RICHTIGER UMGANG MIT KARTENDATEN LAUT PCI-SICHERHEITSRICHTLINIEN

Der PCI-Standard sagt, dass die **dauerhafte Speicherung** von Kreditkartendaten (Kartennummer, Name, Ablaufdatum) auf eigenen Systemen vermieden werden sollte und wenn notwendig nur unter strengen Bedingungen (u.a. Verschlüsselung) erfolgen darf. Kurzfristig notwendige Kreditkartendaten (z.B. für eine Anzahlung oder Nachverrechnung) sind so bald als möglich wieder zu löschen.

Die Speicherung der Daten des **Magnetstreifens** oder die **Kartenprüfnummer** von der Kartenrückseite sind verboten!

Der PCI-Sicherheitsstandard ist für alle **Vertragsunternehmen verpflichtend** und durch die Vertragsbedingungen der Kreditkartenorganisationen (Mastercard, Visa) vorgegeben.

Wer Kredit-/Bankomatkartendaten speichert und diese werden gestohlen, muss mit **hohen Geldstrafen** rechnen!

WER SOLLTE BESONDERS AUF DEN UMGANG MIT KARTENDATEN ACHTEN?
Hotels, die Kartennummern über eine Homepage/elektronische Plattform oder per E-Mail erhalten, die Kartennummern in ihren Kundensystemen speichern oder als Ausdruck aufbewahren.

Vertragsunternehmen mit einer Freischaltung von Kreditkartenzahlungen im Fernabsatz (manuelle Karteneingabe, MOTO).

hobex empfiehlt **keine Kartendaten auf eigenen Systemen** (z.B. in einer Kundenverwaltungssoftware, im E-Mail Posteingang oder auf Papier) zu verarbeiten bzw. längerfristig **aufzubewahren**.
Die Abrechnungsbelege unserer Terminals enthalten die Kreditkartennummer nur ausgesternt.
Dadurch ist gewährleistet, dass Vertragsunternehmen **keine weiteren Nachweise** und **Sicherheitsprüfungen** zur Erfüllung des PCI-Standards erbringen müssen.

hobex AG • Josef-Brandstätter-Straße 2b • 5020 Salzburg
T +43 662 2255-0 • F +43 662 2255-399 • M vertrieb@hobex.at • www.hobex.at
LG Salzburg • DVR 0660868 • FN 37265b • UID-NR. ATU35185508