Wir unterstützen Sie bei Ihrer PCI DSS-Zertifizierung

Nutzen Sie einfach unsere PCI DSS-Plattform, um den Nachweis webbasiert erbringen zu können. Die Plattform unterstützt Sie bei der Ermittlung und Beantwortung des für Ihr Unternehmen gültigen Selbstbeurteilungsfragebogens. Da je nach Abwicklung organisatorische, prozessuale und technische Prozesse zu prüfen und zu beurteilen sind, wird empfohlen, zur Ermittlung und Beantwortung des Fragebogens die mit dem Abwicklungsprozess betrauten Mitarbeiter einzubeziehen. Die Compliance muss einmal jährlich nachgewiesen werden. Das gilt auch, wenn sich an Ihren Prozessen zur Zahlungskartenabwicklung zwischenzeitlich nichts verändert hat.

Sie haben Fragen? Sie brauchen Hilfe? Nehmen Sie Kontakt auf!

Wünschen Sie weitere Informationen zur PCI DSS-Zertifizierung? Benötigen Sie Hilfe beim Ausfüllen der Selbstauskunft? Ihre Selbstauskunft ergibt, dass Sie nicht „compliant" sind? Wir helfen Ihnen weiter, wenn Sie Unterstützung brauchen – zusammen mit unserem Sicherheitspartner, der usd AG.

Unser Tipp:

Platzieren Sie das Siegel auf Ihrer Website und zeigen Sie dadurch unübersehbar, dass das Bezahlen mit Kreditkarte über Ihre Internetseiten sicher ist und dass die eingegebenen Kreditkartendaten geschützt sind!

Kontaktieren Sie uns per E-Mail an
support@kartensicherheit.vr-payment.de

Oder wenden Sie sich telefonisch an unser PCI Competence Center:
Telefon: +49 6102 8631-740
von Montag bis Freitag: 8.00 bis 18.00 Uhr

Was sind meine nächsten Schritte?

1. Melden Sie sich an
Sie finden unsere PCI DSS-Plattform online unter https://kartensicherheit.vr-payment.de. Melden Sie sich mit Ihren Zugangsdaten an, die Sie per E-Mail erhalten haben.

2. Ermitteln Sie den Fragebogen
Starten Sie den Auswahl-Assistenten und beantworten Sie die Fragen entsprechend Ihrer Abwicklungsprozesse.

3. Füllen Sie den Fragebogen aus
Prüfen Sie anhand der Sicherheitsanforderungen, ob Ihr Unternehmen gemäß den Vorgaben der Kartenorganisationen aufgestellt ist.

4. Freischaltung Ihrer Akzeptanzen
Nach der erfolgreichen Durchführung Ihrer PCI DSS-Zertifizierung schalten wir Ihre Kreditkartenakzeptanz(en) frei.

Wo finde ich weitere Informationen?
Antworten auf häufig gestellte Fragen zum PCI DSS finden Sie im geschützten Bereich unserer PCI DSS-Plattform.
Alles rund um den PCI DSS können Sie auf der offiziellen Webseite des PCI Security Standards Council nachlesen:
https://de.pcisecuritystandards.org/index.php

:vr-payment.de

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

VR Payment

Schützen Sie sich und Ihre Kunden

Payment Card Industry
Data Security Standard

Payment Card Industry Data Security Standard

Die Zahl professioneller Hackerangriffe auf Unternehmen steigt rapide an. Kriminelle suchen gezielt Opfer aus, bei denen sie wenig Widerstand erwarten – 2018 trafen laut Studien[1] 58% der Angriffe kleine Unternehmen. Im Fokus stehen dabei insbesondere Händler, die Kartenzahlungen akzeptieren. Ein erfolgreicher Angriff kann hohe Kosten sowie Image- und Vertrauensverlust zur Folge haben und somit schnell zur Existenzbedrohung werden.

Was ist der PCI DSS?

Der PCI DSS (Payment Card Industry Data Security Standard) ist ein von allen Kreditkartenorganisationen entwickelter, international gültiger Sicherheitsstandard für den Schutz von Kreditkartendaten. Er stellt sicher, dass die im Bezahlvorgang verarbeiteten, sensiblen Kreditkartendaten nicht entwendet und zu kriminellen Zwecken missbraucht werden. Jeder Händler, der Kartenzahlungen akzeptiert oder Kreditkartendaten speichert, verarbeitet oder übermittelt, ist verpflichtet, die Sicherheitsvorgaben des PCI DSS einzuhalten. Diese Verpflichtung besteht unabhängig von Unternehmensgröße und Anzahl der jährlich abgewickelten Kreditkartentransaktionen. Die vollständige Einhaltung der Sicherheitsvorgaben wird auch als Konformität oder Compliance bezeichnet. Einmal jährlich muss die PCI DSS Compliance durch einen Nachweisprozess belegt werden. Die Folgen eines erfolgreichen Datenabgriffes sind weitreichend wie beispielsweise der potentielle Verlust von Umsatz, Kunden, Reputation, Vertrauen und eine mögliche Insolvenz. Die Kreditkartenakzeptanz wird unverzüglich gesperrt und der monetäre Schaden durch Folgekosten (Sperrung und Tausch von Kreditkarten, Strafzahlungen an die Kreditkartenorganisationen) ist immens.

[1] Verizon Data Breach Investigations Report 2018 (https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)

Bin ich vom PCI DSS betroffen?

Ja, da Sie Ihren Kunden als Händler die Zahlung mittels Kreditkarte anbieten, sind auch Sie dazu verpflichtet, die Anforderungen des PCI DSS zu erfüllen. Die Verpflichtung besteht auch dann, wenn Sie die Abwicklung aller Kartentransaktionen vollständig an externe Dienstleister ausgelagert haben. In diesem Fall ist der Nachweis Ihrer Konformität mit dem PCI DSS jedoch mit vergleichsweise geringem Aufwand verbunden.

Sollten Sie als Händler Kreditkartendaten selbst verarbeiten und/oder speichern, übernehmen Sie die Verantwortung für die Sicherheit der Daten. Dies birgt ein nicht unwesentliches Risiko, welchem nur mit beträchtlichem Aufwand gegengesteuert werden kann.

Warum ist der PCI DSS für mich wichtig?

Die Einhaltung der Sicherheitsvorgaben des PCI DSS dienen nicht nur dem Schutz Ihrer Kunden, sondern auch Ihrem eigenen: Im Fall eines Diebstahls von Kartendaten haften Sie für alle Schäden und Verluste, die sich daraus ergeben. Darüber hinaus haften Sie unter anderem für:

- Rechtskosten
- Kosten für den Austausch von Kreditkarten
- Kosten für forensische Untersuchungen

Zusätzlich können Ihnen Strafzahlungen sowie weitreichende Sicherheitsmaßnahmen und -prüfungen von den Kreditkartenorganisationen auferlegt werden.

Bitte bedenken Sie, dass im Fall eines Diebstahls von Kartendaten bei Nichterbringung des PCI DSS-Nachweises die Haftung für die Schäden bei Ihnen liegt. Der Nachweis der eigenen Konformität mit dem PCI DSS kann bei Bekanntwerden von Zahlungskartendiebstahl die Haftungsfrage erheblich zu Ihren Gunsten beeinflussen.

Welche konkreten Vorteile habe ich durch die PCI DSS-Zertifizierung?

- Erhöhte Datensicherheit und Schutz vor Angriffen aus dem Internet für Sie und Ihre Kunden
- Gesteigertes Vertrauen, die Basis jedes Kreditkarteneinsatzes
- Schutz Ihrer Reputation durch Vermeidung von Kartendatenmissbrauch
- Prüfsiegel zur Einbindung in Ihren Onlineshop oder Ihre Webseite

Wie weise ich die Compliance nach?

Ihre Konformität (Compliance) mit dem PCI DSS weisen Sie durch einen vollständig ausgefüllten Selbstbeurteilungsfragebogen nach. Da je nach Abwicklung organisatorische, prozessuale und technische Prozesse zu prüfen und zu beurteilen sind, wird empfohlen, zur Ermittlung und Beantwortung des Fragebogens die mit dem Abwicklungsprozess betrauten Mitarbeiter einzubeziehen. Die Compliance muss einmal jährlich nachgewiesen werden. Das gilt auch, wenn sich an Ihren Prozessen zur Zahlungskartenabwicklung zwischenzeitlich nichts verändert hat.