BARCLAYS

Kontrollpflichten externer Lieferanten

Datensicherheitsstandard der Zahlungskartenbranche (PCI-DSS)

Version 12.0, Oktober 2022

PCI-DSS-Anforderung	Beschreibung	Über die Bedeutung
1. Kartendaten-Compliance	Der Lieferant muss sich an die aktuellen Versionen der Datensicherheitsstandards der Zahlungskartenbranche (Payment Card Industry Data Security Standards) halten, wie sie vom Payment Security Standards Council herausgegeben werden, z. B. PCI-DSS, PA-DSS, PCI-P2PE, PCI-PTS, PCI-Kartenproduktion.	Schutz der Karteninhaberdaten: Der anerkannte Standard zu diesem Zweck ist PCI-DSS, eine globale branchenbehördliche Auflage. Bei den PCI-Datensicherheitsstandards handelt es sich um technische und operationelle Anforderungen, die vom Payment Card Industry Security Standards Council festgelegt wurden, um die Daten der Karteninhaber zu schützen.
2. Lieferanten- & Händlerbescheinigung	Je nach Umfang der für Barclays erbrachten Dienste muss der Lieferant vor Vertragsschluss und anschließend in jährlichen Abständen eine Compliance-Bescheinigung (Attestation of Compliance, AoC) für seine Vor-Ort-Prüfungen vorlegen oder, falls zutreffend, einen Selbstbeurteilungsfragebogen (Self-Assessment Questionnaire, SAQ) ausfüllen. Dies muss in Übereinstimmung mit den PCI-DSS-Anforderungen geschehen – siehe www.pcisecuritystandards.org/. Sollten bei der Prüfung der AoC Fragen aufkommen, beispielsweise in Bezug auf den Umfang der Dienste, die Umgebungsbeschreibung oder die PCI-Compliance des Lieferanten, kann der zugrunde liegende Compliance-Bericht (Report on Compliance, RoC) angefordert und für nähere Informationen zurate gezogen werden. Ein redigierter RoC kann akzeptabel sein, sofern er bestätigt, dass der Umfang der PCI-Zertifizierung dem Umfang der erbrachten Dienste entspricht,	Nachweis darüber, dass ein Lieferant oder Händler die entsprechende Kartendaten-Compliance für den Umfang der für Barclays erbrachten Dienste erlangt und die Anforderungen erfüllt hat. Nachweis darüber, dass die AoC/der RoC oder der SAQ des Lieferanten dem erbrachten Dienst entspricht. Wenn Barclays einen beliebigen Lieferanten oder Händler beauftragt, der den PCI-DSS nicht erfüllt, muss sich Barclays per E-Mail mit dem Visa Europe Third Party Risk Team (agentcompliance@visa.com) in Verbindung setzen, um zu bestätigen, dass der Lieferant oder Händler den PCI-DSS implementiert und Visa Europe einen PCI-DSS-Statusplan (mithilfe der Vorlage von Visa Europe) zur Prüfung und Genehmigung vorgelegt hat.

	oder nach der Prüfung der AoC weitere Fragen von Barclays gestellt werden. Der Lieferant muss Barclays informieren, sobald eine Nichteinhaltung eintritt, d. h. schnellstmöglich und nicht später als 30 Tage nach dem Ablaufdatum der Validierungsdokumente.	
3. Lieferantenbestätigung	Der Lieferant muss Barclays vor Vertragsschluss schriftlich bestätigen, dass er im Rahmen der folgenden Dienste für die Sicherheit der Karteninhaberdaten haftet, die sich in seinem Besitz befinden, bzw. dahingehend, dass die Sicherheit der Karteninhaberdaten-Umgebung (CDE) der Barclays-Kunden betroffen sein könnte, z. B. Sicherheitsdienste (wie Authentifizierungsserver), Webhosting usw. Alle Änderungen am erbrachten Dienst müssen Barclays vor ihrer Umsetzung schriftlich mitgeteilt werden.	**Auszug aus PCI-DSS v3.2.1** **Prüfverfahren zu 12.8.2:** Überprüfen Sie, ob schriftliche Vereinbarungen eine Bestätigung der Dienstanbieter enthalten, nach der die Dienstanbieter für die Sicherheit der Karteninhaberdaten haften, die sich in ihrem Besitz befinden bzw. die sie für den Kunden speichern, verarbeiten oder übertragen, bzw. dahingehend, dass die Sicherheit der CDE betroffen sein könnte. Hinweis: In Kombination mit Anforderung 12.9 geht es bei dieser Anforderung für schriftliche Vereinbarungen zwischen Unternehmen und Dienstanbietern darum, ein Grundverständnis über die jeweiligen Verantwortlichkeiten im Rahmen des PCI-DSS herzustellen. So kann die Vereinbarung beispielsweise die anwendbaren PCI-DSS-Anforderungen enthalten, die im Rahmen des bereitgestellten Diensts erfüllt werden sollen. **Leitfaden zu 12.8.2:** Die Bestätigung der Dienstanbieter ist Beleg für deren Verpflichtung, die Karteninhaberdaten, die sie von ihren Kunden anvertraut bekommen, entsprechend zu schützen. Die internen Richtlinien und Verfahren des Dienstanbieters in Verbindung mit seiner Kundeninteraktion und sämtliche Vorlagen für schriftliche Vereinbarungen müssen die Vorlage einer entsprechenden PCI-DSS-Bestätigung bei seinen Kunden beinhalten. Wie der Dienstanbieter diese schriftliche Bestätigung vorlegt, ist zwischen dem Anbieter und seinen Kunden zu vereinbaren.

Ausgliederung an Drittanbieter / Outsourcing

Ein Dienstanbieter oder Händler beauftragt unter Umständen einen Fremdanbieter damit, in seinem Auftrag Karteninhaberdaten zu speichern, zu verarbeiten oder zu übertragen oder Komponenten wie Router, Firewalls, Datenbanken, physische Sicherheit und/oder Server zu verwalten. In diesem Fall kann es zu Auswirkungen auf die Sicherheit der Karteninhaberdaten-Umgebung kommen.

Die Parteien müssen unmissverständlich angeben, welche Services und Systemkomponenten zum Umfang der PCI-DSS-Bewertung des Dienstanbieters gehören. Außerdem muss geklärt werden, welche konkreten PCI-DSS-Anforderungen vom Dienstanbieter erfüllt werden und welche Anforderungen im Verantwortungsbereich der Kunden des Dienstanbieters liegen und von diesen in eigenen PCI-DSS-Prüfungen zu berücksichtigen sind. So muss beispielsweise ein Anbieter von Managed-Hosting-Leistungen klar festlegen, welche IP-Adressen im Rahmen seiner vierteljährlichen Schwachstellenprüfung getestet werden und welche IP-Adressen von dessen Kunden in ihre eigenen vierteljährlichen Prüfungen einbezogen werden müssen.

Dienstanbieter sind dafür verantwortlich, ihre PCI-PSS-Konformität nachzuweisen und können von Kartenunternehmen dazu aufgefordert werden. Dienstanbieter wenden sich an ihren Acquirer beziehungsweise ihr Kartenunternehmen, um eine geeignete Konformitätsüberprüfung zu bestimmen.

Es gibt zwei Möglichkeiten, mit denen Drittdienstanbieter die Konformität validieren können:

1) **Jährliche Beurteilung**: Dienstanbieter können sich selbst einer PCI-DSS-Untersuchung unterziehen und ihren Kunden die entsprechenden Konformitätsnachweise vorlegen; oder
2) **Mehrere Beurteilungen auf Abruf**: Falls sie sich nicht einer eigenen PCI-DSS-Untersuchung unterziehen, haben sich Dienstanbieter auf Anfrage ihrer Kunden einer Untersuchung zu unterziehen beziehungsweise an jeder PCI-DSS-Überprüfung ihrer Kunden teilzunehmen und die Ergebnisse jeder Überprüfung dem jeweiligen Kunden zur Verfügung zu stellen

Falls der Drittanbieter eine eigene PCI-DSS-Untersuchung vornimmt, belegt er den Kunden gegenüber in ausreichendem Umfang, dass die PCI-DSS-Untersuchung des Dienstanbieters die auf den Kunden zutreffenden Services umfasste und dass die relevanten PCI-DSS-Anforderungen geprüft wurden und eingehalten werden. In welcher Form der Dienstanbieter seinen Kunden gegenüber die Belege vorlegt, hängt von den Vereinbarungen/vertraglichen Regelungen zwischen den Parteien ab. So können die Informationen etwa ganz oder teilweise über das AOC und/oder relevante Abschnitte aus dem (im Hinblick auf den Schutz vertraulicher Informationen redigierten) ROC des Dienstanbieters bereitgestellt werden.

Darüber hinaus müssen Händler und Dienstanbieter die PCI-DSS-Konformität aller zugehörigen Dritten mit Zugriff auf Karteninhaberdaten verwalten und überwachen. *Einzelheiten finden Sie in Anforderung 12.8 in diesem Dokument.*