

PROTEL  
PCI  
COMPLIANCE



protel PCI Compliance

**CREDIT CARD TRANSACTIONS WITH CONFIDENCE**

Whitepaper by protel hotelsoftware GmbH

# PROTEL PCI COMPLIANCE



protel Dokumentation | protel PCI Compliance | 1.00 (08/2008)

Binding security standard for the handling of credit card data



➔ Supported by protel

**"PCI" is a credit card data security standard developed by the major credit card companies. The current version of the standard (1.1 | 2008) specifies twelve requirements for compliance. A company processing, storing, or transmitting payment card data must validate their PCI compliance periodically or risk losing their ability to process credit card payments and being audited and/or fined.**

**This article introduces the essential requirements of the Payment Card Industry - Data Security Standard (PCI DSS) and points out how the protel hotel management systems can facilitate its implementation in your hotel.**

## **Call for action: credit card security in the hospitality industry**

Being able to make cashless payments by credit or EC card is - even and especially for the guest in hotels and restaurants - a comfortable everyday occurrence and a service that he nowadays expects as a matter of course.

Whenever a guest settles his account on site or reserves a room via the internet, in other words whenever cashless payment transactions are processed plenty of information about the card holder are sampled and stored. The protection against misuse of information therefore is essential.

Since more and more cashless payments transactions are processed (at present more than 2 billions of cards circulate worldwide!), the risks such as credit card fraud and data misuse become apparent - and the more corrective authorities and institutions press for the implementation of the respective data protection regulations.

## **Data protection: challenge, commitment...**

Thus, as hotelier and entrepreneur, you are subject to numerous legal obligations. The Federal Data Protection Act, EU directives (headword SEPA) as well as international conventions and standards regulate the handling of the sensitive cardholder data - a vast jungle of laws, rules and regulations that in case of disregard impose civil and penal sanctions.

Personally liable managing directors and boards of corporations and companies therefore do well to look into the subject.

## **... and confidence-building measure**

According to Bob Russo, general manager of the PCI Security Standards Council, the ultimate objective of PCI DSS is "... to increase the data security for cardholders and to minimize the risk of data contamination. Because such breaches of security can pose a problem regarding the positive perception of security measures of traders and financial institutions within the payment chain from the public's point of view".

Span between service and protection against fraud

➔ Inadequate data protection can get costly

Demonstrable data security is "good for business"

## The PCI Security Standard:

- Brought out in 2001
- Concerted campaign since 2005
- Valid worldwide since 2007

## The end of confusion: standardized security

In 2001, Visa brought out a program called CISP (Cardholder Information Security Program) with the intention to increase the security of transactions via credit cards. In 2005, this program was adopted in an extended version by all large credit card companies, among them MasterCard, Discover and American Express, and was declared as joint standard under the designation "Payment Card Industry (PCI) Data Security Standard (DSS)". Since the end of 2007, the PCI regulations are a global requirement for all traders who work with credit card data in payments.

## PCI Security Standard: a global requirement

Although PCI DSS was founded in the USA, it is effective for all companies that work with credit card data. The PCI Security Standards Council proposes and gives advice in this process. But as there is no legal relationship between the council and traders or service providers, it is not its task to sanction the disregard of its own specifications.

➔ Implementation controlled by credit card providers and merchant banks

Instead, the "PCI-Compliance", i.e. the conformity of a company's business and IT processes with the specifications of the PCI standard, is verified and certified **by the respective credit card provider**. If the standard is not implemented, the cooperation with the company can be terminated. Moreover, if data gets lost or is stolen, considerable fines to the amount of a six figure sum can be imposed.

## To whom does PDI DSS apply - and in which way?

All companies processing, storing, or transmitting payment card data must be PCI DSS compliant - including hotels and restaurants.

The number of credit card transactions per year determines the measures.

Whenever a Primary Account Number (PAN) is stored, processed, or transmitted, PCI DSS requirements apply. Depending on the number of conducted transactions a hotel can be required to undergo an on-site data security assessment and quarterly network scans. So called "level 4" -merchants with less than 20.000 e-commerce transactions can validate their compliance by performing a self-assessment questionnaire (SAQ).

By the way: This also applies to companies that cooperate with a payment service provider: If you save any cardholder data on your own system, you are subject to PCI Compliance.

### **Six control targets / twelve specifications**

The targets and specifications of the PCI Security Standards are actually quite clear:

#### **Control target 1**

##### **Installation and maintenance of a secure network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

#### **Control target 2**

##### **Protection of card holder data**

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

#### **Control target 3:**

##### **Managing a program in order to cope with security risks**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

#### **Control target 4:**

##### **Implementing imperative access control measures**

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

#### **Control target 5:**

##### **Regular monitoring and testing of networks**

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

#### **Control target 6:**

##### **Managing of information security guidelines**

Requirement 12: Maintain a policy that addresses information security

Detailed on-topic information on the website of the PCI SSC

Background information and instructions on all twelve specifications are provided in the multilingual versions of the actual security standard (Version 1.1, published since February 2008, binding since May 2008). Download "your" PDF:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html)

## Data protection with protel

Depending on the quantity of credit card transactions processed in your hotel, you are obliged to adopt more or less complex measures to ensure credit card security. These can extend from submitting a self assessment questionnaire to a comprehensive "SecurityScan". Although the reasonableness of many of those quasi additional measures are by all means a subject for debate, that does not change the fact that considerable fines are imposed when data gets lost or is misused as a result of disregarding one of the twelve PCI specifications.

## Preliminary strategic considerations

The chief principle of data protection is at the same time its simplest solution: The less data you save, the less data you need to protect. With regard to credit cards this means:

- Confidential identification data (data of the magnetic stripe and the PIN and security number) **must** not be stored at all.
- The storage of cardholder data (PAN (Primary Account Number), name of the cardholder and expiration date) are permitted on condition that no unauthorized access is possible.

## Operate you protel hotel management system in PCI mode

protel can effectively assist you in adhering to the PCI Security Standards:

- Restrictive rights to access control the access to credit card data (cf. requirements 7-9). Only those who actually HAVE to work with credit cards (e.g. not the staff member of the housekeeping) should be allowed to have access.
- Each access is automatically logged and can be reviewed via reports (cf. requirements 8-10).
- Credit card data is exclusively available for the current reservation.
- Credit card data cannot be stored in the guest profile or transferred from the reservation user interface anymore.
- Either it will be deleted from the data base according to a free configurable number of days
- or after the check out at daily closing.

**Get to know the latest protel features that help you obtain PCI compliance in your hotel. On request we will gladly send you a detailed tutorial.**

What is not stored must not be protected.

➔ protel assists you in adhering to the specifications of the PCI Compliance

➔ Step by step with protel to PCI Compliance

# PROTEL PCI COMPLIANCE



protel Dokumentation | protel PCI Compliance | 1.00 (08/2008)

If you have any questions or would like to get more information, please contact us! We'd be happy to help you!

**Contact:**  
protel hotelsoftware GmbH  
Europaplatz 8  
D-44269 Dortmund

fon +49 231 915 93 0  
fax +49 231 915 93 999

[support@protel-net.com](mailto:support@protel-net.com)  
<http://www.protel-hotel-software.com>