

Übersicht der derzeit aktuellen PCI DSS Vorgaben der Kartenorganisationen

	Self Assessment (SAQ)	Schwachstellen Scan	Security Audit
Level 1 >6 Mio. Transaktionen p.a. und per Brand über alle Vertriebskanäle (POS, E-Com, MOTO)	xx	4 mal pro Jahr	1 mal pro Jahr
Level 2 1 - 6 Mio. Transaktionen p.a. und per Brand über alle Vertriebskanäle (POS, E-Com, MOTO)	1 mal pro Jahr	4 mal pro Jahr	1 mal pro Jahr
Level 3 20.000 bis 1 Mio. E-Commerce Transaktionen per Brand	1 mal pro Jahr	4 mal pro Jahr	xx
Level 4 < 20.000 Transaktionen E-Commerce und < 1 Mio. Transaktionen p.a. und per Brand für alle anderen Händler*	1 mal pro Jahr	4 mal pro Jahr	xx

Hinweis:

Für Händler, welche von der First Data bzw. TeleCash bereit gestellte Terminals nutzen und die Transaktionen bei der First Data bzw. TeleCash verarbeiten lassen, kann unter bestimmten Umständen der Scan entfallen und der PCI DSS Prozess vereinfacht werden. Hierzu beraten wir Sie gerne.

Wie können wir Ihnen weiterhelfen?

Das PCI DSS Portal führt Sie durch den gesamten Prozess.

Sollten Sie darüber hinaus weitere Informationen zu Ihrer PCI DSS Compliance haben, stehen wir Ihnen gerne montags bis freitags von 09:00 - 18:00h zur Verfügung:

Deutschland: +49 61 72869 3000

Österreich: +43 720 880 306

Email: pcidss@fdpcidss.com

Weitere Informationen erhalten Sie auf den folgenden Internet-Seiten:

pcisecuritystandards.org

mastercard.com/sdp

visa.com/cis

visaaustralia.com/ais

First Data®

Sicher bargeldlos bezahlen -
ermöglicht durch den PCI DSS Standard

First Data®

Der PCI DSS (Payment Card Industry Data Security Standard) ist ein weltweit gültiger Sicherheitsstandard der führenden internationalen Kreditkartenorganisationen für den Umgang mit Zahlungsdaten

Wer muss den PCI DSS-Sicherheitsstandard einhalten?

Alle Unternehmen, die Debit- und/oder Kreditkartendaten akzeptieren, speichern, verarbeiten oder übermitteln sind verpflichtet, die Vorgaben des PCI DSS einzuhalten und dieses jährlich nachzuweisen.

Händler müssen insgesamt zwölf Punkte innerhalb des PCI DSS Regelwerkes einhalten. Für den Nachweis sind je nach Geschäftsmodell lediglich eine Online-Registrierung samt Beschreibung des Business, ggf. zusätzliche Scans der internen Daten und bei Großkunden zusätzlich ein Audit durch eine seitens der Kartenorganisationen zertifizierte Firma notwendig.

Datenschutz für Sie und Ihre Kunden

Händlern dient der PCI DSS Standard zur Absicherung der eigenen Systeme:

- Entfernen von sensiblen Daten aus den Systemen
- Schutz des internen, externen und WLAN Netzwerkes
- Schutz der Daten durch gezieltes Monitoring und Zugangsbeschränkung zu Karteninhaberdaten
- Sicherung von Karten- und Kundendaten gegen Diebstahl
- Mehr Kundenvertrauen und somit Potenzial für mehr Kreditkarteneinsätze
- Größere Absicherung vor finanziellen Schäden und Schadensersatzklagen
- Bewertung des Sicherheitsschutzes Ihrer Systeme



Welchen Vorteil bietet die Zusammenarbeit mit First Data?

Händler und Dienstleister müssen eine schriftliche Vereinbarung treffen, wer für welche Aspekte der Sicherheit von Karteninhaberdaten verantwortlich ist. Die Zusammenarbeit mit uns erfüllt diese Anforderung und minimiert Ihre Aufwände.

Unsere Leistungen:

1. Unterstützung bei der Reduzierung Ihrer PCI DSS Aufwände und Beratung zu allen Fragen rund um PCI DSS.

Sie reduzieren Ihre Aufwände, bei Nutzung

- unseres Netzbetriebs / Prozessings, welche den PCI DSS Anforderungen entsprechen
- unserer bereitgestellten Terminals, welche den aktuellen PCI DSS Standard unterstützen
- unseres Internet Payment Gateway (IPG), so dass Sie alle sensiblen Daten zu First Data auslagern

2. Durchführung des PCI DSS Prozesses durch unseren PCI DSS Dienstleister.

First Data bietet Ihnen den kompetenten Service, sich umfassend überprüfen und zertifizieren zu lassen.

- Sie erhalten von uns ein Begrüßungsschreiben mit den notwendigen Login Daten und Support-Nummern
- Sie registrieren sich online und geben alle erforderlichen Daten ein
- Unser PCI DSS Portal leitet Sie dann intuitiv durch alle notwendigen Schritte für die Prüfung und Zertifizierung
- Unterstützung steht Ihnen per Live-Chat, Telefon und Online-Hilfe zur Verfügung

3. Link zum PCI DSS Portal der First Data: fdpcidss.com

Welche 12 Punkte müssen geprüft und umgesetzt werden?

1. Installation und regelmäßige Aktualisierung einer Firewall zum Schutz von Karten- und Transaktionsdaten
2. Regelmäßige Änderung der Systempasswörter oder anderer Sicherheitseinstellungen
3. Vermeidung der unnötigen Speicherung von Karten- und Transaktionsdaten
4. Verschlüsselte Übertragung von Karten- und Transaktionsdaten in offenen Netzwerken
5. Verwendung und regelmäßige Aktualisierung von Antivirenprogrammen
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen
7. Beschränkung des Datenzugriffs auf Karten- und Transaktionsdaten gem. dem Grundsatz: „Kenntnis nur wenn nötig“
8. Zuteilung einer eindeutigen Benutzerkennung für jede Person mit Zugang zum Computersystem
9. Restriktive Vergabe von Berechtigungen zum Zugriff auf sensible Karten- und Transaktionsdaten
10. Protokollierung und Überwachung aller Zugriffe auf Netzwerke sowie auf Transaktionsdaten
11. Regelmäßige Überprüfung von Sicherheitssystemen und Prozessabläufen
12. Festlegung unternehmensweiter Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner