

PCI DSS = Payment Card Industry Data Security Standard = PCI

PCI DSS ist ein Sicherheitsstandard mit strengen Vorgaben, der den sorgfältigen und geschützten Umgang mit Zahlungskartendaten sicherstellen soll. Dieser wurde von den wichtigsten Kreditkartenunternehmen (Visa, MasterCard, American Express und JCB) ins Leben gerufen.

Um die sensiblen Finanzdaten der Vertragsunternehmen sowie der teilnehmenden Karteninhaber zu schützen, ist es notwendig, dass die vom Vertragsunternehmen verarbeiteten Karteninhaberdaten gesichert und vor Hacker-Angriffen geschützt werden.

Folgende Anforderungen beinhaltet PCI DSS:

1. Einrichtung und Betrieb einer Firewall zum Schutz der Daten von Karteninhabern
2. Änderung der von Herstellern vorgegebenen Standardpasswörter und Sicherheitseinstellungen
3. Schutz der gespeicherten Daten von Kreditkarteninhabern
4. Verschlüsselte Übertragung der Daten von Kreditkarteninhabern in öffentlichen Netzwerken
5. Einsatz und regelmäßige Aktualisierung von Virenschutzlösungen
6. Entwicklung und Verwendung sicherer Systeme und Anwendungen
7. Einschränkung des Zugriffs auf Kreditkartendaten nach dem Grundsatz „Kenntnis nur wenn nötig“
8. Zuweisung einer eindeutigen Benutzerkennung an jede Person mit Zugang zum Computersystem
9. Einschränkung des physikalischen Zugriffs auf Karteninhaberdaten
10. Protokollierung und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Karteninhaberdaten
11. Regelmäßige Überprüfung von Sicherheitssystemen und -abläufen
12. Einrichtung einer Unternehmensrichtlinie mit Vorgaben zur Informationssicherheit für Mitarbeiter und Vertragspartner

**Diesem verbindlichen Standard unterliegen alle Unternehmen,
die Kredit- und Debit-Kartendaten speichern, verarbeiten und/oder übermitteln.**

Sie können Sie auch hier direkt informieren: <https://www.pcisecuritystandards.org/>

Durch die Einhaltung der verbindlichen PCI-DSS-Regeln schützen Sie sich und auch Ihre Kunden vor kriminellen Angriffen. Diese wichtige Sicherheit werden Ihre Kunden schätzen.

Die Vorteile für Ihr Unternehmen:

- ✓ Erhöhte Datensicherheit und Schutz für Ihre Kunden
- ✓ Gesteigertes Kundenvertrauen
- ✓ Schutz des Unternehmens-Images
- ✓ Minimierung des Unternehmensrisikos durch Minimierung und Vermeidung sensibler Daten
- ✓ Absicherung von finanziellen Schäden und möglichen Schadenersatzansprüchen aufgrund von Sicherheitsverletzungen