Payment Services

Weisung betreffend Einhaltung der Payment Card Industry Sicherheitsvorschriften («PCI-Weisung»)

1. Präambel

Die Angriffe auf Informatiksysteme haben weltweit zugenommen. Insbesondere Kartendaten sind für Angreifer ein lohnendes und attraktives Ziel. Aus diesem Grunde haben die internationalen Kartenorganisationen in Zusammenarbeit mit Datensicherheitsspezialisten, sowie Vertretern des Handels, gemeinsam das Payment Card Industry Security Standards Council ins Leben gerufen. Dieses Gremium definiert diverse Datensicherheitsstandards (z.B. Payment Card Industry Data Security Standard [nachstehend «PCI DSS»] PIN Transaction Security [nachstehend «PCI PTS»] und Payment Application Data Security Standard [nachstehend «PA DSS»]), welche für alle Vertragspartner (nachstehend «VP») sowie für die in die Abwicklung oder Speicherung von Kreditkartendaten involvierten Akteure bindend sind. Bei Nichteinhaltung dieser Standards drohen der SIX Payment Services AG (nachstehend «SPS») erhebliche Bussen und/oder Schadenersatzforderungen seitens der internationalen Kartenorganisationen.

2. Anwendungsbereich

Die Weisung betreffend Einhaltung der Payment Card Industry Sicherheitsvorschriften ist für alle VP der SPS bindend und integraler Bestandteil zum Akzeptanzvertrag für Präsenzgeschäfte und/oder Distanzgeschäfte. Die Weisung umfasst ebenso allfällige Beauftragte oder Lieferanten des VP, sobald diese für den VP zahlungsrelevante Daten abwickeln, speichern oder zwischenspeichern. Der VP ist verpflichtet, die aus der Weisung resultierenden Pflichten auf allfällige Drittdienstleister zu überbinden sowie deren Einhaltung zu überwachen.

3. Datenspeicherung

3.1 Verbot der Datenspeicherung

Jegliches Speichern (kurz- und langfristiges Aufbewahren von Daten in elektronischer oder physischer Form) von sensitiven Kartendaten ist – ausser für das sofortige Einholen der Autorisation – in jedem Falle verboten. Unter die Kategorie sensitive Kartendaten fallen die Daten des Magnetbandes der Karte (Track2-Daten), der Sicherheitscode der Karte (CVC2/CVV2) sowie jegliche Daten in Zusammenhang mit der persönlichen Identifikationsnummer (PIN) des Karteninhabers.

3.2 Einschränkungen der Datenspeicherung

Die Kartennummer (in der Regel sechzehnstellig) darf elektronisch nur in verschlüsselter und besonders gesicherter Form abgespeichert werden. Dies gilt ebenso für das Verfalldatum und den Namen des Karteninhabers, sofern diese zusammen mit der Kartennummer gespeichert werden. Physische Dokumente, welche die obigen Informationen enthalten, dürfen nur in speziell gesicherter Art aufbewahrt werden. Die Datenspeicherung hat sich auf ein betriebsnotwendiges Minimum zu beschränken.

3.3 Weitere Daten

Jegliche übrigen gespeicherten Daten des Karteninhabers sind gegen unberechtigte Zugriffe von innen und aussen mittels geeigneter logischer und physischer Sicherheitsmassnahmen zu schützen. Wird der bei Vertragsabschluss verwendete Webshop hinsichtlich Darstellung sowie Kundeninteraktion grundlegend verändert, ist die SPS vorgängig schriftlich zu informieren und die Einwilligung der SPS abzuwarten.

4. Payment Card Industry Data Security Standard Zertifizierung

Die Payment Card Industry Data Security Standards umfassen eine Reihe von verbindlichen Regeln für alle Parteien, die Kartendaten verarbeiten, speichern oder bearbeiten. Der PCI DSS wird durch das PCI Security Standards Council definiert und regelmässig aktualisiert. Weitere Informationen können direkt auf der offiziellen Webseite des PCI Security Standards Council bezogen werden: https://www.pcisecuritystandards.org.

Grundsätzlich sind alle VP der SPS gehalten, sich mittels der vorgegebenen Zertifizierungsmassnahmen gegenüber dem PCI DSS zu zertifizieren. Die SPS ist ermächtigt, eine PCI DSS-Zertifizierung bei Vertragsabschluss oder während der Vertragslaufzeit jederzeit zu verlangen. Eine Nicht-Zertifizierung des VP trotz schriftlicher Aufforderung der SPS oder das Nichtbestehen einer entsprechenden Zertifizierung gilt als Grund für eine ausserordentliche fristlose Vertragsauflösung.

Die Vorgaben für das Erlangen der Zertifizierung sind je nach Transaktionsvolumen gestaffelt (siehe Ziffer 4.2).

4.1 Pflicht zur Zertifizierung
Alle VP mit einem Akzeptanzvertrag für Distanzgeschäfte und mehr als 20 000 Transaktionen mit MasterCard (inkl. Maestro) und/oder Visa Karten pro Jahr sind verpflichtet, eine PCI DSS-Zertifizierung zu erlangen und aufrechtzuerhalten. Alle VP mit einem Akzeptanzvertrag für Präsenzgeschäfte und einer Transaktionsanzahl über 1 000 000 mit MasterCard (inkl. Maestro) und/oder Visa Karten pro Jahr sind verpflichtet, eine PCI DSS-Zertifizierung zu erlangen und aufrechtzuerhalten.

Alle VP mit einem Akzeptanzvertrag für Distanzgeschäft sind, sofern sie Kartendaten in ihren eigenen Systemen ganz oder teilweise abwickeln, verpflichtet, eine PCI DSS-Zertifizierung zu erlangen und aufrechtzuerhalten.

4.2 Erlangen und Aufrechterhalten der PCI DSS-Zertifizierung
Die PCI DSS-Zertifizierung ist abhängig von der Anzahl der jährlich abgewickelten Transaktionen. Abhängig von der Anzahl der Transaktionen sind regelmässig unterschiedliche Zertifizierungsmassnahmen zu ergreifen, diese lauten wie folgt:

Level	Bezeichnung	Zertifizierungsmassnahmen	Zertifizierungspflicht
1	- VP mit mehr als 6 Mio. Transaktionen p.a. mit MasterCard (inkl. Maestro) oder Visa über alle Vertriebskanäle - VP mit Datenverlust/erfolgreicher Hackerattacke	- Jährliches On-Site Audit durch QSA - Vierteljährlicher Network-Scan durch ASV	Pflicht
2	- VP mit 1 Mio. bis 6 Mio. Transaktionen p.a. mit MasterCard (inkl. Maestro) oder Visa über alle Vertriebskanäle (Präsenzgeschäft und/oder Distanzgeschäft)	- Jährliches On-Site Audit durch QSA oder jährlicher Self Assessment Questionnaire durch einen ISA-akkreditierten Mitarbeiter - Vierteljährlicher Network-Scan durch ASV	Pflicht
3	- VP mit 20 000 bis 1 Mio. E-Commerce-Transaktionen p.a. mit MasterCard oder Visa	- Jährlicher Self Assessment Questionnaire - Vierteljährlicher Network-Scan durch ASV	Pflicht
4	- VP mit E-Commerce Transaktionen, welche Kartendaten in ihren eigenen Systemen abwickeln	- Jährlicher Self Assessment Questionnaire - Vierteljährlicher Network-Scan durch ASV	Pflicht
5	- Alle übrigen VP	- Jährlicher Self Assessment Questionnaire - Vierteljährlicher Network-Scan durch ASV	Auf Verlangen SIX Payment Services AG

Begriffsdefinitionen vgl. Ziffer 8

4.3 Informationspflicht
Der VP hat die SPS regelmässig und unaufgefordert über die Resultate der Zertifizierungsmassnahmen zu informieren. Dies beinhaltet das Zurverfügungstellen des Reports on Compliance (ROC) sofern dies als Zertifizierungsmassnahme vorgesehen ist, der Resultate der Network-Scans sowie des Self Assessment Questionnaires.

Der VP hat die SPS umgehend und unaufgefordert zu informieren, falls der geforderte PCI DSS-Zertifizierungsgrad nicht aufrechterhalten werden kann (aufgrund Systemanpassungen, negativer Resultate bei der Zertifizierung o.ä.).

Änderungen bezüglich des Einsatzes von Drittdienstleistern sind der SPS umgehend mitzuteilen.

Sind Applikationen von Drittdienstleistern im Lizenzmodell in die Abwicklung oder Speicherung von Kartendaten involviert, sind diese Applikationen der SPS zu melden.

Der VP ermächtigt die SPS, Informationen zum Zertifizierungsgrad direkt bei den beauftragten Zertifizierungsstellen einzufordern.

5. Payment Application Data Security Standard (PA DSS)

Applikationen (z.B. Webshop-Applikationen, Customer Relationship Management Systeme, Hotel Property Management Systeme), die verkauft, weitergegeben oder an Dritte lizenziert werden, unterliegen mit Ausnahmen den Anforderungen des PA DSS. Innerbetriebliche Zahlungsanwendungen, die vom VP oder Drittdienstleistern entwickelt und nicht an Dritte verkauft oder lizenziert werden, unterliegen nicht den Anforderungen des PA DSS.

Ab dem **01.07.2012** müssen jegliche in einem Lizenzmodell von Drittdienstleistern genutzten oder standardisierte, eingekaufte Applikationen, welche Kartendaten abwickeln oder speichern, eine Zertifizierung gemäss PA DSS aufweisen. Alle PA DSS-zertifizierten Applikationen sind auf der Website des PCI Security Standard Councils veröffentlicht.

6. Drittdienstleister

Drittdienstleister sind externe Unternehmen, die im Auftrag des VP Kartendaten verarbeiten, abwickeln, speichern oder weiterleiten (z.B. Payment Service Provider, Web-Hosting-Anbieter, Buchungsportale).

Alle durch den VP genutzten Drittdienstleister müssen jederzeit PCI DSS-zertifiziert sowie durch die internationalen Kartenorganisationen formal akzeptiert und registriert sein. Die SPS kann die Nutzung eines Drittdienstleisters jederzeit untersagen oder mit individuellen Restriktionen verbinden. Grundsätzlich dürfen nur Drittdienstleister genutzt werden, die auf der von SPS publizierten Liste der autorisierten Drittdienstleister aufgeführt sind.

7. POS Terminals

Alle eingesetzten POS Terminals müssen über gültige PCI PTS-Zertifikate verfügen.

8. Begriffe

Datenspeicherung
Die Datenspeicherung umfasst das Aufbewahren von Daten in elektronischer oder physischer Form, sowohl langfristig als auch kurzfristig (Zwischenspeicherung).

Qualified Security Assessor (QSA)
Ein Qualified Security Assessor ist eine durch das PCI Security Standards Council akkreditierte natürliche Person, die ermächtigt ist, vor Ort beim VP oder bei einem Dritten, eine Überprüfung durchzuführen und einen Report of Compliance (ROC) zu erstellen.

Approved Scanning Vendor (ASV)
Ein Approved Scanning Vendor ist ein Sicherheitsunternehmen, welches vom PCI Security Standards Council akkreditiert worden ist und Network-Scans durchführt.

Network-Scan
Ein Network-Scan ist ein periodischer und nach Absprache mit dem VP durchgeführter Hacking-Angriff, um mögliche Schwachstellen im System des VP zu ermitteln. Ein Network-Scan darf nur durch einen Approved Scanning Vendor durchgeführt werden.

On-Site Audit
Ein On-Site Audit ist eine beim VP oder Drittdienstleister durch einen Qualified Security Assessor durchgeführte Überprüfung hinsichtlich der Einhaltung des PCI DSS. Das Resultat wird in einem Report on Compliance festgehalten.

Self Assessment Questionnaire (SAQ)
Ein Self Assessment Questionnaire ist eine Selbstdeklaration hinsichtlich der Einhaltung des PCI DSS. Dazu muss ein ausführlicher Sicherheitsfragebogen ausgefüllt werden. Zertifiziert ist, wer alle Fragen mit «Ja» respektive mit «nicht zutreffend» beantworten kann.

Report on Compliance (ROC)
Ein Report on Compliance wird nach erfolgtem On-Site Audit durch einen Qualified Security Assessor erstellt und bestätigt das vollständige Einhalten des PCI DSS.

Internal Security Assessor Program (ISA)
Das durch das PCI Security Standards Council angebotene Internal Security Assessor Program richtet sich an internes Fachpersonal beim VP und bietet ein umfassendes Trainingsprogramm hinsichtlich der Anforderungen des PCI DSS. Das Programm wird mit einer Akkreditierungsprüfung abgeschlossen. Die Akkreditierung muss jährlich wiederholt werden.

110.0901.01 CHE_DE/06.2018

SIX Payment Services AG
Hardturmstrasse 201, Postfach
8021 Zürich

www.six-payment-services.com/welcome