First Data.

PCI DSS - FAQ

Was ist PCI?

PCI steht für Payment Card Industry (Kreditkartenindustrie), wird im Sprachgebrauch aber oft als Abkürzung für eine der beiden folgenden Begriffe genutzt.

Das Payment Card Industry Security Standards Council ist ein Industriegremium, das sich aus Organisationen wie Visa, Mastercard, American Express und Discover zusammensetzt. Ziel des Councils ist es, einen einheitlichen Industriesicherheitsstandard zu vereinbaren, den Händler erfüllen müssen.

Der Payment Card Industry Data Security Standard (PCI DSS) ist der tatsächliche Sicherheitsstandard, der vom oben beschriebenen Council festgelegt wird. Händler müssen diese Sicherheitsanforderungen erfüllen, wenn ihr Unternehmen bargeldlose Zahlungsmittel von Kunden – z. B. Kredit- und/oder Debit-Karten – akzeptiert, überträgt oder verarbeitet.

Erfüllen Händler diese Anforderungen nicht, können diverse Konsequenzen folgen. Dies kann von speziellen Gebühren bis zur Kündigung des Akzeptanzvertrages führen. Damit wäre es für sie nicht mehr möglich, bargeldlose Zahlungsmittel von Kunden zu akzeptieren.

Zur Website des Payment Card Industry Security Standards Councils
https://de.pcisecuritystandards.org/minisite/env2/

Gilt PCI DSS für alle Unternehmen und Dienstleister?

Der Payment Card Industry Data Security Standard (PCI DSS) gilt für alle Organisationen und Händler jedweder Größe, die Informationen zu bargeldlosen Zahlungsmitteln akzeptieren, übertragen oder speichern. Das bedeutet: Bezahlt auch nur ein Kunde bei dieser Organisationen oder Händler jemals mit Kreditkarte oder Debit-Karte zahlt, gelten die PCI DSS-Anforderungen.

First Data.

Was muss ein Händler tun, um den PCI-Anforderungen zu entsprechen?

Um die Anforderungen der Kreditkartenindustrie zu erfüllen, muss ein Händler zwei Dinge umsetzen:

1. Alle Anforderungen des Data Security Standards erfüllen.

2. Die Erfüllung des Data Security Standards nachweisen (Validierung). Das heißt, dass der Händler belegen muss (in einer der Situation und Betriebsgröße entsprechenden Art und Weise), dass er sich an den Data Security Standard hält.

Für manche Händler, z. B. jene mit einem hohen Kartentransaktionsvolumen oder mit bekannten Sicherheitsproblemen, beinhaltet der Nachweis entsprechende Kontrollen vor Ort durch zertifizierte Experten.

Für die meisten Händler genügen allerdings die beiden folgenden Anforderungen:

- Die jährliche Abgabe eines PCI-Selbsteinschätzungsfragebogens (SAQ) durch den Händler.
- Das Ausführen eines vierteljährlichen Netzwerk-Schwachstellenscans durch eine zertifizierte Scan-Firma, sofern es notwendig ist.

Wichtig: Erfüllt der Händler die Regelkonformität bedeutet dies nicht automatisch, dass er auch die Validierungsanforderung erfüllt.

Was ist der PCI-Selbsteinschätzungsfragebogen (SAQ)?

Der PCI-Selbsteinschätzungsfragebogen (SAQ) ist ein Formular, das vom Payment Card Industry Security Standards Council erstellt wurde. Dieses Formular muss der Händler jedes Jahr ausfüllen und bei First Data einreichen.

Das Ausfüllen des Fragebogens hilft Händlern bei zwei Dingen:

- Die Händler können für sich selbst überprüfen, ob sie den Data Security Standard erfüllen.
- Die Händler haben etwas in der Hand um die Erfüllung des Data Security Standard nachzuweisen – und diese Validierung gegenüber First Data zu erbringen.

Seit Februar 2008 gibt es keinen Fragebogen mehr, der für alle gleich ist. Die Händler müssen nun anhand des Geschäftsmodells selbst entscheiden, in welche der fünf Kategorien sie passen – und den entsprechenden Fragebogen zur Selbsteinschätzung für ihre Kategorie ausfüllen. Für manche Händler ist der Fragebogen kurz und einfach, während der Fragebogen für andere Händler länger und fachspezifisch ist.

Wichtig: Der Händler kann mit dem Fragebogen die Erfüllung der Anforderungen nur nachweisen, wenn er auf alle Fragen die erforderliche Antwort geben kann oder Fragen mit „nicht zutreffend“ kennzeichnet.

Was bedeutet die Erfüllung des Data Security Standards?

Die Erfüllung des Data Security Standards oder die Regelkonformität bedeutet, dass der Händler alle Anforderungen des Payment Card Industry Data Security Standards erfüllt.

Was bedeutet Validierung?

Validierung bedeutet, dass ein Händler durch Standarddokumente und/oder Tests nachweisen kann, dass er den Payment Card Industry Data Security Standard (PCI DSS) erfüllt. Dabei müssen unterschiedliche Händlertypen unterschiedliche Fragen beantworten.

Ist PCI DSS ein Programm oder Gesetz der Regierung?

Nein, der Payment Card Industry Data Security Standard (PCI DSS) ist an sich kein Gesetz. Der Standard wurde von Unternehmen wie Visa, Mastercard und anderen großen Kartenfirmen festgelegt.

Händler, die sich nicht an PCI DSS halten, brechen nicht zwangsläufig ein Gesetz, aber sie verletzen die Vertragsbedingungen mit First Data und die der Kartenorganisationen. Dies bedeutet, dass der Händler möglicherweise Strafgebühren zahlen muss – oder dass Unternehmen es gegebenenfalls ablehnen, mit diesem Händler zu arbeiten. In der Folge könnte der Händler keine Kredit- oder Debit-Karten mehr akzeptieren und verarbeiten.

First Data.

Was ist ein Netzwerk-Schwachstellenscan?

Ein Netzwerk-Schwachstellenscan ist nicht bei allen Unternehmen erforderlich. Der Netzwerk-Schwachstellenscan ein automatisierter, nicht störender Prozess, der das Netzwerk und die Web-Anwendungen des Händlers via Internet beurteilt (über externe IPs). Dabei werden Schwachstellen oder Lücken identifiziert, die es einem Unbefugten oder böswilligen Nutzer erlauben könnten, sich Zugang zum Netzwerk zu verschaffen und gegebenenfalls Daten von Karteninhabern zu stehlen.

Was passiert, wenn ich nicht Data Security Standard nicht erfülle?

Wenn Ihr Unternehmen den Payment Card Industry Data Security Standard (PCI DSS) nicht erfüllt, bedeutet das für ihr Unternehmen ein größeres Risiko, da die wachsende Bedrohung durch Datenpannen und Datendiebstahl zu beträchtlichen Strafen (z. B. Bußgelder durch Banken, Ordnungsbehörden und Kartenverbände), Betrug und Rücklastschriften sowie zu Prozesskosten bis hin zu dem Verlust von Kunden führen kann.

Wenn Sie nicht PCI DSS-konform sind oder Ihren PCI DSS-konformen Status bei einem Drittanbieter nicht an First Data melden, kann es sein, dass Sie eine monatliche Gebühr an First Data zahlen müssen, bis Sie wieder PCI DSS-konform werden.

Falls es in Ihrem Unternehmen zu einer Verletzung der Datensicherheit kommt, könnte Ihnen die Erlaubnis zur Verarbeitung von Kartenzahlungen entzogen werden. Darüber hinaus riskieren Sie, Kunden zu verlieren. Die Statistik zeigt, dass 43 Prozent der Kunden, die Opfer eines Betrugs wurden, mit dem Händler, bei dem der Betrug vorkam, keine Geschäfte mehr tätigen.[1]

1 Javelin Strategy & Research, Juni 2009

Wie kann ich den Data Security Standard erfüllen und eine Validierung erreichen?

First Data stellt ein benutzerfreundliches Online-Tool zur Verfügung, welches Sie dabei unterstützt, den Payment Card Industry Data Security Standard (PCI DSS) schneller und leichter zu erfüllen und beizubehalten.

Was Ihnen die First Data Lösung bietet:

- Eine Schritt-für-Schritt-Anleitung zum Ausfüllen des jährlichen Selbsteinschätzungsfragebogens (SAQ). Die Anleitung führt Sie zu dem SAQ-Fragebogen, der zu Ihrem Unternehmen passt (A, B, C, C-vt oder D). Sie können den SAQ dann mit Unterstützung ausfüllen und so sicherstellen, dass jede Frage sorgfältig beantwortet wird.
- Bis zu 85 Prozent weniger Fragen, die zu beantworten sind. Durch „Vorab-SAQ"-Fragen können wir für Sie die passenden SAQ-Antworten vorausfüllen. Dadurch lässt sich die Anzahl der Fragen, die Sie beantworten müssen, minimieren und der Ausfüllprozess beschleunigen.
- Umfassende Unterstützung, welche die Beantwortung Ihrer Fragen sicherstellt. Wenn Sie eine Frage haben, könne wir Ihnen mit unserer integrierten Hilfs-, Führungs- und Sicherheitskompetenz zu jeder PCI DSS-Frage die passende Antwort geben – online sowie per Chat, E-Mail und Telefon.

Fallen zusätzliche Gebühren für die Nutzung des PCI Portals Lösung an?

First Data erhebt einen Jahresbetrag von 25,95 € für die Nutzung des PCI Portals, sowie dem integrierten Service wie Hilfestellungen bei der Beantwortung der Fragen und Schwachstellen-Scan.

Wenn Sie nicht PCI DSS-konform sind, stellt Ihnen First Data eine monatliche Gebühr von 14,95 € in Rechnung bis Sie die PCI DSS Konformität erreichen und nachweisen können.

Muss ich die PCI Lösung von First Data nutzen?

Als Ihr Dienstleister hoffen wir, dass Sie sich für die Nutzung unseres PCI Portals entscheiden. Es steht Ihnen jedoch frei, Dienstleistungen zur Erfüllung des Data Security Standards von Drittanbietern zu nutzen.

Die Vorteile der First Data Lösung liegen darin, dass sie eine Schritt-für-Schritt-Hilfe zum Ausfüllen des jährlichen Selbsteinschätzungsfragebogens zur Verfügung gestellt bekommen. Des Weiteren die Nutzung unseres integrierten Scan-Tools für Händler, die vierteljährliche Netzwerk-Schwachstellenscans bestehen müssen, sowie eine umfassende Unterstützung (online, per Chat, E-Mail und Telefon), um die Beantwortung Ihrer Fragen jederzeit sicherzustellen.

Falls Sie sich für die Dienstleistungen eines Drittanbieters entscheiden, bekommen Sie von diesem Anbieter eine separate Rechnung für dessen Leistungen.

Warum wird First Data nicht als ein PCI-anerkannter QSA (Qualified Security Assessor) auf der Website des PCI-Councils aufgeführt? Warum muss First Data kein QSA sein?

Die PCI Lösung ist ein automatisiertes Online-Tool zur Selbsteinschätzung, welches wir als First Data anbieten, um unsere Händler durch den PCI DSS-Compliance-Prozess zu führen. Die Lösung bietet die Unterstützung eines Live-Help-Desks, Informationen zu potenziellen Schwachstellen sowie innovative Sicherheitsverbesserungen, die das Abwicklungsumfeld unserer Händler noch weiter schützen können.

PCI-Händler mit Level 3 oder 4 müssen ihre Erfüllung des Data Security Standards nicht durch einen Qualified Security Assessor (QSA) mittels Selbsteinschätzung validieren. Deshalb muss First Data kein QSA sein. Jedoch wurde die PCI Lösung gemeinsam mit einem QSA entwickelt, um den Selbsteinschätzungs-Validierungsprozess für Händler viel einfacher zu gestalten. Des Weiteren unterstützt ein Approved Scanning Vendor (ASV) vierteljährliche Netzwerk-Schwachstellenscans, die für Händler, die Zahlungen über das Internet abwickeln, vorgeschrieben sind.

Für Händler mit Level 1 und 2, die einen QSA für ihre PCI DSS-Compliance-Validierung benötigen, finden sich PCI-anerkannte QSAs auf der Website des PCI-Councils.