Händlerservice

Zertifizierung leicht gemacht

Der Sparkassen-Händlerservice unterstützt Sie

Die PCI-Compliance (Einhaltung aller PCI DSS-Anforderungen) muss von Kreditkarten-Akzeptanzstellen per Zertifizierung nachgewiesen werden. Unser Service für Sie: Für unsere Kunden übernehmen wir die Kosten für die jährliche Selbstauskunft über ein Zertifizierungs-Portal.

Wie weisen Sie die PCI DSS-Compliance nach?

Neben den von allen Händlern mit Kreditkartenakzeptanz zu beachtenden zwölf PCI-Regeln sind jährliche Selbstauskünfte notwendig. Um sie bequem abschließen zu können, haben wir für Sie ein Online-Portal und einen Beratungsservice über ein speziell geschultes Competence-Center bereitgestellt.

Bei der Betreuung rund um die PCI DSS-Zertifizierung kooperiert der S-Händlerservice mit dem bundesweit führenden Dienstleister in diesem Bereich – der usd AG. Über den vom PCI Security Standards Council zugelassenen Auditor können unsere Kunden zu Sonderkonditionen auch darüber hinaus notwendige Schwachstellenanalysen oder Sicherheitsprüfungen vor Ort buchen.

→ **Registrieren und Anmelden**
Besuchen Sie das von uns bereitgestellte Zertifizierungs-Portal für den Nachweis der PCI DSS-Compliance unter: https://pci.s-haendlerservice.de

→ **Selbstauskunft**
Direkt nach der Anmeldung können Sie die Fragen im Online-Portal beantworten. Nach bisherigen Erfahrungen ist eine Beantwortung bereits in wenigen Minuten möglich. Dabei können Sie jederzeit Fragen telefonisch mit dem PCI DSS-Competence Center klären.

→ **Bestätigung**
In rund 95 Prozent der Fälle ist eine abschließende Zertifizierung bereits über die Selbstauskunft möglich. Nach erfolgreichem Nachweis erhalten Sie ein Sicherheitssiegel, mit dem Sie gern im POS-Bereich bzw. auf Ihrer Website auf Ihre Zahlungssicherheit hinweisen können.

→ **So geht's weiter**
Neben der erstmaligen Zertifizierung ist eine jährliche Bestätigung Ihrer PCI DSS-Compliance erforderlich. Zu dieser informiert Sie unser PCI DSS-Competence Center, das ebenfalls die notwendigen regelmäßigen, automatischen Sicherheitsscans koordiniert.

Sie benötigen Unterstützung?

Gern können Sie Fragen oder weiterführende Informationen zum Thema PCI DSS-Zertifizierung an das Competence Center richten. Es ist von Montag bis Freitag in der Zeit von 08.00 bis 18.00 Uhr für Sie erreichbar.

E-Mail: support@pci.s-haendlerservice.de

Telefon: 069 6630-5531

Händlerservice

Hintergrundinformation: PCI DSS

Der Standard für die maximale Sicherheit Ihrer Kartenzahlungen

Der weltweite von den Kreditkartenorganisationen definierte Standard zielt auf die Sicherheit von Zahlungsdaten gegenüber Diebstahl und Missbrauch. Er verpflichtet alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder weiterleiten, auf die Einhaltung definierter Vorgaben zu achten.

Vorteile für Sie und Ihre Kunden

Mit Beachtung des internationalen Sicherheitsstandards beugen Sie als Händler der kriminellen Nutzung schützenswerter Zahlungsdaten vor. Dies schafft Vertrauen und verbessert den Schutz vor finanziellen Belastungen durch Geldstrafen bei Regelverstößen oder Schadensersatzansprüche.

- → Sicherung von Karten- und Kundendaten gegen Diebstahl
- → Optimierung des Schutzes vor Angriffen auf die eigene Website
- → Schutz der Reputation des eigenen Unternehmens
- → Vorbeugung gegen Online-Identitätsmanipulation (missbräuchliche Nutzung von Mail- und Webadressen)

Regeln für mehr Sicherheit: Die zwölf Punkte des PCI DSS-Regelwerks

Unabhängig von der eigenen Umsatzhöhe oder der Branchenzugehörigkeit schützen Sie als Akzeptanzstelle die Daten mit Beachtung der PCI-Anforderungen optimal davor in falsche Hände zu geraten. Ein Überblick:

- → Installation und regelmäßige Aktualisierung einer Firewall zum Schutz von Daten
- → Keine Verwendung vorgegebener Werte (seitens Lieferanten/Hersteller) für System-Passwörter oder andere Sicherheitsparameter
- → Absicherung gespeicherter Daten: Karten- und Transaktionsdaten nicht unnötig speichern, wie etwa die vollständige Kartennummer, Daten der Magnetstreifenspuren, Kartenverifizierungscode (CVV2) oder PIN
- → Verschlüsselte Übertragung von Karteninhaberdaten und sensiblen Informationen in offenen Netzwerken
- → Verwendung und regelmäßige Aktualisierung einer anerkannten Anti-Viren-Software
- → Entwicklung und Verwendung sicherer Systeme und Anwendungen
- → Beschränkung des Datenzugriffs – ausschließlich für geschäftliche Zwecke
- → Zuteilung einer persönlichen ID für jede Person mit Zugang zum Computersystem
- → Zugriffsberechtigungen im Zusammenhang mit sensiblen Karteninhaberdaten einschränken
- → Nachvollziehbarkeit und Überwachung aller Zugriffe auf Netzwerk-Ressourcen und Karteninhaberdaten
- → Regelmäßige Überprüfung von Sicherheitssystemen und Prozessabläufen
- → Unternehmensrichtlinie, die das Thema Informationssicherheit regelt

Sparkassen-Händlerservice GmbH · 11/2013 · PCI DSS-Zertifizierung