Questions and Answers about PCI and protel

Why is PCI important for me as a hotelier?

The Payment Card Industry Data Security Standards, or PCI DSS for short, are the global security standards for cashless payment transactions of leading international credit card organizations. These IT security standards define technical and organizational requirements for the secure saving, processing and transmitting of card owner data and are mandatory for all companies that work with credit card payments. These leading card organizations demand compliance with the standards. Hotels that do not comply with these standards and do not get certified can be held liable by the credit card organizations in case of damages and be subject to legal recourse. To avoid the risk of claims for damages and possible damage to your reputation, a hotel should have its business certified in accordance with PCI DSS. Being certified in accordance with the PCI Data Security Standard can significantly impact the question of liability for damages if it can be proven that all PCI security standards were complied with up to the time of the incident.

Who is responsible for fulfilling the PCI requirements?

All companies that accept credit card payments are responsible for fulfilling and complying with the PCI standard. protel’s products and services assist businesses who want to comply with the requirements of the PCI standard.

Is my business automatically PCI compliant if I operate my protel PMS in compliance with PCI?

No. protel offers you a software solution that makes it possible for you to use your protel PMS in compliance with PCI. To be completely PCI compliant, all workflows and processes within the hotel must be audited and the entire IT environment must be inspected with respect to PCI requirements. A data privacy officer will provide advice and suggestions for implementation to assist you in this process.

How does a business get PCI DSS certified?

An SAQ (self-assessment questionnaire) is used to certify a business. There are various SAQs, which differ not only in the number of questions but also in whether they have additional requirements for the devices used in the hotel (computers, payment terminals, internet connection, etc.). In the easiest case – i.e. using a protel interface to a P2PE cloud payment system – compliance can be demonstrated by filling out an SAQ of the lowest category once per year (for more information about cloud payment systems, see the section “Interfaces to Electronic Payment Systems”).

Interfaces to Electronic Payment Systems
How does PCI DSS work in protel?

A central provision of the PCI DSS is the prohibition against saving unencrypted credit card data in the hotel. protel products use a “tokenization” process to avoid saving credit card data. In this process, credit card data are encrypted and saved in a specially protected and PCI-certified area of the protel Cloud Center together with a random substitute value known as a token. Instead of the credit card number, only the token is used in the protel PMS.

How secure are credit card data in the protel Cloud Center (pCC)?

The specially protected area of the pCC is certified in accordance with the PCI DSS standard and is therefore optimally protected against criminal attacks. The annually recurring inspection ensures that any new additions to the standard are also fulfilled.

What happens during the changeover to tokenization?

When the protel PMS changes over to the tokenization method, credit card data are completely deleted from the protel PMS and replaced by a token, meaning that no credit card data are saved in the protel PMS. The credit card number, which has been replaced by a token, is stored in the protected and certified area of the protel Cloud Center (pCC) in encrypted form. In the protel PMS, the credit card number is obscured except for a few digits.

What happens to credit card data that are already in PMS?

protel has developed a special validation and cleanup tool for existing credit card data. All valid credit card data in the protel PMS database are encrypted, converted to a token and deleted from the protel database during the changeover to PCI. Invalid credit card data can be corrected and cleaned in collaboration with the hotelier. Credit card data that is “hiding” in inappropriate free text fields (e.g. address fields, guest requests, comment boxes, etc.) are concealed (masked) except for a few digits so that no legible credit card numbers remain in protel. Data masked in this manner can no longer be used or recovered.

How is credit card information saved?

Tokens are saved in protel with a reference to the respective reservation. The token is deleted from the protel PMS after a configurable number of days after check-out.

Who may decrypt the tokens?

Only protel users with the necessary access rights may decrypt and show the credit card number saved for a token. You decide which protel users have these rights. This is done by creating cloud user accounts for these protel users in the protel Cloud Center. The users’ individual e-mail addresses are required to create the cloud user accounts; shared e-mail accounts cannot be used.
How can I access credit card data from protel after the changeover to PCI?

To access the credit card data manually, hotel employees can log in to the protel Cloud Center via a secure connection from a web browser. Once there, they can use the “Detokenizer” tool to access the credit card data. Restrictive access rights regulate access, i.e. only those who are actually working with the credit card data and have the necessary rights are authorized to access them.

Do I need to make any special settings in the protel system data?

All credit cards accepted at the hotel (Mastercard, Visa, etc.) must be set as a CC payment method in protel and be available online. protel handles all the other settings for you.

How can I enter credit card data after the changeover to PCI?

The following generally applies: Credit card data can no longer be entered directly in the protel Front Office! To enter credit card data manually, hotel employees can log in to the protel Cloud Center via a secure connection from a web browser. After entering the reservation or guest profile number, employees can then enter credit card data in the Tokenizer, which encrypts the data and saves it in the protected and certified area of the protel Cloud Center together with a generated substitute value, the token. Naturally, this function can be restricted to only certain employees.

As an alternative to manual entry, the protel interface to cloud payment systems allows for the PCI compliant recording of credit card data via a credit card terminal (see below: “protel Interfaces to Electronic Payment Systems”).

How will the protel view change after the PCI changeover?

The following generally applies: There will no longer be unencrypted or legible credit card data in the Front Office! The encrypted credit card data are displayed in the Navigator. The credit card numbers are replaced by “x” characters except for a few digits (example: xxxxxxxxx7203 0120).

The function for entering credit card data in the reservation dialog will be disabled. Legible credit card data will no longer be stored anywhere in the system!

Will my protel PMS remain PCI compliant over the long term after the PCI changeover?

That depends on whether you and your employees are PCI compliant when working in protel. If, for example, individual employees enter credit card data in improper locations in protel (comment field, guest requests, etc.), this is a clear violation of the PCI regulations. It is therefore necessary to create appropriate instructions and guidelines so that all employees know how to securely handle credit card data in protel. If it is necessary to enter credit card data by hand, make sure that the data are entered only in the protel Tokenizer in the protel Cloud Center!

How long will I be unable to use protel during the PCI changeover?

While the conversion of the credit card data is running, you can continue working in protel as long as you do not perform any operations in which credit card data are viewed, modified or saved. The time required for the conversion will depend on the volume of data. Expect approximately 4 to 6 hours for protel SPE and approximately 8 to 12 hours for protel MPE (hotel chains).
protel Interfaces to Electronic Payment Systems

Which protel payment system interfaces support compliance with PCI DSS?

protel offers interfaces to local payment systems or cloud payment systems.

Local payment systems. Whether a protel interface to a local payment system can be operated in compliance with PCI depends on the method of operation:

1. If the payment system transmits a masked card number to protel, no legible credit card data are saved in protel. This method can be certified according to PCI DSS.

   Disadvantage: For each new transaction with the same credit card number (e.g. corrections after check-out, no-show charges, redeeming of payment guarantees) the guest’s credit card has to be reinserted into a payment terminal (i.e. the guest must be present).

2. If the payment system transmits a complete card number to protel, the interface encrypts the card number and saves it in protel. Since not all encryption requirements are met, this method cannot be certified according to PCI DSS.

Cloud payment systems. The protel interface to cloud payment systems is PCI compliant without restriction when used with protel PMS. Because the interface is between two secure data centers – the protel pCC on the one hand and the payment system’s data center on the other – a hotel using such an interface and payment system can even certify itself according to PCI DSS, provided the connected payment system is a P2PE (point-to-point encryption) solution. In this case, the hotel need only fill out a self-assessment questionnaire (SAQ) of the lowest category to be PCI compliant.

Furthermore, by interfacing to a cloud payment system, you can execute all transactions without having to decrypt the token, i.e. if necessary, you can execute credit card transactions without the guest having to insert their card into a card terminal for each transaction (e.g. no-show).

PCI compliant interfacing to a cloud payment system is currently only possible with the provider 3C Payments. protel is currently in contact with additional payment providers, including the companies CCV and BS-PayOne in the German-speaking countries. CCV is a service provider that works closely with the company Concardis, with which many protel customers currently do business.

Questions and Answers regarding Connected Booking Portals

What should I keep in mind when using an IDS interface?

In general, any IDS interface can be operated in compliance with PCI DSS. protel offers a service in pCC for communicating with booking portals that replaces the credit card numbers from the transmitted reservations with a token and saves the credit card numbers in pCC in encrypted form. Here, again, only the tokens are saved in the protel PMS. The tokens can then be used if needed, e.g. for a no-show. Please ask our sales team whether a particular booking portal operator delivers credit card numbers or not.
Questions and Answers about the protel WBE

Which WBE version do I need to be PCI compliant?
WBE5 or WBE4 is required for PCI compliant operation with protel.

Are credit card data that are recorded through the WBE secure?
Yes. All credit card data that pass through the protel Web Booking Engine are replaced by a token, and the credit card numbers are stored in the pCC in encrypted form.

What should I keep in mind when incorporating a payment provider?
If the amount owed by the guest is to be paid immediately when the booking is made, the guest is transferred to the payment provider’s page to complete the payment (as is the case in other online shops). After completing the payment, the guest is redirected back to the protel WBE. For payments carried out in this manner, no information about the payment method used is transmitted to protel. The payment displayed in protel therefore contains no sensitive information.

How are credit card data handled via the protel WBE?
Whether credit card data are recorded as backup information or not can be set in the WBE settings and depends on which rate code applies for the booking. Before the booking is completed, the guest is redirected to a page in the protel Cloud Center, enters their credit card information and then is returned to the protel WBE. From the credit card information entered, the credit card number is encrypted, saved and replaced by a token. The card information recorded in the protel PMS contains only the token.

Questions and Answers about POS Systems

What should I keep in mind when incorporating a POS system?
For an interface between a POS and protel, no credit card numbers are transmitted to the protel PMS.

Do you have any questions?
If you have any questions or would like additional information, please contact us! We will be happy to advise you!

protel hotelsoftware GmbH
Europaplatz 8
44269 Dortmund
Germany
T: +49 231 915 93 0
F: +49 231 915 93 999
info@protel.net
www.protel.net