

PCI DSS

PCI DSS steht für Payment Card Industry Data Security Standard und enthält ein Regelwerk zur sicheren Abwicklung von Kreditkartentransaktionen. Grundsätzlich unterliegen alle Beteiligten an einer Kreditkartenzahlung (also beispielsweise Händler und PSP) diesen Regeln, sobald sie Kreditkartendaten verarbeiten, übertragen oder speichern.

Hier eine kleine Übersicht über die grundlegenden 12 Anforderungen aus dem PCI DSS Standard:

1. Installation und Pflege einer Firewall, um die Kartendaten zu schützen
2. Ersetzen von Standard-Zugangsdaten oder anderen Standard-Werten in Sicherheitseinrichtungen
3. Schutz gespeicherter Kartendaten
4. Verschlüsselte Übertragung von Kartendaten über öffentliche Netzwerke
5. Installation und regelmäßige Aktualisierung von Anti-Viren-Software oder Programmen
6. Entwicklung und Pflege von sicheren Systemen und Applikationen
7. Zugriffsbeschränkungen auf Kartendaten "Need-to-Know"-Prinzip
8. Jeder Computer-Zugang muss eindeutig einer Person (nicht Gruppe) zugeordnet werden können
9. Physikalische Zugriffsbeschränkungen auf Kartendaten
10. Verfolgung und Beobachtung aller Zugriffe auf Netzwerk-Ressourcen und Kartendaten
11. Regelmäßige Tests der Sicherheitssysteme und -prozesse
12. Sicherheitsrichtlinien für Mitarbeiter und Dienstleister

Das vollständige PCI-DSS-Regelwerk ist hier veröffentlicht: https://www.pcisecuritystandards.org/document_library

Die Einhaltung dieser Regeln wird im Rahmen einer PCI-DSS-Zertifizierung überprüft. Ihr Acquirer ist für die Überprüfung Ihrer PCI-DSS-Zertifizierung verantwortlich.

Der Nachweis erfolgt

- entweder über Fragebögen, welche von Ihnen auszufüllen sind. Diese Fragebögen werden als SBF (Selbstbeurteilungsfragebogen) bzw. als SAQ (Self-Assessment Questionnaire) bezeichnet. Die Fragebögen werden abhängig von der Art, wie Sie Kreditkartendaten verarbeiten, in verschiedene Klassen eingeteilt (SAQ A, SAQ A-EP, ... bis hin zu SAQ D).
- Alternativ zum Fragebogen kann auch ein persönliches PCI DSS Audit erforderlich sein. Diese Entscheidung obliegt dem Acquirer bzw. dem PCI-DSS-Prüfer.

Computop und Computop Paygate werden jedes Jahr erneut gemäß PCI DSS Level 1 zertifiziert - dem strengsten PCI DSS level. Sie können unser aktuelles PCI DSS Zertifikat hier finden und herunterladen: <https://computop.com/de/support/developers-downloads>



Vereinfachen Sie Ihre PCI DSS Zertifizierung

Computop Paygate unterstützt Sie bei der Einhaltung dieser Regeln, indem es Ihnen die direkte Verarbeitung der Kreditkartendaten abnimmt, wenn Sie die "[Hosted Payment Page](#)" oder das [Kreditkartenformular \(PaySSL\)](#) verwenden. In der einfachsten Form ist dann der Nachweis gemäß SAQ A möglich.

Die **PcNr (Pseudokartenummer, PKN)** unterliegt nicht den PCI-DSS-Regeln, da es sich nicht um eine Kreditkarte handelt, sondern nur um einen internen Token, welches eine Kreditkarte referenziert.