Payment Services

Reset

Checkliste zur Überprüfung der PCI DSS Compliance

Checklist for reviewing PCI DSS compliance

Der Vertragspartner ist verpflichtet, alle Systeme und Datenträger, die Kartendaten enthalten (vgl. Ziff. 13 AGB) gegen Verlust und Zugriff durch unbefugte Dritte zu sichern. Er ist zudem verpflichtet, die Anforderungen der internationalen Kartenorganisationen sowie SIX Payment Services, insbesondere PCI DSS jederzeit einzuhalten.

Wenn im Vertrag mindestens eine der PCI-Fragen mit «nein» beantwortet wurde, müssen die folgenden Felder ausgefüllt werden:

Angaben zur Firma **Company details**

Firma Company

Strasse/Nr. Street/No. | Land Country

PLZ/Ort Postal code/City | Vertragspartnernr. Merchant number

Bitte teilen Sie uns mit, mit welchen Hard- und Softwaretypen Sie arbeiten und wer bei Ihnen die Kassenlösung eingerichtet hat.

Kassenintegrierte Lösungen **Cash register integrated solutions**

Hersteller/Marke Manufacturer/Brand

Typ Type | Seriennr. Serial number

Software (Versionsnr.) Software (version number)

☐ PCI-zertifiziert PCI-certified ☐ nicht PCI-zertifiziert not PCI-certified

Kassenintegrator **Cash register integrator**

Firma Company

Strasse/Nr. Street/No.

PLZ/Ort Postal code/City

Land Country | Telefon Phone

Terminal/POS-Geräte **Terminal/POS device**

Hersteller/Marke Manufacturer/Brand

Typ Type | Seriennr. Serial number

Terminal-ID Terminal ID

Software (Versionsnr.) Software (version number)

☐ PCI-zertifiziert PCI-certified ☐ nicht PCI-zertifiziert not PCI-certified

Andere Lösungen **Other solutions**

Hersteller/Marke Manufacturer/Brand

Typ Type | Seriennr. Serial number

Software (Versionsnr.) Software (version number)

☐ PCI-zertifiziert PCI-certified ☐ nicht PCI-zertifiziert not PCI-certified

Andere Integrationen **Other integrations**

Hersteller/Marke Manufacturer/Brand

Typ Type | Seriennr. Serial number

Software (Versionsnr.) Software (version number)

☐ PCI-zertifiziert PCI-certified ☐ nicht PCI-zertifiziert not PCI-certified

Bestätigung zur Erreichung der PCI DSS Compliance

In den vergangenen Jahren haben Hacking-Angriffe auf Informatiksysteme und Abrechnungssysteme für Kartenzahlungen massiv zugenommen, bei denen zum Teil Millionen von Karteninhaberdaten gestohlen wurden. Dadurch entstanden bei allen Beteiligten erhebliche Schäden. Mit der Einführung von PCI DSS (Payment Card Industry Data Security Standard) wollen die Kartengesellschaften (Visa, MasterCard, American Express, JCB und Discover) die Sicherheit von Kartenzahlungen weiter erhöhen und dadurch Händler, Karteninhaber sowie die gesamte Branche noch wirkungsvoller vor Kartendatendiebstahl und -missbrauch schützen.

Weltweit sind alle Vertragspartner, die Kartendaten übermitteln, verarbeiten oder speichern, verpflichtet, die im PCI DSS definierten Sicherheitsrichtlinien einzuhalten. Wenn diese missachtet werden, können die Kartenorganisationen Bussen und Schadenersatzforderungen aussprechen. Als direkte Konsequenz aus einem solchen Fall, könnte sich SIX Payment Services veranlasst sehen, ein bestehendes Vertragsverhältnis fristlos zu kündigen und die gestellten Schadenersatzforderungen sowie allfällige Bussen gegenüber dem involvierten Vertragspartner geltend machen.

Nebst dem Einhalten der Sicherheitsrichtlinien bei den eigenen Systemen und Applikationen, sind die Vertragspartner zudem auch dafür verantwortlich, dass beauftragte Drittunternehmen, wie Payment Service Provider (PSP) oder Data Storage Entities (DSE), die in ihrem Namen Kartendaten übermitteln, verarbeiten oder speichern, die Sicherheitsrichtlinien ebenfalls einhalten.

Grundsätzlich liegt es im eigenen Interesse jedes Vertragspartners, die Sicherheitsrichtlinien von PCI DSS umzusetzen und einzuhalten. Die Kartenorganisationen nehmen jedoch den Vertragsanbieter (Acquirer) – in Ihrem Fall SIX Payment Services – in die Verantwortung, sicherzustellen, dass jeder Vertragspartner PCI DSS einhält. Dazu gehört auch, dass die Vertragspartner die von ihnen getroffenen Sicherheitsmassnahmen deklarieren (zertifizieren) lassen. Der Umfang der Deklarierung (Zertifizierung) ist abhängig von der Anzahl der verarbeiteten Transaktionen und davon, ob der Vertragspartner mit Kartendaten bei der Übermittlung, Verarbeitung oder Speicherung in Berührung kommt.

Hiermit bestätigt der Vertragspartner, sich auf dem SAQ-Webportal* (SAQ-Self Assessment Questionnaire) einzuschreiben und die Zertifizierung durchzuführen, sofern er von SIX Payment Services hierzu schriftlich aufgefordert wird. Weiter verpflichtet sich der Vertragspartner, die ihm dazu gestellten Fristen einzuhalten.

Ort/Datum Place/Date

Firma Company

Vor- und Nachname(n) des Unterzeichnenden (in Druckbuchstaben)
The signatory's first and last name(s) (in block letters)

Rechtsgültige Unterschrift des Vertragspartners
The merchant's legal signature

* Das SAQ-Webportal dient dazu, dass SIX Payment Services Vertragspartner die Deklaration ihrer Sicherheitsvorkehrungen nach PCI DSS bequem online vornehmen können.

Ihr persönlicher Kontakt: www.six-payment-services.com/kontakt

SIX Payment Services AG
Hardturmstrasse 201
8005 Zürich
Schweiz

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxemburg

110.0114.01 INT_DE/04.2012