September 2020

Weisung zur Einhaltung der PCI DSS Sicherheitsvorschriften für Vertragspartner

Allgemeines
Swisscard AECS GmbH (Swisscard) hat sich 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 Karteninhaber, Vertragspartner, Dienstleister und Kartenherausgeber aus. Die Einführung von Payment Card Industry Data Security Standards (PCI DSS) 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 Swisscard wissen wir, dass Vertragspartner unser Anliegen teilen. Wir setzen daher als Teil Ihrer Verantwortung voraus, dass Sie die Datenschutzbestimmungen der Bedingungen für die Akzeptanz von American Express Karten und diese Weisung, die wir von Zeit zu Zeit überarbeiten, einhalten.

PCI DSS
Die Payment Card Industry Data Security Standards (PCI DSS) wurden bereits vor einigen Jahren von Visa International, MasterCard, American Express, JCB und Discover entwickelt, um die weltweite Einführung konsistenter Datensicherheitsmaßnahmen zu unterstützen und Kartendaten präventiv zu schützen und damit die Sicherheit beim Umgang mit Kartendaten zu erhöhen. Sie werden vom PCI Security Standards Council publiziert und regeln die technischen und betrieblichen Anforderungen für alle Parteien, die Kartendaten speichern, verarbeiten oder übermitteln.
Die detaillierten Anforderungen der jeweils gültigen Fassung sind jederzeit unter www.pcisecuritystandards.org einsehbar.

Verantwortlichkeiten
PCI DSS ist verpflichtend für Vertragspartner, Banken, Prozessoren und Payment Service Provider, die Karteninhaberdaten für eigene Zwecke oder im Namen anderer Organisationen speichern, verarbeiten oder übermitteln. Es liegt in der Eigenverantwortung der Vertragspartner die PCI DSS einzuhalten. Vertragspartner sind auch für die Einhaltung der PCI DSS durch beigezogene Dritte wie z.B. Payment Service Provider, die in Ihrem Namen, Kartendaten verarbeiten, speichern oder übermitteln, verantwortlich. Die Kosten für die Zertifizierungsmassnahmen gehen vollumfänglich zu Lasten des Vertragspartners bzw. des beigezogenen Dritten.

Wie geht der Vertragspartner vor
Gemäss PCI DSS ist der Vertragspartner verpflichtet die von ihm getroffenen Sicherheitsmassnahmen zu dokumentieren (Zertifizierungsmassnahmen). In der nachstehenden Tabelle, finden Vertragspartner basierend auf der jährlichen Transaktionsanzahl, welche Pflichten sie haben und welche Dokumente eingereicht werden müssen, um die Einhaltung der PCI DSS gegenüber Swisscard nachzuweisen.
Vertragspartner der Stufe 2 und 3 müssen nur auf Verlangen von Swisscard Zertifizierungsdokumente einreichen, unterliegen aber dennoch der Haftung und allen anderen Bestimmungen der PCI DSS. Swisscard informiert diese designierten Vertragspartner der Stufe 2 und 3 schriftlich mindestens neunzig (90) Tage vor der erforderlichen Einreichung der Dokumente.

Tabelle „Vertragspartner“

Stufe	Jährliches Transaktionsvolumen	Zertifizierungsnachweise	Anforderungen
1	Mehr als 2,5 Millionen American Express Kartentransaktionen pro Jahr	• Bericht über das „Annual Onsite Security Assessment “	Obligatorisch
2	50.000 bis 2,5 Millionen American Express Kartentransaktionen pro Jahr	• Fragebogen „Annual PCI Data Security Assessment“SAQ	Empfohlen oder auf Verlangen von Swisscard
3	Weniger als 50.000 American Express Kartentransaktionen pro Jahr	• Fragebogen „Annual PCI Data Security Assessment“SAQ	Empfohlen oder auf Verlangen von Swisscard

Fragen und Informationen
Für anfragen betreffend PCI können Sie sich unter der Nummer 044 659 64 44 melden

Vorgehen bei einem Datenvorfall
Sie müssen Swisscard **unverzüglich, spätestens jedoch innerhalb von vierundzwanzig (24) Stunden** nach der Entdeckung eines Datenvorfalls telefonisch benachrichtigen unter **044 659 64 44** (24-h-Telefonservice)

September 2020

Glossar

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.

Annual PCI Data Security Assessment: Bei der jährlichen Selbsteinschätzung dient der PCI DSS Fragebogen „PCI Data Security Assessment" (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.