Payment Card Industry (PCI)

Datensicherheitsstandard

Konformitätsbescheinigung für Vor-Ort-Beurteilung - Dienstanbieter

Version 3.2

April 2016

1. Abschnitt: Informationen zur Beurteilung

Anleitung zum Einreichen

Diese Konformitätsbescheinigung muss zur Bestätigung der Ergebnisse der Beurteilung des Dienstanbieters gemäß dem *Datensicherheitsstandard der Zahlungskartenbranche (Payment Card Industry Data Security Standard, kurz PCI DSS) und den Sicherheitsbeurteilungsverfahren ausgefüllt werden.* Füllen Sie alle Abschnitte aus: Der Dienstanbieter ist dafür verantwortlich, dass alle Abschnitte von den betreffenden Parteien ausgefüllt werden. Für Reporting- und Sendeverfahren wenden Sie sich an die Marke, die die Zahlung angefordert hat.

Teil 1. Informationen zu Dienstanbietern und zum Qualified Security Assessor					
Teil 1a. Informationen zum Dienstanbieterunternehmen					
Firma:			DBA (Geschäftstätigkeit als):		
Name des Ansprechpartners:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 1b. Informationen zur Firma des Qualified Security Assessors (falls vorhanden)					
Firma:					
QSA-Leiter:			Titel:		
Telefonnr.:			E-Mail:		
Geschäftsadresse:			Ort:		
Bundesland/Kreis:		Land:		PLZ:	
URL:					

Teil 2. Zusammenfassung für die Geschäftsleitung

Teil 2a. Prüfung des Umfangs/Geltungsbereichs

Dienste, die in der PCI-DSS-Beurteilung BERÜCKSICHTIGT WURDEN (alle zutreffenden auswählen):

Name der beurteilten Dienste:		
Art der beurteilten Dienste:		
Hosting-Anbieter: ☐ Anwendungen/Software ☐ Hardware ☐ Infrastruktur/Netzwerk ☐ Physischer Speicherplatz (gemeinsam) ☐ Speicher ☐ Web ☐ Sicherheitsdienste ☐ 3-D Secure-Hosting-Anbieter ☐ Anbieter für gemeinsame Hosting-Dienste ☐ Andere Hosting-Anbieter (bitte angeben):	**Verwaltete Dienste (bitte angeben):** ☐ Systemsicherheitsdienste ☐ IT-Support ☐ Physische Sicherheit ☐ Terminalverwaltungssystem ☐ Andere Dienste (bitte angeben):	**Zahlungsabwicklung:** ☐ POS/Karte liegt vor ☐ Internet/E-Commerce ☐ MOTO/Call Center ☐ Geldautomat ☐ Andere Zahlungsabwicklung (bitte angeben):
☐ Kontoführung	☐ Betrugsmanagement und Ausgleichszahlungen	☐ Zahlungs-Gateway/Switch
☐ Backoffice-Dienste	☐ Ausstellungsdienste	☐ Prepaid Services
☐ Rechnungsverwaltung	☐ Treueprogramme	☐ Archivmanagement
☐ Abwicklung und Abrechnung	☐ Händlerservices	☐ Steuern/Zahlungen an den Staat
☐ Netzwerkanbieter		
☐ Sonstige (bitte angeben):		

***Hinweis**: Diese Kategorien werden ausschließlich zur Hilfestellung aufgeführt und sollen die Dienstbeschreibung einer Stelle in keinster Weise beschränken oder vorbestimmen. Wenn diese Kategorien nicht auf Ihre Dienste zutreffen, machen Sie Ihre Angaben im Bereich „Sonstige“. Wenn Sie sich nicht sicher sind, ob eine Kategorie auf Ihren Dienst zutrifft, wenden Sie sich an das entsprechende Kartenunternehmen.*

Teil 2a. Verifizieren des Umfangs*(Fortsetzung)*		
Dienste, die vom Dienstanbieter geleistet wurden, jedoch im Rahmen der PCI-DSS-Beurteilung NICHT BERÜCKSICHTIGT WURDEN (alle zutreffenden auswählen):		
Name der nicht beurteilten Dienste:		
Art der nicht beurteilten Dienste:		
Hosting-Anbieter: ☐ Anwendungen/Software ☐ Hardware ☐ Infrastruktur/Netzwerk ☐ Physischer Speicherplatz (gemeinsam) ☐ Speicher ☐ Web ☐ Sicherheitsdienste ☐ 3-D Secure-Hosting-Anbieter ☐ Anbieter für gemeinsame Hosting-Dienste ☐ Andere Hosting-Anbieter (bitte angeben):	**Verwaltete Dienste (bitte angeben):** ☐ Systemsicherheitsdienste ☐ IT-Support ☐ Physische Sicherheit ☐ Terminalverwaltungssystem ☐ Andere Dienste (bitte angeben):	**Zahlungsabwicklung:** ☐ POS/Karte liegt vor ☐ Internet/E-Commerce ☐ MOTO/Call Center ☐ Geldautomat ☐ Andere Zahlungsabwicklung (bitte angeben):
☐ Kontoführung	☐ Betrugsmanagement und Ausgleichszahlungen	☐ Zahlungs-Gateway/Switch
☐ Backoffice-Dienste	☐ Ausstellungsdienste	☐ Prepaid Services
☐ Rechnungsverwaltung	☐ Treueprogramme	☐ Archivmanagement
☐ Abwicklung und Abrechnung	☐ Händlerservices	☐ Steuern/Zahlungen an den Staat
☐ Netzwerkanbieter		
☐ Sonstige (bitte angeben):		
Geben Sie eine kurze Begründung an, warum die ausgewählten Dienste nicht in der Beurteilung berücksichtigt wurden:		

Teil 2b. Beschreibung des Zahlungskartengeschäfts	
Beschreiben Sie, wie und in welchem Umfang Ihr Unternehmen Karteninhaberdaten speichert, verarbeitet und/oder überträgt.	
Beschreiben Sie, wie und in welchem Umfang Ihr Unternehmen an der Sicherheit von Karteninhaberdaten beteiligt ist und inwieweit es Einfluss darauf nehmen kann.	

Teil 2c. Standorte

Führen Sie alle Einrichtungen und Standorte auf (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter, usw.), sowie eine Zusammenfassung der in der PCI-DSS-Prüfung enthaltenen Standorte.

Art der Einrichtung:	Anzahl der Einrichtungen dieser Art	Standorte der Einrichtung (Ort, Land):
Beispiel: Einzelhandelsgeschäfte	*3*	*Boston, MA, USA*

Teil 2d. Zahlungsanwendungen

Nutzt das Unternehmen eine oder mehrere Zahlungsanwendungen? ☐ Ja ☐ Nein

Geben Sie folgende Informationen bezüglich der Zahlungsanwendungen an, die in Ihrem Unternehmen genutzt werden:

Name der Zahlungsanwendung	Versionsnummer	Anbieter der Anwendung	Steht die Anwendung auf der PA-DSS-Liste?	Ablaufdatum der PA-DSS-Liste (falls zutreffend)
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	
			☐ Ja ☐ Nein	

Teil 2e. Beschreibung der Umgebung

Beschreiben Sie ***in allgemeiner Form*** die in dieser Beurteilung berücksichtigte Umgebung. *Beispiel:* • *Ein- und ausgehende Verbindungen zur/von der CDE (cardholder data environment, Karteninhaberdaten-Umgebung).* • *Wichtige Systemkomponenten in der CDE, etwa POS-Geräte, Datenbanken und Webserver sowie weitere notwendige Zahlungskomponenten (falls zutreffend).*	
Nutzt Ihr Unternehmen die Netzwerksegmentierung auf eine Weise, dass der Umfang	☐ Ja ☐Nein

Ihrer PCI-DSS-Umgebung davon betroffen ist? *(Hinweise zur Netzwerksegmentierung finden Sie im PCI DSS im Abschnitt „Netzwerksegmentierung“.)*	

Teil 2f. Externe Dienstanbieter	
Hat Ihr Unternehmen eine Beziehung mit einem Qualified Integrator & Reseller (QIR) zu Prüfungszwecken der Dienste? Falls ja: Name des QIR-Unternehmens: Individuelle Bezeichnung des QIR: Beschreibung der vom QIR erbrachten Dienstleistungen:	☐ Ja ☐ Nein
Hat Ihr Unternehmen eine Beziehung mit einem oder mehreren Drittanbietern (z. B. Qualified Integrator Reseller (QIR), Gateways, Zahlungsabwickler, Zahlungsdienstleister, Webhosting-Anbieter, Flugreiseagenturen, Anbieter von Kundenbindungsprogrammen usw.) zu Prüfungszwecken der Dienste?	☐ Ja ☐ Nein

Falls ja:

Name des Dienstanbieters:	**Beschreibung der erbrachten Dienstleistungen:**

Hinweis: *Anforderung 12.8 gilt für alle Stellen in dieser Liste.*

Teil 2g. Zusammenfassung der getesteten Anforderungen

Wählen Sie für jede PCI-DSS-Anforderung eine der folgenden Optionen aus:

- **Vollständig** – die Anforderung und alle Unteranforderungen wurden beurteilt, und keine Unteranforderungen wurden im Konformitätsbericht als „Nicht getestet“ oder „Nicht zutreffend“ gekennzeichnet.
- **Teilweise** – eine oder mehrere Unteranforderungen der Anforderung wurden im Konformitätsbericht als „Nicht getestet“ oder „Nicht zutreffend“ gekennzeichnet.
- **Keine** – alle Unteranforderungen der Anforderung wurden im Konformitätsbericht als „Nicht getestet“ und/oder „Nicht zutreffend“ gekennzeichnet.

Geben Sie für alle Anforderungen, die als „Teilweise“ oder „Keine“ gekennzeichnet wurden, Details in der Spalte „Begründung für Vorgehensweise“ an, inklusive Informationen zu Folgendem:

- Details zu speziellen Unteranforderungen, die im Konformitätsbericht als „Nicht getestet“ und/oder „Nicht zutreffend“ gekennzeichnet wurden
- Grund dafür, dass Unteranforderung(en) nicht getestet wurden oder nicht zutrafen

Hinweis: *Für jeden Dienst, der in der Konformitätsbescheinigung abgedeckt wird, muss eine Tabelle ausgefüllt werden. Zusätzliche Kopien dieses Abschnitts finden Sie auf der PCI-SSC-Webseite*.

Name des beurteilten Diensts:	

	Details zu den beurteilten Anforderungen			
PCI-DSS-Anforderung	**Vollständig**	**Teilweise**	**Keine**	**Begründung für Vorgehensweise** (Erforderlich für alle Anforderungen mit der Antwort „Teilweise“ und „Keine“. Geben Sie an, welche Unteranforderungen nicht getestet wurden, und nennen Sie den Grund dafür.)
Anforderung 1:	☐	☐	☐	
Anforderung 2:	☐	☐	☐	
Anforderung 3:	☐	☐	☐	
Anforderung 4:	☐	☐	☐	
Anforderung 5:	☐	☐	☐	
Anforderung 6:	☐	☐	☐	
Anforderung 7:	☐	☐	☐	
Anforderung 8:	☐	☐	☐	
Anforderung 9:	☐	☐	☐	
Anforderung 10:	☐	☐	☐	
Anforderung 11:	☐	☐	☐	
Anforderung 12:	☐	☐	☐	

Anhang A1:	☐	☐	☐	
Anhang A2:	☐	☐	☐	

2. Abschnitt: Konformitätsbericht

Diese Konformitätsbescheinigung spiegelt die Ergebnisse einer Vor-Ort-Beurteilung wider, die in einem zugehörigen Konformitätsbericht dokumentiert ist.

Die in dieser Bescheinigung und im Konformitätsbericht dokumentierte Beurteilung wurde abgegeben am:		
Wurden ausgleichende Kontrollen eingesetzt, um irgendeine Anforderung im Konformitätsbericht zu erfüllen?	☐ *Ja*	☐ Nein
Wurden irgendwelche Anforderungen im Konformitätsbericht als nicht zutreffend identifiziert?	☐ *Ja*	☐ Nein
Wurden irgendwelche Anforderungen nicht getestet?	☐ *Ja*	☐ Nein
Konnten irgendwelche Anforderungen im Konformitätsbericht wegen rechtlicher Verpflichtungen nicht erfüllt werden?	☐ *Ja*	☐ Nein

3. Abschnitt: Validierungs- und Bescheinigungsdetails

Teil 3. PCI-DSS-Validierung

Diese Konformitätsbescheinigung basiert auf den Ergebnissen, welche im Konformitätsbericht (ROC) mit Datum vom *(Abschlussdatum des ROC) notiert wurden.*

Auf der Grundlage der Ergebnisse des Konformitätsberichts vom (Abschlussdatum) stellen die in Teil 3b bis 3d angegebenen Unterzeichner den folgenden Konformitätsstatus für die in Teil 2 dieses Dokuments vom (Datum) ermittelte Stelle fest (***eine Option angeben):***

☐	**Konform:** Alle Abschnitte des PCI-DSS-Konformitätsberichts sind vollständig und alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **KONFORM**. *(Name des Dienstanbieterunternehmens)* hat somit vollständige Konformität mit dem PCI DSS gezeigt.
☐	**Nicht konform:** Nicht alle Abschnitte des PCI-DSS-Konformitätsberichts sind vollständig und nicht alle Fragen wurden mit „Ja“ beantwortet. Daraus ergibt sich die Gesamtbewertung **NICHT KONFORM**. *(Name des Dienstanbieterunternehmens)* hat somit keine vollständige Konformität mit dem PCI DSS gezeigt. **Zieldatum** für Konformität: Eine Stelle, die dieses Formular mit dem Status „Nicht konform“ einreicht, muss evtl. den Aktionsplan in Teil 4 dieses Dokuments ausfüllen. *Sprechen Sie sich mit Ihren Zahlungsmarken ab, bevor Sie Teil 4 ausfüllen.*
☐	**Konform, jedoch mit gesetzlicher Ausnahme:** Eine oder mehrere Anforderungen sind aufgrund einer gesetzlichen Einschränkung, die das Erfüllen der jeweiligen Anforderung(en) unmöglich macht, mit „Nicht zutreffend“ gekennzeichnet. Bei dieser Option ist eine zusätzliche Prüfung durch den Acquirer oder das Kartenunternehmen erforderlich. *Falls diese Option markiert ist, arbeiten Sie folgende Punkte ab:*

Betroffene Anforderung	Beschreibung, inwieweit die gesetzlichen Einschränkungen das Erfüllen der Anforderung verhindern

Teil 3a. Feststellung des Status

Unterzeichner bestätigt:

(Zutreffendes ankreuzen)

☐	Der Konformitätsbericht wurde nach den Vorgaben der *PCI-DSS-Anforderungen und Sicherheitsbeurteilungsverfahren*, Version *(Versionsnummer)* durchgeführt und anhand der hier vorliegenden Anweisungen ausgefüllt.
☐	Alle Informationen im oben genannten Konformitätsbericht und in dieser Bescheinigung stellen die Ergebnisse meiner Beurteilung in allen materiellen Aspekten korrekt dar.
☐	Mein Zahlungsanwendungsanbieter hat mir bestätigt, dass in meinem Zahlungssystem nach der Autorisierung keine empfindlichen Authentifizierungsdaten gespeichert werden.
☐	Ich habe den PCI DSS gelesen und erkenne an, dass ich jederzeit die für meine Umgebung geltende PCI-DSS-Konformität aufrechterhalten muss.

☐	Für den Fall, dass sich meine Umgebung ändert, erkenne ich an, dass ich meine Umgebung erneut beurteilen und etwaige zusätzliche PCI-DSS-Anforderungen erfüllen muss.

Teil 3a. Feststellung des Status (Fortsetzung)

☐	Auf KEINEM der bei dieser Beurteilung überprüften Systeme wurde festgestellt, dass nach der Transaktionsautorisierung vollständige Spurdaten („Full-Track-Daten“)[1], CAV2-, CVC2-, CID-, CVV2[2]- oder PIN-Daten[3] gespeichert wurden.
☐	ASV-Scans werden vom PCI SSC Approved Scanning Vendor *(Name des ASV) durchgeführt.*

Teil 3b. Dienstanbieterbescheinigung

Unterschrift des Beauftragten des Dienstanbieters ↗	*Datum:*
Name des Beauftragten des Dienstanbieters:	*Titel:*

Teil 3c. Bestätigung durch den QSA (Qualified Security Assessor) (sofern zutreffend)

Falls ein QSA an dieser Beurteilung beteiligt war, beschreiben Sie bitte dessen Aufgabe:	

Unterschrift des ordnungsgemäß ermächtigten Vertreters des QSA Unternehmens ↗	*Datum:*
Name des ordnungsgemäß ermächtigten Vertreters:	*Unternehmen des QSA:*

Teil 3d. Beteiligung eines ISA (Internal Security Assessor) (sofern zutreffend)

Falls ein ISA an dieser Beurteilung beteiligt war oder dabei geholfen hat, identifizieren Sie bitte den ISA-Mitarbeiter und beschreiben Sie dessen Aufgabe:	

[1] Im Magnetstreifen verschlüsselte Daten oder gleichwertige Daten auf einem Chip, die bei der Autorisierung während einer Transaktion bei vorliegender Karte verwendet werden. Einheiten dürfen nach der Transaktionsautorisierung keine vollständigen Spurdaten speichern. Die einzigen Spurdatenelemente, die aufbewahrt werden dürfen, sind die primäre Kontonummer (PAN), das Ablaufdatum und der Name des Karteninhabers.

[2] Der drei- oder vierstellige Wert, der neben dem Unterschriftenfeld bzw. vorne auf einer Zahlungskarte aufgedruckt ist und zur Verifizierung von Transaktionen bei nicht vorliegender Karte verwendet wird.

[3] Persönliche Identifizierungsnummer, die vom Karteninhaber bei einer Transaktion bei vorliegender Karte eingegeben wird, bzw. ein verschlüsselter PIN-Block in der Transaktionsnachricht

Teil 4. Aktionsplan für Status „Nicht konform“

Wählen Sie zu jeder Anforderung die zutreffende Antwort auf die Frage nach der Konformität mit PCI-DSS-Anforderungen aus. Wenn Sie einen der Punkte mit „Nein“ beantworten, müssen Sie möglicherweise das Datum angeben, zu dem das Unternehmen die Anforderung voraussichtlich erfüllen wird und außerdem eine kurze Beschreibung der Maßnahmen, die zur Erfüllung der Anforderung ergriffen werden.

Sprechen Sie sich mit den entsprechenden Zahlungsmarken ab, bevor Sie Teil 4 ausfüllen.

PCI-DSS-Anforderung	Anforderungsbeschreibung	Konform mit PCI-DSS-Anforderungen *(zutreffende Antwort auswählen)*		Datum bis zur Mängelbeseitigung und Abhilfemaßnahmen (falls „Nein“ ausgewählt wurde)
		JA	NEIN	
1	Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten	☐	☐	
2	Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden	☐	☐	
3	Schutz gespeicherter Karteninhaberdaten	☐	☐	
4	Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze	☐	☐	
5	Schutz sämtlicher Systeme vor Malware und regelmäßige Aktualisierung von Antivirensoftware und Programmen	☐	☐	
6	Entwicklung und Wartung sicherer Systeme und Anwendungen	☐	☐	
7	Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf	☐	☐	
8	Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten	☐	☐	
9	Physischen Zugriff auf Karteninhaberdaten beschränken	☐	☐	
10	Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten	☐	☐	
11	Regelmäßiges Testen der Sicherheitssysteme und -prozesse	☐	☐	
12	Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.	☐	☐	
Anhang A1	Zusätzliche PCI DSS-Anforderungen für Anbieter von gemeinsamem Hosting	☐	☐	

Anhang A2	Zusätzliche PCI-DSS-Anforderungen für Einheiten, welche SSL/eine frühe Version von TLS verwenden	☐	☐