

PROTEL
PCI
COMPLIANCE



protel PCI Compliance

MIT PROTEL ZUR PCI-COMPLIANCE

Beschreibung des PCI-Modus in protel

Dieses Dokument beschreibt ausführlich, mit welchen Maßnahmen und Einstellungen in protel Sie die PCI-Compliance in Ihrem Hause vorantreiben können.

Datenschutz im Hotel

Handlungsbedarf

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.

Strafen drohen bei Nichtbeachtung

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

protel Whitepaper zur PCI-Compliance

Detaillierte Informationen zum Thema haben wir für Sie im protel PCI Whitepaper zusammengestellt, das wir Ihnen auf Wunsch gern zusenden.

Erster Grundsatz:

So wenig Daten wie möglich speichern

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.

Strategische Vorüberlegungen

Strategische Vorüberlegungen

Es empfiehlt sich, vor diesem Hintergrund einige strategische Überlegungen zur Handhabung von Kreditkartendaten in Ihrem Hause anzustellen:

- Welche Daten müssen unbedingt gespeichert werden?
- Wem muss es unbedingt möglich sein, Daten einzulesen / einzugeben?
- Wer benötigt im Anschluss unbedingt Zugriff auf die Daten?
- Wie lange müssen die Daten unbedingt aufbewahrt werden?

Planung der Umsetzung in protel

Planung der Umsetzung

Die Umsetzung sollte dann so restriktiv wie möglich dafür sorgen, dass

- von Vornherein so wenig wie möglich gespeichert wird.
- die Eingabe neuer Daten kontrolliert erfolgt.
- jeder Zugriff auf gespeicherte Daten kontrolliert wird.
- die Daten so schnell wie möglich wieder gelöscht werden.

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

PCI Compliance mit protel

Die protel Hotelmanagement-Systeme verfügen über eine Reihe von Funktionen, die Sie dabei unterstützen, zentrale Vorgaben der zwölf PCI-Richtlinien einzuhalten.

Wir haben im Folgenden die wichtigsten Einstellungen für Sie zusammengestellt.

WICHTIG!

VORAUSSETZUNGEN

➡ Um die folgenden Einstellungen vornehmen zu können

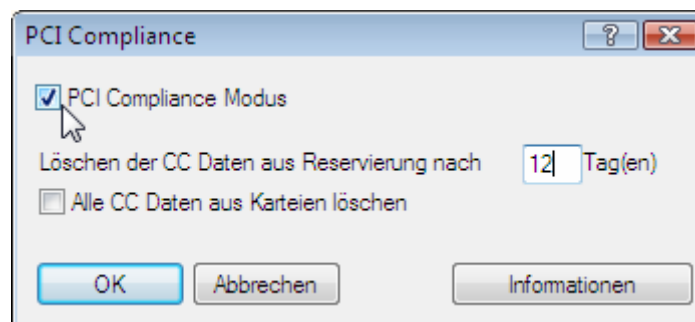
- benötigen Sie protel in der Version 12.167 (oder höher). Falls ein Update notwendig ist, unterstützt Sie Ihr protel-Support bei der Durchführung.
- brauchen Sie Zugriff auf die Stammdaten.
- benötigen Sie das Benutzerrecht 000 "Bedienerverwaltung"

Den PCI-Compliance-Modus in protel SD aktivieren

Öffnen Sie protel SD.

Buchhaltung → Allgemeine Einstellungen → PCI-Compliance:

- protel SD
- Menü Buchhaltung
- Allgemeine Einstellungen
- PCI-Compliance



Aktivieren Sie den PCI-Compliance-Modus, indem Sie ein Häkchen in die Checkbox setzen.

Legen Sie anschließend fest, nach **wieviele(n) Tagen nach dem Check-out** die Kreditkartendaten aus den Reservierungen gelöscht werden sollen.

Bestätigen Sie mit [OK].

➤ Zu den Auswirkungen dieser Einstellungen auf das Speichern und Bearbeiten von Kreditkartendaten in protel FO (Reservierungsdialog und Gästekartei) lesen Sie bitte mehr in den folgenden Abschnitten.

Hintergrundinfo zur PCI-Compliance im protel-Web

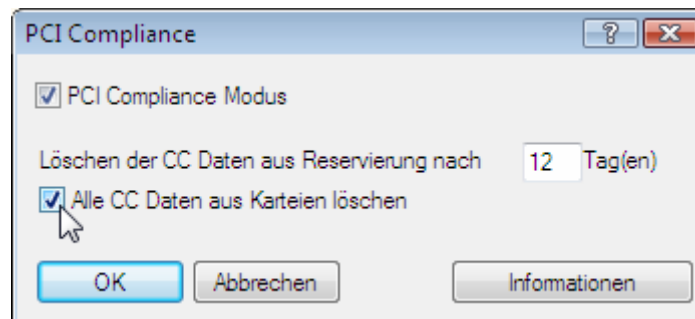
➤ Ein Klick auf die Schaltfläche [Informationen] führt Sie auf eine Seite der protel Website mit einer detaillierte Anleitung dazu, wie Sie zentrale Maßgaben des PCI-Sicherheitsstandards in protel umsetzen (identisch mit den Inhalten dieses Dokuments).

Außerdem finden Sie dort auch unser Whitepaper mit interessanten Hintergrundinformationen zum Thema als PDF zum Download.

Speichern von Kreditkartendaten verhindern Altdatenbestände aus den Gästekarteien entfernen

Im selben Dialog bietet protel Ihnen an, Kreditkartendaten aus der Zeit "vor PCI" zu löschen:

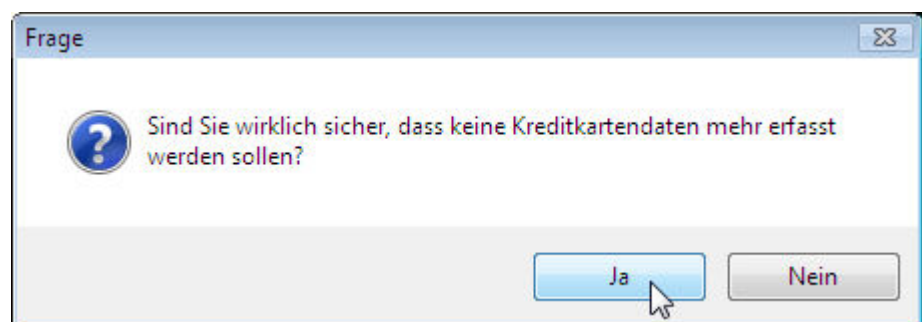
- protel SD
- Menü Buchhaltung
- Allgemeine Einstellungen
- PCI-Compliance



Wenn Sie alle Kreditkartendaten aus allen Gästekarteien löschen möchten, setzen Sie ein Häkchen in die entsprechende Checkbox und bestätigen Sie mit [OK].

Beantworten Sie die folgenden Sicherheitsabfragen:

Keine Kreditkartendaten mehr speichern - ja oder nein?



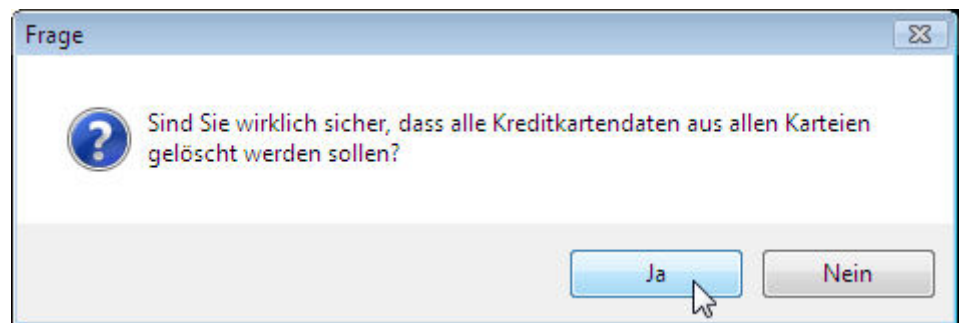
➡ "Ja, über die Gästekartei sollen ab sofort keine Kreditkartendaten mehr erfasst werden."

PROTEL PCI COMPLIANCE



protel Dokumentation | PCI Compliance - Umsetzung in protel | 1.0 (06/2008)

ALLE Kreditkartendaten löschen -
ja oder nein?



➡ "Ja, lösche ALLE Kreditkartendaten aus ALLEN Gästekarteien!"

Alternative:
Kreditkartendaten von Hand löschen

Falls Ihnen diese Lösung zu weit geht, besteht natürlich auch die Möglichkeit, die Gästekarteien "von Hand" zu durchforsten. Bei der Erstellung einer entsprechenden Datenbankabfrage ist Ihnen auf Anfrage der protel-Support behilflich.

In diesem Fall klicken Sie hier auf [Nein].

Schließen Sie zuletzt den Vorgang im PCI-Dialog mit [OK] ab.

Hintergrundinfo zur PCI-Compliance im
protel-Web

➡ Ein Klick auf die Schaltfläche [Informationen] führt Sie auf eine Seite der protel Website mit einer detaillierte Anleitung dazu, wie Sie zentrale Maßgaben des PCI-Sicherheitsstandards in protel umsetzen (identisch mit den Inhalten dieses Dokuments).

Außerdem finden Sie dort auch unser Whitepaper mit interessanten Hintergrundinformationen zum Thema als PDF zum Download.

VORHER / NACHHER 1

Zum Vergleich: protel OHNE PCI-Modus

Ist der PCI-Modus NICHT aktiviert, können im **Reservierungsdialog** Kreditkarteninformationen hinterlegt, gespeichert und an die / von der Gästekartei übertragen werden.

Dazu öffnet man mit einem Klick auf die Schaltfläche [CC] den kleinen Zusatzdialog "Reservierungszusatzinformationen". Dort können Kartentyp und Kartennummer, die Gültigkeitsdauer und der Name des Karteninhabers eingetragen werden. Mit [OK] werden diese Angaben gespeichert:

protel FO
Dialog "Reservierung"
→ [CC]
→ "Zusatzinformationen"

Die Daten können wahlweise in die **Gästekartei** übertragen oder auch von dort übernommen werden, falls bereits schon bei früheren Reservierungen dort Daten abgespeichert worden sind.

In der Gästekartei findet man sie auf der Registerkarte "Persönliche Daten" in der Baumstruktur unter "Kreditkarten" zur Ansicht und/oder zur Bearbeitung:

protel FO
Dialog "Gast - ..."
→ Pers. Daten
→ Kreditkarten

VORHER / NACHHER 2

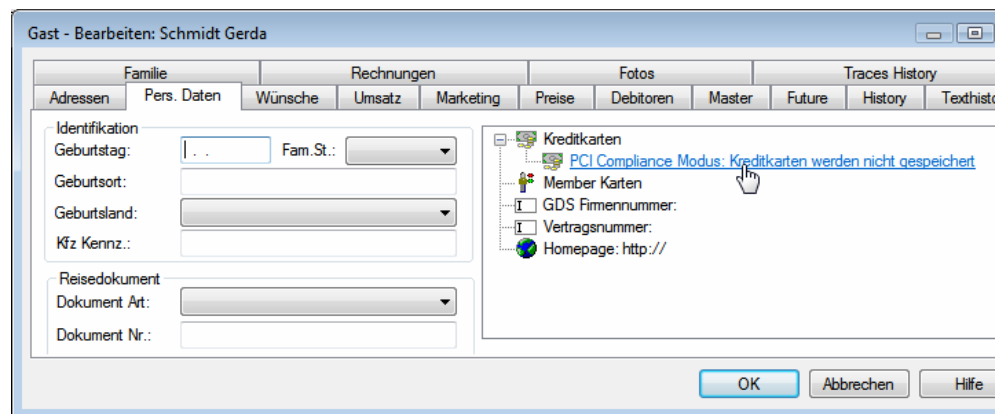
protel IM PCI-Modus

Ist der PCI-Modus aktiviert, werden die Kreditkartendaten, die im Reservierungsdialog eingegeben werden, nur noch für die Dauer der Reservierung vorgehalten.

Nach Ablauf der hinterlegten Anzahl von Tagen nach dem Check-out werden sie automatisch gelöscht. (Die Anzahl der Tage definieren Sie im PCI-Compliance-Dialog, s.o.)

In der Gästekartei können gar keine Kreditkartendaten mehr eingelesen, eingegeben und gespeichert werden:

Keine Kreditkartendaten in der Gästekartei



Zugriff auf Altdatenbestände kontrollieren

➡ Kreditkartendaten, die noch in der "Vor-PCI-Zeit" in Gästekarteien gespeichert wurden, bleiben vom PCI-Modus zunächst unberührt!

Solche Daten werden zwar in der Gästekartei nicht mehr angezeigt, können aber auch weiterhin über die Funktion "Übernahme aus Gastdaten" in den Reservierungsdialog übernommen werden.

Wie Sie den Zugriff auf solche Altdatenbestände vermeiden, erfahren Sie im folgenden Kapitel zu den Benutzerrechten.

➡ Falls Sie es bevorzugen, sich von solchen Altdaten auf einen Schlag zu trennen, wählen Sie die Funktion "Alle CC-Daten aus Karteien löschen" (vergl. dazu oben Seiten 5f).

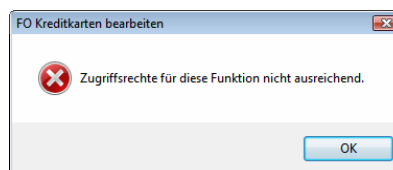
Altdatenbestände sichern

Zugriff auf Kreditkartendaten über die Benutzerrechte steuern

Über die Benutzeradministration steuern und kontrollieren Sie punktgenau, wer wie auf die sensiblen Kreditkartendaten zugreifen kann. Wir empfehlen Ihnen, diese Rechte entsprechend restriktiv zu setzen und auf einen möglichst kleinen Personenkreis zu beschränken. Nur diejenigen, die tatsächlich mit den Kreditkartendaten arbeiten (und z. B. nicht die Mitarbeiter des Housekeeping), sollten darauf zugreifen können.

Es sind im Wesentlichen fünf Benutzerrechte, die mit dem Thema PCI-Compliance in Verbindung stehen:

Recht Nr.	Bezeichnung	Wirkung / Empfehlung
370	FO Reservierung CC aus Gastdaten lesen	Regelt die Übernahme von Kreditkartendaten aus der Gästekartei (Registerkarte "Pers. Daten") in den Reservierungsdialog ([CC] → Reservierungszusatzinformationen) Dieses Recht sollte allen Benutzern entzogen werden.
371	FO Reservierung CC in Gastdaten speichern	Regelt die Übertragung der Kreditkartendaten aus dem Reservierungsdialog ([CC] → Reservierungszusatzinformationen) in die Gästekartei (Registerkarte "Pers. Daten"). Dieses Recht sollte allen Benutzern entzogen werden.
373	FO Reservierung CC Nummer anzeigen	Regelt die Ansicht der Kreditkartennummer im Reservierungsdialog ([CC] → Reservierungszusatzinformationen). ➡ Auch OHNE dieses Recht kann die Nummer in der Gästekartei gesehen und bearbeitet werden. Dieses Recht sollte alle Benutzern entzogen werden.
822	FO Kreditkarten bearbeiten	Regelt den Zugriff auf die Reservierungszusatzinformationen aus dem Reservierungsdialog (über Button [CC]):



Dieses Recht sollten nur die Benutzer haben, die wirklich mit den Daten arbeiten müssen.

PROTEL PCI COMPLIANCE



protel Dokumentation | PCI Compliance - Umsetzung in protel | 1.0 (06/2008)

So setzen Sie die Rechte:

Öffnen Sie protel SD.

Manager → Bedienerverwaltung → Bedienerverwaltung

protel SD

→ Manager

→ Bedienerverwaltung

Klicken Sie im linken Teil des Dialogs "Bedienerverwaltung" auf die Benutzergruppe, deren Rechte Sie bearbeiten möchten und anschließend auf die Schaltfläche [Gruppenrechte ändern]:

protel SD

→ Manager

→ Bedienerverwaltung

→ Gruppenrechte für ...

Im Dialog "Gruppenrechte für ..." scrollen Sie durch die linke Liste der "Erlaubten Funktionen".

Markieren Sie die Rechte, die Sie dieser Gruppe entziehen möchten (halten Sie

die Taste [strg] gedrückt, um mehrere Rechte gleichzeitig zu markieren).
Klicken Sie auf die Schaltfläche [Verbieten], um die ausgewählten Rechte in die Liste der "Verbotenen Funktionen" zu verschieben.
Bestätigen Sie den Vorgang mit [OK].

Zugriff kontrollieren

Jeder Zugriff wird von protel automatisch überwacht und protokolliert. Diese Ereignisprotokolle können jederzeit abgefragt werden und geben detailliert Auskunft darüber, welcher Benutzer an welcher Stelle des Systems welche Funktionen ausgeführt hat.

Diese Log-Funktion ist immer aktiv; sie kann nicht abgeschaltet werden.

Die diversen Berichte finden Sie in protel FO unter Büro → Berichtswesen → Aktionsprotokoll.

Haftungsausschluss

Wir übernehmen keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen; Irrtümer, Druckfehler und abweichende Abbildungen vorbehalten.

Haftungsansprüche gegen uns, die sich auf Schäden materieller oder ideeller Art beziehen, welche durch die Nutzung oder Nichtnutzung der dargebotenen Informationen verursacht wurden sind grundsätzlich ausgeschlossen, sofern kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden durch uns vorliegt.

Wir behalten es uns ausdrücklich vor, Teile der Anleitung oder das gesamte Dokument ohne gesonderte Ankündigung zu verändern, zu ergänzen oder zu löschen.

PROTEL PCI COMPLIANCE



protel Dokumentation | PCI Compliance - Umsetzung in protel | 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

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