

PROTEL  
PCI  
COMPLIANCE



protel PCI Compliance

**SICHERER UMGANG MIT KREDITKARTENDATEN**

Whitepaper der protel hotelsoftware GmbH

# PROTEL PCI COMPLIANCE



protel Dokumentation | protel PCI Compliance | 1.0 (06/2008)

Verpflichtender Sicherheitsstandard für den Umgang mit Kreditkartendaten



➔ Unterstützung durch protel

„**PCI-Compliance**“ ist der seit 2007 global verbindliche Sicherheitsstandard der weltweit größten Kreditkartenfirmen. Er besteht im Wesentlichen aus zwölf konkreten Handlungsanweisungen. Händlerbanken und Providern obliegt es, die Umsetzung dieser Regeln bei allen, die mit Kreditkarten arbeiten, zu überwachen und durchzusetzen.

Dieser Artikel macht Sie mit den wichtigsten Vorgaben der PCI-Compliance bekannt und informiert Sie darüber, wie die protel Hotelmanagement-Systeme Sie bei deren Umsetzung in Ihrem Haus unterstützen.

## Kreditkarten in der Hotellerie: Chance und Risiko

Per Kredit- oder Euroscheckkarte bargeldlos bezahlen können – auch und gerade für den Gast in Hotels und Restaurants ist das heutzutage eine bequeme Alltäglichkeit und ein Service, den er ganz selbstverständlich erwartet.

Bei jedem dieser Zahlungsvorgänge, sei es bei der Begleichung der Rechnung vor Ort oder der Buchung eines Hotelzimmers über das Internet, werden zahlreiche Informationen über den Kontoinhaber bekannt und gespeichert. Diese gilt es vor Missbrauch zu schützen.

Denn je mehr sich der bargeldlose Zahlungsverkehr etabliert (weltweit sind zur Zeit mehr als 2 Milliarden Karten im Umlauf!), desto deutlicher zeigen sich seine Risiken wie Kreditkartenbetrug und Datenmissbrauch - und desto mehr drängen die regulierenden Behörden und Institutionen auf die Einhaltung einschlägiger Datenschutzbestimmungen.

## Datenschutz: Herausforderung und Verpflichtung ...

Sie, als Hotelier und Unternehmer, unterliegen deshalb zahlreichen rechtlichen Verpflichtungen. Das Bundesdatenschutzgesetz, EU-Richtlinien (Schlagwort SEPA) sowie internationale Konventionen und Standards regeln den Umgang mit den sensiblen Kundendaten – ein schier unüberschaubares Dickicht von Gesetzen, Regeln und Bestimmungen, bei deren Missachtung zivilrechtliche und auch strafrechtliche Sanktionen drohen.

Besonders persönlich haftende Geschäftsführer und Vorstände von GmbHs und AGs tun deshalb gut daran, sich mit dem Thema „Datensicherheit beim Umgang mit Kreditkartendaten“ zu befassen.

## ... und vertrauensbildende Maßnahme

Nach Bob Russo, General Manager, PCI Security Standards Council ist es das vordringliche Ziel des PCI-Sicherheitsstandards „... die Datensicherheit für Karteninhaber zu steigern und das Risiko von Datenverletzungen gering zu

Spagat zwischen Service und Schutz vor Kriminalität

➔ Fehlender Datenschutz kann teuer werden

Nachweislicher Datenschutz ist „gut für's Geschäft“

halten. Denn derartige Sicherheitsverstöße können für die positive Wahrnehmung der Sicherheitspraktiken von Händlern und Finanzinstitutionen in der Zahlungskette in den Augen der Öffentlichkeit ein Problem darstellen“.

Der PCI-Sicherheitsstandard:

- 2001 auf den Weg gebracht
- Seit 2005 allgemein gültig
- Seit 2007 weltweit verbindlich

### Das Ende der Verwirrung: standardisierte Sicherheit

2001 brachte Visa ein Programm namens CISP (Cardholder Information Security Program) auf den Weg, dessen Ziel es war, die Sicherheit von Transaktionen mit Visa-Kreditkarten zu erhöhen. 2005 wurde diese Programm in erweiterter Form von allen großen Kreditkartenfirmen, darunter auch MasterCard, Discover und American Express, übernommen und zum gemeinsamen Standard unter der Bezeichnung „Payment Card Industry (PCI) Data Security Standard (DSS)“ erklärt. Seit Ende 2007 ist das PCI-Regelwerk für alle Händler, die im Zahlungsverkehr mit Kreditkartendaten arbeiten, **weltweit verbindlich**.

### Verbindlichkeit des PCI-Sicherheitsstandards

PCI DSS hat zwar seinen Ursprung in den USA, gilt jedoch weltweit für jede Organisation, die mit Kreditkartendaten arbeitet. Das PCI Security Standards Council schlägt dabei lediglich vor und berät; da jedoch kein Rechtsverhältnis zwischen ihm und Händlern oder Dienstleistern besteht, ist es nicht seine Aufgabe, die Nichteinhaltung seiner Vorgaben zu sanktionieren.

➔ Umsetzung im Einzelunternehmen wird durch Kreditkartenanbieter und Händlerbanken geprüft

Die „PCI-Compliance“, d.h. also die nachweisliche Übereinstimmung der Verfahren eines Unternehmens mit den Vorgaben dieses Regelwerkes, wird **vom jeweiligen Kreditkartenanbieter geprüft** und attestiert. Wird der Standard nicht umgesetzt, kann dem Unternehmen die Zusammenarbeit aufgekündigt werden. Darüber hinaus drohen empfindliche Strafen in sechsstelliger Höhe, wenn Daten verloren gehen oder gestohlen werden.

### Wer ist denn nun betroffen – und wie?

Registrieren oder Zertifizieren?

Der Nachweis der PCI -Compliance wird von allen Händlern und Dienstleistern verlangt, die Kreditkartentransaktionen vornehmen – also auch von Hotels.

Die Anzahl der Kreditkartentransaktionen pro Jahr bestimmt die Maßnahmen

Ob sich ein Hotel **prüfen und zertifizieren** lassen muss oder ob es genügt, sich **registrieren** zu lassen, hängt von der Menge der durchgeführten Transaktionen ab. Die zeitliche Dauer der Verarbeitung (kurzfristige oder langfristige Speicherung, Verarbeitung oder Weiterleitung) spielt dabei keine Rolle.

Unter 20.000 ist eine Prüfung nicht erforderlich.

Dies gilt übrigens auch für Unternehmen, die mit einem Payment Service Provider zusammen arbeiten: Sobald Sie Daten auch auf Ihren eigenen Systemen speichern, unterliegen Sie der Pflicht zur PCI-Compliance.

In der Regel müssen sich Händler oder Dienstleister, die weniger als 20.000 Kreditkartentransaktionen im Jahr abwickeln, zwar an die Regelungen halten, eine Prüfung ist jedoch – wenn auch empfohlen - nicht obligatorisch.

## Sechs Kontrollziele / zwölf Richtlinien

Die Ziele und Vorgaben des PCI-Sicherheitsstandards sind eigentlich recht übersichtlich:

### Kontrollziel 1

#### **Einrichtung und Unterhaltung eines sicheren Netzwerks**

Anforderung 1: Installation und Verwaltung einer Firewallkonfiguration zum Schutz von Karteninhaberdaten

Anforderung 2: Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter

### Kontrollziel 2

#### **Schutz von Karteninhaberdaten**

Anforderung 3: Schutz von gespeicherten Karteninhaberdaten

Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke

### Kontrollziel 3:

#### **Verwalten eines Programms zur Bewältigung von Sicherheitsrisiken**

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen

Anforderung 6: Entwicklung und Verwaltung sicherer Systeme und Anwendungen

### Kontrollziel 4:

#### **Implementieren strikter Zugriffssteuerungsmaßnahmen**

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten auf die geschäftlich erforderlichen Daten

Anforderung 8: Zuweisung einer eindeutigen ID zu jeder Person mit Computerzugriff

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

### Kontrollziel 5:

#### **Regelmäßiges Überwachen und Testen von Netzwerken**

Anforderung 10: Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten

Anforderung 11: Regelmäßiger Test von Sicherheitssystemen und –prozessen

### Kontrollziel 6:

#### **Verwalten einer Informationssicherheitsrichtlinie**

Anforderung 12: Verwaltung einer Richtlinie zur Informationssicherheit

Hintergrundinformation und Handlungsanweisungen zu jedem der zwölf Punkte liefert die 19-seitige deutsche Version des derzeit geltenden Sicherheitsstandards (Version 1.1, veröffentlicht seit Februar 2008, verbindlich seit Mai 2008). Sie kann von der Website des PCI SSC unter

[https://www.pcisecuritystandards.org/pdfs/german\\_pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/german_pci_dss_v1-1.pdf) als PDF heruntergeladen werden.

Umfassende Informationen zum Thema auf der Website des PCI SSC

## Datenschutz mit protel

Je nach Menge der in Ihrem Haus getätigten Kreditkartentransaktionen sind Sie zu mehr oder weniger aufwändigen Maßnahmen verpflichtet, die vom freiwilligen Ausfüllen eines Fragebogens bis zum ausgewachsenen "SecurityScan" des gesamten Unternehmens reichen (wobei die Sinnhaftigkeit vieler dieser gewissermaßen nachgeschobenen Maßnahmen durchaus kontrovers diskutiert wird).

Auch wenn die Sinnhaftigkeit vieler dieser gewissermaßen nachgeschobenen Maßnahmen durchaus kontrovers diskutiert, ändert das nicht daran, dass empfindliche Strafen drohen, wenn durch die Nichtbeachtung einer der zwölf PCI-Richtlinien Daten verloren gehen oder missbraucht werden.

## Was nicht gespeichert wird, muss nicht geschützt werden

Der erste Grundsatz des Datenschutzes und gleichzeitig die einfachste Lösung: Je weniger Daten Sie speichern, desto weniger Daten müssen Sie schützen.

Dabei gilt besonders beim Umgang mit Kreditkarten:

- Vertrauliche Identifizierungsdaten (Daten des Magnetstreifens und die Kartenprüfnummer) **dürfen** gar nicht gespeichert werden.
- Die Speicherung von Karteninhaberdaten (PAN, Karteninhabername und Ablaufdatum) sind unter der Voraussetzung erlaubt, dass **kein unbefugter Zugriff** darauf erfolgen kann.

## protel und PCI Compliance

protel kann Sie wirkungsvoll bei der Umsetzung des PCI-Sicherheitsstandards unterstützen:

- Restriktive Zugriffsrechte kontrollieren den Zugriff auf Kreditkartendaten (vergl. Anforderung 7 - 9). Nur diejenigen, die tatsächlich mit den Kreditkartendaten arbeiten (und z. B. nicht die Mitarbeiter des Housekeeping), dürfen darauf zugreifen.
- Jeder Zugriff wird geloggt und kann über Berichte abgefragt werden (vergl. Anforderung 8 und 10).
- Kreditkartendaten werden nur für die aktuelle Reservierung vorgehalten.
- Kreditkartendaten können nicht mehr in der Gästekartei gespeichert oder aus der Reservierungsmaske übernommen werden.
- Sie werden entweder nach einer frei konfigurierbaren Anzahl von Tagen aus der Datenbank gelöscht
- oder nach dem Check-out beim Tagesabschluss.

**Auf Wunsch schicken wir Ihnen gern eine detaillierte Anleitung dazu, wie Sie protel zur Umsetzung der PCI-Sicherheitsregeln konfigurieren.**

➔ protel unterstützt Sie bei der Einhaltung der Vorgaben zur PCI-Compliance

➔ Mit protel Schritt für Schritt zur PCI-Compliance

# PROTEL PCI COMPLIANCE



protel Dokumentation | protel PCI Compliance | 1.0 (06/2008)

Wenn Sie Fragen haben oder weitere Informationen wünschen, sprechen Sie uns an! Wir beraten Sie gern!

**Kontakt:**

protel hotelsoftware GmbH  
Europaplatz 8  
D-44269 Dortmund

- fon +49 231 915930  
- fax +49 231 91593999

[support@protel-net.com](mailto:support@protel-net.com)

<http://www.protel-net.com>