Payment Services

Reset

Checklist voor de controle van de PCI DSS compliance

Checklist for reviewing PCI DSS compliance

De acceptant is verplicht om alle systemen en informatiedragers die kaartgegevens bevatten (vgl. punt 13 van de Algemene Voorwaarden) te beveiligen tegen verlies en tegen toegang door onbevoegde derden. Hij is bovendien verplicht om de eisen van de internationale kaartorganisaties en SIX Payment Services, met name PCI DSS, te allen tijde na te leven.

Als in het contract ten minste één van de PCI-vragen met 'nee' is beantwoord, moeten de volgende velden worden ingevuld:

Bedrijfsgegevens Company details

Firma Company

Straat/nr. Street/No. | Land Country

Postcode/plaats Postal code/City | Acceptantnummer Merchant number

Deelt u ons alstublieft mee met welke typen hard- en software u werkt en wie bij u de kassa's heeft geïnstalleerd.

In de kassa geïntegreerde oplossingen Cash register integrated solutions

Fabrikant/merk Manufacturer/Brand

Type Type | Serienummer Serial number

Software (versienummer) Software (version number)

☐ PCI-gecertificeerd PCI-certified ☐ niet PCI-gecertificeerd not PCI-certified

Kassa-installateur Cash register integrator

Firma Company

Straat/nr. Street/No.

Postcode/plaats Postal code/City

Land Country | Telefoon Phone

Terminal/POS-apparatuur Terminal/POS device

Fabrikant/merk Manufacturer/Brand

Type Type | Serienummer Serial number

Terminal-ID Terminal ID

Software (versienummer) Software (version number)

☐ PCI-gecertificeerd PCI-certified ☐ niet PCI-gecertificeerd not PCI-certified

Andere oplossingen Other solutions

Fabrikant/merk Manufacturer/Brand

Type Type | Serienummer Serial number

Software (versienummer) Software (version number)

☐ PCI-gecertificeerd PCI-certified ☐ niet PCI-gecertificeerd not PCI-certified

Andere integraties Other integrations

Fabrikant/merk Manufacturer/Brand

Type Type | Serienummer Serial number

Software (versienummer) Software (version number)

☐ PCI-gecertificeerd PCI-certified ☐ niet PCI-gecertificeerd not PCI-certified

Bevestiging van het voldoen aan de PCI DSS compliance

In de afgelopen jaren hebben aanvallen van hackers op computersystemen en afrekeningssystemen voor betalingen met betaalkaarten sterk toegenomen, waarbij deels miljoenen kaarthoudergegevens zijn gestolen. Daardoor is bij alle betrokkenen aanzienlijke schade ontstaan. Met de invoering van PCI DSS (Payment Card Industry Data Security Standard) willen de maatschappijen die de betaalkaarten uitgeven (Visa, MasterCard, American Express, JCB en Discover) de veiligheid van betalingen met betaalkaarten verder verhogen en daardoor bedrijven, kaarthouders en de gehele branche nog effectiever beschermen tegen diefstal van en fraude met kaartgegevens.

Wereldwijd zijn alle acceptanten die kaartgegevens versturen, verwerken of opslaan verplicht om de in de PCI DSS gedefinieerde veiligheidsrichtlijnen na te leven. Als deze niet in acht worden genomen, kunnen de kaartorganisaties boetes en schadevergoedingsclaims uitspreken. Als directe consequentie van een dergelijk geval zou SIX Payment Services zich gedwongen kunnen zien om een bestaande contractuele betrekking per omgaande op te zeggen en de ingediende schadevergoedingsclaims alsmede eventuele boetes op de betrokken acceptant te verhalen.

Naast het naleven van de veiligheidsrichtlijnen bij de eigen systemen en applicaties, zijn de acceptanten er bovendien ook voor verantwoordelijk dat in opdracht werkende derden, zoals Payment Service Providers (PSP) of Data Storage Entities (DSE), die in hun naam gegevens versturen, verwerken of opslaan, deze veiligheidsrichtlijnen eveneens naleven.

In principe is het in het eigen belang van elke acceptant om de veiligheidsrichtlijnen van PCI DSS te implementeren en na te leven. De kaartorganisaties maken echter de aanbieder van de overeenkomsten (acquirer) – in uw geval SIX Payment Services – ervoor verantwoordelijk te garanderen dat elke acceptant PCI DSS naleeft. Daartoe behoort ook dat de acceptanten de door hen genomen veiligheidsmaatregelen laten certificeren. De omvang van de certificering is afhankelijk van het aantal verwerkte transacties en van het feit of de acceptant in contact komt met kaartgegevens bij het versturen, verwerken of opslaan ervan.

Hierbij bevestigt de acceptant om zich in te schrijven op het SAQ-webportal* (SAQ-Self Assessment Questionnaire) en de certificering uit te voeren indien hij hiertoe door SIX Payment Services schriftelijk wordt verzocht. Verder verplicht de acceptant zich om de hem daarvoor gestelde termijnen na te leven.

Plaats/datum Place/Date

Firma Company

Voor- en achterna(a)m(en) van de ondergetekende (in blokletters)
The signatory's first and last name(s) (in block letters)

Rechtsgeldige handtekening van de acceptant
The merchant's legal signature

* Het SAQ-webportal dient om contractpartners van SIX Payment Services de gelegenheid te bieden de certificering van hun veiligheidsmaatregelen conform PCI DSS gemakkelijk online aan te geven.

Uw contactpersoon: www.six-payment-services.com/contact

SIX Payment Services Ltd
Hardturmstrasse 201
8005 Zürich
Zwitserland

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

110.0114.07 INT_NL/04.2012