

Diese «Weisungen über die Sicherheit von Kredit- und Debitkartendaten» sind als technische und organisatorische Weisungen und Anleitungen bindende Bestandteile der Vertragsbeziehungen zu Telekurs Multipay. Sie sind deshalb vom Vertragspartner zu beachten und einzuhalten (vergleiche Ziffer 14.1 der «Allgemeinen Geschäftsbedingungen für das bargeldlose Zahlen» und Ziffern 12.4 in den «Besonderen Geschäftsbedingungen für die Akzeptanz von Kreditkarten bei Abwesenheit der Kreditkarte» und in den «Besonderen Geschäftsbedingungen für die Akzeptanz von Debitkarten bei Abwesenheit der Debitkarte»). Die Nichtbeachtung stellt eine Vertragsverletzung durch den Vertragspartner dar und hat die in den Allgemeinen und Besonderen Geschäftsbedingungen festgehaltenen Rechtsfolgen. Namentlich berechtigt sie Telekurs Multipay zur fristlosen Kündigung des Vertragsverhältnisses und zur Geltendmachung von Schadenersatzansprüchen zufolge Bussen der Kartenorganisationen und Ersatzforderungen der Kartenherausgeber.

Um Vertragspartner, Karteninhaber und das gesamte Zahlungssystem vor Schäden durch missbräuchlich genutzte Kartendaten zu bewahren, haben MasterCard und VISA Sicherheitsvorschriften für die Verarbeitung, Übermittlung und Speicherung von Kartendaten aufgestellt. Bei Akzeptanz von Kredit- oder Debitkarten hat der Vertragspartner zumindest die nachstehenden Sicherheitsvorschriften einzuhalten, falls er keine Kartendaten übermittelt, verarbeitet oder speichert. Tut er dies, gelten für ihn die «Weisungen über die Einhaltung der PCI Sicherheitsvorschriften für Vertragspartner».

Sicherheitsvorschriften für Vertragspartner	Alle Vertragspartner, welche keine Kartendaten übermitteln, verarbeiten oder speichern, sind verpflichtet, zumindest die in diesem Merkblatt festgehaltenen Sicherheitsvorschriften einzuhalten. Vertragspartner, die auf ihren Systemen Kartendaten übermitteln, verarbeiten oder speichern, sind darüber hinaus verpflichtet, die Sicherheitsvorgaben des Payment Card Industry Data Security Standards (PCI DSS) einzuhalten (siehe dazu Merkblatt «Weisung über die Einhaltung der PCI Sicherheitsvorschriften für Vertragspartner»).
Service Provider, beauftragte Dritte	Vom Vertragspartner beauftragte Dritte (DSE Data Storage Entities, wie Informatik-Lieferanten, Payment Service Provider), welche Kartendaten übermitteln, verarbeiten oder speichern, sind der Telekurs Multipay zu melden. Der Vertragspartner ist verantwortlich dafür, dass diese Dritten die Sicherheitsvorgaben des Payment Card Industry Data Security Standards (PCI DCC) einhalten (siehe dazu Merkblatt «Weisung über die Einhaltung der PCI Sicherheitsvorschriften für Vertragspartner»).
Speicherung und Ablage von Kartendaten	Wenn überhaupt, darf nur der geschäftlich relevante Teil der Kartendaten gespeichert und abgelegt werden: Name des Karteninhabers, Kartenummer und Verfallsdatum. Datenträger mit solchen Daten (z. B. Autorisationslogs, Transaktionslisten, Bestätigungen, Auto-Mietverträge, Durchschläge, Telefaxe, Talons) sind in sicherer Umgebung mit Zutrittsbeschränkung aufzubewahren. Folgende Daten dürfen unter keinen Umständen gespeichert werden, auch nicht verschlüsselt : <ul style="list-style-type: none">• der volle Inhalt jeglicher Spur auf dem Magnetstreifen der Karte• der Kartenprüfwert (CVC2/CVV2, dreistelliger Wert im Unterschriftsfeld auf der Rückseite der Karte)• PIN-Code• Passwörter für die Authentisierung der Karteninhaber bei «MasterCard SecureCode» und «Verified by VISA»

Vernichtung von Kartendaten

Belege mit Kartendaten sind nach Ablauf der Aufbewahrungsfrist gemäss BGB (24 Monate) zu vernichten.

Meldepflicht von
Sicherheitsvorfällen

Sollten Unbefugte auf Kartendaten zugegriffen haben, muss der Vertragspartner dies unverzüglich der Telekurs Multipay melden und bei der Aufklärung mit Telekurs Multipay zusammenarbeiten. Nur bei sofortiger Meldung können die bestehenden Verfahren zur Verhinderung des unbefugten Gebrauchs der Kartendaten aktiviert werden. Dadurch begrenzt der Vertragspartner das Schadensrisiko für alle Beteiligten und mögliche an ihn gestellte Schadenersatzforderungen.