

Sonderbedingungen zur Zusatzvereinbarung PCI DSS Compliance Rules Version-Nr. 2008/0112 PCI der Lufthansa AirPlus Servicekarten GmbH zu den Allgemeinen Geschäftsbedingungen der Lufthansa AirPlus Servicekarten GmbH zur Akzeptanzvereinbarung „Verkauf mit persönlicher Kartenvorlage“ und/oder „Verkauf ohne persönliche Kartenvorlage“ in ihrer jeweils anwendbaren Fassung

Die Lufthansa AirPlus Servicekarten GmbH, Hans-Böckler-Straße 7, 63263 Neu-Isenburg (nachfolgend „AirPlus“ genannt), schließt als zugelassener Acquirer verschiedener Kreditkartenorganisationen Akzeptanzvereinbarungen mit Vertragsunternehmen und Zusatzvereinbarungen zu den „PCI DSS Compliance Rules“. Die nachfolgenden Bestimmungen sind wesentlicher Bestandteil dieser Zusatzvereinbarungen.

1. Präambel

Um Vertragsunternehmen, Kreditkarteninhaber und die Zahlungssysteme vor Vertrauensverlust und Schäden durch missbräuchlich genutzte Kartendaten zu schützen, haben Visa International und MasterCard Worldwide Sicherheitsvorschriften für den Umgang mit Kartendaten aufgestellt. Diese Richtlinien sind im Payment Card Industry Data Security Standard (PCI DSS) niedergelegt, die auf den offiziellen Internetseiten von Visa (<http://www.visaeurope.com/aboutvisa/security/ais/main.jsp>) und MasterCard (<https://sdp.mastercardintl.com>) einsehbar sind und auf Wunsch zugesendet werden. Das Vertragsunternehmen verpflichtet sich daher, bei Akzeptanz von Karten der Zahlungssysteme Visa International und MasterCard Worldwide insbesondere die nachstehenden Sicherheitsvorschriften einzuhalten.

2. Darstellung von Kartendaten

Die Darstellung von Kreditkartendaten ist zu vermeiden.

Durch das Anzeigen von Kreditkartendaten (z.B. auf dem Display eines Kassensystems) kann das Ausspähen dieser Daten ermöglicht werden. Daher dürfen nur die **ersten sechs und/oder die letzten vier Stellen der Kartennummer** dargestellt werden. Nur wenn es für die Aufrechterhaltung des Geschäftsbetriebs unbedingt erforderlich ist, dürfen die Daten einer einzelnen Karte in voller Länge dargestellt werden. Jeder Zugriff ist dann sorgfältig und ausführlich gemäß den Anforderungen des PCI DSS zu protokollieren. Dieselben Anforderungen gelten für den Beleg, der dem Kunden ausgehändigt wird (Kundenbeleg). Auch hier dürfen lediglich die ersten sechs und/oder die letzten vier Stellen abgedruckt werden. Die übrigen Stellen sind zu maskieren (z.B. 1234 56XX XXXX 4321).

3. Übertragung von Kartendaten über einen PC

Die Übertragung von Kartendaten muss gesichert erfolgen.

Die Übertragung von Karten- und Transaktionsdaten erfolgt bei Transaktionen „Verkauf ohne persönliche Kartenvorlage“ typischerweise elektronisch über einen PC, welcher mit einem z.B. durch den Acquirer zur Verfügung gestellten Zahlungssystem bzw. einem Zugang zu diesem ausgestattet ist.

Grundsätzlich sind auf diesen Systemen folgende Sicherheitsmaßnahmen umzusetzen:

1. Für jeden Benutzer ist eine eigene Benutzerkennung einzurichten.
2. Gemeinsam genutzte Kennungen sind unzulässig.
3. Eine nachträgliche Installation von Software durch die Benutzer ist untersagt.
4. Das Kopieren von Daten vom oder auf das System ist zu verhindern.
5. Die Installation eines Virenschanners und die tägliche Aktualisierung sind verpflichtend.
6. Die Nutzung des Systems zum Surfen im Internet ist zu vermeiden.

4. Sichere Aufbewahrung von Kartendaten

Eine Aufbewahrung von Kreditkartendaten ist soweit wie möglich zu verhindern.

Nachfolgende Kartendaten dürfen, sofern dieses zur Aufrechterhaltung des Geschäftsbetriebs erforderlich ist, gespeichert oder aufbewahrt werden:

- Name des Karteninhabers,
- Kartennummer und
- Verfalldatum.

Weitere Kartendaten, wie z.B. die Daten des Magnetstreifens sowie die Kartenprüfziffer (CVV2 / CVC2) dürfen nach der Autorisierung der Transaktion unter keinen Umständen gespeichert werden – weder dauerhaft noch vorübergehend. Diese Informationen sind z.B. auf dem jeweiligen Händlerbeleg enthalten und müssen daher vor unberechtigtem Zugriff geschützt werden. Die Vernichtung der Daten/Händlerbelege hat zu erfolgen, sobald die Kreditkartendaten nicht weiter benötigt werden. Kartendaten, die von Kassensystemen oder auf anderen IT-Systemen gespeichert werden, sind gemäß den Anforderungen des PCI DSS zu verschlüsseln und dürfen nur auf nicht direkt mit dem Internet verbundenen Servern gespeichert werden. Datenträger mit solchen Daten (z.B. Autorisationslogs, Transaktionslisten, Bestätigungen, Auto-Mietverträge, Durchschläge, Kopien, Telefaxe, Briefe) sind in sicherer Umgebung (z.B. Tresor, Bankschließfach) aufzubewahren und vor unberechtigtem Zugriff zu schützen.

Wichtig: Das Speichern der Magnetstreifenendaten nach der Autorisierung der Transaktion ist unter keinen Umständen erlaubt!

5. Verschlüsselung von Datenträgern

Wenn die elektronische Speicherung von Kreditkartendaten auf einem Computer unvermeidlich ist, ist die Festplatte zu verschlüsseln. Nur so kann sichergestellt werden, dass die Kreditkartendaten (z.B. bei einem Diebstahl des Gerätes) nicht in falsche Hände geraten.

6. Vernichten von Kreditkartendaten

Aufbewahrte Daten (z.B. in Kundenkarteien, Faxsendungen, Briefen, Händlerbelegen etc.) sind sicher zu vernichten (z.B. durch einen Aktenvernichter), wenn die Daten nicht mehr benötigt werden. Diese sind in einer Form zu vernichten, die eine elektronische oder physikalische Rekonstruktion der Kartendaten unmöglich machen.

Die gesetzlichen und vertraglichen Aufbewahrungsfristen sind bei der Vernichtung von Kreditkartendaten entsprechend einzuhalten.

Wichtig: Auch Datensicherungen (z.B. auf CDs, DVDs) sind ebenfalls zu verschlüsseln!

7. Einbindung von Dienstleistungspartnern

Dienstleistungspartner, die Zugang zu Kreditkartendaten haben könnten, sind die auf die Beachtung der PCI DSS Regeln hinzuweisen und auf deren Einhaltung schriftlich zu verpflichten.

Dazu zählen z.B. Reinigungsfirmen, die physikalisch Zugang zu Papierbelegen und EDV-Systemen haben, aber auch EDV-/Software-Dienstleister, die Systeme vor Ort, über das Internet oder über Einwahl-Modems warten.

Das Vertragsunternehmen wird nur mit Payment Service Providern zusammen arbeiten, die seitens Visa International und MasterCard Worldwide als PCI konform bewertet wurden und setzt – sofern relevant – ebenfalls nur als PCI konform eingestufte Payment-Applikationen (PCI PA-DSS) bzw. Payment-Terminals (PCI PED Payment Entry Devices) ein.

Ebenso ist eine schriftliche Verpflichtung von externen Leistungsanbietern und Payment Service Providern, die Zugang zu Kreditkartendaten/-informationen haben einzuholen.

8. Meldepflicht von Sicherheitsvorfällen

Sicherheitsvorfälle sind ohne Verzögerung zu melden!

Sollten Unbefugte auf Kartendaten zugegriffen haben (z.B. durch einen Einbruch in die Verkaufsräume, Diebstahl eines PC- oder Kassensystems, auf dem Kartendaten abgelegt sind), oder der Verdacht besteht, so ist das Vertragsunternehmen verpflichtet, dieses bei Bekanntwerden unverzüglich AirPlus und/oder weiteren Acquirern schriftlich zu melden. Nur bei sofortiger Meldung können die bestehenden Verfahren zur Verhinderung des unbefugten Gebrauchs der Kartendaten aktiviert und das Schadensrisiko für alle Beteiligten und mögliche an das Vertragsunternehmen gestellte Schadenersatzforderungen minimiert werden.

9. Meldepflicht von Geschäftsänderungen

Jede Änderung des Geschäftes ist ohne Verzögerung AirPlus zu melden!

Sollten sich Unternehmensdaten ändern oder der Geschäftsbereich erweitert werden, sind diese Anpassungen sofort in schriftlicher Form an AirPlus zu melden. Diese Zusatzvereinbarung wird dann unter Umständen im Falle einer Geschäftsänderung hinfällig und eine neue Zertifizierung ist notwendig.

10. Einbeziehung aller Mitarbeiter

Kartendaten sind wertvoll!

Der Schaden, der durch die missbräuchliche Nutzung einer Kreditkarte entsteht, beläuft sich auf durchschnittlich EUR 2.500,00 pro Karte. Daher erfordert der Schutz der Kartendaten die Einbeziehung aller Mitarbeiter, die potenziell Zugang zu Kartendaten haben. Das Vertragsunternehmen muss alle Mitarbeiter regelmäßig über die Notwendigkeit des Schutzes dieser Daten informieren und sicherstellen, dass nur vertrauenswürdige Mitarbeiter Zugang zu Kartendaten haben.