

Allgemeine Datensicherheitsrichtlinien für Vertragspartner

2

Diese Datensicherheitsrichtlinien von American Express Payment Services Limited, Zweigniederlassung Frankfurt am Main, Theodor-Heuss-Allee 112, 60486 Frankfurt am Main („American Express“ bzw. „wir“) sind Bestandteil Ihres Vertrags für die Akzeptanz von American Express® Karten („Vertrag“) und gelten für Ihre sämtlichen Geräte, Systeme und Netzwerke, mit denen Informationen von American Express Kreditkarteninhabern erhoben, gespeichert, verarbeitet und übertragen werden.

American Express Datensicherheitsrichtlinien für Vertragspartner

§ 1 Datensicherheitsstandards für Vertragspartner

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

1. Informationen in Bezug auf Kreditkarteninhaber nur zu speichern, um die Abwicklung von Kreditkartentransaktionen nach Maßgabe Ihres Vertrages zu ermöglichen, sowie
2. die aktuelle Fassung des Datensicherheitsstandards der Zahlungskartenbranche (Payment Card Industry Data Security Standard – PCI-Standard, abrufbar unter www.pcisecuritystandards.org) spätestens ab dem Stichtag zur Implementierung dieser Fassung einzuhalten. Sie sind verpflichtet, den PCI-Standard regelmäßig von der angegebenen Website abzurufen und stets die aktuellste Version zu implementieren.

Zur Klarstellung wird darauf hingewiesen, dass die Datenelemente, die die Karteninhaberinformationen bilden, je nach ihrer jeweiligen Bedeutung als „Karteninhaberdaten“ und „sensible Authentifizierungsdaten“ im Sinne des gültigen PCI-Standards zu behandeln sind. Sie sind verpflichtet, sämtliche nach Maßgabe Ihres Vertrags aufzubewahrenden 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. Ihre Datensicherheitsmaßnahmen für die Karte dürfen die Sicherheitsvorkehrungen für von Ihnen akzeptierte Andere Zahlungsprodukte (im Sinne von Ziffer 2 Absatz 3 Buchstabe d der Allgemeinen Bedingungen für Vertragspartner) nicht unterschreiten. 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 die Datensicherheitsbestimmungen haften Sie.

(2) „Eingeschaltete Dritte“ im Sinne des Absatzes 1 bezeichnet Ihre Mitarbeiter, Bevollmächtigte, Vertreter, Ihre Subunternehmer, Verarbeiter bzw. Processing-Agents im Sinne von Ziffer 14 der Allgemeinen Bedingungen für Vertragspartner, Ihre Dienstleister, Ihre Lieferanten von POS-Geräten oder -Systemen oder Zahlungsabwicklungslösungen sowie jede sonstige Partei, der Sie nach Maßgabe des Vertrages Zugang zu Kreditkarteninhaberdaten gewähren.

§ 2 Pflichten und Haftung des Vertragspartners bei einem Datenvorfall

(1) Pflichten zur Benachrichtigung von American Express bei einem Datenvorfall: Sie müssen American Express sofort benachrichtigen, wenn Sie Kenntnis davon haben oder den Verdacht hegen, dass auf Karteninhaberdaten ohne Genehmigung zugegriffen wurde oder dass solche Daten ohne Genehmigung verwendet wurden oder auf eine Art und Weise verwendet wurden, die gegen den Vertrag, insbesondere gegen die Bestimmungen zur Geheimhaltung sowie zur Informationsverarbeitung und zum Datenschutz, verstößt.

Die in Satz 1 aufgeführten Ereignisse werden im Folgenden jeweils einzeln als „Datenvorfall“ bezeichnet.

Kontaktieren Sie Ihren Client-Manager oder rufen Sie den Notfallservice für American Express Vertragspartner unter +49 69 9797-2222 an, wenn Sie der Meinung sind, dass auf Kreditkarteninhaberdaten unbefugt zugegriffen wurde. Bitte halten Sie Ihre American Express Vertragspartner-Nummer bereit, wenn Sie anrufen.

(2) Untersuchungspflichten: Bei einem Datenvorfall sind Sie verpflichtet, auf eigene Kosten ein umfassendes Gutachten (siehe auch nachstehenden Absatz 4) durch einen externen unabhängigen Sachverständigen über diesen Datenvorfall erstellen zu lassen oder uns zu beauftragen, einen solchen Sachverständigen auf Ihre Kosten zum Zwecke der Erstellung des Gutachtens einzuschalten. In letzterem Fall sind Sie verpflichtet, mit uns und dem von uns eingeschalteten Sachverständigen uneingeschränkt zu kooperieren und Zutritt zu Ihren Büros innerhalb der üblichen Bürozeiten zum Zwecke der Untersuchung des Datenvorfalles zu gewähren. Etwaige hierzu erforderliche Verzichts- und/oder Einwilligungserklärungen haben Sie einzuholen.

(3) Informationspflichten: Sie sind verpflichtet, American Express unverzüglich alle American Express Karten-Kontonummern, die mit dem Datenvorfall zusammenhängen, sowie das über den Datenvorfall gemäß Absatz 2 und 4 erstellte Sachverständigengutachten zur Verfügung zu stellen.

Sie müssen mit American Express zusammenarbeiten, um jegliche Probleme und Vorfälle im Zusammenhang mit dem Datenvorfall zu beheben bzw. zu korrigieren. Dies beinhaltet

1. die Zusammenarbeit mit American Express bei der Benachrichtigung der vom Datenvorfall betroffenen Kreditkarteninhaber und
2. das Zur-Verfügung-Stellen aller relevanten Informationen an American Express (und die Einholung etwaiger erforderlicher Verzichts- und/oder Einwilligungserklärungen für das Zur-Verfügung-Stellen der Informationen), damit wir prüfen können, ob Sie in der Lage sind, Datenvorfällen in Zukunft im Einklang mit dem vorliegenden Vertrag vorzubeugen.

(4) Das nach Absatz 2 zu erstellende Gutachten muss den tatsächlichen Hergang darstellen und die Ursache des Datenvorfalles feststellen sowie dazu Stellung nehmen, ob diese Richtlinien und der PCI-Standard zum Zeitpunkt des Datenvorfalles eingehalten wurden.

(5) Haftung:

1. Sie haften für sämtliche Schäden im Zusammenhang mit einem von Ihnen zu vertretenden Datenvorfall.
2. Sie sind verpflichtet,
 - a) American Express von allen Ansprüchen Dritter freizustellen, die diese im Zusammenhang mit einem Datenvorfall gegenüber American Express geltend machen,
 - b) die Haftung für alle betrügerischen Transaktionen, die auf den Datenvorfall zurückzuführen sind, zu übernehmen,
 - c) American Express sämtliche Schäden, insbesondere Kosten und Auslagen, zu ersetzen, die American Express selbst oder den unabhängigen Lizenznehmern der American Express Gruppe und/oder Kreditkartenausstellern aufgrund des Datenvorfalles entstehen (insbesondere etwaige Ansprüche Dritter und sämtliche American Express in Verbindung mit der Benachrichtigung von Kreditkarteninhabern, der Sperrung der Karten und Zusendung von Ersatzkarten, der Aufklärung und dem Monitoring der Betrugsfälle entstehenden Kosten, Rechtsanwalts- und Prozesskosten und Auslagen in angemessener Höhe sowie Kosten für Ermittlungen, Prozessführung, Vergleichsvereinbarungen, Urteile, Zinsen),

es sei denn, folgende Voraussetzungen sind kumulativ erfüllt:

- a) Sie benachrichtigen American Express bei Verdacht auf einen oder Kenntnis eines Datenvorfalles gemäß § 2 Absatz 1 und
- b) Sie haben die Sicherheitsrichtlinien und den PCI-Standard nach § 1 Absatz 1 Nummer 2 zum Zeitpunkt des Datenvorfalles eingehalten und
- c) der Datenvorfall wurde nicht durch Ihr schuldhaftes Verhalten oder durch einen Ihrer Mitarbeiter oder Bevollmächtigten schuldhaft verursacht.

§ 3 Nachweis der Einhaltung der Datensicherheitsrichtlinien

(1) Sie müssen – wie nachfolgend beschrieben – jährlich bzw. vierteljährlich die folgenden Schritte vornehmen, um die Einhaltung dieser Datensicherheitsrichtlinien und des PCI-Standards nach § 1 Absatz 1 Nummer 2 nachzuweisen (wobei ein jeder solcher Zeitraum einen Berichtszeitraum darstellt).

(2) Schritt 1 – Einstufung Ihres Unternehmens (Merchant-Level) und die Validierungsanforderungen: Die Merchant-Levels richten sich grundsätzlich nach dem Umfang der von Ihnen mit American Express Kreditkarten abgewickelten Transaktionen, die von Ihnen und Ihren Niederlassungen eingereicht werden und die für das Erreichen des höchsten Merchant-Levels bei American Express maßgeblich sind.

Darüber hinaus bewirkt ein vorangegangener Datenvorfall die Einstufung des Vertragspartners als Level 1.

American Express behält sich das Recht vor, Sie aus einem sonstigen Grund als Level 1 einzustufen, und wird Ihnen diese Einstufung und den Grund hierfür schriftlich mitteilen.

Alle Vertragspartner werden einem der in der nachfolgenden Tabelle aufgeführten drei Levels zugeordnet:

Level	Definition	Einzureichende Validierungsdokumente	Erfordernis
1	Mindestens 2,5 Millionen American Express Kreditkarten-Transaktionen pro Jahr	Bericht über die jährliche Vor-Ort-Sicherheitsprüfung (nachstehend „Annual Onsite Security Assessment“ – vgl. Absatz 3) und der vierteljährliche Netzwerk-Scan (nachstehend „Quarterly Network Scan“ – vgl. Absatz 4)	Obligatorisch
1	Jeder Vertragspartner, bei dem es einen Datenvorfall gegeben hat	Bericht über die jährliche Vor-Ort-Sicherheitsprüfung (nachstehend „Annual Onsite Security Assessment“ – vgl. Absatz 3) und der vierteljährliche Netzwerk-Scan (nachstehend „Quarterly Network Scan“ – vgl. Absatz 4)	Obligatorisch
1	Jeder Vertragspartner, den American Express aus einem sonstigen Grund als Level-1-Merchant einstuft	Bericht über die jährliche Vor-Ort-Sicherheitsprüfung (nachstehend „Annual Onsite Security Assessment“ – vgl. Absatz 3) und der vierteljährliche Netzwerk-Scan (nachstehend „Quarterly Network Scan“ – vgl. Absatz 4)	Obligatorisch

Level	Definition	Einzureichende Validierungsdokumente	Erfordernis
2	50.000 bis 2,5 Millionen American Express Kreditkarten-Transaktionen pro Jahr	Quarterly Network Scan (vgl. Absatz 4) und jährliche Selbsteinschätzung (nachstehend „Annual Self-Assessment“ – vgl. Absatz 5)	Obligatorisch
3	Weniger als 50.000 American Express Kreditkarten-Transaktionen pro Jahr	Quarterly Network Scan (vgl. Absatz 4) und Annual Self-Assessment (vgl. Absatz 5)	Dringend empfohlen

Sie sind verpflichtet, Ihren Merchant-Level und die entsprechenden Unterlagen, die Sie an American Express an die unter Absatz 7 genannte Adresse schicken müssen, nach obiger Tabelle zu bestimmen, um die Einhaltung dieser Richtlinien durch Ihr Unternehmen zu dokumentieren.

(3) Validierungsdokumente in Bezug auf das Annual Onsite Security Assessment

Bei dem Annual Onsite Security Assessment handelt es sich um eine detaillierte Vor-Ort-Prüfung Ihrer Geräte, Systeme und Netzwerke (inklusive Komponenten), mit denen Kreditkarteninhaberdaten verarbeitet, gespeichert und übertragen werden. Sie ist durchzuführen

- entweder von einem unter nachstehender Internetadresse angegebenen Qualified Security Assessor (QSA) oder
- von Ihnen selbst und ist anschließend von Ihrem Vorstandsvorsitzenden, dem Finanzvorstand oder Geschäftsführer zu bescheinigen.

Level-1-Vertragspartner müssen die Ergebnisse des Annual Onsite Security Assessments zusammenfassen und diese Zusammenfassung (sowie auf Verlangen die vollständigen Ergebnisse des Annual Onsite Security Assessments) einmal jährlich bei American Express Payment Services Limited unter der unter Absatz 7 angegebenen Adresse einreichen.

Eine Liste der QSA ist abrufbar unter www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

(4) Validierungsdokumente in Bezug auf den Quarterly Network Scan

Der Quarterly Network Scan ist ein Verfahren, mittels dessen mit dem Internet verbundene Computernetzwerke des Vertragspartners und Webserver online auf potenzielle Schwachstellen und Verwundbarkeit getestet werden. Er ist von einem Approved Scanning Vendor (ASV) durchzuführen. Eine Liste der ASV ist abrufbar unter www.pcisecuritystandards.org/pdfs/asv_report.html

Level-1- und Level-2-Vertragspartner müssen die Ergebnisse des Scans zusammenfassen und diese Zusammenfassung (sowie auf Verlangen die Ergebnisse des vollständigen Quarterly Network Scans) einmal vierteljährlich bei American Express Payment Services Limited unter der unter Absatz 7 angegebenen Adresse einreichen.

(5) Validierungsdokumente in Bezug auf den Annual Self-Assessment Questionnaire

Der Selbsteinschätzungsfragebogen der Zahlungskartenbranche (Payment Card Industry [PCI] Self-Assessment Questionnaire) ist vom Level-2-Vertragspartner als „Checkliste“ zu verwenden, um sicherzustellen, dass kritische Sicherheitsmaßnahmen zum Schutz der Kreditkarteninhaberdaten vorhanden sind. Der Fragebogen hat sämtliche Systeme oder Systemkomponenten einzuschließen, die mit der Verarbeitung, Speicherung oder Übertragung von Kreditkarteninhaberdaten zu tun haben. Der Self-Assessment Questionnaire ist abrufbar unter www.pcisecuritystandards.org/tech/supporting_documents.htm

Level-2-Vertragspartner müssen den Fragebogen wahrheitsgemäß ausfüllen und einmal jährlich bei American Express Payment Services Limited unter der unter Absatz 7 angegebenen Adresse einreichen.

(6) Voraussetzung zur Einhaltung dieser Datensicherheitsrichtlinien

Diese Sicherheitsrichtlinien gelten unter folgenden Voraussetzungen als von den Vertragspartnern der unterschiedlichen Levels eingehalten:

1. Level-1-Vertragspartner
 - Zusammenfassung des Annual Onsite Security Assessments gem. Absatz 3 bescheinigt die Einhaltung sämtlicher Anforderungen des PCI-Standards nach § 1 Absatz 1 Nummer 2 und
 - Zusammenfassung des Quarterly Network Scans gem. Absatz 4 bescheinigt, dass keine hohen Risiken bestehen.
2. Level-2-Vertragspartner
 - Zusammenfassung des Quarterly Network Scans gem. Absatz 4 bescheinigt, dass keine hohen Risiken bestehen und
 - der wahrheitsgemäß ausgefüllte Annual Self-Assessment Questionnaire gem. Absatz 5 bescheinigt, dass der Vertragspartner sämtliche Anforderungen des PCI-Standards nach § 1 Absatz 1 Nummer 2 erfüllt.
3. Level-3-Vertragspartner müssen keine Validierungsdokumente einreichen, unterliegen jedoch der Verpflichtung zur Einhaltung aller sonstigen Bestimmungen dieser Datensicherheitsrichtlinien und haften für schuldhaft Verstöße gegen diese Datensicherheitsrichtlinien und den PCI-Standard nach § 1 Absatz 1 Nummer 2. Die Durchführung eines Quarterly Network Scans gem. Absatz 4 und die Beantwortung des Annual Self-Assessment Questionnaire gem. Absatz 5 werden daher dringend empfohlen.

(7) Schritt 2 – Versand der Validierungsdokumente an American Express

Level-1- und Level-2-Vertragspartner müssen American Express die Validierungsdokumente, die in der Tabelle unter Schritt 1 (Absatz 2) als „obligatorisch“ gekennzeichnet sind, in der nachstehend jeweils aufgeführten Form übermitteln.

1. Validierungsdokumente in verschlüsselter Form auf CD an folgende Anschrift senden:

American Express Payment Services Limited
 Zweigniederlassung Frankfurt am Main
 Vertragspartnerservice, Key Account Management
 Theodor-Heuss-Allee 112
 60486 Frankfurt

Die Formel zur Entschlüsselung der Validierungsdokumente sowie der Name des Vertragspartners, der – sofern vorhanden – Sicherheitskontakt des Vertragspartners einschließlich Name, Anschrift und Telefonnummer und die 10-stellige American Express Vertragspartner-Nummer müssen an die folgende E-Mail-Adresse geschickt werden:

AmericanExpressDataSecurityEMEA@aexp.com

2. Validierungsdokumente über das sichere Portal von American Express hochladen, das von unserem Partner Trustwave zur Verfügung gestellt wird:

Bitte nehmen Sie unter der Telefonnummer +800 9000 1140 oder per E-Mail an americanexpresscomplianceDEU@trustwave.com Kontakt mit Trustwave auf, um eine Anleitung zur Nutzung dieses Portals zu erhalten.

- Validierungsdokumente von Level-1-Vertragspartnern müssen die unter Absatz 6 Nummer 1 aufgeführten Dokumente enthalten.
- Validierungsdokumente von Level-2-Vertragspartnern müssen die unter Absatz 6 Nummer 2 aufgeführten Dokumente enthalten.
- Für Level-3-Merchants gilt Absatz 6 Nummer 3.

Die Einhaltung dieser Richtlinien und des PCI-Standards nach § 1 Absatz 1 Nummer 2 sowie die Erstellung der Gutachten nach § 2 Absatz 2 und 4 und der Validierungsdokumente sowie alle damit verbundenen Maßnahmen, insbesondere nach § 3 Absatz 3 bis 5, haben Sie auf eigene Kosten sicherzustellen.

Sie haben außerdem sicherzustellen, dass Sie berechtigt sind, die in den Validierungsdokumenten enthaltenen Informationen offenzulegen, und dass diese in den Validierungsdokumenten zur Verfügung gestellt werden, ohne dass damit die Rechte Dritter verletzt werden.

(8) Schadensersatz bei verspäteter Einreichung, Kündigung des Vertrages

1. Sie werden im Falle einer verspäteten Einreichung der Validierungsdokumente an American Express einen pauschalierten Schadensersatz, wie in der folgenden Tabelle festgeschrieben, bezahlen. American Express wird Sie in jedem Berichtszeitraum separat über die geltenden Fristen zur Einreichung der Validierungsdokumente informieren.

	Level 1	Level 2
Schadenspauschale, wenn die Validierungsdokumente nicht bis zum Ablauf der ersten Frist eingehen	EUR 19.000	EUR 4.000
Weitere Schadenspauschale, wenn die Validierungsdokumente nicht binnen 30 Tagen nach Ablauf der ersten Frist eingehen	EUR 26.000	EUR 7.500
Weitere Schadenspauschale, wenn die Validierungsdokumente nicht binnen 60 Tagen nach Ablauf der ersten Frist eingehen	EUR 34.000	EUR 11.000

Der Nachweis, dass American Express gar kein Schaden oder ein geringerer Schaden als die Pauschale entstanden ist, bleibt Ihnen unbenommen. Die Geltendmachung weiterer Ansprüche, insbesondere Schadensersatzansprüche, durch American Express bleibt unberührt.

2. Darüber hinaus kann American Express den Vertrag mit Ihnen im Falle einer von Ihnen zu vertretenden verspäteten Einreichung oder der schuldhaften Nichteinhaltung dieser Richtlinien oder des PCI-Standards gem. § 1 Absatz 1 Nummer 2 aus wichtigem Grund fristlos kündigen. Die Kündigung des Vertrages schließt die Geltendmachung weiterer Ansprüche, insbesondere Schadensersatzansprüche, durch American Express nicht aus.

(9) Vertraulichkeitsverpflichtung

American Express wird angemessene Maßnahmen treffen, um die von Ihnen eingereichte Zusammenfassung bzw. die vollständige Version der Ergebnisse eines Annual Onsite Security Assessments, des PCI Self-Assessment Questionnaires und die Zusammenfassung bzw. die vollständige Version der Ergebnisse eines Quarterly Network Scans (die Validierungsdokumente) vertraulich zu behandeln, und die Validierungsdokumente für einen Zeitraum von zwei Jahren ab Zugang der Dokumente Dritten gegenüber nicht offenlegen. Dritte im vorgenannten Sinne sind nicht: Bevollmächtigte und/ oder Vertreter sowie Dienstleister und Subunternehmer von American Express, die damit beauftragt sind, American Express bei der Durchführung der Datensicherheitsrichtlinien zu unterstützen. Diese Dienstleister und Subunternehmer sind damit beauftragt, die erforderlichen Validierungsdokumente zu sammeln, auf Vollständigkeit zu prüfen und zu archivieren. Insoweit erfolgt die Erhebung und Verarbeitung personenbezogener Daten im Rahmen einer Auftragsdatenverarbeitung gemäß § 11 des Bundesdatenschutzgesetzes (BDSG); American Express bleibt „Herr der Daten“. Die Dienstleister und Subunternehmer sind bei der Ausführung ihrer Tätigkeit den vertraglich fixierten Weisungen von American Express unterworfen sowie zur Wahrung der Vertraulichkeit und des Datengeheimnisses gemäß § 5 BDSG verpflichtet. Die Vertraulichkeitsverpflichtung besteht nicht in Bezug auf Informationen,

1. die American Express bereits vor deren Offenlegung durch Sie bekannt waren und die keiner Vertraulichkeitsvereinbarung unterliegen,
2. die – ohne eine Verletzung der Bestimmungen dieses Absatzes durch American Express – der Öffentlichkeit bereits zugänglich sind oder noch zugänglich gemacht werden,
3. die American Express rechtmäßig von einem Dritten ohne eine Vertraulichkeitsverpflichtung erhalten hat,
4. die American Express unabhängig entwickelt hat oder
5. die 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 Regulierungsbehörde, einer Kontrollstelle, einer Prüfstelle oder einer Vollstreckungsbehörde) offengelegt werden müssen.

§ 4 Haftung

(1) Die Einhaltung dieser Datensicherheitsrichtlinien befreit Sie nicht von Ihrer Verpflichtung, sämtliche erforderlichen Maßnahmen zur Vermeidung eines Datenvorfalles zu ergreifen und die Karteninhaberdaten sorgfältig zu verwahren und entsprechend zu schützen. Insofern bleibt Ihre Haftung gegenüber American Express für etwaige Datenvorfälle unberührt, sofern nicht in § 2 Absatz 5 anders vereinbart. Vorstehendes berührt Ihre Haftung nach dem Vertrag nicht. Sie sind auf eigene Kosten dafür verantwortlich, diejenigen zusätzlichen Datensicherheitsmaßnahmen zu ergreifen, die notwendig sind, um ihre speziellen Daten und Interessen zu schützen.

(2) 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 Vertragspartners 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.

Ebenso übernimmt American Express keine Haftung für die ordnungsgemäße Ausführung der Tätigkeit eines Qualified Security Assessors (QSA) und/oder eines Approved Scanning Vendors (ASV) im Rahmen dieser Datensicherheitsrichtlinien.

Die Haftungsausschlüsse nach diesem Absatz gelten nicht (i) bei Vorsatz und grober Fahrlässigkeit seitens American Express, (ii) im Falle von Körper- und Gesundheitsschäden, (iii) im Falle der Verletzung wesentlicher Vertragspflichten („Kardinalpflichten“) von American Express sowie (iv) im Falle 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.

§ 5 Änderungen dieser Bestimmungen

American Express ist berechtigt, diese Datensicherheitsrichtlinien jederzeit für die Zukunft zu ändern oder zu ergänzen. American Express wird Sie in diesem Fall in Textform über die Änderungen und Ergänzungen informieren. Sie können den Änderungen und Ergänzungen innerhalb einer Frist von 30 Tagen ab Zugang der Änderungsmitteilung widersprechen. Nach fruchtlosem Ablauf dieser Frist gelten die Änderungen/Ergänzungen als genehmigt und werden Vertragsinhalt. Auf die Frist sowie auf die Folgen im Falle der Nichteinhaltung der Frist wird American Express stets in der Änderungsmitteilung hinweisen.

§ 6 Salvatorische Klausel

Sollte eine Bestimmung dieser Datensicherheitsrichtlinien unwirksam sein, so wird dadurch die Wirksamkeit der Bestimmungen im Übrigen nicht berührt. Die Vertragsparteien werden anstelle der unwirksamen Bestimmung eine wirksame vereinbaren, die in ihrem wirtschaftlichen Gehalt dem der unwirksamen Bestimmung am nächsten kommt.

Nützliche Websites:

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

PCI Security Standards Council, LLC für:

- PCI Data Security Standards
- Self-Assessment Questionnaire
- Liste der Qualified Security Assessors
- Liste der Approved Scanning Vendors

www.pcisecuritystandards.org

American Express Payment Services Limited

Zweigniederlassung Frankfurt am Main

Theodor-Heuss-Allee 112, 60486 Frankfurt am Main

Registergericht Frankfurt am Main; HRB 85745

Geschäftsleitung: Carola Paschola, Robert Oesterschlink

Zweigniederlassung einer Gesellschaft mit beschränkter Haftung nach dem Recht des Vereinigten Königreichs, Sitz in London. Directors: Lan Tu, Jonathan Halfacre, Paul Abbott, Alexander Filshie, Peter Wright, Murielle Pycock; Registrar of Companies for England and Wales, No. 06301718.

American Express Payment Services Limited hält eine Erlaubnis der Financial Services Authority zur Erbringung von Zahlungsdiensten gemäß den Vorschriften über die Erbringung von Zahlungsdiensten 2009 (484347).

Postanschrift: Theodor-Heuss-Allee 112
60486 Frankfurt am Main

Kontakt

Telefon: +49 69 9797-2222

Telefax: +49 69 9797-2760

E-Mail: AmericanExpressDataSecurityEMEA@aexp.com

American Express Payment Services Limited, Zweigniederlassung Frankfurt am Main, Theodor-Heuss-Allee 112, 60486 Frankfurt am Main; Registergericht Frankfurt am Main, HRB 85745; Geschäftsleitung: Carola Paschola, Robert Oesterschlink; Zweigniederlassung einer Gesellschaft mit beschränkter Haftung nach dem Recht des Vereinigten Königreichs, Sitz in London. Directors: Lan Tu, Jonathan Halfacre, Paul Abbott, Alexander Filshie, Peter Wright, Murielle Pycock. Registrar of Companies for England and Wales, No. 06301718.

American Express Payment Services Limited hält eine Erlaubnis der Financial Services Authority zur Erbringung von Zahlungsdiensten gemäß den Vorschriften über die Erbringung von Zahlungsdiensten 2009 (484347).

