

Schutz für Kreditkartendaten bei POS-Händlern

Um Vertragspartner, Kreditkarteninhaber und die Zahlungssysteme vor Vertrauensverlust und Schäden durch missbräuchlich genutzte Kreditkartendaten zu schützen, haben MasterCard und VISA Sicherheitsvorschriften für den Umgang mit Kreditkartendaten aufgestellt. Diese Richtlinien sind im Payment Card Industry (PCI) Data Security Standard niedergelegt.

Bei Akzeptanz von Karten der Zahlungssysteme MasterCard oder Visa sind von Vertragspartnern/Vertragsunternehmen die nachstehenden Sicherheitsvorschriften einzuhalten.

Sichere Aufbewahrung von Kartendaten

Eine Aufbewahrung von Kreditkartendaten ist soweit wie möglich zu verhindern.

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

- Name des Karteninhabers,
- Kartenummer und
- Verfalldatum.

Weitere Kartendaten, wie z.B. die Daten des Magnetstreifens, 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 Data Security Standard 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.

Bei der Vernichtung von Kreditkartendaten sind gesetzliche und vertragliche Aufbewahrungsfristen zu berücksichtigen. Gesetzlich oder vertraglich vorgegebene Aufbewahrungsfristen müssen eingehalten werden. Die Vernichtung hat in einer Form zu erfolgen, dass eine Rekonstruktion der Kartendaten nicht mehr möglich ist.

Wichtig: das Speichern der Magnetstreifendaten nach der Autorisierung der Transaktion ist unter keinen Umständen erlaubt!

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 Kartenummer 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 Data Security Standard 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).

Einbeziehung aller Mitarbeiter

Kreditkartendaten sind wertvoll!

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

Meldepflicht von Sicherheitsvorfällen

Melden Sie ihrem Acquirer Sicherheitsvorfälle ohne Verzögerung!

Sollten Unbefugte auf Kreditkartendaten zugegriffen haben (z.B. durch einen Einbruch in die Verkaufsräume, Diebstahl eines PC auf dem Kartendaten abgelegt sind), oder Sie den Verdacht haben, so ist der Vertragspartner verpflichtet, dieses bei Bekanntwerden **unverzüglich** dem zuständigen Acquirer 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 ihn gestellte Schadenersatzforderungen minimiert werden.