

be compliant 

PCI DSS Händlerportal

Zertifizierung leicht gemacht

- >> Webbasierte Anwendung für alle notwendigen Zertifizierungsprozesse
- >> Kostenlose Registrierung und Klassifizierung
- >> Schrittweise Führung durch den Zertifizierungsprozess
- >> Levelgerechte Selbstauskunft (PCI Self Assessment Questionnaire)
- >> Externe PCI Schwachstellen-Scans und Scan Reports
- >> Compliance Feststellung mit allen zugehörigen Dokumenten
- >> Online Dokumentenarchiv
- >> Benachrichtigung über Re-Zertifizierungsfristen

Als Händler sind Sie dazu verpflichtet, ihre PCI Konformität (Compliance) nachzuweisen, indem sie eine Selbstauskunft („Self Assessment Questionnaire“ - SAQ) abgeben und regelmäßig externe Schwachstellen-Scans durchführen lassen.

Mit dem PCI Händler Portal unterstützt die Acertigo AG Sie in der Durchführung der PCI DSS Zertifizierung. Die einfach zu handhabende webbasierte Anwendung führt Sie durch den gesamten Zertifizierungsprozess. Schritt für Schritt erhalten Sie im Compliance Portal Hilfestellung, um die Zertifizierung zu erreichen und regelmäßig zu erneuern. Der Online-Fragebogen führt Sie durch alle Einzelfragen mit Refe-

renzen zum Standard und gibt Hinweise zu Best Practice Methoden. Den Termin für den Schwachstellenscan können Sie selbst festlegen. Dadurch erlangen Sie einen hohen Grad an Flexibilität und können Ihre betriebsbedingten Anforderungen berücksichtigen. Die Ergebnisberichte des Schwachstellen-Scans bieten Ihnen eine klare Darstellung der gefundenen Schwachstellen, sowie detaillierte und umfassende Informationen über mögliche Maßnahmen, falls Sie welche ergreifen müssen. Damit werden Sie bei notwendigen Korrekturmaßnahmen bestmöglich unterstützt, um im Anschluss eine Zertifizierung zu erreichen.

Payment Card Industry Data Security Standard (PCI DSS)

Der PCI Data Security Standard ist ein umfassender Katalog von Anforderungen an die Sicherheit der kartendatenverarbeitenden Systeme, die betroffenen Prozesse und die beteiligten Mitarbeiter mit dem Fokus auf Datensicherheit und Missbrauchsprävention der Kartendaten der Kunden.

Der Standard wurde von den Kartenorganisationen Visa, MasterCard, Ameri-

can Express, JCB und Discover als verpflichtende Grundlage für alle Unternehmen etabliert, die Kartendaten speichern, verarbeiten oder übermitteln. Er gilt weltweit. Somit ist der Standard u.a. für Prozessoren, Service Provider, Hosting Provider und Händler die relevante Richtlinie, wenn es um die Sicherheit ihrer Systeme geht.

Schritt für Schritt zur PCI DSS Zertifizierung

Durch die weitgehende Automatisierung ermöglicht Ihnen die Portallösung einen kostengünstigen und übersichtlichen Weg zu Ihrer Zertifizierung. Dadurch ist die Handhabung ganz einfach, denn Sie werden durch das System geführt und bekommen bei Bedarf Hilfestellungen und Informationen.

Die **Registrierung** dient der Erfassung von Adresse und Kontaktdaten Ihres Unternehmens, sowie des organisatorischen und technischen Ansprechpartners.

Diese Informationen werden zum Teil für die Reports der Selbstauskunft, der Schwachstellen-Scans und der Visa/MasterCard Reports benötigt. In der Folge wird ein Login Account erzeugt und durch einen Authentifizierungsvorgang erfolgt die Freischaltung. Die Registrierung ist nach wenigen Minuten abgeschlossen und Sie können mit der Klassifizierung beginnen.

Die **Klassifizierung** legt fest, welche Zertifizierungsmaßnahmen Sie in welchem Umfang ergreifen müssen. Die Maßnahmen hängen von der Art der Kartenverarbeitung und der Anzahl der Transaktionen mit den Kreditkarten der verschiedenen Kartenorganisationen ab.

Anschließend erfolgt die **Feststellung des SAQ Typus (A-D)**, aus dem der Umfang des Fragebogens für die Selbstauskunft resultiert. Nach Abschluss dieser Schritte erhalten Sie eine Benachrichtigung, welche Maßnahmen von Ihnen zur Zertifizierung durchzuführen sind.

Über den Navigationspunkt **„Vertrag“** können Sie sich ein Angebot erstellen lassen. Der SAQ ist grundsätzlich kostenfrei. Gibt es jedoch IP-Adressen, die gemäß Ihrer Klassifizierung gescannt werden müssen, wird Ihnen ein individuelles Angebot erstellt, welches Sie durch zusätzliche Leistungspakete, wie z.B. telefonische Unterstützung bei der Bearbeitung des SAQ, erweitern können.

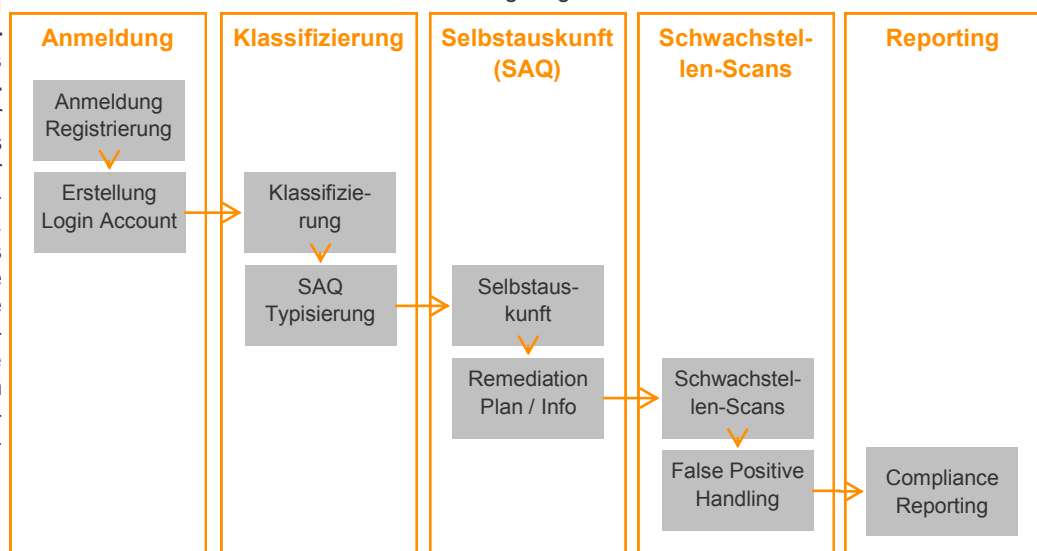
Sobald der Vertrag freigeschaltet ist, können Sie die **Selbstauskunft** starten.

Der Fragebogen zur Selbstauskunft wird Ihnen online zur direkten Bearbeitung zur Verfügung gestellt. Zusätzlich zu den verbindlichen englischen Originalfragen wird Ihnen eine Übersetzung in der von Ihnen gewählten Sprache zur Verfügung gestellt. Derzeit unterstützt das Portal die **Sprachen Deutsch, Französisch, Englisch und Italienisch**. Nach Abschluss des Fragebogens

wird über das Portal eine formale Prüfung durchgeführt und der daraus resultierende Compliance-Status bestätigt.

Der **Schwachstellen-Scan** erfolgt weitgehend automatisiert. Sie werden per E-Mail über einen bevorstehenden Scantermin informiert. Daraufhin können Sie den konkreten Scantermin und die zu scannenden IP-Adressen festlegen. Der Start des Scans erfolgt automatisch, nach dessen Abschluss erhalten Sie eine E-Mail über das Ergebnis und die Verfügbarkeit Ihrer Systeme. Falls zu behebende Schwachstellen identifiziert wurden, erhalten Sie eine ausführliche Information zu den Möglichkeiten der Behebung im Ergebnisbericht. Sie geben das Signal zum Re-Scan zur Validierung Ihrer Maßnahmen. Rechtzeitig vor dem nächsten Scantermin werden Sie wieder per E-Mail informiert.

Be compliant - mit Acertigo!



Kontakt

Stuttgart (Hauptsitz)
Acertigo AG
Wilhelmsplatz 8
70182 Stuttgart, Germany
+49 711 6 20 30 300
pci@acertigo.com

Büro Zürich
c/o Excelsis Business Solutions AG
Rautstrasse 8
8047 Zürich, Schweiz
+41 44 567 81 31
pci-switzerland@acertigo.com

Büro Riyadh
c/o IT Matrix
Kingdom Tower, Level 23
11391 Riyadh
Saudi Arabia
pci-gcc@acertigo.com