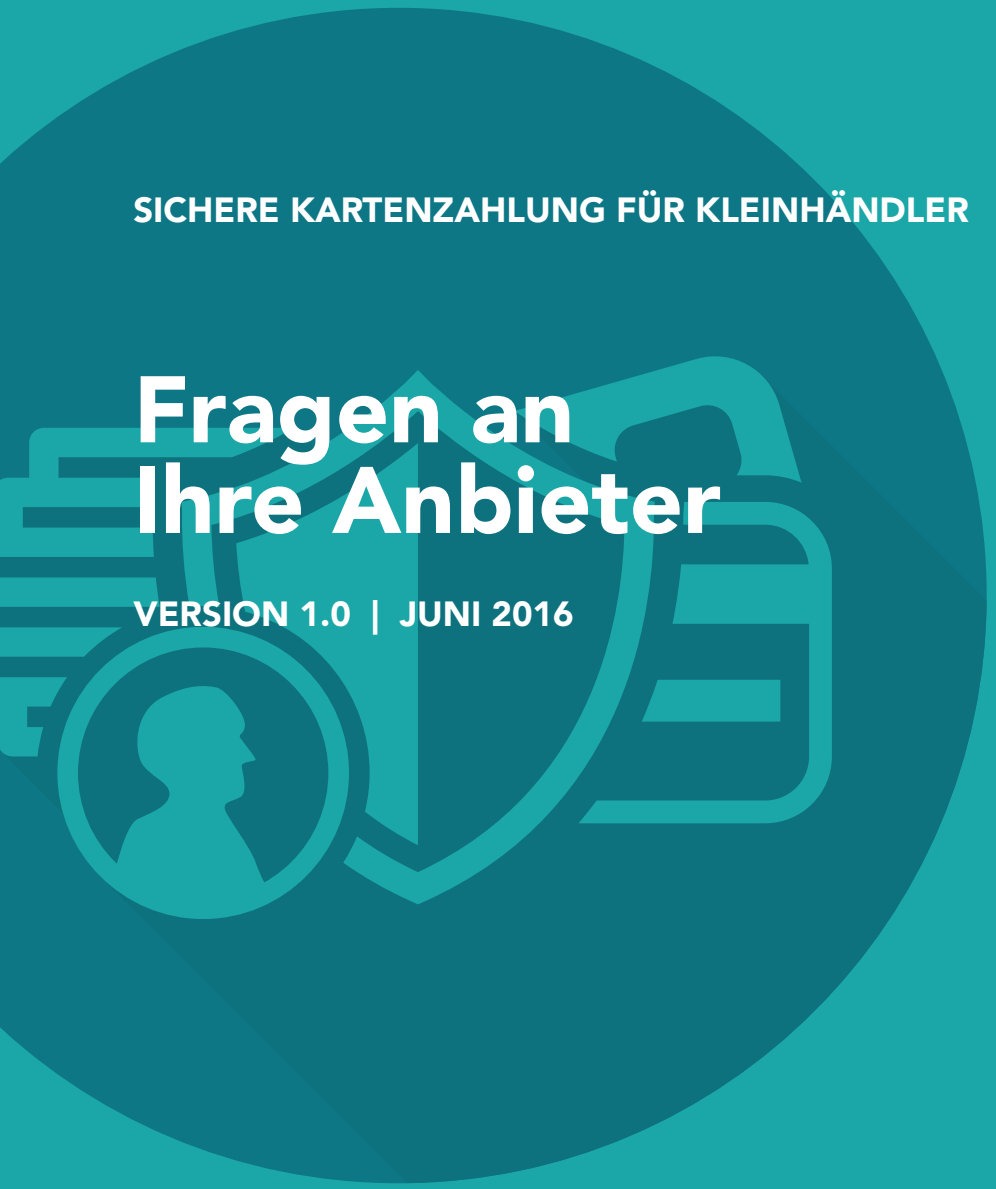
SICHERE KARTENZAHLUNG FÜR KLEINHÄNDLER

Fragen an Ihre Anbieter

VERSION 1.0 | JUNI 2016



PCI Security Standards Council®

Einleitung

Dieses Dokument soll die Geschäfts- und Betriebsleitung von Kleinhändlern unterstützen. Es stellt Fragen bereit, die Sie Ihren Anbietern und Dienstanbietern stellen können. Anhand der Fragen können Sie besser verstehen, wie diese Anbieter den Schutz der Kartendaten Ihrer Kunden unterstützen.

Fragen an Ihre Anbieter dient als Ergänzung zum *Leitfaden für sichere Zahlungsverfahren* als Teil der Dokumentenreihe „Sichere Kartenzahlung für Kleinhändler". Wir möchten Sie auch auf die anderen Dokumente *Leitfaden für sichere Zahlungsverfahren* und die Ressourcen für „Sichere Kartenzahlung für Kleinhändler" hinweisen:

QUELLE	URL
Leitfaden für sichere Zahlungsverfahren	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Gängige Zahlungssysteme	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossar zu Begrifflichkeiten aus dem Zahlungsverkehr und der Informationssicherheit	https://de.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Anbieter und Dienstanbieter und ihre Funktionsabläufe

Mittelständische Unternehmen/Kleinhändler können mit zahlreichen Zahlungs- oder Dienstanbietern in Kontakt kommen. Es ist wichtig, dass sie verstehen, um welche Art von Anbieter es sich handelt, und dass der Anbieter geeignete Maßnahmen ergreift, um die Kartendaten zu schützen.

Die Tabelle auf Seite 2 erläutert die häufigsten Arten von Zahlungs- und Dienstanbietern, und worauf die Händler bei den jeweiligen Anbietern achten sollten.

Die Tabelle ab Seite 3 enthält Fragen, die Händler ihren Anbietern oder Dienstanbietern stellen können, um besser zu verstehen, wie der Anbieter oder Dienstanbieter die Kartendaten schützt.

Anbieter und Dienstanbieter

Die folgende Tabelle erläutert die häufigsten Arten von Zahlungs- und Dienstanbietern, und worauf die Händler bei den jeweiligen Anbietern achten sollten.

ART DES ANBIETERS/ DIENSTANBIETERS	FUNKTION	PCI STANDARD ODER PROGRAMM	PRÜFUNG AUF:
Anbieter der Zahlungsanwendung	Verkauf und Support von Anwendungen zum Speichern, Verarbeiten bzw. Übertragen von Karteninhaberdaten.	Zahlungsanwendung Datensicherheitsstandard (PA-DSS)	Anwendung ist auf der List of PCI PA-DSS of Validated Payment Applications (Liste PCI PA-DSS-validierter Zahlungsanwendungen).
Zahlungsterminal-Anbieter	Verkauf und Support von Geräten zur Annahme von Kartenzahlungen (z. B. Zahlungsterminal).	PIN Transaktionssicherheit (PTS)	Zahlungsterminal steht auf der List of PCI Approved PTS Devices (Liste PCI-zugelassener PTS-Geräte).
Zahlungsabwickler, E-Commerce-Hosting-Anbieter/-Abwickler	Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten in Ihrem Auftrag. Kann auch Ihre(n) E-Commerce-Server/-Website hosten und verwalten bzw. Ihre Website entwickeln und unterstützen.	PCI Datensicherheitsstandard (PCI DSS)	Fragen Sie nach ihrer PCI DSS Konformitätsbescheinigung, und ob ihre Bewertung den von Ihnen genutzten Dienst beinhaltet. Dienstanbieter steht auf einer dieser Listen: MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard) Visa Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa) Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)
Anbieter von Software-as-a-Service	Entwicklung, Hosten bzw. Verwalten Ihrer cloudbasierten Web-Anwendung oder Zahlungsanwendung (z. B. Online-Ticket- oder -Buchungsanwendung).	PCI DSS	Fragen Sie nach ihrer PCI DSS Konformitätsbescheinigung, und ob ihre Bewertung den von Ihnen genutzten Dienst beinhaltet. Dienstanbieter steht auf einer dieser Listen: MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard) Visa Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa) Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)
Integratoren/Wiederverkäufer	Installation von PA DSS-validierten Zahlungsanwendungen in Ihrem Auftrag	Qualifizierte Integratoren und Wiederverkäufer (QIR)	Fragen Sie, ob der Anbieter PCI-qualifizierter Integrator oder Wiederverkäufer (QIR) ist. Anbieter steht auf der List of PCI QIRs (Liste der PCI-QIRs).
Dienstanbieter, die die PCI DSS Anforderungen erfüllen	Verwaltung/Betrieb von Systemen oder Diensten in Ihrem Auftrag (z. B. Firewallverwaltung, Patching-/AV-Dienste).	PCI DSS	Fragen Sie nach ihrer PCI DSS Konformitätsbescheinigung, und ob ihre Bewertung den von Ihnen genutzten Dienst beinhaltet. Dienstanbieter steht auf einer dieser Listen: MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard) Visa Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa) Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)

Fragen

Die folgende Tabelle enthält eine Reihe von Fragen, die Händler ihren Anbietern/Dienstanbietern stellen können, um zu ermitteln, ob geeignete Kontrollmechanismen zum Schutz der Kartendaten implementiert sind.

FRAGE *Des Händlers an den Anbieter*	**ERWÜNSCHTE ANTWORT DES ANBIETERS**	**EMPFOHLENE MASSNAHME** *Je nach Antwort des Anbieters*
WIE SICHER IST IHRE LÖSUNG BZW. IHR PRODUKT?		
1. Stellt Ihre Lösung/Ihr Produkt die sichere Erfassung und Übertragung von Karteninhaberdaten sicher?	**Bei Zahlungstransaktionen, bei denen die Karte persönlich vorgelegt wird:** **JA** • Überprüfen Sie hier, ob das Zahlungsterminal von PCI PTS zugelassen ist: List of PCI Approved PTS Devices (Liste PCI-zugelassener PTS-Geräte) BZW. • Überprüfen Sie hier, ob die Zahlungsanwendung PCI PA-DSS-validiert ist: List of PCI PA-DSS of Validated Payment Applications (Liste PCI PA-DSS-validierter Zahlungsanwendungen) ODER • Überprüfen Sie hier, ob die Verschlüsselungslösung PCI P2PE-validiert ist: List of PCI P2PE Validated Solutions (Liste PCI P2PE-validierter Lösungen)	Falls **NEIN**, stellen Sie Frage 2.
	Bei Zahlungstransaktionen, bei denen die Karte nicht vorliegt (einschließlich E-Commerce, schriftlicher/telefonischer Bestellung): **JA** • Überprüfen Sie hier, ob die Zahlungsanwendung PCI PA-DSS-validiert ist: List of PCI PA-DSS of Validated Payment Applications (Liste PCI PA-DSS-validierter Zahlungsanwendungen) ODER • Überprüfen Sie hier, ob der Dienstanbieter ein PCI DSS-konformer Dienstanbieter ist: MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard) Visa Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa) Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)	

Fragen

FRAGE *Des Händlers an den Anbieter*	ERWÜNSCHTE ANTWORT DES ANBIETERS	EMPFOHLENE MASSNAHME *Je nach Antwort des Anbieters*
WIE SICHER IST IHRE LÖSUNG BZW. IHR PRODUKT? *(Fortsetzung)*		
2. Beinhaltet unsere Vereinbarung mit Ihnen (dem Anbieter) Bestimmungen, denen zufolge Sie PCI DSS-Konformität für Ihr Produkt/Ihren Dienst wahren (oder PCI DSS-validiert werden)?	**JA** Anbieter mit Produkten/Lösungen, die PCI DSS-konform sind oder werden, sollten bereit sein, diesen Status in einer schriftlichen Vereinbarung festzuhalten. Weitere Informationen zu Belegen für PCI DSS-konforme Produkte/Lösungen, auf die Sie prüfen können, finden Sie bei Frage 1 oben.	Falls **NEIN**, erwägen Sie einen anderen Anbieter/eine andere Lösung.
3. Speichert Ihr Produkt/Ihre Lösung Zahlungskarteninformationen lokal (im Geschäft vor Ort)?	**NEIN** Falls ja, können Händler eine Tokenisierungs- oder Verschlüsselungslösung erwägen, um Kartendaten besser zu schützen. Weitere Informationen zu Verschlüsselung und Tokenisierung finden Sie im *Leitfaden für sichere Zahlungsverfahren*.	Falls **JA**, sollte der Händler sich vom Anbieter bestätigen lassen, dass die Daten gemäß den PCI DSS-Anforderungen gespeichert werden. Falls nein, erwägen Sie, einen anderen Anbieter einzusetzen.
4. Schützt Ihr Produkt/Ihre Lösung Zahlungskarteninformationen mit starker Verschlüsselung?	**JA** Verschlüsselung ist ein Verfahren zum Schutz von Informationen, um Datendiebstahl zu erschweren. Falls möglich, wählen Sie aus der List of PCI P2PE Validated Solutions (Liste PCI P2PE-validierter Lösungen), bei denen Kartendaten geschützt werden, sobald Sie sie empfangen, und auf ihrem Weg durch Ihr Netzwerk ebenfalls geschützt sind.	Falls **NEIN**, erwägen Sie einen anderen Anbieter/eine andere Lösung.

Fragen

FRAGE *Des Händlers an den Anbieter*	ERWÜNSCHTE ANTWORT DES ANBIETERS	EMPFOHLENE MASSNAHME *Je nach Antwort des Anbieters*
WIE SICHER IST DIE INSTALLATION MEINES PRODUKTS?		
5. Wenn der Anbieter eine Zahlungsanwendung von der List of Validated Payment Applications (Liste validierter Zahlungsanwendungen) des PCI Council installiert, fragen Sie: Sind Sie PCI-qualifizierter Integrator oder Wiederverkäufer (QIR)?	**JA** Ein QIR ist geschult und vom Council dafür zugelassen, PA-DSS Zahlungsanwendungen zu installieren und zu integrieren. Die Installationen bieten das Vertrauen, dass die PA-DSS Zahlungsanwendung in einer Weise implementiert wurde, die Ihre PCI DSS-Konformität stützt. Überprüfen Sie hier, ob der Anbieter auf der Liste steht: List of PCI QIRs (Liste der PCI-QIRs).	Falls **NEIN**, stellen Sie die Zusatzfragen auf der linken Seite.
Zusatzfragen, wenn die Antwort auf die obige Frage NEIN lautet: Wenn die Anwendung, die der Anbieter installiert, nicht PCI SSC-validiert ist, oder der Anbieter kein QIR ist, fragen Sie: • Bieten Sie während der Installation Support, um sicherzustellen, dass unsere Implementierung die PCI DSS-Anforderungen erfüllt? • Stellen Sie einen Implementierungsleitfaden bereit? • Bieten Sie Leitlinien bei der Installation dazu, wie sich sicherstellen lässt, dass Kartendaten geschützt sind, egal wo sie gespeichert, verarbeitet oder übertragen werden?	**JA** Der Anbieter sollte Prozesse festgelegt haben, die Sie bei der Installation der Lösung gemäß den PCI DSS-Anforderungen unterstützen. Eine mangelhafte Installation kann die Lösung für Datensicherheitsverletzungen verwundbar machen. Was Sie möchten, ist eine Aussage des Anbieters dazu, wie er Sie dabei unterstützt, sicherzustellen, dass die PCI DSS-Anforderungen für das Produkt/die Lösung erfüllt werden bzw. erfüllt werden können.	Falls **NEIN**, erwägen Sie, einen anderen Anbieter einzusetzen.

Fragen

FRAGE *Des Händlers an den Anbieter*	ERWÜNSCHTE ANTWORT DES ANBIETERS	EMPFOHLENE MASSNAHME *Je nach Antwort des Anbieters*
BIETEN SIE MIR KONTINUIERLICHE UNTERSTÜTZUNG UND WARTUNG FÜR DAS PRODUKT/DIE LÖSUNG? FALLS JA, WIE?		
6. Wird Ihr Produkt/Ihre Lösung in meinem Netzwerk bzw. auf meinen Systemen installiert?	**JA** Der Anbieter sollte kontinuierliche Wartung und Support für Softwareaktualisierungen und Sicherheitspatches bereitstellen. Des Weiteren sollte er Support für zukünftige Versionen bieten. Für Sie ist es wichtig, über Anbieter zu verfügen, die ihre Produkte umfassend unterstützen und Ihnen bei Installationen und Patches helfen, um sicherzustellen, dass das System den PCI-Anforderungen entspricht.	Falls die Antwort **JA** lautet, fahren Sie mit den Zusatzfragen auf der linken Seite fort. Falls **NEIN**, fahren Sie mit Frage 7 fort.
Zusatzfragen, wenn die Antwort auf die obige Frage JA lautet: • Installieren Sie Patches und Aktualisierungen für das System/die Lösung? • Tun Sie dies auf eine Weise, die die PCI DSS-Anforderungen erfüllt? • Wie benachrichtigen Sie mich, wie werden Patches verfügbar gemacht und welche Art von Support stellen Sie bereit?	**JA** Wenn die Lösung nie aktualisiert wird, kann sie für zukünftige Sicherheitsverletzungen verwundbar werden.	Falls **NEIN**, erwägen Sie, einen anderen Anbieter einzusetzen.
7. Ist die Lösung auf Systemen installiert, die dem Dienstanbieter gehören und die von ihm verwaltet (gehostet) werden?	**JA** Dies wird als „Managed Service" bezeichnet. Wenn der Dienstanbieter die Lösung hostet, fragen Sie nach seiner PCI DSS Konformitätsbescheinigung, und ob seine Bewertung den von Ihnen genutzten Dienst beinhaltet. Prüfen Sie, ob der Dienstanbieter auf einer dieser Listen steht: MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard) Visa Global Registry of Service Providers (Globales Dienstanbieterverzeichnis von Visa) Visa Europe Registered Member Agents (Registrierte Mitgliedsbeauftragte von Visa Europe)	Falls **JA**, stellen Sie die Zusatzfrage auf der linken Seite. Falls **NEIN** – wenn der Managed Service nicht PCI DSS-konform ist –, erwägen Sie eine andere Lösung.
Zusatzfrage, wenn die Antwort auf die obige Frage **JA** lautet: Ist die Umgebung des Dienstanbieters PCI DSS-konform?		

Fragen

FRAGE *Des Händlers an den Anbieter*	ERWÜNSCHTE ANTWORT DES ANBIETERS	EMPFOHLENE MASSNAHME *Je nach Antwort des Anbieters*
BIETEN SIE MIR KONTINUIERLICHE UNTERSTÜTZUNG UND WARTUNG FÜR DAS PRODUKT/DIE LÖSUNG? *(Fortsetzung)*		
8. Benötigen Sie für den Support meines Zahlungssystems/meiner Zahlungslösung Remote-Zugriff?	**NEIN** Remote-Zugriff wird häufig bei Sicherheitsverletzungen in Bezug auf Zahlungsdaten ausgenutzt. Die Remote-Zugriffsfunktion sollte auf kurze Perioden beschränkt werden und ansonsten immer deaktiviert sein.	Falls **NEIN**, fahren Sie mit Frage 9 fort. Falls **JA**, stellen Sie die Zusatzfragen auf der linken Seite.
Zusatzfragen, wenn die Antwort auf die obige Frage JA lautet: • Müssen Sie den Remote-Zugriff immer aktiviert haben?	**NEIN** Die Remote-Zugriffsfunktion sollte auf kurze Perioden beschränkt werden und ansonsten immer deaktiviert sein.	Falls **JA** – falls der Remote-Zugriff immer aktiv sein muss –, erwägen Sie einen anderen Anbieter oder eine andere Lösung.
• Welche Schritte ergreifen Sie, um Remote-Zugriffsverbindungen zu schützen?	**Ihr Anbieter sollte Multi-Faktor-Authentifizierung UND für jeden Kunden, für den Remote-Zugriff genutzt wird, einen anderen Benutzernamen und ein anderes Kennwort verwenden.** Remote-Zugriffsverbindungen können geschützt werden, indem für jede Person, die das System nutzt, eigene Benutzer-IDs und Kennwörter verwendet werden. Darüber hinaus sollte die Identität der Person, die auf das System zugreift, auf mehrere Weisen überprüft werden (Multi-Faktor-Authentifizierung). Anbieter, die für jeden Kunden einen anderen Benutzernamen/ein anderes Kennwort verwenden, verhindern, dass eine Sicherheitsverletzung bei einem Kunden zu einer Sicherheitsverletzung bei allen Kunden führt (wie es der Fall ist, wenn für alle Kunden derselbe Benutzername und dasselbe Kennwort verwendet wird).	Wenn das Produkt/die Lösung keine Multi-Faktor-Authentifizierung für den Remote-Zugriff anbietet, erwägen Sie eine andere Lösung.
9. Muss sich die Lösung/das Produkt mit meinen anderen Systemen – z. B. Zahlungsterminals, Debitorenbuchhaltung und anderen Systemen, die Karteninhaberdaten umfassen – integrieren lassen?	**NEIN** Ein eigenständiges Zahlungsterminal lässt sich einfacher schützen als ein komplexeres Zahlungssystem mit möglicherweise vielen damit verbundenen Systemen. Wenn die Lösung eine Integration mit anderen Systemen erfordert, vereinfacht sie Ihre Verarbeitungsumgebung bzw. wie liefert sie Mehrwert für Ihr Unternehmen? Für die Integration sollte eine starke betriebliche Notwendigkeit vorliegen, da eine integrierte Lösung den PCI DSS Umfang erweitert, indem sie Ihre Karteninhaberdaten-Umgebung vergrößert und komplexer macht. MasterCard List of Compliant Service Providers (Liste konformer Dienstanbieter von MasterCard)	Falls **JA**, erwägen Sie einen anderen Anbieter/ein anderes Produkt, sofern nicht eine starke betriebliche Notwendigkeit für eine komplexere Lösung mit Verbindungen zu anderen Systemen besteht.

Fragen

FRAGE *Des Händlers an den Anbieter*	ERWÜNSCHTE ANTWORT DES ANBIETERS	EMPFOHLENE MASSNAHME *Je nach Antwort des Anbieters*
WAS PASSIERT, WENN EINE DATENSICHERHEITSVERLETZUNG AUFTRITT?		
10. Falls eine Datensicherheitsverletzung auftritt und Ihr Produkt/Ihre Lösung betroffen ist: • Bieten Sie Unterstützung und Absicherung, wenn mir Strafgebühren auferlegt werden? • Wie und wann benachrichtigen Sie mich, wenn eine Sicherheitsverletzung auftritt? • Welche Überwachungsmaßnahmen in Bezug auf Datensicherheitsverletzungen und verdächtige Aktivitäten bieten Sie?	**JA** Der Anbieter/Dienstanbieter sollte bei einer Karteninhaberdaten-Sicherheitsverletzung Unterstützung bieten. Der Anbieter/Dienstanbieter sollte einverstanden sein, mit einem Forensics Investigator (Forensiker) zusammenzuarbeiten, wenn es Fragen zu dem Dienst oder der Lösung gibt, die von ihm bereitgestellt werden. Der Anbieter/Dienstanbieter sollte den Händler in Bezug auf Strafzahlungen schadlos halten, wenn eine Sicherheitsverletzung auftritt und festgestellt wird, dass die Anbieterlösung die eigentliche Ursache ist.	Falls **NEIN**, erwägen Sie einen anderen Anbieter/eine andere Lösung.
11. Hat der Anbieter/Dienstanbieter eine Versicherung, die Datensicherheitsverletzungen in Bezug auf sein Produkt/seine Lösung abdeckt?	**JA** Wenn der Anbieter/Dienstanbieter eine Versicherung hat, zeigt das, dass er über seine Verantwortung und Haftbarkeit in Bezug auf Kartendaten-Sicherheitsverletzungen nachgedacht hat. Falls **JA**, fragen Sie nach dem Umfang der Abdeckung, und ob Ihre Implementierung abgedeckt ist.	Falls **NEIN** – wenn der Anbieter keine Versicherung hat oder nicht bereit ist, sich selbst zu versichern –, erwägen Sie, Ihre eigene Versicherung abzuschließen oder einen anderen Anbieter einzusetzen.
12. Unterstützt mich der Anbieter/Dienstanbieter im Falle einer Datensicherheitsverletzung mit Benachrichtigungen meiner Kunden, wenn die Produktlösung die eigentliche Ursache ist?	**JA** Anbieter/Dienstanbieter sollten dazu bereit sein, Händler mit Benachrichtigungen zu Sicherheitsverletzungen zu unterstützen, wenn ihr Zahlungssystem die eigentliche Ursache der Sicherheitsverletzung ist.	Falls **JA**, stellen Sie die Zusatzfragen auf der linken Seite. Falls **NEIN** – wenn der Anbieter Sie nicht mit Benachrichtigungen unterstützt –, sollten Sie einen Plan für Benachrichtigungen erstellen bzw. erwägen, einen anderen Anbieter einzusetzen.
Falls **JA**, in welchem Umfang bieten Sie Unterstützung bei Benachrichtigungen? • Übernehmen Sie die Kosten? • Senden Sie die Benachrichtigungen? • Bieten Sie eine Finanzmittelüberwachung für die betroffenen Kunden?		