Payment Card Industry (PCI)

Datensicherheitsstandard

Konformitätsbescheinigung für Vor-Ort-Beurteilungen - Händler

Version 3.2.1

Juni 2018

1. Abschnitt: Informationen zur Beurteilung

Anleitung zum Einreichen

Diese Konformitätsbescheinigung muss zur Bestätigung der Ergebnisse der Beurteilung des Händlers 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 Händler ist dafür verantwortlich, dass alle Abschnitte von den betreffenden Parteien ausgefüllt werden. Wenden Sie sich hinsichtlich Reporting- und Sendeverfahren an Ihren Acquirer (Handelsbank) oder die Zahlungsmarken.

Teil 1. Informationen zum Qualified Security Assessor und Händler					
Teil 1a. Händlerinformationen					
Firma:			DBA (Geschäftstätig-keit 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. Handelstätigkeit (alle zutreffenden Optionen auswählen)		
☐ Einzelhändler	☐ Telekommunikation	☐ Lebensmitteleinzelhandel und Supermärkte
☐ Erdöl/Erdgas	☐ E-Commerce	☐Schriftliche/Telefonische Bestellung (MOTO)
☐ Sonstiges (bitte angeben):		

Welche Arten von Zahlungskanälen werden von Ihrem Unternehmen bedient?	Welche Zahlungskanäle sind durch diese Beurteilung abgedeckt?
☐ Schriftliche/Telefonische Bestellung (MOTO)	☐ Schriftliche/Telefonische Bestellung (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Vorlage der Karte (persönlich)	☐ Vorlage der Karte (persönlich)

Hinweis: *Wird einer der Zahlungskanäle oder -prozesse Ihres Unternehmens durch diese Beurteilung nicht abgedeckt, wenden Sie sich bezüglich der Validierung für die anderen Kanäle an Ihren Acquirer oder Ihr Kartenunternehmen.*

Teil 2b. Beschreibung des Zahlungskartengeschäfts

Wie und in welcher Kapazität speichert, verarbeitet bzw. überträgt Ihr Unternehmen Karteninhaberdaten?	

Teil 2c. Standorte

Listen Sie alle Einrichtungen (beispielsweise Einzelhandelsgeschäfte, Büroräume, Rechenzentren, Callcenter usw.) sowie eine Zusammenfassung der Standorte auf, die in der PCI-DSS-Prüfung berücksichtigt wurden.

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

Teil 2d. Zahlungsanwendung

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	Versions-nummer	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	

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

Teil 2f. Externe Dienstanbieter

Verwendet Ihr Unternehmen einen Qualified Integrator & Reseller (QIR)? Falls ja: Name des QIR-Unternehmens: Individuelle Bezeichnung des QIR: Beschreibung der vom QIR erbrachten Dienstleistungen:	☐ Ja ☐ Nein
Gibt Ihr Unternehmen Karteninhaberdaten an externe Dienstanbieter (beispielsweise Gateways, Qualified Integrator & Resellers (QIR), Zahlungsabwickler, Zahlungsdienstleister (PSP), Webhosting-Unternehmen, Flugreiseagenturen, Anbieter von Kundenbindungsprogrammen) weiter?	☐ Ja ☐ Nein

Falls ja:

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

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

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 Händlerunternehmens)* 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 Händlerunternehmens)* 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 Ihrem Acquirer oder Ihrem/Ihren Kartenunternehmen 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. Bescheinigung des Händlers	
Unterschrift des Beauftragten des Händlers ↗	*Datum:*
Name des Beauftragten des Händlers:	*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, an dem das Unternehmen die Anforderung voraussichtlich erfüllen wird. Geben Sie außerdem eine kurze Beschreibung der Maßnahmen an, die zur Erfüllung der Anforderung ergriffen werden.

Sprechen Sie sich mit Ihrem Acquirer oder Ihrem/Ihren Kartenunternehmen 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 A2	Zusätzliche PCI-DSS-Anforderungen für Einheiten, die SSL/frühe Versionen von TLS in POS-POI-Terminalverbindungen mit vorliegender Karte verwenden	☐	☐