PCI DSS

# DIE HÄUFIGSTEN FRAGEN ZU PCI DSS

## Schutz vor Kartenmissbrauch

**Mit dem Payment Card Industry DataSecurity Standard (PCI DSS) schützen Sie die Kreditkarten-Daten Ihrer Kunden. Sie beugen Datenmissbrauch und Datendiebstahl vor.**

## Inhalt

# I. Allgemeine Erklärungen

## Was ist PCI DSS?

Der PCI DSS (Payment Card Industry Data Security Standard) ist ein Sicherheitsstandard mit strengen Vorgaben, der den sorgfältigen und geschützten Umgang mit Kreditkartendaten sicherstellen sollen. Dieser Standard wurde von den fünf wichtigsten Kreditkartenunternehmen (MasterCard, Visa, American Express, JCB und Discover Financial Services) ins Leben gerufen und umfasst 12 technische und organisatorische Anforderungen.

## Wer ist von PCI DSS betroffen?

Jedes Unternehmen, das Kreditkartenzahlungen akzeptiert, muss sich an die Sicherheitsvorgaben des PCI DSS halten. Hierbei sind die Größe und das Geschäft des Unternehmens und der Umfang der Kartentransaktionen unerheblich. Die PCI DSS Richtlinien betreffen sowohl Daten in digitaler Form, als auch jene, die der Akzeptanzstelle papierhaft vorliegen. Unternehmen, die für die Vernichtung dieser Unterlagen professionelle externe Datenvernichter beauftragen, müssen dafür Sorge tragen, dass diese Subunternehmer ebenfalls mit dem PCI DSS konform gehen.

## Was bedeutet "compliant"?

Unternehmen die nachweislich den PCI DSS einhalten, erhalten eine Konformitätsbescheinigung. Diese Unternehmen haben erfolgreich dokumentiert, dass sie die Sicherheitsanforderungen der Kreditkartenorganisationen im Umgang mit Kreditkartendaten kennen und einhalten. Im Falle einer Kompromittierung (Datenklau und –missbrauch), nach Analyse durch einen Forensiker, greift die so genannte „Safe Harbour Rule": Die Akzeptanzstelle kann dann mit einer teilweisen oder vollständigen Befreiung von Geldstrafen seitens der Kreditkartenorganisationen bzw. des Acquirers rechnen.

## Warum werde ich angeschrieben?

Ihr Unternehmen bietet Kreditkartenzahlung an und muss deshalb den PCI DSS nachweislich erfüllen. Daher hat Ihr Acquirer Sie kontaktiert mit der Bitte, den Compliance Nachweis zu erbringen.

## Ich habe die Abwicklung von Kreditkartenzahlungen extern vergeben. Warum muss ich mich trotzdem anmelden?

Unternehmen, die mit der Speicherung, Verarbeitung oder Übertragung von Kreditkartendaten einen Drittdienstleister beauftragt haben, müssen den Nachweis erbringen, dass der gewählte Dienstleister PCI compliant ist und dass sie regelmäßig den PCI Status des Dienstleisters überprüfen. Darüber hinaus benötigt Ihr Acquirer selbst in dem Fall der Beauftragung eines Drittdienstleisters den Nachweis, dass Ihr Unternehmen PCI compliant ist und Sie die Verarbeitung der Daten auslagern.

## Wie kann ich prüfen, ob mein Dienstleister PCI DSS compliant ist?

Die Kreditkartenorganisationen MasterCard und Visa haben, unter den folgenden Links, eine Liste mit PCI DSS konformen Dienstleistern im Internet veröffentlicht:

Visa
http://www.visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx
*„List of PCI DSS validated service providers"*

MasterCard
http://www.mastercard.com/us/company/en/whatwedo/compliant_providers.html
"*Click Here for the MasterCard Compliant Service Provider List*"

Oder Sie sprechen den Dienstleister direkt an und fragen diesen nach seinem PCI Zertifikat.

### Mein Dienstleister gibt mir die Auskunft, dass ich mich nicht nach dem PCI DSS zertifizieren muss.

Jedes Unternehmen, das Kreditkartenzahlung anbietet, ist verpflichtet den PCI DSS einzuhalten und diesen nachzuweisen. Haben Sie einen PCI DSS konformen Dienstleister gewählt und speichern, verarbeiten oder übertragen keine Kreditkartendaten auf Ihren IT-Systemen, gilt für Sie ein vereinfachter Weg zum Nachweis der PCI Compliance.

## II. Registrierung

### Ich habe das Passwort geändert und kann mich damit jetzt nicht mehr einloggen. Was muss ich tun?

Bitte prüfen Sie Ihre genutzten Zugangsdaten:

- Haben Sie Ihre registrierte E-Mail-Adresse genutzt?
- Haben Sie beim Passwort auf Groß- und Kleinschreibung geachtet?
- Haben Sie darauf geachtet, dass kein Leerzeichen eingegeben wurde?

Sind die genutzten Zugangsdaten korrekt und ein Login weiterhin nicht möglich, nutzen Sie bitte die Funktion „Neues Passwort anfordern".

### Ich kann mich mit den von Ihnen geschickten Daten (Initialdaten) nicht einloggen?

Haben Sie sich bereits auf der PCI DSS Plattform registriert? In diesem Fall sind die Initialdaten nicht mehr gültig. Bitte nutzen Sie als Benutzername die registrierte E-Mail-Adresse und das von Ihnen angelegte, persönliche Passwort. Sind die Zugangsdaten bisher noch nicht genutzt worden, ein Login jedoch mit den vorliegenden Daten nicht möglich, kontaktieren Sie bitte das PCI Competence Center.

### Ich habe mein Passwort vergessen. Was kann ich tun?

Bitte fordern Sie sich über die PCI DSS Plattform www.sichere-kartenakzeptanz.de ein neues Passwort an. Klicken Sie auf die

Funktion „Neues Passwort anfordern". Dort geben Sie die registrierte E-Mail-Adresse ein. Das neue Passwort wird Ihnen per E-Mail zugeschickt.

### Wie viele Ansprechpartner können auf der Plattform gelistet sein?

Im Rahmen des Registrierungsprozesses können Sie einen speziellen Ansprechpartner für PCI angeben. Sollte zu einem späteren Zeitpunkt ein weiterer Ansprechpartner notwendig sein, wenden Sie sich an das PCI Competence Center.

## III. Stammdaten:

### Welche Standorte muss ich angeben?

Bitte geben Sie den oder die Orte an, an denen sich die Niederlassung Ihres Unternehmens befindet, für die die PCI Zertifizierung durchgeführt wird.

### Was ist eine Zahlungssoftware?

Die Zahlungssoftware ist ein Programm, das auf Ihren eigenen Systemen installiert ist und die Kreditkartenzahlung Ihrer Kunden verarbeitet. Nicht zu verwechseln mit einer Payment-Page, ein Zahlungsmodul Ihres Zahlungsdienstleisters, in die der Kunde bei der Zahlung mit Kreditkarte seine Kartendaten eingibt. In diesem Fall kommen die Kreditkartendaten nicht mit Ihren eigenen IT Systemen in Berührung (keine Weiterleitung, Verarbeitung oder Speicherung).

### Was ist ein Drittdienstanbieter?

Drittdienstanbieter sind zum Beispiel Anwendungsdienstleister (Payment Gateways), Webhosting-Unternehmen (Dienstleister, die Ihnen über deren Server Netzanbindung, Internetbereitstellung und Betrieb anbieten), Internet Zahlungsdienstleister (Payment Service Provider) oder Anbieter von Kundenbindungsprogrammen.

## Was ist ein Acquirer?

Der Acquirer ist Ihr Partner zur Akzeptanz und Abrechnung von Kreditkarten und Debitkarten, mit dem Sie den Kreditkarten Service Vertrag abgeschlossen haben. In der genossenschaftlichen FinanzGruppe ist dies z. B. die DZ BANK AG.

## Was ist ein Point of Sale (POS)?

Point of Sale ist ein Zahlungssystem, in dessen Rahmen der Kunde bei der Akzeptanzstelle mit seiner Kreditkarte bezahlt. Die Legitimation des Kunden erfolgt dabei durch Unterschrift. Der Point of Sale kann ein eigenständiges Terminal sein, welches über Telefonleitung mit einem Zahlungsdienstleister verbunden ist oder es kann ein Zahlungssystem sein, welches mit der Ladenkasse und/oder dem Internet verbunden ist.

## Wann speichere, verarbeite oder leite ich Kreditkarten weiter?

Sie speichern, verarbeiten oder leiten Kreditkartendaten weiter, wenn Sie Kreditkartendaten auf Ihren eigenen Systemen von Ihren Kunden entgegennehmen, sei es zur dauerhaften Speicherung oder nur zur kurzfristigen Verarbeitung, um die Daten anschließend z. B. an einen Zahlungsdienstleister weiterzuleiten. Dies ist beispielsweise der Fall, wenn Sie eine direkte Schnittstelle (API - Application Programming Interface) zu einer Payment-Lösung Ihres Zahlungsdienstleisters nutzen. Maßgeblich an dieser Stelle ist, ob Ihre Kunden die Kreditkartendaten an Ihr(e) System(e) schicken. Ob die Kreditkartendaten von Ihrem System dann nur noch weitergereicht werden, hat keinen Einfluss mehr, denn Sie erfüllen bereits die Kriterien zur Verarbeitung von Kreditkartendaten. Nur genau dann, wenn Sie zu KEINEM Zeitpunkt Kreditkartendaten (Kartennummer, Verfallsdatum) auf Ihren eigenen Systemen speichern oder verarbeiten (auch entgegennehmen), speichern oder verarbeiten Sie keine Kreditkartendaten. Dies ist beispielsweise der Fall, wenn Sie Ihre Kunden zum Abschluss des Einkaufs in einem Web-Shopsystem auf eine Bezahlmaske (Payment-Page) Ihres Acquirers/Zahlungsdienstleisters weiterleiten, so dass diese die Zahlungsinformationen auf einem System des Acquirers/Zahlungsdienstleisters eingeben, oder bei Offline-Transaktionen im Terminal bei Face-To-Face-Geschäften.

### Was ist JCB, CUP und Discover?

JCB (Japan Credit Bureau) und CUP (China Union Pay) sind Kreditkarten, die im asiatischen Raum weit verbreitet sind. Die Discover Card ist eine amerikanische Kreditkarte.

### Ich kenne meine jährlichen Transaktionszahlen mit Kreditkarten nicht. Was soll ich angeben?

Bitte schätzen Sie die Anzahl der Transaktionen, wenn Ihnen die genauen Zahlen nicht vorliegen.

### Wieso muss ich die Anzahl meiner Kreditkarten-Transaktionen angeben?

Akzeptanzstellen werden je nach Umfang ihrer jährlichen Transaktionen in vier Kategorien eingestuft. Abhängig von der Kategorie müssen Akzeptanzstellen unterschiedliche externe und interne Prüfungen bestehen, um den PCI DSS Compliance Status zu erreichen und aufrecht zu erhalten.

## IV. SAQ (Self-Assessment Questionnaire = Selbstbeurteilungsbogen)

### Welcher SAQ ist der richtige für mich?

Bei der Wahl des für Ihr Unternehmen zutreffenden SAQs unterstützt Sie der SAQ-Auswahl-Assistent PCI DSS Plattform. Mit Hilfe von gezielten Fragen zur Akzeptanz und Abwicklung von Kreditkartendaten wird der für Ihr Unternehmen passende SAQ ermittelt. Sollten Sie den passenden SAQ-Typ bereits kennen, finden Sie im SAQ-Auswahl-Assistenten einen Link, der Sie direkt in die Übersicht der SAQs führt und Sie den passenden SAQ auswählen können. Im Zweifelsfall ist es aber immer zu empfehlen, den Weg über den SAQ-Auswahl-Assistent zu wählen, damit Sie auch wirklich den für Ihr Unternehmen aktuellen SAQ ermitteln.

### Warum muss ich einen SAQ ausfüllen?

Mit dem SAQ (Selbstbeurteilungsbogen) wird die Einhaltung der Sicherheitsanforderungen des PCI DSS geprüft.

## Die Fragen des SAQ A treffen auf mich nicht zu, da ich alle Kreditkarten-Funktionen extern vergeben habe. Wie soll ich antworten?

Auf Ihr Unternehmen nicht zutreffende Fragen können Sie mit „N/A" (nicht anwendbar) beantworten. Anschließend geben Sie eine Erklärung an, warum diese Frage auf ihr Unternehmen nicht anwendbar ist. Bei dem SAQ A geht es um den Nachweis, dass Sie einen Dienstleister nutzen, der den PCI DSS einhält, und Sie diesen Status bei Ihrem Dienstleister regelmäßig überprüfen.

## Welche Antwortmöglichkeiten gibt es?

Sie können mit „Ja", „Nein", „N/A" und „Compensating Controls" die SAQ - Fragen beantworten.

## Was bedeutet N/A?

N/A bedeutet „nicht anwendbar" und kann als Antwort auf Fragen im SAQ genutzt werden, wenn die gestellte Frage nicht auf Ihr Unternehmen passt. Nutzen Sie diese Antwort-möglichkeit, werden Sie aufgefordert die Auswahl zu begründen.

## Was bedeutet Compensating Controls?

Compensating Controls bedeutet „ausgleichende Maßnahmen". Wenn Sie die technische Spezifikation einer Anforderung nicht erfüllen können, Sie das damit verbundene Risiko aber auf andere Weise ausreichend gemindert haben, wählen Sie bitte "Compensating Controls" (ausgleichende Maßnahme) als Antwort aus. In diesem Fall werden Sie nach Abschluss des SAQ aufgefordert, genauere Angaben zu den getroffenen Maßnahmen zu machen.

## Meine eigenen IT-Systeme speichern, verarbeiten oder übertragen Kreditkarten-daten. Der SAQ C/D ist ausgefüllt. Was muss ich jetzt tun, damit ich compliant werde?

Ihre eigenen IT-Systeme speichern, verarbeiten oder übertragen Kreditkartendaten. Daher ist es nicht ausreichend, nur den SAQ auszufüllen. Ihre IT-Systeme, welche mit den Kreditkartendaten in Berührung kommen, müssen alle 90 Tage extern von einem Approved Scanning Vendor (ASV) auf Schwachstellen überprüft werden. Ergibt diese Prüfung, dass Ihre IT-Systeme keine Schwachstellen aufweisen, muss das Ergebnis (Executive Summary Report) auf der PCI DSS Plattform hochgeladen werden. In Kombination mit dem ausgefüllten SAQ haben Sie somit den Nachweis, PCI DSS compliant zu sein, erbracht. Die usd AG ist empfohlener Kooperationspartner Ihres Acquirers, ASV (Approved Scanning Vendor) und QSA (Qualified Security Assessor). Die usd AG unterbreitet Ihnen gerne ein Angebot über die Durchführung der Schwachstellen-Scans und/oder Audits. Bitte fordern Sie ein Angebot an: Telefonnummer 06102 / 8631-750 oder per E-Mail: pci@usd.de.

## Was passiert, wenn ich nicht PCI DSS compliant bin?

Die Akzeptanzstelle kann seitens der Kreditkartenorganisationen bzw. Acquirer mit Geldstrafen belegt werden.