte der Akzeptanzpartner[2] eingesetzt
Erweiterte Reduzierung: 75 % bis 100 %	>75 % der gesamten Transaktionen auf chipfähigen Geräten[1] verarbeitet UND eine weitere Technologie zur Risikominderung an >75 % der Standorte der Akzeptanzpartner[2] eingesetzt

[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 weitere Technologie zur Risikominderung eingesetzt wurde, wobei der niedrigere Prozentsatz maßgeblich ist. Die folgenden Beispiele veranschaulichen die Ermittlung der Reduzierung der Schadensersatzverpflichtung.
- Damit eine Technologie zur Risikominderung geltend gemacht werden kann, müssen Sie eine effektive Nutzung derselben in Übereinstimmung mit deren 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.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

- Der Prozentsatz der Standorte, die eine Technologie zur Risikominderung einsetzen, wird anhand der PFI-Untersuchung ermittelt.
- Die Reduzierung der Schadensersatzverpflichtung gilt nicht für mögliche Strafgebühren wegen Nichteinhaltung von Vorschriften, die in Verbindung mit dem Datenvorfall zu zahlen sind.

Bsp.:	Eingesetzte Technologien zur Risikominderung	Voraussetzungen für eine erweiterte Reduzierung der Schadensersatz-Verpflichtung erfüllt?	Reduzierung
1	80 % der Transaktionen erfolgen über chipfähige Geräte 0 % der Standorte verwenden eine andere Technologie zur Risikominderung	Nein	50 %: Standardreduzierung (wird bei weniger als 75 % der Transaktionen eine Technologie zur Risikominderung eingesetzt, ist eine erweiterte Reduzierung nicht möglich)[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, ist eine erweiterte Reduzierung nicht möglich)

[1] Bei einem Datenvorfall mit 10.000 betroffenen American Express Kartenkonten in Höhe von $5 je Kontonummer (10.000 x $5 = $50.000) kann eine Reduzierung von 50 % möglich sein. Damit würde die Schadensersatzverpflichtung von $50.000 auf $25.000 sinken, ausschließlich eventuell anfallender Strafgebühren wegen Nichteinhaltung von Vorschriften.

(2) American Express verlangt keinen Schadensersatz von Ihnen für einen Datenvorfall, wenn

(a) weniger als 10.000 individuelle Kontonummern betroffen sind oder

(b) Sie American Express den Datenvorfall gemäß § 2 dieser Richtlinien gemeldet haben,

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

- Sie zum Zeitpunkt des Datenvorfalls den PCI-DSS-Standard (wie bei der Untersuchung des Datenvorfalls durch den PFI bestimmt) eingehalten haben und
- der Datenvorfall nicht auf ein Fehlverhalten Ihrerseits, eines Ihrer Mitarbeiter oder Bevollmächtigten oder seitens der von Ihnen eingeschalteten Dritten zurückzuführen ist.

§4–WICHTIG! Periodische Validierung Ihrer Systeme

Sie müssen – wie nachfolgend beschrieben – jährlich bzw. vierteljährlich die folgenden Schritte vornehmen, um den Status der von Ihnen und Ihren Franchisenehmern verwendeten Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), durch welche Karteninhaber- oder vertrauliche Authentifizierungsdaten gespeichert, verarbeitet oder übertragen werden, gemäß PCI-DSS-Standard zu validieren.

Für die Validierung sind folgende vier Schritte erforderlich:

Schritt 1 – Anmeldung beim American Express Complianceprogramm im Rahmen dieser Richtlinien

Schritt 2 – Einstufung Ihres Unternehmens und Bestimmung der Validierungsanforderungen

Schritt 3 – Bestimmung der bei American Express einzureichenden Validierungsdokumentation

Schritt 4 – Übermittlung der Validierungsdokumentation an American Express

Schritt 1 – Anmeldung beim American Express Complianceprogramm im Rahmen dieser Richtlinien

Akzeptanzpartner der Stufen 1 und 2 sowie Akzeptanzpartner der Stufe 3 (designiert), die von American Express entsprechend eingestuft wurden (wie unten beschrieben), und alle Dienstleister, wie unten beschrieben, müssen sich beim American Express Complianceprogramm unter dieser Richtlinie anmelden und dabei den vollständigen Namen, die E-Mail-Adresse, Telefonnummer und Postanschrift eines allgemeinen Ansprechpartners für die Datensicherheit angeben. Sie müssen diese Informationen auf einem der in Schritt 4 unten angeführten Wege an Trustwave, den von American Express beauftragten Programmverwalter, senden. Änderungen an diesen Informationen müssen Trustwave mitgeteilt werden.

Unter Umständen kann American Express bestimmte Akzeptanzpartner der Stufe 3 schriftlich anweisen, sich beim Complianceprogramm von American Express im Rahmen dieser Richtlinie anzumelden. Die Designierten Akzeptanzpartner der Stufe 3 müssen sich spätestens neunzig (90) Tage nach Erhalt des Schreibens anmelden.

Das Ergebnis Ihres PCI-Validierungsprozesses kann von American Express überprüft werden, einschließlich durch Beauftragung eines Qualified Security Assessor (QSA) unserer Wahl und auf unsere Kosten.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Schritt 2 – Einstufung Ihres Unternehmens und Bestimmung der Validierungsanforderungen

Es gibt fünf Stufen für Akzeptanzpartner und zwei Stufen für Dienstleister. Die Einteilung der Stufen richtet sich grundsätzlich nach dem Umfang der von Ihnen 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. Sie werden einer der in den folgenden Tabellen angegebenen Stufen für Akzeptanzpartner und Dienstleister zugeordnet.

Business-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 POS-Systems oder Dienstleisters vorschreiben, müssen die Validierungsdokumentation ebenfalls für die betroffenen Franchisenehmer einreichen.

Akzeptanzpartner-Anforderungen

Für Akzeptanzpartner (nicht Dienstleister) gibt es fünf 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 der Stufe 1 zuordnet.

Akzeptanzpartner Stufe 2: 50.000 bis 2,5 Millionen American Express Kartentransaktionen pro Jahr.

Akzeptanzpartner Stufe 3 (designiert): weniger als 50.000 American Express Kartentransaktionen pro Jahr und von American Express aus einem sonstigen Grund als Akzeptanzpartner der Stufe 3 eingestuft, der Validierungsdokumente einreichen muss. Gesondert eingestufte Akzeptanzpartner werden von American Express mindestens neunzig (90) Tage vor der erforderlichen Einreichung der Dokumente schriftlich benachrichtigt.

Akzeptanzpartner Stufe 3 (nicht designiert): weniger als 50.000 American Express Kartentransaktionen pro Jahr und nicht von American Express als Akzeptanzpartner eingestuft, der Validierungsdokumente einreichen muss.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

STEP (Security Technology Enhancement Program) – Akzeptanzpartner, die den PCI-DSS-Standard einhalten, sind unter Umständen 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 (siehe www.emvco.com), das die Verarbeitung von AEIPS-konformen Chipkartentransaktionen unterstützt
- P2PE (Point-to-Point-Verschlüsselung) – über ein vom PCI SSC zugelassenes oder durch einen QSA genehmigtes P2PE-Verschlüsselungssystem an den Prozessor des Akzeptanzpartners übermittelt

Für Akzeptanzpartner, die die Voraussetzungen für das STEP-Programm erfüllen, gelten geringere Anforderungen bezüglich der PCI-DSS-Validierungsdokumentation, wie weiter unten in Schritt 3 beschrieben.

Tabelle „Akzeptanzpartner“

Stufe (oben definiert)	Genehmigungsdokumentation (in Schritt 3 unten definiert)	Anforderung
1	• Bericht über das „Annual Onsite Security Assessment“ • Vierteljährlicher Netzwerkscan	Obligatorisch
2	• Fragebogen „Annual Self Assessment“ • Vierteljährlicher Netzwerkscan	Obligatorisch
3 (designiert)	• Fragebogen „Annual Self Assessment“ • Vierteljährlicher Netzwerkscan	Obligatorisch
3*	• Fragebogen „Annual Self Assessment“ • Vierteljährlicher Netzwerkscan	Dringend empfohlen
STEP**	• STEP-Jahresnachweis	Obligatorisch für VP, die für STEP infrage kommen möchten

* Zur Klarstellung: Akzeptanzpartner Stufe 3 (außer Designierten Akzeptanzpartnern der Stufe 3) müssen keine Validierungsdokumentation einreichen, unterliegen aber dennoch der Haftung und allen anderen Bestimmungen dieser Allgemeinen Datensicherheitsrichtlinien.

** STEP gilt nicht für Akzeptanzpartner, bei denen innerhalb der letzten zwölf (12) Monate vor der Einreichung des STEP-Jahresnachweises ein Datenvorfall aufgetreten ist oder die aus anderen Gründen nicht für STEP infrage kommen.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

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 Validierungsdokumente 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 (oben definiert)	Genehmigungsdokumentation (in Schritt 3 unten definiert)	Anforderung
1	• Bericht über das „Annual Onsite Security Assessment“ • Vierteljährlicher Netzwerkscan	Obligatorisch
2	• Fragebogen „Annual Self Assessment“ • Vierteljährlicher Netzwerkscan	Obligatorisch

Schritt 3 – Bestimmung 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. Es muss durchgeführt werden von

- einem Qualified Security Assessor (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.

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

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Fragebogen „Annual Self Assessment“: Bei der jährlichen Selbsteinschätzung dient der PCI-DSS-Fragebogen „Self Assessment Questionnaire“ ***(SAQ)*** der Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), durch die Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden. Er muss von Ihnen ausgefüllt werden und von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Haupt-verantwortlichen bestätigt werden. Der AOC-Abschnitt des SAQ muss jährlich bei American Express eingereicht werden. Im AOC-Abschnitt des SAQ muss die Einhaltung aller PCI-DSS-Standards bestätigt werden, auf Anforderung sind vollständige Kopien des SAQ hinzuzufügen (Akzeptanzpartner der Stufen 2 und 3 sowie Dienstleister der Stufe 2).

Vierteljährlicher Netzwerkscan (Quarterly Network Scan): 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 muss vierteljährlich bei American Express eingereicht werden (auf Verlangen sind Kopien des vollständigen Scans beizufügen). In der AOSC bzw. Zusammenfassung muss bestätigt werden, dass die Ergebnisse den im PCI-DSS-Standard definierten Scanverfahren entsprechen, dass keine hohen Risiken bestehen und dass der Scan standardkonform ist (alle Akzeptanzpartner außer STEP-Berechtigten, alle Dienstleister).

STEP-Jahresnachweis (Security Technology Enhancement Program) – Der American Express STEP-Jahresnachweis beinhaltet ein auf den Anforderungen des PCI DSS basierendes Verfahren der Selbstprüfung Ihrer Geräte, Systeme und Netzwerke (und der zugehörigen Komponenten), durch die Karteninhaber- oder vertrauliche Authentifizierungsdaten (oder beides) gespeichert, verarbeitet oder übertragen werden. Es muss von Ihnen durchgeführt und von Ihrem Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer oder Ihrem gesetzlichen Vertreter bestätigt werden. Das STEP-Nachweisformular muss jährlich bei American Express eingereicht werden (nur VP, die die Voraussetzungen für STEP erfüllen). Das Formular für den jährlichen STEP-Nachweis steht über das sichere Portal von Trustwave zum Download bereit.

Compliance-Zusammenfassung (Summary of Compliance, SOC) – Mit dem SOC-Dokument kann ein Franchisegeber den PCI-Compliancestatus seiner Franchisenehmer melden. Die SOC-Vorlage steht über das sichere Portal von Trustwave zum Download bereit.

Nichteinhaltung des PCI-DSS-Standards: Wenn Sie den PCI-DSS-Standard nicht einhalten, müssen Sie zwecks Bestätigung Ihrer Compliance eine AOC-Bescheinigung einschließlich Teil 4 „Action Plan for Non-Compliant Status“ oder eine Projektplanvorlage (Download über das sichere Portal von Trustwave) ausfüllen und ein Datum für eine entsprechende Korrektur angeben, das innerhalb von zwölf Monaten ab AOC liegt. Die AOC-Bescheinigung muss mit dem „Action Plan for Non-Compliant Status“ auf einem der in Schritt 4 unten angeführten Wege an American Express übermittelt werden. Sie müssen American Express regelmäßig über Ihre aktuellen Fortschritte bei der Korrektur im Rahmen des „Action Plan for Non-Compliant Status“ informieren (Akzeptanzpartner der Stufen 1, 2

und Designierte Akzeptanzpartner der Stufe 3; 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 Gebühren (siehe unten), was Sie jedoch nicht von jeglichen Schadensersatzverpflichtungen für einen Datenvorfall gegenüber American Express befreit; weiterhin unterliegen Sie allen sonstigen Bestimmungen dieser Richtlinien.

Schritt 4 – Übermittlung der Validierungsdokumentation an American Express

Akzeptanzpartner der Stufen 1 und 2, Designierte Akzeptanzpartner der Stufe 3, STEP-berechtigte Akzeptanzpartner, sowie alle Dienstleister müssen die in den Tabellen unter Schritt 2 als obligatorisch markierte Validierungsdokumentation einreichen. Die Validierungsdokumentation muss auf einem der folgenden Wege an Trustwave übermittelt werden:

Secure Portal: Die Validierungsdokumentation kann über das sichere Trustwave-Portal unter https://login.trustwave.com hochgeladen werden.

Anweisungen zur Verwendung dieses Portals erhalten Sie bei Trustwave unter den Rufnummern 00800 9000 1140 oder +1 312 267-3208 bzw. per E-Mail an AmericanExpressCompliance@trustwave.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 Vertragspartnernummer an.

Wenn Sie allgemeine Fragen zum Programm oder zu den oben beschriebenen Verfahren haben, wenden Sie sich bitte an Trustwave unter den Rufnummern 00800 9000 1140 oder +1 312 267-3208 bzw. per E-Mail an AmericanExpressCompliance@trustwave.com

Die Kosten für Compliance und Validierung sind von Ihnen zu tragen. Mit dem Einreichen der Validierungsdokumentation vertreten 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.

Schadensersatz bei Nichtvalidierung, Kündigung des Vertrags

American Express hat das Recht, bei Nichtvalidierung einen pauschalen Schadensersatz gemäß nachfolgender Tabelle zu erheben, 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. Der Nachweis, dass American Express gar kein Schaden oder ein wesentlich geringerer Schaden als die Pauschale entstanden ist, bleibt unbenommen.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Beschreibung (Währung EUR)	Akzeptanzpartner oder Dienstleister Stufe 1	AAkzeptanzpartner oder Dienstleister Stufe 2, STEP-Akzeptanzpartner	Designierte Akzeptanz-partner Stufe 3
Schadenspauschale, wenn die Validierungsdokumentation nicht innerhalb der ersten Frist eingeht	EUR 19.000	EUR 4.000	EUR 15 pro Monat
Weitere Schadenspauschale, wenn die Validierungsdokumentation nicht binnen 30 Tagen nach Ablauf der ersten Frist eingeht	EUR 26.000	EUR 7.500	
Weitere Schadenspauschale, wenn die Validierungsdokumentation nicht binnen 60 Tagen nach Ablauf der ersten Frist eingeht	EUR 34.000	EUR 11.000	

Wenn Ihre obligatorische Validierungsdokumentation nicht innerhalb von sechzig (60) Tagen nach Ablauf der ersten Frist bei American Express eingeht, hat American Express darüber hinaus das Recht, den Vertrag aus wichtigem Grund fristlos zu kündigen. Die Kündigung des Vertrags schließt die Geltendmachung weiterer Ansprüche, insbesondere Schadensersatzansprüche, durch American Express nicht aus.

§ 5 – Vertraulichkeit

American Express wird angemessene Maßnahmen treffen (und seine Vertreter und Subunternehmer, einschließlich Trustwave, entsprechend anweisen), um die von Ihnen eingereichten Complianceberichte, inklusive der Validierungsdokumentation, vertraulich zu behandeln und die Validierungs- dokumentation für einen Zeitraum von drei (3) Jahren ab dem Datum des Zugangs der Dokumente nicht an Dritte (die nicht zu den mit American Express verbundenen Gesellschaften, Bevollmächtigten, Vertretern, Dienstleistern und Subunternehmern gehören) weiterzugeben. Diese Vertraulichkeitsverpflichtung gilt nicht für Validierungsdokumente, die

- American Express bereits vor der Offenlegung durch Sie bekannt waren;
- ohne eine Verletzung der Bestimmungen dieses Absatzes durch American Express der Öffentlichkeitbereits zugänglich sind oder noch zugänglich gemacht werden;
- American Express rechtmäßig von einem Dritten ohne eine Vertraulichkeitsverpflichtung erhalten hat;
- American Express unabhängig entwickelt hat oder
- 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.

§6–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).

Die vorstehenden Haftungsausschlüsse gelten nicht (i) bei Vorsatz und grober Fahrlässigkeit seitens American Express, (ii) im Fall von Körper- und Gesundheitsschäden, (iii) im Fall der Verletzung wesentlicher Vertragspflichten („Kardinalpflichten“) von American Express sowie (iv) im Fall der Übernahme einer Beschaffenheits- und Haltbarkeitsgarantie durch American Express. Unter wesentlichen Vertragspflichten, auch sog. Kardinalpflichten im Sinne ständiger Rechtsprechung, sind Pflichten zu verstehen, die die ordnungsgemäße Durchführung des Vertrags erst ermöglichen und auf deren Erfüllung Sie deshalb vertrauen und vertrauen dürfen.

Nützliche Webseiten

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

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

American Express Payments Europe, S.L. – Austrian Branch | Rathausstraße 1 | 1010 Wien
Zweigniederlassung einer Gesellschaft mit beschränkter Haftung nach spanischem Recht mit Sitz in Madrid. Avenida Partenón 12–14, 28042, Madrid, Spanien, eingetragen im Registro Mercantil de la Provincia de Madrid, Hoja M-664153, Tomo 37236, Folio 20.

Firmenbuchgericht: Handelsgericht Wien | Firmenbuchnummer: FN 493466 k | UID Nr: ATU73463147

American Express Payments Europe, S.L. hat eine Lizenz der Banco de España, Madrid, zur Erbringung von Zahlungsdienstleistungen (Referenznummer 6883).

Postanschrift:

American Express Payments Europe, S.L. – Austrian Branch,

Niederlassung Wien, Abteilung Vertragspartnerservice

Rathausstraße 1

1010 Wien

Kontakt:

Telefon: 0800 900 930, Mo–Fr 08.30–17.30 Uhr

Telefax: 0800 900 931

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Anhang A: Glossar

Im Rahmen der vorliegenden Richtlinien gelten folgende Begriffsdefinitionen:

American Express Karte oder Karte

- bezieht sich auf 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 oder einem seiner Partnerunternehmen verwenden und die von einem Kartenherausgeber herausgegeben wurden, oder
- eine Kartennummer.

Attestation of Compliance (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.

Approved Scanning Vendor (ASV) bezeichnet einen vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenbranche) zugelassenen Scanning-Anbieter, der die Einhaltung bestimmter PCI-DSS-Anforderungen validiert und Umgebungen mit Internetanschluss auf potenzielle Sicherheitslücken überprüft.

Attestation of Scan Compliance (AOSC) ist die 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.

Karteninhaberdaten bestehen mindestens aus der vollständigen Kontonummer. Karteninhaberdaten können auch folgende Datenelemente umfassen: Name und/oder Adresse des Karteninhabers Verfallsdatum, Servicecode und/oder Kartenidentifikationsnummern ***(CID)***. Siehe auch die entsprechende Definition im jeweils aktuellen Glossar für den PCI-DSS-Standard.

Karteninhaber stellt eine natürliche oder juristische Person dar, (i) die mit einem Kartenherausgeber einen Vertrag zur Herausgabe einer Karte und zur Einrichtung eines Kartenkontos abgeschlossen hat oder (ii) deren Name auf der Karte eingetragen ist.

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

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

Chip bezieht sich auf den integrierten Mikrochip auf einer Karte, auf dem Daten gespeichert sind (darunter bestimmte Karteninhaberdaten).

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

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; manchmal auch „Smart-Karte“, „EMV-Karte“ oder „ICC-Karte“ („Integrated Circuit Card“).

Chipfähiges Gerät bezieht sich auf ein POS-Gerät mit einer gültigen und aktuellen EMVCo-Zulassung/-Zertifizierung (siehe www.emvco.com), das die Verarbeitung von AEIPS-konformen Chipkartentransaktionen unterstützt.

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

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 Karteninhaberdaten 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 Zwischenfall, bei dem die American Express Verschlüsselungscodes oder eine oder mehrere American Express Kartennummern unberechtigt genutzt werden oder auf diese unberechtigt zugegriffen wurde. Als Datenvorfall gilt:

- der nicht autorisierte Zugriff auf oder die 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 Netzwerken (und 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 bis zu 365 Tage vor dem Benachrichtigungsdatum beginnt und 30 Tage nach dem Benachrichtigungsdatum endet.

Designierte Akzeptanzpartner der Stufe 3 bezeichnet Akzeptanzpartner, die von American Express benachrichtigt wurden, dass sie verpflichtet sind, am American Express PCI-Complianceprogramm teilzunehmen und über ihren Compliancestatus Bericht zu erstatten.

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

EMV-Spezifikationen sind die durch EMVCo, LLC herausgegebenen Spezifikationen, die unter http://www.emvco.com abgerufen werden können.

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

Verschlüsselungscode (American Express Verschlüsselungscode) bezieht sich auf alle beim Verarbeiten, Generieren, Laden und Schützen von Karteninhaber- und vertraulichen Authentifizierungsdaten verwendeten Codes. Dies umfasst beispielsweise folgende Codes:

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

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.

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

Akzeptanzpartner der Stufe 2: 50.000 bis 2,5 Millionen American Express Kartentransaktionen pro Jahr.

Akzeptanzpartner der Stufe 3: weniger als 50.000 American Express Kartentransaktionen pro Jahr und nicht von American Express designiert.

Akzeptanzpartner der Stufe 3 (designiert) bezeichnet Akzeptanzpartner, die von American Express benachrichtigt wurden, dass sie verpflichtet sind, am American Express PCI-Complianceprogramm teilzunehmen und über ihren Compliancestatus Bericht zu erstatten.

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

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

Akzeptanzpartner der Stufe EMV: Akzeptanzpartner, die innerhalb der letzten zwölf (12) Monate nicht an einem Datenvorfall beteiligt waren und darüber hinaus

- mindestens 50.000 American Express Kartentransaktionen pro Jahr abwickeln;
- mindestens 75% aller Transaktionen mit der physischen Karte über POS-Systeme abgewickelt haben, die die EMV-Spezifikationen von American Express erfüllen.

Benachrichtigungsdatum bezieht sich auf den von American Express festgelegten Termin, an dem die Kartenherausgeber über den Datenvorfall benachrichtigt werden.

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

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

Prioritized Approach ist im jeweils aktuellen Glossar für den PCI-DSS-Standard definiert.

PCI Forensic Investigator (auch PFI) bezeichnet eine forensische PCI-Ermittlungsstelle, die vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenbranche) zugelassen ist, um forensische Untersuchungen von Sicherheitslücken oder der unberechtigten Nutzung von Zahlungskartendaten durchzuführen.

PCI-PIN-Sicherheitsanforderungen bezieht sich auf die Sicherheitsanforderungen gemäß Payment Card Industry Data Security Standard (Datensicherheitsstandard der Zahlungskartenindustrie), verfügbar unter https://www.pcisecuritystandards.org

PIN ist im jeweils aktuellen Glossar für die Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements definiert (verfügbar unter https://www.pcisecuritystandards.org)

POS-System oder-Gerät ist ein Informationsverarbeitungssystem oder -gerät (z. B. Terminal, PC, elektronische Registrierkasse, berührungsloser Leser oder Zahlungsmaschine/-prozess), das von einem Akzeptanzpartner genutzt wird, um Autorisierungen zu erhalten oder Transaktionsdaten entgegenzunehmen (oder beides).

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

American Express Payments Europe, S.L. – Austrian Branch,
Firmenbuchgericht: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr.: ATU73463147

Qualified Security Assessor (QSA) bezeichnet einen vom PCI Security Standards Council, LLC (Rat für Sicherheitsstandards in der Zahlungskartenbranche) qualifizierten Sicherheitsprüfer, der die Einhaltung des PCI-DSS-Standards überwacht, siehe auch die Definition dazu im jeweils aktuellen Glossar für den PCI-DSS-Standard.

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

Vertrauliche Authentifizierungsdaten sind im jeweils aktuellen Glossar für den PCI-DSS-Standard definiert.

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

SOC (Summary of Compliance) bezeichnet ein PCI-Validierungsdokument mit einer Compliance-Zusammenfassung, das Franchisegeber verwenden, um den PCI-Compliancestatus ihrer betroffenen Franchisenehmer anzugeben.

STEP (Security Technology Enhancement Program, Programm zur Verbesserung der IT-Sicherheit) ist ein Programm von American Express, das die Akzeptanzpartner zum Einsatz von Technologien zur Verbesserung der Datensicherheit anregen soll. Damit ein Akzeptanzpartner die Voraussetzungen für das STEP-Programm erfüllt, darf es in seinem Geschäft in den letzten 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 stellt eine mit einer Karte abgewickelte Belastung oder eine Gutschrift dar.

Transaktionsdaten sind im jeweils aktuellen Glossar für den PCI-DSS-Standard definiert.

Validierungsdokumentation ist die eingereichte AOC-Bescheinigung in Verbindung mit einer jährlichen Vor-Ort-Sicherheitsprüfung oder einem Selbsteinschätzungsfragebogen, der AOSC-Bescheinigung sowie Zusammenfassungen der in Verbindung mit dem vierteljährlichen Netzwerkscan oder dem jährlichen STEP-Nachweis eingereichten Ergebnisse.

American Express Payments Europe, S.L. – Austrian Branch, Rathausstraße 1, 1010 Wien,
Zweigniederlassung einer Gesellschaft mit beschränkter Haftung nach spanischem Recht mit Sitz in Madrid. Avenida Partenón 12–14, 28042, Madrid, Spanien, eingetragen im Registro Mercantil de la Provincia de Madrid, Hoja M-664153, Tomo 37236, Folio 20.

Firmenbuchgericht der Zweigniederlassung: Handelsgericht Wien, Firmenbuchnummer: FN 493466 k, UID Nr: ATU73463147

American Express Payments Europe, S.L. hat eine Lizenz der Banco de España, Madrid, zur Erbringung von Zahlungsdienstleistungen (Referenznummer 6883).

DSOP-AP_AT_202402