

HANDBUCH FÜR TRANSAKTIONEN MIT ZAHLUNGSKARTEN



ANLEITUNG FÜR HÄNDLER

ÜBER DIESES DOKUMENT	3	7. CHARGEBACK	25
BEGRIFFSDEFINITIONEN	4	7.1. Die häufigsten Chargeback-Arten	25
1. AKZEPTANZ VON ZAHLUNGSKARTEN	6	7.2. Wie sich das Chargeback-Risiko reduzieren lässt	25
1.1. Transaktionskarten	6	8. FRAUD-/BETRUGSFÄLLE	27
1.2. Akzeptanz von Karten durch Zahlungsterminals	6	8.1. Empfohlene Vorgehensweisen zur Betrugsprävention	27
2. VERARBEITUNG UND ABRECHNUNG VON TRANSAKTIONEN	8	9. PCI DSS – SCHUTZ VON KARTENDATEN	28
2.1. Tagesende am POS-Terminal	8	9.1. Empfohlene Vorgehensweisen	28
2.2. Fristen zur Verarbeitung von Transaktionen	8	9.2. Was geschieht, wenn Sie die Richtlinien der „PCI DSS“-Standards nicht erfüllen?	28
2.3. Fristen zur Zahlungsgutschrift auf Ihr Konto	8	10. WEITERE WICHTIGE INFORMATIONEN	29
2.4. Abgelehnte Transaktionen	8	10.1. Verwendung eines eigenen Zahlungsterminals	29
2.5. Stornierung einer Transaktion	8	10.2. Anschluss des Terminals an ein Kassensystem (ECR)	29
2.6. Akzeptanz von Karten über das Internet/GP webpay	9	10.3. Verkaufsbeleg-Kopie	29
3. TRANSAKTIONSÜBERSICHT – BENUTZERPORTALE	10	10.4. Telefonat mit der Meldung „CODE 10“	30
3.1. Händlerportal (Merchantportal)	10	10.5. Einbehalt der Karte	30
3.2. Portal GP webpay	10	10.6. Kartenfund oder vergessene Karte in Ihren Geschäftsräumen	31
4. WEITERE TRANSAKTIONSARTEN	11	10.7. Testkauf	31
4.1. Autorisierung	11	10.8. Papierrollen für POS-Terminals	32
4.2. Kontaktlose Kartenzahlungen	12	10.9. Erstellung Ihrer eigenen Werbung	32
4.3. Dynamic currency conversion (DCC)	12	10.10. Wir halten Sie am Laufenden	32
4.4. Trinkgeld	13	11. WICHTIGE KONTAKTE	33
4.5. Cashback	13		
4.6. Inkrementelle Vorautorisierung	13		
5. ÜBERPRÜFUNG VON ZAHLUNGSKARTEN	15		
6. AKZEPTANZ VON ZAHLUNGSKARTEN IN SPEZIFISCHEN BRANCHEN	21		
6.1. Transaktionen in Hotels und Mietwagenfirmen	21		
6.2. Wechselstuben/Casinos	24		

ÜBER DIESES DOKUMENT

Diese Anleitung für Händler bildet, zusammen mit den unter Paragraph 1.1. der Allgemeinen Geschäftsbedingungen angeführten Dokumenten, den Vertrag zur Akzeptanz von Zahlungskarten welchen Sie mit uns abgeschlossen haben (hiernach „Vertrag“ genannt).

In Ihrem eigenen Interesse sowie zu Ihrem eigenen Schutz sollten Sie sich dieses Dokument aufmerksam durchlesen und die darin enthaltenen Anleitungen beachten.

Folgende Informationen und Anleitungen sind für Sie in diesem Handbuch enthalten:

- Allgemeine Anleitungen bezüglich der Akzeptanz von Zahlungskarten
- Anleitungen bezüglich der Akzeptanz von Zahlungskarten in ausgewählten Bereichen
- Informationen zur Verarbeitung von Transaktionen mit Zahlungskarten
- Wichtige Informationen zu Risiken in Bezug auf die Akzeptanz von Zahlungskarten, sowie die Vermeidung dieser Risiken. Im Handbuch sind nützliche Tipps und Hinweise angeführt, welche bei der Akzeptanz von Zahlungen mit Karten eingehalten werden sollten.

Diese Anleitung finden Sie auch online im Merchant Portal auf www.globalpayments.at.

Anmerkungen und Feedback sind stets willkommen. Bei Fragen oder Anmerkungen in Bezug auf diese Anleitungen oder bei anderen Aspekten bezüglich der von uns erbrachten Leistungen, zögern Sie bitte nicht, uns zu kontaktieren. Eine Übersicht mit allen Kontaktdaten finden Sie auf Seite 33.

BEGRIFFSDEFINITIONEN

AS/AUTORISIERUNGSSERVICE	Alle Transaktionen werden von dem Aussteller autorisiert. Dieses Service wird Autorisierungsservice genannt.
ZAHLUNGSKARTENSYSTEM/ KARTENORGANISATION	Internationales Unternehmen, welches an Banken Lizenzen zur Ausgabe von Zahlungskarten sowie zur Verarbeitung der mit Zahlungskarten getätigten Transaktionen vergibt (Visa Intl., Mastercard Intl., Diners Club Intl., Japan Credit Bureau Intl., Union Pay Intl.).
GENEHMIGUNG	Prozess, in dessen Rahmen überprüft wird, ob eine bargeldlose Zahlung mit einer Zahlungskarte getätigt werden kann. Dient zur Überprüfung der Gültigkeit der Karte und ob die entsprechende Deckung für die Kartentransaktion vorhanden ist.
GENEHMIGUNGSCODE	Vier- bis siebenstellige Zahlenkombination bzw. Zahlen- und Buchstabenkombination, welche dem Händler als Referenz für die Berechtigung eine Kartentransaktion durchzuführen mitgeteilt wird.
GENEHMIGUNGSLIMIT	Maximale Betragshöhe, welche mit einer Zahlungskarte an einem Geschäftsort des Händlers während eines Kalendertages erfolgen kann, ohne dass zwingend eine Genehmigung für die Kartentransaktion über AS eingeholt werden muss. Die Betragshöhe kann aufgrund eines an PSP gesandten Antrags für einige Segmente geändert werden.
KONTAKTLOSE TECHNOLOGIE (CONTACTLESS) – NFC (Near Field Communication)	Kontaktlose Akzeptanz von Zahlungskarten. Bei kontaktlosen Zahlungen befindet sich auf der Zahlungskarte neben den standardmäßigen Sicherheitselementen auch ein Symbol, mit welchem der Karteninhaber zur Durchführung von kontaktlosen Transaktionen berechtigt ist. Bei der NFC-Technologie (Near Field Communication) handelt es sich um eine drahtlose Technologie um die Funkübertragung von Daten auf eine kurze Entfernung, welche eine einfache sowie sichere beidseitige Kommunikation zwischen elektronischen Geräten ermöglicht. Bspw. die Vornahme von kontaktlosen Transaktionen mit einem Mobiltelefon, Anhänger, Uhr, Sticker, Zahlungen über QR-Code, etc.
	
KONTAKTLOSES LESEGERÄT	Kontaktloses Lesegerät, welches sich außerhalb des Zahlungsterminals befindet oder zum Bestandteil des Zahlungsterminals gehört und welches zur Akzeptanz von Zahlungskarten sowie von anderen Geräten mit kontaktloser Technologie entwickelt wurde.
KARTENINHABER	Natürliche Person, an welche eine Zahlungskarte aufgrund eines Vertrags mit einer kartenausgebenden Bank ausgegeben wurde und deren Vor- und Nachname auf der Zahlungskarte aufgedruckt sind.
GP	Abkürzung für das Unternehmen Global Payments, s.r.o., www.globalpayments.at
mPOS	Mobiles Gerät zur elektronischen Akzeptanz und Verarbeitung von Kontakt- (Magnetstreifen oder Chip) und kontaktlosen Kartentransaktionen.

GESCHÄFTSORT/VERKAUFSORT	Ort, an welchem vom Händler bargeldlose Zahlungen mit Zahlungskarten oder NFC-Geräten für erbrachte Leistungen und verkaufte Waren akzeptiert werden. Adresse, an der sich die Räumlichkeiten des Händlers befinden und wo die betreffende Transaktion initiiert wurde. Allerdings gilt: a) bei Verträgen, welche im Sinn von Art. 2, Punkt 7 der Richtlinie 2011/83/EU im Fernabsatz abgeschlossen wurden, handelt es sich beim Verkaufsort um den dauerhaften Unternehmensort, an welchem der Händler seine Geschäftstätigkeit ausübt - unabhängig vom Standort der Internetseiten oder des Servers - und über welchen die Zahlungstransaktion initiiert wird; b) wenn der Händler keinen dauerhaften Unternehmensort hat, handelt es sich beim Verkaufsort um die Adresse, für die der Händler über eine gültige Lizenz für die unternehmerische Tätigkeit verfügt und für welche die Zahlungstransaktion initiiert wird; c) wenn der Händler keinen dauerhaften Unternehmensort hat sowie auch über keine gültige Lizenz für die unternehmerische Tätigkeit verfügt, gilt als Verkaufsort die Postadresse, welche für Steuerzahlungen im Zusammenhang mit seiner Geschäftstätigkeit festgelegt wurde und über welche die Zahlungstransaktion initiiert wird.
PIN PAD	Externes Gerät zur Eingabe der PIN, welches eigenständig funktioniert oder an ein Zahlungsterminal angeschlossen ist.
KARTENZAHLUNG	Kartentransaktion, welche mit einer Zahlungskarte oder einem NFC-Gerät zugunsten des Händlers zur Bezahlung der gekauften Waren oder der erbrachten Leistungen erfolgt.
PUSH-ZAHLUNGEN	Mit PUSH Zahlungen kann der Händler dem Karteninhaber Zahlungsdetails per E-Mail senden. Diese Lösung ersetzt die sogenannten Mail/Telefon Auftragstransaktionen.
ZAHLUNGSTERMINAL/POS	Elektronisches Zahlungsterminal zur elektronischen Akzeptanz und Verarbeitung von Kontakt- (Magnetstreifen und Chip) und kontaktlosen Kartentransaktionen. Zum Bestandteil des Zahlungsterminals kann auch ein Zusatzgerät zur Eingabe der PIN- das PIN PAD gehören.
TRANSAKTIONSUNTERLAGEN	Allgemeine Bezeichnung für alle Dokumente, welche sich auf die Transaktion beziehen, einschließlich der Bestätigung in elektronischer oder Papierform über die erfolgte Transaktion/Belege.
ZAHLUNGSDIENSTLEISTER/PSP/ACQUIRER	Lieferant von Zahlungsleistungen, welcher mit dem Händler einen Vertrag über die Akzeptanz von Zahlungskarten abschließt und die Leistungen liefert, welche im Zusammenhang mit der Akzeptanz von Zahlungskarten stehen. PSP steht für Payment Service Provider im Sinne der EU-Verordnungen.
LEGITIMATIONS-/IDENTITÄTSNACHWEIS	Personalausweis, Führerschein oder Reisepass.
AGB	Allgemeine Geschäftsbedingungen

1. AKZEPTANZ VON ZAHLUNGSKARTEN

Nach den Regeln der Kartenverbände ist der Händler verpflichtet, bei der Annahme einer Zahlungskarte wie folgt vorzugehen:

- Der Händler akzeptiert Zahlungskarten ausschließlich, damit verkaufte Waren oder erbrachte Leistungen bezahlt werden können, wobei die Betragshöhe für die Transaktion nicht beschränkt ist.
- Der Händler zahlt dem Karteninhaber kein Bargeld aus, außer er hat mit PSP über einen schriftlichen Nachtrag zum Vertrag etwas anderes vereinbart. Mehr Informationen zu Cashback-Transaktionen finden Sie im *Kapitel 4.9. Cashback*.
- Der Händler nimmt keine Transaktionen vor, wenn der Karteninhaber nicht anwesend ist, außer er hat mit PSP über einen schriftlichen Nachtrag zum Vertrag etwas anderes vereinbart, mehr Informationen zu Transaktionen mit manueller Eingabe finden Sie im *Kapitel 1.1. Transaktionsarten*.

1.1. TRANSAKTIONSARTEN

Die Ausführung aller genannten Transaktionsarten ist in den entsprechenden Handbüchern der POS-Terminals angeführt.

Transaktionen, bei denen die Karte vorhanden ist (CP, Card Present). Das bedeutet, alle Transaktionen, bei denen die Karte und deren Inhaber zum Zeitpunkt der Transaktion physisch anwesend sind und man sich vom Vorhandensein der Karte überzeugen kann, indem der Chip gelesen wird, die Karte mit dem Magnetstreifen durch das Lesegerät gezogen oder an das Terminal mittels NFC gehalten wird.

Transaktionen, bei denen die Karte nicht vorhanden ist (CNP, Card Not Present). Das bedeutet, alle Transaktionen, bei denen die Karte und deren Inhaber zum Zeitpunkt der Transaktion nicht physisch anwesend sind. Diese Transaktionen sind mit einem Risiko verbunden, wenn Sie nicht belegen können, dass die Transaktion vom tatsächlichen Inhaber der Zahlungskarte getätigt wurde. Es sind zwei Transaktionsarten möglich, ohne dass die Zahlungskarte vorhanden ist.

- **Transaktionen, welche über die Tastatur am Terminal eingegeben werden** – für diese Möglichkeit muss am Terminal die Funktion „manuelle Eingabe“ aktiviert sein.
- **E-commerce Transaktionen über GP webpay**

1.2. AKZEPTANZ VON KARTEN DURCH ZAHLUNGSTERMINALS

Sie können Karten entweder über das von uns gelieferte Terminal oder – nach vorheriger gegenseitiger Vereinbarung – über Ihr eigenes Gerät akzeptieren. Mehr Informationen zum Einsatz eines eigenen Geräts finden Sie im *Kapitel 10.1. Verwendung eines eigenen Zahlungsterminals, Seite 29*. Hier finden Sie weitere Informationen zu den Bedingungen, unter deren Einhaltung Sie Zahlungskarten über Ihr eigenes Gerät akzeptieren können. Dieses muss von GP zertifiziert werden.

- Vor Beginn lesen Sie sich bitte das Benutzerhandbuch für Ihren Terminaltyp durch. Bitte halten Sie den genannten Ablauf für die einzelnen Transaktionsarten ein.
- In Bezug auf den Standort des Terminals oder PIN PADS sollten Sie berücksichtigen, dass es einfach zugänglich ist und die Privatsphäre aller Karteninhaber gewahrt bleibt, einschließlich der Karteninhaber mit Behinderung. Der Karteninhaber soll während der gesamten Transaktion seine Karte sowie die Eingabe von Daten vor Blicken schützen können.
- Sorgen Sie dafür, dass ein einfacher Zugang zu den sich in der Nähe des Terminals befindlichen Steckdosen, Telefonanschlüssen und Netzwerkanschlüssen gewährleistet ist. Dies ist wichtig falls technische Probleme auftreten und wir Sie auffordern, im Rahmen der Identifizierung des Problems bestimmte Tests vorzunehmen. Bei mobilen Terminals sollten Sie für eine entsprechende Netzabdeckung mittels W-LAN sorgen bzw. wählen Sie einen Terminalstandort, der eine Netzabdeckung durch einen Mobilfunkbetreiber ermöglicht.

- Stellen Sie sicher, dass keine Aufnahmen vom Kunden bei der PIN-Eingabe durch Sicherheitsanlagen (z. B. durch Überwachungskameras) erfolgen können.
- Bei allen Änderungen an Ihrem Terminal, einschließlich dessen Austausch, Entfernung oder Aufstellung an einem anderen Standort, bitten wir Sie, mit uns Rücksprache zu halten. Mobile Terminals dürfen natürlich im Rahmen der normalen Nutzung jeden Tag an einem anderen Standort innerhalb Österreichs aufgestellt werden.
- Sie haften für das Terminal. Aus diesem Grund empfehlen wir Ihnen, besonders auf den Standort des Terminals zu achten sowie das Gerät regelmäßig zu kontrollieren. Des Weiteren haften Sie auch für alle Verluste infolge des Eingriffs Dritter, welche nicht berechtigt sind, das Gerät auf andere Weise als im Rahmen des normalen üblichen Transaktionsverlaufs – d. h. zum Beispiel PIN-Eingabe – zu betätigen bzw. zu bedienen.

TRANSAKTIONSABLAUF

- 1. Der berechtigte Karteninhaber führt am Geschäftsort eine Zahlungstransaktion entsprechend den Terminalanweisungen aus und bestätigt seine Identität** durch Eingabe der PIN oder indem er auf dem Beleg oder Display des mobilen Geräts (bei mPOS) unterschreibt. Die Zahlung kann auch über andere Geräte mit implementierter kontaktloser NFC-Technologie erfolgen. Der Händler ist berechtigt, die sich auf der Karte befindlichen Sicherheitselemente auch dann zu überprüfen, wenn der Karteninhaber die Chipkarte selbst in das Lesegerät steckt.

Wenn eine Transaktion anhand der, seitens des Karteninhabers auf der Zahlungskarte geleisteten Unterschrift überprüft werden muss, überprüft der Händler die Unterschrift auf der Karte und vergleicht diese mit der Unterschrift auf dem Beleg. Wenn der Karteninhaber unterschreibt, darf er seine Unterschrift auf der Zahlungskarte nicht sehen.

- 2. Genehmigung einer Transaktion**

Die Genehmigung einer Transaktion am POS-Terminal erfolgt automatisch. Über das POS-Terminal erhält der Händler eine Genehmigungsantwort. Es kann auch eine Genehmigung der Transaktion im Vorfeld erfolgen (mehr Informationen dazu finden Sie im *Kapitel 4.1. Autorisierung, S. 11*).

- 3. Aushändigung des Verkaufsbelegs**

Der Händler ist verpflichtet, dem Karteninhaber den Beleg über die erfolgte Transaktion auszuhändigen sowie alle Unterlagen, durch welche die Ausführung der Transaktion dokumentiert wird (d. h. die Aufzeichnungen über die erfolgte Kommunikation mit dem Karteninhaber in Papier- oder elektronischer Form sowie andere entsprechende Aufzeichnungen). Diese Dokumentation (Händlerbeleg) ist über einen Zeitraum von zwei Jahren ab dem Datum der Transaktionsausführung in leserlicher Form aufzubewahren sowie auf Verlangen von GP auszuhändigen.

2. VERARBEITUNG UND ABRECHNUNG VON TRANSAKTIONEN

2.1. TAGESENDE AM POS-TERMINAL

In der Grundeinstellung ist jedes Terminal so eingestellt, dass das Tagesende automatisch, spätestens um 22:55 Uhr (- 30 Minuten bis + 30 Minuten ab Geschäftsschluss) erfolgt.

Das automatische Tagesende kann auf manuelles Tagesende umgestellt werden. Zur Einstellung Ihres Zeitfensters (in der Zeit zwischen 0:00 Uhr und 22:55 Uhr) wenden Sie sich bitte an den Helpdesk (S. 33).

2.2 FRISTEN ZUR VERARBEITUNG VON TRANSAKTIONEN

Die Systemfrist zur Transaktionsabrechnung ist um 22:55 Uhr.

Alle Transaktionen, welche vor dieser Frist zur Abrechnung vorliegen, werden in der Regel am darauffolgenden Tag – also D+1 – von unserem Konto auf Ihr Konto überwiesen. Alle Transaktionen, welche nach dieser Systemfrist getätigt werden, werden in der Regel am 2. darauffolgenden Tag – also D+2 (wobei es sich bei „D“ um den Tag handelt, an welchem die Transaktion erfolgt ist) – von unserem Konto auf Ihr Konto überwiesen.

2.3 FRISTEN ZUR ZAHLUNGSGUTSCHRIFT AUF IHR KONTO

Die Gutschrift der Transaktionen auf dem Konto erfolgt am Termin D+1.

2.4 ABGELEHNTE TRANSAKTIONEN

Im Rahmen des durch uns erfolgenden Transaktionsüberprüfungsprozesses werden von uns alle Transaktionen abgelehnt sowie zurückgegeben, bei denen die Überprüfung nicht erfolgreich war, wie zum Beispiel mit abgelaufener Karte getätigte Transaktionen. Abgelehnte Transaktionen sind für Sie mit einem Verlust verbunden.

Bevor es dazu kommt, überprüfen wir die Transaktionsdetails sowie unsere Systeme. Sollten wir Fehler finden, werden diese behoben. Kann das Problem nicht gelöst werden, werden wir Sie per Brief/E-Mail informieren und der Ihrem Konto gutgeschriebene Betrag wird auf die entsprechende Art und Weise berichtigt.

Wird eine komplette Transaktionsdatei abgelehnt, werden wir mit Ihnen Kontakt aufnehmen und Sie über die Abhilfemaßnahmen informieren. Auf diese Weise wird vermieden, dass Ihrem Konto keine finanziellen Beträge fälschlicherweise gutgeschrieben werden.

2.5. STORNIERUNG EINER TRANSAKTION

Wenn sich der Karteninhaber entscheidet eine Ware oder Leistung doch nicht zu kaufen, müssen Sie die Transaktion stornieren. Die von Ihnen vorzunehmenden Schritte sind davon abhängig, wie Sie die Karte akzeptiert haben sowie von der Phase, in welcher sich die Transaktion zu dem Zeitpunkt befunden hat, zu dem der Karteninhaber entschieden hat, diese zu stornieren.

Abbruch einer nicht abgeschlossenen Transaktion

- Transaktion mit PIN: Die Transaktion kann während der Betragseingabe auf der Tastatur des Terminals storniert werden. Alternativ kann die Stornierung der Transaktion durch den Karteninhaber während der Eingabe der PIN erfolgen.
- Transaktion mit Unterschrift: Sie können die Transaktion zu dem Zeitpunkt stornieren, an dem Sie vom Terminal aufgefordert werden, die Unterschrift des Karteninhabers zu bestätigen

Wenn eine Vorautorisierung nicht innerhalb von 30 Tagen ab dem Datum der Vorautorisierung abgeschlossen wird, ist die Transaktion nicht garantiert.

Stornierung einer abgeschlossenen Transaktion

- **innerhalb von 95 Tagen ab Transaktionsdatum:** die Vorgehensweise erfolgt entsprechend dem Benutzerhandbuch für Ihr Terminal, Kapitel „Storno einer beliebigen Transaktion“. Der Betrag kann entweder in voller Höhe oder teilweise storniert werden, wenn diese Funktion am POS-Terminal zulässig ist. Wenn bei der stornierten Transaktion der DCC-Service genutzt wurde, kann nur die gesamte Transaktion storniert werden und der Stornobetrag ist in der Währung einzugeben, in welcher die Transaktion erfolgte.
- **nach mehr als 95 Tagen ab Transaktionsdatum:** wenden Sie sich bitte an den Helpdesk und bitten Sie, die Transaktion zu stornieren.

Händigen Sie dem Karteninhaber einen Beleg über die Stornierung der Transaktion aus.

Die Beträge dürfen nur auf die gleiche Karte zurückerstattet werden, welche bei der ursprünglichen Transaktion verwendet wurde und der Betrag darf den Betrag der ursprünglichen Transaktion nicht übersteigen. Erstaten Sie nie Beträge auf andere Art und Weise zurück und lassen Sie sich nicht auf die Möglichkeit ein, Beträge in bar oder per Überweisung auf das Konto zurückzuerstatten.

2.6. AKZEPTANZ VON KARTEN ÜBER DAS INTERNET/GP WEBPAY

Bei GP webpay handelt es sich um ein Zahlungsportal im Internet zum schnellen und sicheren Bezahlen mit Karte. Online stehen Ihnen unter www.gpwebpay.cz/en detaillierte Benutzerhandbücher für alle über diese Zahlungsmöglichkeit erfolgten Transaktionen zur Verfügung. Um alle Transaktionsarten komplett nutzen zu können, halten Sie bitte die in diesen Handbüchern angeführten Anleitungen ein.

3. TRANSAKTIONSÜBERSICHT - BENUTZERPORTALE

Eine Übersicht über alle Transaktionen steht dem Händler auf folgenden Kundenportalen zur Verfügung:

- Merchant Portal – am POS sowie über E-Commerce erfolgte Transaktionen
- GP webpay Portal – für E-Commerce-Transaktionen

3.1. HÄNDLER PORTAL (MERCHANT PORTAL)

Beim Kundenportal handelt es sich um ein System, welches für alle Händler bestimmt ist, die Zahlungskarten akzeptieren. Es ist unter **www.globalpayments.at** zugänglich. Detailliertere Informationen mit der genauen Beschreibung aller verfügbaren Funktionen sind im Benutzerhandbuch für das Kundenportal zu finden, welches im Bereich „Downloads“ zur Verfügung steht.

- Menüpunkt „Genehmigung“: Transaktions- und Genehmigungsübersicht, einschließlich der abgelehnten Transaktionen
- Menüpunkt „Auszüge“: enthält alle generierten Transaktionsübersichten
- Menüpunkt „Einstellungen“: Einstellung des Transaktionsübersicht-Formats, Definition der E-Mail-Adresse zum Versand von Dateien mit Transaktionsübersicht und Rechnungen
- Generierung der Datenauszüge/Zahlungsanzeigen in den Formaten PDF, FLAT, XML, CSV
- Frequenz der Generierung des Versands von Transaktionsübersicht: Einstellung über Anforderung an den Sales Support
 - o PDF – wöchentlich, monatlich
 - o FLAT, XML, CSV – täglich, wöchentlich, monatlich

Auf Wunsch des Händlers wird das Dateiformat sowie eine Testdatei bereitgestellt um das passende Format zu finden.

3.2. PORTAL GP WEBPAY

Über das Portal GP webpay hat der Händler folgende Möglichkeiten:

- Suche und Verwaltung von Zahlungen
- Erstellung, Versand, Suche und Verwaltung von PUSH-Zahlungen (die Einzelheiten zur Vorgehensweise bei der PUSH-Zahlung finden Sie im GP webpay Benutzerhandbuch unter www.gpwebpay.cz/Content/downloads/GP_webpay_Gateway_EN.pdf)
- Benutzeranlage und -verwaltung
- Anzeige von Statistiken und zulässigen Funktionen für den E-Shop und Zahlungen
- Schlüsselanlage und -verwaltung
- Herunterladen der technischen Dokumentation sowie weiterer Quellen zur Integration mit der Schnittstelle des Zahlungsportals GP webpay

4. WEITERE TRANSAKTIONSARTEN

4.1. AUTORISIERUNG

Bei einer Autorisierung handelt es sich um den Prozess, in dessen Rahmen die Gültigkeit der Zahlungskarte überprüft wird und festgestellt wird, ob das Konto des Karteninhabers die erforderliche Deckung für die beabsichtigte Zahlungstransaktion aufweist. Bei einer Autorisierung erfolgt keine Bestätigung der Identität des Karteninhabers und es handelt sich auch nicht um eine Zahlungsgarantie.

VORAUTHORISIERUNG

Eine Vorautorisierung findet häufig im Tourismus Anwendung, vor allem in Unterkunftseinrichtungen und Mietwagenfirmen, da in diesen Anwendungsfällen der finale Transaktionsbetrag zum Zeitpunkt der ursprünglichen Transaktion nicht immer bekannt ist.

Eine Vorautorisierung kann für alle Kartentypen erfolgen, mit Ausnahme der Zahlungskarten Maestro, Mastercard Electronic, Visa Electron und V PAY.

Der Händler ist verpflichtet, eine Vorautorisierung innerhalb von 30 Tagen ab dem Datum der Vorautorisierung abzuschließen.

Der Betrag der Vorautorisierung muss immer dem im Vorfeld zwischen dem Händler und dem Karteninhaber vereinbarten Waren- oder Leistungspreis entsprechen. Der Karteninhaber muss im Vorfeld über die Vorautorisierung informiert werden und der Vorautorisierung zustimmen.

ABSCHLUSS EINER VORAUTHORISIERUNG

Bei der Abschlusstransaktion für eine Vorautorisierung handelt es sich praktisch um den Verkaufsabschluss, für welchen vorher eine Vorautorisierung erfolgt ist. Der Abschlussbetrag der Vorautorisierung kann vom im Rahmen der Vorautorisierung eingegebenen Betrag abweichen.

Wenn der Kunde beispielsweise zwei Waren bestellt hat und nur eine bezahlt werden muss, unterscheidet sich der Vorautorisierungsbetrag für zwei Waren von dem Betrag des Abschlusses der Vorautorisierung. Bei Transaktionen innerhalb der Reisebranche ist ein Limit definiert.

Der Abschluss der Vorautorisierung kann auch erfolgen, wenn der Karteninhaber nicht anwesend ist. Für diese Transaktionsart können Magnet-, Chip- sowie auch kontaktlose Karten verwendet werden.

Zu dem Zeitpunkt, an dem Sie die Vorautorisierung abschließen möchten, müssen Sie die 6-stellige Autorisierungsnummer sowie den 9-stelligen Identifikator vom Beleg der Vorautorisierung bereithalten. Des Weiteren muss Ihnen auch der tatsächliche Betrag zum Abschluss der Vorautorisierung bekannt sein.

Zu dem Zeitpunkt, an dem die Autorisierungsanfrage automatisch generiert wurde, wird am Terminal die entsprechende Meldung als Antwort auf die Anforderung angezeigt. Mehr über die einzelnen Terminal-Meldungsarten erfahren Sie im aktuellen Handbuch für das betreffende POS-Terminal.

Ist Ihr Terminal nicht so eingestellt dass die Autorisierung automatisch erfolgen kann oder ist aufgrund eines Fehlers am POS-Terminal die automatische Autorisierung nicht möglich, wenden Sie sich bitte an den Helpdesk (die Kontaktdaten befinden sich auf S. 33).

4.2. KONTAKTLOSE KARTENZAHLUNGEN

Mit kontaktlosen NFC-Kartenzahlungen können Transaktionen ausgeführt werden, indem die Zahlungskarte nur an das POS-Terminal gehalten wird.

Bei Transaktionen bis zu einem Limit von EUR 25,- wird keine PIN-Eingabe verlangt. Dennoch wird aufgrund der Sicherheitseinstellungen der kartenausgebenden Bank bei manchen Transaktionen bis EUR 25,- die PIN-Eingabe durch den Karteninhaber verlangt- in so einem Fall muss die weitere Vorgehensweise wie bei Transaktionen mit Einlesen des Chips oder mit PIN-Eingabe erfolgen.

Zusätzlich zu diesem Limit können vom Kartenaussteller weitere Limits festgelegt werden, um die Transaktion abzusichern und den Karteninhaber zu schützen.

Die Kontaktlos-Technologie kann darüber hinaus auch in weiteren Geräten integriert werden, zum Beispiel in Smartwatches, Armbändern, Smartphones, Tablets sowie in elektronischen Schlüsselanhängern.

4.3. DYNAMIC CURRENCY CONVERSION (DCC)

Der DCC-Service ist für Transaktionen mit Visa und Mastercard verfügbar. Diese Transaktionsart ist für ausländische Karteninhaber bestimmt, welche Einkäufe in ihrer heimischen Währung bevorzugen.

Nach Abschluss der Transaktion erhält der Karteninhaber einen Beleg, auf welchem der Betrag der Verkaufstransaktion in der Währung vor Ort, der Wechselkurs sowie der finale Betrag angeführt ist, der in der Währung des Landes abgerechnet wird, das die Karte herausgegeben hat.

Ihr Terminal am Verkaufsort steht zur Nutzung des DCC-Services bereit und nimmt eine automatische Erkennung vor, ob die Karte für den DCC-Service geeignet ist. Zur Aktivierung des Services ist unsere schriftliche Zustimmung im Vorfeld erforderlich. Berücksichtigen Sie bitte, dass Ihr Kunde die Möglichkeit erhalten muss, eine eindeutige Wahl zu treffen, ob er die Transaktion in der heimischen oder in einer anderen vorgeschlagenen Währung vornehmen möchte.

Der Betrag wird auf dem Konto des Karteninhabers in seiner heimischen Währung belastet. Für den Karteninhaber fallen somit keine weiteren Kosten für Währungsumrechnungen bei seiner kartenausgebenden Bank an. Ihrem Bankkonto wird der Betrag in EUR gutgeschrieben, dadurch benötigen Sie keine Fremdwährungen auf Ihrem Konto.

Bei der Rückerstattung von Beträgen bei DCC-Transaktionen müssen Sie den Betrag in EUR eingeben sowie anschließend nach Aufforderung die DCC-Möglichkeit wählen. Überprüfen Sie am Beleg die ursprüngliche Transaktion, damit Sie sichergehen können, dass er als DCC bearbeitet wurde.

Aufgrund von Wechselkursdifferenzen kann der dem Karteninhaber erstattete finale Betrag vom ursprünglichen Transaktionsbetrag in dessen heimischer Währung abweichen. Über diese Tatsache müssen Sie den Karteninhaber – zusammen mit der Information, wie der Rückerstattungsprozess für den Betrag erfolgt – informieren.

DCC UND CHARGEBACKS

Wird eine DCC-Transaktion aufgrund einer Reklamation auf die Karte des Kunden zurückerstattet, wird der Transaktionsbetrag entweder durch das Unternehmen VISA oder durch das Unternehmen Mastercard von der heimischen Währung des Karteninhabers in Euro umgerechnet, bevor wir Ihr Konto damit belasten. Aufgrund der Wechselkursdifferenzen ist es wahrscheinlich, dass der finale Chargeback-Betrag vom ursprünglichen Euro-Transaktionsbetrag abweicht. Sie werden von uns über alle Details bei einem Chargeback-Prozess informiert.

DCC-VORAUUTORISIERUNG

Die Anwendung des DCC-Services kann auch bei Vorautorisierungen von Transaktionen erfolgen, wenn sich der Karteninhaber anmeldet bzw. registriert (zum Beispiel im Hotel oder in einer Mietwagenfirma).

Der beim DCC-Service aktuell verwendete Wechselkurs und der Betrag der DCC-Währung müssen dem Karteninhaber angezeigt werden.

Dem Karteninhaber ist klar und deutlich zu erklären, dass die Festlegung des finalen DCC-Wechselkurses sowie des DCC-Betrags in dessen heimischer Währung erst zu dem Zeitpunkt erfolgt, an dem die Verarbeitung dieser Transaktion im Rahmen der Anmeldung vom betreffenden Gerät aus (im Hotel, etc.) erfolgt. Es kann sein, dass sich Karteninhaber die Verwendung von DCC bei der Anmeldung überlegen. Sollte es dazu kommen, werden sie gebeten, die Rezeption (des betreffenden Hotels oder Mietwagenfirma) aufzusuchen. Nähere Informationen sind im Handbuch für DCC-Service zu finden.

4.4. TRINKGELD

Beim Trinkgeld handelt es sich um einen zusätzlichen Betrag, den der Karteninhaber der Transaktion hinzufügt, zum Beispiel wenn der Karteninhaber die Rechnung im Restaurant bezahlt.

4.5. CASHBACK

Beim Cashback-Service können Karteninhaber gleichzeitig mit dem Kauf von Waren oder Leistungen Bargeld erhalten.

Dieser Service ist nur bei den Karten VISA, VISA Electron, Mastercard und Maestro verfügbar, welche in Österreich ausgegeben wurden. Voraussetzung zur Nutzung des Services ist, dass Ware oder Leistungen im Mindestwert von EUR 1,- EURO gekauft werden. Die Bargeldabhebung ist bis zu einem Betrag von maximal EUR 200,- möglich.

4.6. INKREMENTELLE VORAUUTORISIERUNG

Diese Transaktion ist für das Tourismussegment bestimmt. Mit einer inkrementellen (schrittweise erfolgenden) Vorautorisierung kann der gewählte Betrag auf dem Konto des Karteninhabers reserviert, sowie mehrere Vorautorisierungen zu einer Transaktionskette zusammengefasst werden, wodurch ein Abschluss der Vorautorisierung für diese gesamte Kette erfolgen kann. Ebenso kann dadurch die Gültigkeit einer bestehenden Vorautorisierung verlängert werden. Falls das Terminal an eine Kasse angeschlossen ist, kann dies auch automatisch erfolgen.

Dieser Betrag wird dann auf dem Konto des Karteninhabers über den festgelegten Zeitraum geblockt (welcher entsprechend der kartenausgebenden Bank oder dem Land unterschiedlich sein kann). Wenn Sie den Abschluss der Vorautorisierung nicht innerhalb des entsprechenden Zeitraums durchführen, wird der Betrag für den Karteninhaber für weitere Zahlungen freigegeben.

Durch diese Funktion, kann ein Hotel sowohl eine Vorautorisierung als auch eine inkrementelle Vorautorisierung von einem beliebigen Terminal des Hotels aus vornehmen und abschließen.

Beispiel:

Ein Gast kommt ins Hotel und checkt für fünf Nächte ein. Während der Anmeldung des Gastes an der Rezeption nimmt der Rezeptionist eine Vorautorisierung in Höhe des Preises für fünf Nächte - zum Beispiel in Höhe von EUR 5.000,- vor. Dieser Betrag wird auf dem Konto des Gastes reserviert. Am vierten Tag seines Aufenthalts kommt der Gast an die Rezeption und teilt mit, dass er seinen Aufenthalt gerne um weitere zwei Nächte verlängern möchte. Der Rezeptionist nimmt also eine inkrementelle Vorautorisierung in Höhe des Übernachtungspreises für zwei Nächte - also in Höhe von EUR 2.000,- vor. Der betreffende Betrag wird auf dem Konto des Gastes reserviert. Beim Verlassen des Hotels teilt der Gast mit, dass er einen Minibar-Konsum in Höhe von EUR 300,- hatte. In diesem Fall nimmt der Rezeptionist wieder eine inkrementelle Vorautorisierung vor, diesmal in der Höhe von EUR 300,-. Bei der Abreise des Gastes kann der Rezeptionist am Terminal den Abschluss aller verbundenen Vorautorisierungen einfach mit einer Abschlusstransaktion für die Vorautorisierungen in der Höhe von EUR 7.300,- vornehmen.



Vorautorisierung Nr. 1
Betrag: EUR 500,-



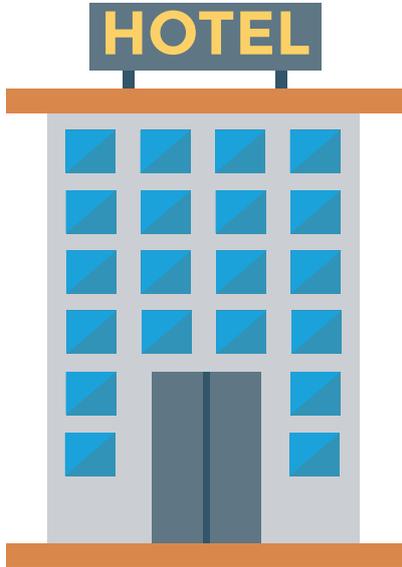
Vorautorisierung Nr. 2
Betrag: EUR 200,-



Vorautorisierung Nr. 3
Betrag: EUR 30,-



Abschluss Vorautorisierung
Betrag: EUR 730,-



Verkäuferbeleg	
GP merchant test Pragerstrasse 1 Wien	
16/05/2019	12:48:32
ABGABE: 045	ZETTLE:0007
TERMINAL ID:	18219022

Letzte 4 Z. PAN:	0011
INCREMENTAL PRE-AUTHOR.	
Betrag EUR:	5,00
TID:	18219022
Sequence Nr.:	001045006
Datum:	16.05.2019

5. ÜBERPRÜFUNG VON ZAHLUNGSKARTEN

Die Forderung zur Vornahme einer physischen bzw. visuellen Kartenüberprüfung ist davon abhängig, ob Sie die Karte während der Transaktion tatsächlich physisch in den Händen halten z. B. wenn der Karteninhaber aufgefordert wird, auf dem Beleg zu unterschreiben.

VORGEHENSWEISE BEI DER ZAHLUNGSKARTENÜBERPRÜFUNG

Durch den Kartentyp wird festgelegt, welche Überprüfung erforderlich ist. Die Beschreibung der nachfolgend angeführten Überprüfungen gilt für die meisten Karten welche von Banken oder anderen Finanzinstitutionen herausgegeben werden. Falls Sie diese Überprüfungen nicht vornehmen, kann gegen Sie gegebenenfalls ein Chargeback erfolgen.

1. CHIP

- Überprüfen Sie, ob der Chip Merkmale aufweist die darauf schließen lassen, dass versucht wurde ihn zu entfernen, auszuwechseln oder zu beschädigen.

2. KARTENUMMER

- Die Kartennummern beginnen für die nachfolgenden Kartenarten mit folgender Ziffer: 2 oder 5 für Mastercard, 6 für Maestro, 4 für VISA, 36 für Diners Club, 6011, 64 oder 65 für Discover, 62 für UnionPay (UnionPay-Karten mit Dual-Brand beginnen auch mit den Ziffern 3, 4, 5 oder 9), 35 für JCB.
- Die ersten vier Ziffern der Karte können sich am Anfang – oberhalb oder unterhalb der geprägten Kartennummer – wiederholen. Überprüfen Sie, ob diese mit den ersten vier Ziffern der geprägten Kartennummer übereinstimmen, sofern sie auf der Karte angegeben sind.
- Die letzten vier Ziffern der Kartennummer auf der Vorderseite müssen mit der Nummer auf der Rückseite auf dem Unterschriftsfeld (sofern auf der Karte angegeben), sowie auch mit den letzten vier Zahlen der Kartennummer, übereinstimmen, welche durch das Terminal auf dem Beleg gedruckt wurde.
- Überprüfen Sie bei geprägten Karten die Zahlen. Wenn der Bereich um die Zahlen beschädigt ist, kann dies darauf hindeuten, dass die ursprünglichen Zahlen entfernt und durch neue ersetzt wurden.
- Die Kartennummer auf der Vorderseite kann auch aufgedruckt statt geprägt sein. Aus diesem Grund kann sich diese bei Berührung eher glatt als hervorstehend anfühlen.

3. ANREDE UND NAME DES KARTENINHABERS

- Überprüfen Sie, dass zwischen dem Karteninhaber und den Angaben auf der Karte keine offensichtlichen Diskrepanzen bestehen, wie zum Beispiel, dass die Karte von einer Frau verwendet wird, auf welcher die Anrede „Hr.“ angegeben ist oder wenn ein Teenager eine Karte mit dem Titel "Doktor" verwendet.

4. GÜLTIG AB/ABGELAUFENE GÜLTIGKEIT/GÜLTIG BIS

- Die Karte ist sorgfältig in Bezug auf die Gültigkeit zu überprüfen. Akzeptieren Sie keine Karten welche vor dem „gültig ab“-Datum bzw. nach dem „gültig bis“-Datum/nach Ablauf der Gültigkeit zur Ausführung der Transaktion vorgelegt werden. Durch das Terminal erfolgen auf der Karte automatische bestimmte Überprüfungen. GP kann jedoch nicht dafür haftbar gemacht werden, wenn das Terminal eine Karte akzeptiert welche noch nicht gültig bzw. deren Gültigkeit abgelaufen ist.

5. HOLOGRAMM

- Überprüfen Sie, ob die Karte Merkmale einer Manipulation aufweist. Das Hologramm sollte sich beim Berühren glatt anfühlen und es sollte keine raue oder verkratzte Oberfläche haben. Die 3-D-Abbildung sollte sich beim Neigen bewegen. Bei gefälschten Karten ist die Hologramm-Nachbildung häufig mangelhaft.
- Das Hologramm kann sich auf der Vorder- oder Rückseite der Karte befinden, außer bei Karten mit Hologrammstreifen (holografischer Magnetstreifen) wo es anstelle des klassischen Magnetstreifens verwendet wird.
- Zu den häufigsten Hologrammformen gehören:
 - Mastercard – Abbildung der Erdkugel
 - Visa – fliegende Taube oder mehrere sich im Flug befindliche Tauben
 - Visa Electron – nicht auf allen Karten befindet sich ein Hologramm. Wenn sich ein Hologramm auf der Karte befindet, sieht es wie eine fliegende Taube aus.
 - UnionPay – 3-D-Abbildung vom Himmelstempel
 - Diners – geteilter Kreis
 - JCB – Morgendämmerung

6. UNTERSCHRIFTSFELD

- Zur Erinnerung – wenn die Überprüfung der Karte über die PIN erfolgt, muss die Unterschrift nicht überprüft werden.
- Die Unterschrift sollte deutlich geschrieben sein und sollte sich bei Berührung glatt anfassen. Es sollten keine offensichtlichen Merkmale einer Löschung oder Überschreibung vorhanden sein.
- Wird Ihnen eine nicht unterschriebene Karte vorgelegt, bitten Sie den Karteninhaber, seine Identität nachzuweisen sowie in Ihrer Gegenwart auf der Karte zu unterschreiben. Notieren Sie die Art und Nummer des Legitimations-/Identifikationsdokuments auf dem Verkaufsbeleg und holen Sie eine Genehmigung für die Transaktion unabhängig von der Höhe des Transaktionslimits ein.
- Überprüfen Sie, ob die Unterschrift mit dem auf der Vorderseite der Karte angegebenen Namen übereinstimmt.
- Überprüfen Sie, dass das Unterschriftsfeld keine Merkmale von Manipulation, Überkleben, etc. aufweist.
- Überprüfen Sie, ob die Unterschrift auf der Karte mit der Unterschrift auf dem ausgedruckten Beleg übereinstimmt.

7. PRÜFNUMMER (CVV2, CVC2)

- Drei- oder vierstellige Überprüfungsnummer. Bei Mastercard, Visa und Maestro handelt es sich bei der CVV2- bzw. CVC2-Nummer um die letzten drei aufgedruckten Zahlen auf der Rückseite der Karte, welche sich hinter den vier letzten Zahlen der Kartennummer befinden, sofern diese dort angegeben sind. Die CVV2- bzw. CVC2-Nummer kann sich auch auf dem Unterschriftsfeld oder im weißen Feld rechts vom Unterschriftsfeld befinden. Bei „American Express“-Karten besteht diese Nummer aus vier Zahlen und ist auf der Vorderseite der Karte aufgedruckt.

8. MAGNETSTREIFEN

- Vergewissern Sie sich, dass sich auf der Rückseite der Karte ein Magnetstreifen befindet. Fühlt sich der Magnetstreifen bei Berührung ungewöhnlich rau oder verkratzt an, sollten Sie Verdacht schöpfen, dass die Karte gefälscht wurde.
- Manche Karten verfügen anstelle des klassischen Magnetstreifens über einen Holomag-Streifen (holografischer Magnetstreifen). Wenn die Karte über einen Holomag-Streifen verfügt, muss sich dieser immer auf der Rückseite der Karte befinden und auf der Karte darf kein weiteres Hologramm vorhanden sein.

9. ULTRAVIOLETTE ELEMENTE

- Wenn Sie ein UV-Geldscheinprüfgerät besitzen, können Sie das auf der Vorderseite der Karte befindliche ultraviolette Element überprüfen.

10. FOTO

- Auf einigen Karten befindet sich ein Foto des Karteninhabers – konkret rechts auf der Vorderseite der Karte. Wenn Ihnen eine Karte vorgelegt wird, auf welcher sich dieses Element befindet, überprüfen Sie, dass das Foto der Person entspricht, welche die Karte zur Ausführung der Transaktion vorlegt. Falls das Foto und der Inhaber nicht identisch sind, sollten Sie Verdacht schöpfen.

11. LOGOS DER KARTENUNTERNEHMEN

- Die Logos auf den Karten befinden sich in der Regel auf der Vorderseite der Karte, können jedoch auch auf der Rückseite vorhanden sein. Sie sollten klar und in markanten Farben aufgedruckt sein – ein Logo, das sich nicht markant vom Umfeld abhebt bzw. dass in niedriger Qualität aufgedruckt ist, kann ein Anzeichen dafür sein, dass die Karte gefälscht wurde.

Wenn Sie irgendeinen Verdacht bezüglich der Karte oder des Karteninhabers haben, wenden Sie sich telefonisch an unser Helpdesk und melden „Code 10“ (siehe Seite 33).

BEISPIELE FÜR KARTENLOGOS



Mastercard



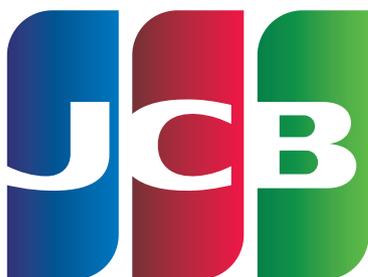
Discover



Visa



UnionPay



JCB



Diners

BEISPIELE FÜR KARTEN UND ELEMENTE AUF DEN KARTEN

Legende zu den Kartenabbildungen:

1. Chip
2. Kartenummer
3. Titel und Name des Karteninhabers
4. „Gültig bis“-Datum: Datum, an dem die Gültigkeit abläuft („Valid Thru“ gibt die letzten drei Gültigkeitsmonate an)
5. Kontaktlos-Logo (sofern auf der Karte vorhanden)
6. Kartenlogo
7. Hologramm
8. Unterschriftsfeld
9. Kartensicherheitscode (CSC)
10. Magnetstreifen/Holomag-Streifen
11. Sonstige Merkmale zur Kartenakzeptanz

Mastercard

Vorderseite



Rückseite

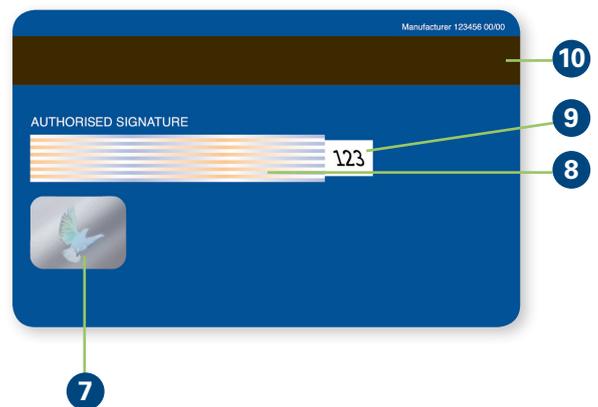


Visa

Vorderseite



Rückseite



Diners Club International

Vorderseite



Rückseite



Discover

Vorderseite



Rückseite



UnionPay

Vorderseite



Rückseite



JCB (Japan Credit Bureau)

Vorderseite



Rückseite

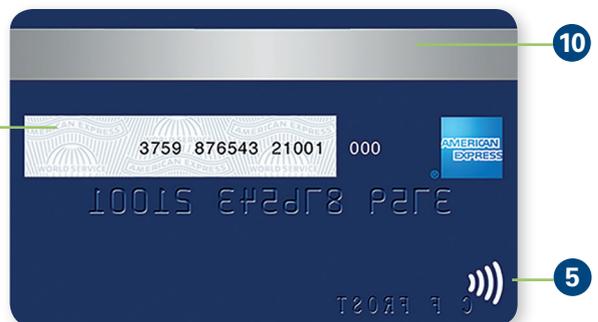


American Express

Vorderseite



Rückseite



6. AKZEPTANZ VON ZAHLUNGSKARTEN IN SPEZIFISCHEN BEREICHEN

Dieser Bereich gilt für Händler, welche aufgrund einer Sondergenehmigung von GP die Möglichkeit zur Vornahme von spezifischen Transaktionsarten (z. B. Vorautorisierung) haben.

6.1. TRANSAKTIONEN IN HOTELS UND MIETWAGENFIRMEN

Die Zahlungskartenbetreiber haben für diese Transaktionen spezifische Regeln aufgestellt. Dieser Bereich gibt Auskunft zu den Schritten und der Vorgehensweise, welche Sie bei der Ausführung dieser Transaktionen vornehmen müssen. Ihr Terminal muss für Transaktionen mit Vorautorisierungen konfiguriert sein. Wenn Sie diese Möglichkeit aktivieren möchten, wenden Sie sich bitte an uns (die Kontaktdaten finden Sie auf S. 33). Detaillierte Beschreibungen zur Durchführung von Vorautorisierungen sind im Benutzerhandbuch für Ihr Zahlungsterminal beschrieben.

In diesem Bereich werden Gäste und Personen, die einen Mietwagen mieten, als Karteninhaber bezeichnet.

GENERELLE SCHRITTE UND ABLÄUFE, WELCHE BEI DER AKZEPTANZ VON KARTEN EINZUHALTEN SIND

- Alle Belege welche einem ausländischen Karteninhaber zur Verfügung gestellt werden, müssen mindestens zweisprachig sein (Landessprache/Englisch/Heimatsprache des Karteninhabers).
- Der Händler muss bei einer Reservierung oder Stornierung (einschließlich Reservierungen oder Stornierungen über das Internet) die Akzeptanz des Karteninhabers bezüglich der Reservierungs-/Stornobedingungen einholen.
- Der Händler ist verpflichtet, den kompletten Schriftverkehr mit dem Karteninhaber zum gegebenenfalls später benötigten Nachweis gegenüber der Bank und zur Klärung von strittigen Transaktionen (Reklamationen), aufzubewahren.

RESERVIERUNGEN

Bei einer Reservierung informieren Sie den Karteninhaber über folgende Punkte:

- den Übernachtungspreis/Mietwagenpreis, einschließlich der Mitteilung der Reservierungsnummer
- die Reservierungsdetails
- die Geschäftsbedingungen
- die Stornobedingungen sowie die Kontaktdaten/Ansprechpartner bei Stornierung der Reservierung.

Wenn Sie Reservierungen für Hotels und Mietwagenfirmen annehmen, vergewissern Sie sich, dass Sie folgende Unterlagen und Daten erhalten haben:

- den Namen des Karteninhabers
- die Adresse und Telefonnummer
- die Nummer seiner Zahlungskarte, das „gültig ab“-Datum der Karte (sofern vorhanden) und das Datum, wann die Gültigkeit endet
- die Einwilligung zur Verwendung der Zahlungskarte zur Bezahlung
- die Akzeptanz der Geschäftsbedingungen
- die Akzeptanz des Gesamtpreises, welcher am Tag der Reservierungserstellung berechnet wird

Wenn Sie Zimmerreservierungen über Mastercard und Visa annehmen, müssen Sie garantieren, dass Sie – sofern die reservierte Unterkunftsmöglichkeit nicht verfügbar sein sollte – eine alternative Unterkunftsmöglichkeit mit gleichem oder besserem Standard zur Verfügung stellen, für welche Sie keine zusätzlichen Kosten verlangen.

GARANTIERTE RESERVIERUNG

Bei einer garantierten Reservierung handelt es sich um eine Reservierung ohne sofortigen Einzug des Betrags seitens des Händlers. Der Händler nimmt für den Karteninhaber eine Reservierung vor und hält die Unterkunftsmöglichkeit bis zum geplanten Anreisetag frei. Dem Karteninhaber ist eine 24-stündige Frist ab der Zustellung der Reservierung zur kostenlosen Stornierung der Reservierung zu gewähren. Die Transaktion erfolgt erst in Gegenwart des Karteninhabers.

ÜBERNACHTUNGSRESERVIERUNG MIT ADVANCE DEPOSIT

Gewährt das Hotel eine Reservierung mit „Advance Deposit“-Möglichkeit (nicht rückzahlbare Anzahlung), ist diese Möglichkeit in den Reservierungsbedingungen anzuführen, welche der Karteninhaber akzeptieren muss.

Der Händler ist verpflichtet, auf dem Beleg „Advance Deposit“ statt der Unterschrift des Karteninhabers anzugeben.

ANMELDUNG (CHECK-IN)

- Bitten Sie den Karteninhaber bei der Ankunft auf dem Anmeldeformular zu unterschreiben. Auf diesem ist angeführt, dass der Karteninhaber Sie ermächtigt, Geld von seiner Karte abzubuchen. Überprüfen Sie, ob die Unterschrift mit der Unterschrift auf der Karte übereinstimmt.
- Nehmen Sie eine Vorautorisierung vor - eventuell unter Einsatz der „Inkrementellen Vorautorisierung“ (mehr dazu finden Sie auf S.13).
- Informieren Sie den Karteninhaber über den Betrag der Vorautorisierung und teilen Sie ihm mit, was in diesem Betrag enthalten ist (z. B. Aufenthalts-/Mietdauer, Zimmerpreis/Mietwagenpreis, betreffende Steuern, Servicekosten und Kilometerkosten).

ABMELDUNG (CHECK-OUT)

- Wählen Sie über die Tastatur am Terminal die Schritte "Menü - Transaktionen - Vorautorisierung abschließen" aus, ziehen Sie die Karte durch bzw. stecken Sie diese ein, geben Sie den ursprünglichen Betrag der Vorautorisierung sowie die Genehmigungsnummer und das Identifizierungszeichen vom Beleg der Vorautorisierung ein, und gehen Sie entsprechend den Anweisungen auf Ihrem Zahlungsterminal vor.
- Es kann sein, dass Sie eine nachträgliche Genehmigung vornehmen müssen, wenn der finale Betrag:
 - über Ihrem Genehmigungslimit liegt,
 - über der Summe der zuvor im Rahmen der Vorautorisierung genehmigten Beträge liegt (bei Visa-Karten ist eine Toleranz von plus 15 % gegeben, bei Mastercard nicht). Die Autorisierung wird nur für die Differenz zwischen dem im Rahmen der Vorautorisierung genehmigten Betrag bzw. Beträgen und dem finalen Betrag erteilt.
- Wo dies möglich ist, sollten Sie darauf achten, dass die finale Rechnung in Gegenwart des Karteninhabers beglichen wird und dass die Transaktionsausführung mit PIN-Überprüfung erfolgt.
- Vergessen Sie nicht, alle nicht verwendeten Autorisierungsnummern zu stornieren, wenn Sie den Betrag von der Vorautorisierung um mehr als 15 % bei Transaktionen mit Visa überschritten haben.

RESERVIERUNGSSTORNIERUNGEN/FRISTEN UND TERMINE FÜR RESERVIERUNGSSTORNIERUNGEN

Der Karteninhaber ist bereits bei der Reservierungserstellung über die Reservierungs-Stornierungsbedingungen zu informieren. Allgemein müssen folgende Regeln gelten:

- Garantierte Reservierungen werden bis zum nächsten Tag nach dem geplanten Anreisetag aufrecht gehalten. Die Stornierungsfrist für die Reservierung ist 18:00 Uhr (Ortszeit) am geplanten Anreisetag.
- Wenn Sie eine frühere Frist als 18:00 Uhr (Ortszeit) am geplanten Anreisetag festlegen, teilen Sie diese Tatsache dem Karteninhaber mit.

- Tag und Uhrzeit der Frist sowie die Regeln zur Reservierungsstornierung sollten dem Karteninhaber schriftlich mitgeteilt werden.
- Der Händler darf keine Bedingung festlegen, bei denen eine kostenlose Stornierung nur bei Einhaltung einer Frist von mehr als 72 Stunden vor der Anreise des Gastes möglich ist. Wird eine Frist von mehr als 72 Stunden vor Anreise festgelegt, gilt eine Reklamation seitens des Karteninhabers als berechtigt. Wird die Reservierung nicht in Anspruch genommen oder nicht fristgerecht storniert, wird dem Karteninhaber der Preis für die erste Nacht (einschließlich MwSt.) berechnet- die sogenannte No-Show-Rechnung.
- Der Händler muss dem Karteninhaber die Nummer der stornierten Reservierung mitteilen.

NO-SHOW

Transaktionen vom Typ No-show dienen zur nachträglichen Berechnung/Belastung von Leistungen. Ein Beispiel: der Karteninhaber hat eine Leistung bestellt (Zimmerreservierung/Mietwagenreservierung) und diese nicht bzw. nicht rechtzeitig storniert. Wenn dieser Fall eintritt, ist der Händler berechtigt, Schadenersatz für eine Nacht/einen Tag entsprechend den Richtlinien des Zahlungskartensystems zu berechnen.

Bedingungen:

- Der Händler muss den Karteninhaber schriftlich über die Belastung informieren.
- Der Händler muss über die Kartendaten verfügen (Kartenummer, Gültigkeit der Karte).
- Der Händler muss über eine schriftliche Waren- oder Leistungsbestellung verfügen.
- Das Recht des Händlers zur Nachberechnung/Nachbelastung muss in dessen Bedingungen zur Leistungserbringung schriftlich festgelegt sein und der Karteninhaber muss der Nachberechnung zustimmen.
- Über die Funktion „Verkauf“ nimmt der Händler die Transaktion am Zahlungsterminal vor und auf der für die Unterschrift vorgesehene Stelle trägt er leserlich in Blockschrift „No Show“ (bzw. „N. S.“) ein.

WEITERE KOSTEN

Zur Berechnung von „weiteren Kosten“, wie z. B. Verlust, Diebstahl oder Beschädigung der Hoteleinrichtung benötigen Sie immer die Zustimmung des Karteninhabers. Diese nachträglichen Kosten sind nicht garantiert und können Ihrem Konto wieder belastet werden, wenn der Karteninhaber eine derartige Transaktion erfolgreich reklamiert.

Mietwagenfirmen: Nur bei VISA ist es zulässig, den Kunden mit Rück- oder abgeänderten Beträgen infolge der Beschädigung des Mietwagens, für Kraftstoff, Versicherung, Parken, Strafen, Mietkosten und Steuern zu belasten. Sie müssen jedoch die nachfolgend genannten Unterlagen **komplett** vorlegen können:

- eine Kopie des Mietvertrags,
- eine Schätzung der Schadenshöhe von der Organisation, welche zur Vornahme der Reparatur in dem Land berechtigt ist, in dem die Mietwagenfirma ihren Sitz hat,
- ein Unfallprotokoll von der Polizei, sofern zutreffend und verfügbar,
- Dokumentation der Einwilligung des Karteninhabers, dass er den Schaden mit seiner Visa-Karte bezahlt,
- jede andere verfügbare relevante Dokumentation, durch welche die Haftung des Karteninhabers für den entstandenen Schaden belegt wird,
- eine Kopie der Fahrzeugversicherung, wenn Sie vom Karteninhaber verlangen die Versicherung zu bezahlen. In diesem Fall wird die Höhe der Fahrzeugversicherung von der Höhe des Schadens abgezogen. Statt Ihrer Mietwagen-Versicherungspolize können Sie eine Kopie des Mietwagenvertrags vorlegen, durch den die Zustimmung des Karteninhabers bestätigt wird, den entsprechenden Anteil zur Deckung des Versicherungsfalls zu tragen. In diesem Fall muss der Karteninhaber im Vorfeld auf dem Teil des Vertrags unterschreiben bzw. seine Initialen hinzugefügt haben, auf dem die entsprechenden Informationen zur Versicherung angeführt sind.

Bei Mastercard und Maestro ist es nicht zulässig, dass die Mietwagenfirmen die Kunden mit Rück- oder abgeänderten Beträgen belasten. Alle Kosten für Verlust oder Diebstahl sind gesondert zu bearbeiten und Sie benötigen hierfür die Zustimmung des Karteninhabers.

In Zusammenarbeit mit



globalpayments.at

SERVICE. DRIVEN. COMMERCE

6.2. WECHSELSTUBEN/CASINOS

Um Kartenzahlungen für Wechselstuben- oder Casinoleistungen akzeptieren zu können, benötigen Sie unsere schriftliche Zustimmung im Vorfeld.

Für dieses Segment wurde die spezifische Transaktionsart "Quasi Cash" festgelegt, welchen Sie vor der Zahlung im Menü am POS-Terminal auswählen.

In Wechselstuben und Casinos sind keine Rückerstattungen möglich.

Überprüfen Sie die Zahlungskarte (siehe Seite15) und identifizieren Sie den Karteninhaber und notieren Sie die Daten vom vorgelegten Identifikations-/Legitimationsdokument. Dieser Businessstyp ist mit einem erhöhten Chargeback-Risiko verbunden.

7. CHARGEBACK

Als Chargeback gilt eine Transaktion, bei welcher die kartenausgebende Bank dem Händler den gezahlten Transaktionsbetrag komplett oder teilweise wieder belastet, in der Regel aufgrund einer Reklamation seitens des Karteninhabers.

Jedes Chargeback Verfahren verfügt über spezifische Regeln, welche von den jeweiligen Kartenunternehmen definiert werden und von GP bei Reklamationsverfahren einzuhalten sind.

7.1. DIE HÄUFIGSTEN CHARGEBACK-ARTEN:

- Forderung bezüglich des Nachweises der Dokumentation: der befugte Karteninhaber ist sich nicht sicher, ob er diese Transaktion getätigt hat
- unberechtigte Transaktion: der befugte Karteninhaber hat für eine derartige Transaktion nicht seine Zustimmung erteilt und war nicht an dieser beteiligt,
- Fehler bei der Verarbeitung: zum Beispiel doppelt verarbeitete Transaktionen
- stornierte/zurückgegebene Ware oder Leistungen: der Karteninhaber hat die Bestellung storniert oder die Ware zurückgegeben und das Geld wurde ihm nicht zurückerstattet, die Rückerstattung des Geldes wurde nicht bearbeitet oder das zurückerstattete Geld wurde nicht der gleichen Karte gutgeschrieben, der es belastet wurde
- nicht erhaltene Waren/Leistungen: zum Beispiel bei verspäteter Waren- oder Leistungslieferung bzw. bei Lieferung der falschen Ware

Wir werden Sie über ein Chargeback immer per Brief oder E-Mail informieren bevor der betreffende Betrag Ihrem Konto belastet wird. Sollten wir von Ihnen weitere Informationen/Dokumentation verlangen, erhalten Sie von uns eine schriftliche Aufforderung dazu. Es ist sehr wichtig, dass Sie die geforderten Informationen klar und deutlich innerhalb der von uns festgelegten Frist zur ordnungsgemäßen Klärung der Streitigkeit liefern. Der strittige Betrag wird Ihnen erst nach Abschluss des kompletten Chargeback-Verfahrens berechnet.

Forderungen zur Lieferung dieser Dokumentation können innerhalb eines Zeitraums von 540 Tagen nach der Transaktion zum Zeitpunkt der Belastung des Kontos des Karteninhabers bzw. des Empfangs der betreffenden Leistung gestellt werden. Allerdings können Dokumente in manchen Fällen, zum Beispiel in Betrugsfällen, bis zu einem Zeitraum von zwei Jahren nach Transaktionsdatum angefordert werden.

7.2. WIE SICH DAS CHARGEBACK-RISIKO REDUZIEREN LÄSST

Transaktionen, bei denen die Karte vorhanden ist (Card Present):

- Bei Chipkarten muss die Transaktion durch Einlesen des Chips bzw. durch Eingabe der PIN erfolgen (sofern hierzu vom Terminal die entsprechende Anweisung erteilt wird).
- Wird vom Terminal die Anweisung zur Unterschrift des Karteninhabers erteilt, überprüfen Sie die Unterschrift mit der Unterschrift auf der Zahlungskarte.

Transaktionen, bei denen die Karte nicht vorhanden ist (Card Not Present), besteht für Sie ein erhöhtes Chargeback-Risiko. Weder der Karteninhaber ist bei der Transaktion persönlich anwesend, noch liegt die Karte physisch vor:

- Wenn der Kunde die Ware im Geschäft abholen möchte, führen Sie die Transaktion bei Abholung der Ware als Card Present Transaktion am Terminal aus.
- Versenden Sie die Ware wenn möglich mit einer Zustellungsart bei der die Ware persönlich entgegengenommen werden muss z.B. per Einschreiben oder durch ein vertrauenswürdigen und sicheres Transportunternehmen. Bestehen Sie darauf, dass ein Zustellungsbeleg ausgestellt wird, der anschließend vom Karteninhaber unterschrieben werden muss. Bitten Sie den Kurier die Sendung keines Falls zuzustellen, wenn niemand anzutreffen ist und somit die Ware nicht persönlich entgegen genommen werden kann. Denken Sie immer daran, dass der Zahlungsbeleg als solcher keinen ausreichenden Beweis darstellt, der Sie vor einem Chargeback schützt.

In Zusammenarbeit mit



globalpayments.at

SERVICE. DRIVEN. COMMERCE

- Seien Sie besonders aufmerksam bei Transaktionen, bei denen die Rechnungsadresse von der gewünschten Lieferadresse abweicht. Vermeiden Sie Zustellungen an Adressen wie zum Beispiel Hotels, Internetcafés, sowie Adressen von anderen Personen, an denen der Empfänger vorgibt sich aufzuhalten.
- Seien Sie auch besonders aufmerksam, wenn die Bestellung von einem E-Mail-Konto getätigt wurde, bei dem der Kundename in keiner Form in der E-Mail-Adresse enthalten ist.
- Seien Sie misstrauisch bei Transaktionen, welche für Ihren Unternehmenstyp in Betragshöhe und Menge ungewöhnlich hoch sind bzw. bei denen der Verkauf „äußerst einfach“ scheint. Unseren Erfahrungen zufolge ist gerade bei diesen Transaktionen die Wahrscheinlichkeit hoch, dass es sich um betrügerische Transaktionen handelt.
- Wenn Sie Geld zurückerstatten, dann immer auf die gleiche Zahlungskarte, mit welcher die ursprüngliche Transaktion erfolgt ist.
- Führen Sie eine Datenbank mit den reklamierten Transaktionen (Chargebacks), damit Sie bei Betrugstransaktionen ein Muster einfach erkennen können. Wenn der Verkauf „zu gut, um wahr zu sein“ scheint, ist er wahrscheinlich nicht echt. Haben Sie keine Hemmungen, den Karteninhaber zu kontaktieren, um ihm zusätzliche Fragen zu stellen oder eine nachträgliche Identifikation zu verlangen.
- Die meisten Chargebacks sind die Folge von Betrugstransaktionen. Wenn Sie eine Transaktion abschließen, die sich als Betrugstransaktion offenbart, tun Sie dies auf eigenes Risiko. Wenn die Transaktion abgeschlossen, aber die Ware noch nicht versandt wurde, haben Sie immer noch die Möglichkeit, dem Kunden das Geld zurückzuerstatten.
- Es ist Ihre Pflicht dafür zu sorgen, dass die vom Karteninhaber bestellte Ware genau in der Form geliefert bzw. zur Verfügung gestellt wird, wie in Ihrem Katalog oder im Rahmen Ihrer Werbung beschrieben. Falls Sie nicht die exakte Farbe, Größe, Qualität und Quantität liefern können, müssen Sie den Karteninhaber auf diese Änderung hinweisen und ihn um Zustimmung zu den Änderungen bitten.
- Nehmen Sie keine Transaktionen mit Karten vor, deren Gültigkeit abgelaufen ist.
- Belasten Sie den Karteninhaber nicht mit höheren Beträgen als bezogen bzw. über die er informiert wurde.
- Berechnen Sie dem Karteninhaber die Transaktion in der Währung, der er zugestimmt hat.
- Berechnen Sie dem Karteninhaber keine nachträglichen Kosten, wenn Sie im Vorfeld nicht die Zustimmung des Karteninhabers für diese Transaktion erhalten haben.
- Wenn Sie bei einer Warenbestellung eine Anzahlung erhalten haben und der Karteninhaber anschließend den Restbetrag zahlt, ist es wichtig, dass beide Transaktionen getrennt voneinander bearbeitet werden und die zweite Transaktion nicht bearbeitet wird, bevor die Ware versandt wurde.
- Falls Sie beschließen, die 3D Secure-Lösung nicht zu implementieren, tragen Sie die volle Verantwortung für Transaktionen, die nicht über die 3D Secure-Lösung verifiziert wurden.

8.1. EMPFOHLENE VORGEHENSWEISEN ZUR BETRUGSPRÄVENTION:

- Unterteilen Sie eine Transaktion nie in mehrere Teilbeträge.
- Eine Autorisierung stellt keine Zahlungsgarantie dar, eine Autorisierung ist nur eine Bestätigung darüber, dass die erforderlichen finanziellen Mittel auf der Karte vorhanden sind und dass die Karte aktuell nicht als verloren oder gestohlen gemeldet wurde. Dem rechtmäßigen Besitzer ist jedoch womöglich nicht bewusst, dass jemand anderer seine Daten und seine Zahlungskarte benutzt, somit kann sich die Transaktion trotzdem noch als Betrugsfall herausstellen.
- Wenn Sie feststellen, dass eine Transaktion mehrfach abgelehnt wird, sollten Sie aufmerksam sein. Wenn bei Ausführung der Transaktion auf Ihrem Display eine Meldung wie „AC ANRUFEN“ oder „GENEHMIGUNGSDIENST ANRUFEN“ erscheint, sollten Sie unseren Helpdesk kontaktieren (die Kontaktdaten sind auf S. 33 angeführt). Es werden dort weitere Überprüfungen erfolgen um festzustellen, ob Ihr Kunde der tatsächliche Karteninhaber ist.
- **Akzeptieren Sie keine Karten, welche Merkmale von Veränderungen/Manipulation aufweisen.**
- Seien Sie wachsam, wenn vermeintlich zufällige und unlogische Käufe, z.B. große Mengen des gleichen Artikels, getätigt werden.
- Seien Sie misstrauisch, wenn ein Kunde eine Waren- und/oder Leistungsbestellung tätigt und Sie gleichzeitig bittet, eine Zahlung für zusätzliche Leistungen zu akzeptieren, die ein anderes Unternehmen erbringen soll.
- Erstaten Sie Beträge nur auf die Zahlungskarte zurück, welche bei der ursprünglichen Transaktion verwendet wurde. Lehnen Sie eine Rückerstattung von Beträgen auf andere Weise, wie z. B. über Western Union, ab.
- Wir empfehlen für alle E-Commerce-Transaktionen die 3D-Secure-Lösung zu implementieren um den Betrug durch Missbrauch von Kartendaten zu verhindern. Mehr Informationen zum Schutz von Kartendaten finden Sie im *Kapitel PCI-DSS S. 28*.

9. PCI DSS – SCHUTZ VON KARTENDATEN

Das Regelwerk „Payment Card Industry Data Security Standard (PCI DSS)“ ist ein internationaler Standard mit verbindlichen Regeln zum sicheren Umgang mit Zahlungskarten- und Transaktionsdaten, welche von den Kartenorganisationen aufgestellt wurden um die Sicherheit dieser Daten zu erhöhen.

Bei PCI DSS handelt es sich um eine Aufstellung von 12 komplexen Anforderungen die dem Schutz von Kundendaten bei Zahlungskarten dienen.

Das Ziel des Regelwerks besteht darin, Organisationen beim Schutz der Kundendaten von Zahlungskarten zu unterstützen.

Für jeden Händler, egal wie groß sein Unternehmen ist, besteht das Risiko des Datenschwunds. Hierbei kann es zu Strafen seitens der Kartenorganisation kommen, da die Kundendaten nicht ausreichend effektiv sowie nicht entsprechend dem „PCI DSS“ Regelwerk gesichert waren. Diese Strafen beginnen ab einem Betrag von EUR 5.000,- können aber, abhängig von den konkreten Umständen, wesentlich höher sein.

9.1. EMPFOHLENE VORGEHENSWEISEN

- Stellen Sie die Informationen der Zahlungskarten niemand anderem außer GP zur Verfügung.
- Beschränken Sie den Zugang Ihrer Mitarbeiter auf Zahlungskartendaten.
- Speichern Sie unter keinen Umständen die vollständigen auf dem Magnetstreifen oder Chip gespeicherten Daten (auch „Track 2“-Daten genannt), wie zum Beispiel den Überprüfungsbetrag der Karte (Card Verification Value, CVV, Batch Code), den Überprüfungscode der Karte (CVC), sowie den Verifikationswert – die PIN (Pin Verification Value, PVV).
- Bewahren Sie alle Unterlagen, welche Karteninformationen enthalten (z. B. Transaktionsbelege) in einem verschlossenen, sicheren Raum und nur über den erforderlichen Zeitraum auf.
- Sorgen Sie dafür, dass Dritte, welche für Sie sensible Daten verarbeiten oder aufbewahren bzw. Dritte, mit denen Sie über diese Leistungen verhandeln, Ihnen bestätigen, dass sie die PCI DSS-Standards erfüllen.

Die gesamte von uns gelieferte Ausrüstung zur Akzeptanz von Zahlungskarten erfüllt die aktuell gültige Version der PCI DCC-Standards. Dadurch ist es für Ihr Unternehmen einfacher, die PCI DSS-Standards zu erfüllen.

Für weitere Informationen zu den PCI DSS-Standards besuchen Sie die Webseite www.pcisecuritystandards.org. Auf dieser Seite finden Sie die neueste Version der PCI DSS-Standards sowie Empfehlungen dazu, wie diese Standards einzuhalten sind.

9.2. WAS GESCHEINT, WENN SIE DIE RICHTLINIEN DER PCI DSS-STANDARDS NICHT ERFÜLLEN?

Wenn Sie die Erfüllung dieses Standards nicht nachweisen können, müssen Sie mit Kosten für die Nichteinhaltung der Sicherheitsanforderungen rechnen.

Für weitere Informationen bezüglich PCI DSS kontaktieren Sie uns einfach unter pci@globalpayments.at. Wir helfen Ihnen gerne bei der Erfüllung der PCI DSS-Standards.

10. WEITERE WICHTIGE INFORMATIONEN

10.1. VERWENDUNG EINES EIGENEN ZAHLUNGSTERMINALS

Wir bieten Transaktions-Processing auch für Unternehmen an, welche Zahlungskarten über eigene Geräte oder Kartenakzeptanz-Systeme akzeptieren (einschließlich aller Teile dieses Geräts, welches von Dritten zur Verfügung gestellt werden).

Wir können Sie bei den beiden wichtigsten Kartenakzeptanz-Systemen unterstützen:

- Elektronische Handkassen (EPOS) mit welchen Karten akzeptiert werden können
- Elektronische Terminals zur Akzeptanz von Zahlungskarten die unabhängig von Ihrem Kassensystem funktionieren

Für beide Systeme stellen wir Ihnen gerne unsere detaillierte Systemspezifikation samt Systemanforderungen und Schnittstellen zur Verfügung.

Alle Geräte müssen vor Implementierung von uns getestet und genehmigt werden. Wenn Sie ein eigenes Gerät verwenden, müssen Sie sich an alle Schritte und Abläufe halten, welche in dieser Anleitung angeführt sind. Werden von uns alternative und/oder zusätzliche Schritte und Abläufe vereinbart, werden diese gesondert dokumentiert.

Sie müssen uns über alle geplanten Änderungen bezüglich der Geräte informieren, einschließlich deren Einstellungen und Übertragungsverbindungen. Wenn Sie dies nicht tun, kann es dazu führen, dass wir Transaktionen nicht verarbeiten können und es somit zu einer Verzögerung bezüglich der Gutschrift dieser Transaktionen auf Ihrem Bankkonto kommt.

Wenn Sie Dritte als Betreiber einsetzen, müssen Sie uns über jede Änderung dieses Betreibers informieren. Sie müssen des Weiteren gewährleisten, dass der Betreiber alle „Payment Card Industry Data Security Standards“ (Regelwerk PCI DSS, siehe Seite 28) einhält.

Sie müssen gewährleisten, dass Ihr Gerät zur Akzeptanz von Zahlungskarten die für die betreffende Branche üblichen Sicherheitsstandards erfüllt. Sie müssen alle Upgrades hierfür vornehmen, welche wir oder der Lieferant Ihres Geräts bei Bedarf verlangen und dafür ggfs. anfallende Kosten tragen. Dies umfasst auch alle Änderungen die vorgenommen werden müssen, um Änderungen in den Regeln des Betreibers zu entsprechen. Wird auf diese Änderungen nicht reagiert, kann es zur Diskrepanz mit den oben erwähnten Richtlinien führen und Kosten und Strafen, sowie ein erhöhtes Chargeback-Risiko zur Folge haben.

10.2. ANSCHLUSS DES TERMINALS AN EIN KASSENSYSTEM (ECR)

Die von uns angebotenen Terminals können an ein Kassensystem angeschlossen werden. Das Kommunikationsprotokoll zwischen beiden Geräten ermöglicht die Fernbedienung der Terminalfunktion sowie die Steuerung des Zahlungsprozesses direkt vom angeschlossenen Gerät. Die Verbindung zum Terminal ist über die RS232-, USB- oder TCP / IP-Schnittstelle möglich. Während des gesamten Zeitraums, bei welchem das Kommunikationsprotokoll implementiert wird, ist unsererseits komplette technische Unterstützung gewährleistet, einschließlich der Möglichkeit eines Leih-Terminals.

Eine Übersicht zu allen integrierten Kassensystemen steht auf der Produkt-Webseite zur Verfügung <https://www.mufterminal.cz/propojeni-terminalu-s-pokladnou?lang=en>

10.3. VERKAUFSBELEG-KOPIE

Wir können jederzeit Verkaufsbeleg-Kopien von Ihnen anfordern. Wir bitten Sie, auf eine derartige Anforderung unverzüglich zu reagieren, da es andernfalls zum Chargeback kommen kann. Bewahren Sie die Verkaufsbeleg-Kopien immer sicher auf. Bitte denken Sie daran, dass Sie alle Transaktionsbelege über einen Zeitraum von zwei Jahren ab der Zustellung der Ware bzw. ab dem Abschluss der erbrachten Leistung aufbewahren sollten (siehe Regelwerk „PCI DSS“-Standard, S. 28).

In Zusammenarbeit mit



globalpayments.at

SERVICE. DRIVEN. COMMERCE

10.4. TELEFONAT MIT DER MELDUNG „CODE 10“

Wenn Sie auf ein verdächtiges Verhalten der Person hinweisen möchten, welche die Zahlungskarte vorlegt, teilen Sie im Rahmen der telefonischen Kontaktaufnahme bitte Ihre Händlernummer/Terminalnummer/UID. mit und geben Sie an, dass die Genehmigung mit dem „Code 10“ erfolgt. Der Operator vom Helpdesk wird Ihnen Fragen stellen, auf welche Sie nur mit JA/NEIN antworten können. Auf diese Weise wecken Sie bei der Person, welche die Zahlungskarte vorlegt, keinen Verdacht.

Bitte halten Sie sich auch dann an diese Vorgehensweise, wenn Ihnen der Kunde eine alternative Zahlungsform anbietet, wenn Sie der Kunde um Rückgabe der Karte bittet oder wenn er die Räumlichkeiten verlässt, ohne dass die Transaktion abgeschlossen wurde.

Bitte vergessen Sie nicht:

- Weisen Sie den Karteninhaber darauf hin, dass zeitnah eine Routine-Sicherheitsüberprüfung erfolgt oder dass Ihr Kartendienstleister eine Routine-Sicherheitsüberprüfung angefordert hat. Bis die Sicherheitsüberprüfung erfolgt, lassen Sie die Karte und Ware bitte bei sich.
- Führen Sie kein Telefongespräch unter Angabe des „Code 10“, wenn Sie sich gefährdet fühlen oder wenn Sie vermuten, dass dies nicht sicher ist – zum Beispiel, wenn Sie alleine im Geschäft sind. Rufen Sie uns in diesem Fall gleich an, nachdem der Karteninhaber das Geschäft verlassen hat. Mit diesem Telefonat kann dazu beigetragen werden, weitere Betrugstransaktionen bei anderen Händlern zu verhindern.
- Beim Einbehalt der Karte sollten Sie sich sowie auch Ihre Kollegen keiner Gefahr aussetzen. Beginnt die Person, von welcher die Karte für die Transaktion vorgelegt wurde, sich aggressiv oder gewalttätig zu verhalten, geben Sie ihr die Karte immer zurück – auch dann, wenn wir Sie zum Einbehalt der Karte aufgefordert haben.

10.5. EINBEHALT DER KARTE

Wenn wir Sie zum Einbehalt der Karte auffordern, versuchen Sie dem bitte nachzukommen.

Beginnt die Person, von welcher die Karte für die Transaktion vorgelegt wurde, sich aggressiv oder gewalttätig zu verhalten, geben Sie ihr die Karte immer zurück – auch dann, wenn wir Sie zum Einbehalt der Karte aufgefordert haben. In dieser Situation sollten Sie immer folgendes tun:

- Versuchen Sie, sich alle Details bezüglich des Aussehens der Person einzuprägen von welcher die Karte für die Transaktion vorgelegt wurde, sowie die Überwachungsanlage (z. B. eine Sicherheitskamera) zu verwenden, sofern Sie über eine verfügen.
- Nehmen Sie telefonischen Kontakt zu unserem Helpdesk auf (die Kontaktdaten sind auf S. 33 angegeben) und erklären Sie, warum ein Einbehalt der Karte nicht möglich war als Sie hierzu aufgefordert wurden.

Unter bestimmten Umständen werden wir die Polizei einschalten. Wenn die Polizei die Karte verlangt:

- Händigen Sie die Karte der Polizei aus.
- Notieren Sie sich den Namen des Polizisten sowie dessen Identifikationsnummer und die Telefonnummer der Polizeidienststelle.
- Teilen Sie dem untersuchenden Polizisten mit, ob die Sicherheitskamera im Einsatz war, und bewahren Sie eine eventuelle Videoaufnahme mit dem Beweismaterial über einen Zeitraum von mindestens 30 Tagen auf.

Wenn es zum Einbehalt der Karte kommt:

- Füllen Sie zusammen mit der Person, von welcher die Zahlungskarte vorgelegt wurde, unverzüglich das Formular „Bescheinigung über den Einbehalt der Karte“ aus und händigen Sie dieses der Person aus, von welcher die Zahlungskarte vorgelegt wurde.
- Teilen Sie uns so viele Informationen wie möglich zur Person mit, von welcher die Karte für die Transaktion vorgelegt wurde, sowie weitere relevante Informationen, wie zum Beispiel das internationale Kennzeichen (Länderkennzeichen) ihres Fahrzeugs.

- Schneiden Sie die Karte einmal in der Mitte durch, sodass das Unterschriftsfeld, der Magnetstreifen, die geprägte Kartennummer, das Hologramm und der Chip unbeschädigt bleiben, und senden Sie diese zusammen mit dem ausgefüllten Formular „Meldung über den Einbehalt oder Fund einer Zahlungskarte“ unverzüglich an folgende Adresse:

Global Payments s.r.o.
Risk Operations
V Olšínách 626/80
100 00 Praha 10

- Bewahren Sie eine Kopie des Formulars über den Einbehalt der Karte bei sich auf. Das genannte Formular steht auf dem Merchant Portal zum Download zur Verfügung.

10.6. KARTENFUND ODER VERGESSENE KARTE IN IHREN GESCHÄFTSRÄUMEN

Bewahren Sie die Zahlungskarte entsprechend den PCI DSS-Standards (siehe S. 28) sicher auf.

Meldet sich ein Kunde wegen seiner verlorenen/vergessenen Karte bei Ihnen, händigen Sie ihm die Karte erst aus, nachdem Sie die Identität des Karteninhabers überprüft haben:

- Bitten Sie ihn zusätzlich um Vorlage eines Legitimations-/Identitätsnachweises, wie zum Beispiel des Führerscheins, Personalausweis oder Reisepass.
- Überprüfen Sie die Unterschrift auf der Karte mit der Unterschriftprobe der Person, welche sich wegen der Karten bei Ihnen gemeldet hat.
- Bei Zweifeln wenden Sie sich bitte an unseren Helpdesk (die Kontaktdaten sind auf S. 33 angegeben).

Wenn sich innerhalb von 24 Stunden niemand wegen der Karte bei Ihnen meldet:

- Schneiden Sie die Karte einmal in der Mitte durch, sodass das Unterschriftsfeld, der Magnetstreifen, die geprägte Kartennummer, das Hologramm und der Chip unbeschädigt bleiben.
- Füllen Sie das Formular „Meldung über den Einbehalt oder Fund einer Zahlungskarte“ aus und senden Sie dieses zusammen mit allen Teilen der entwerteten Zahlungskarte an folgende Adresse: Global Payments s.r.o.

Global Payments s.r.o.
Risk Operations
V Olšínách 626/80
100 00 Praha 10

Das genannte Formular steht auf dem Merchant Portal zum Download zur Verfügung.

10.7. TESTKAUF

Mitarbeiter von GP sind berechtigt, beim Händler „Testkäufe“ vorzunehmen. Im Rahmen dieser Testkäufe überprüfen die Mitarbeiter, ob der Händler alle Vorgehensweisen und Abläufe zur Akzeptanz von Zahlungskarten wie im Vertrag festgelegt einhält. Nachdem sich der Mitarbeiter ausgewiesen und dem Händler mitgeteilt hat, dass er einen Testkauf vorgenommen hat, nimmt der Händler die Ware gleich nach der erfolgten Transaktion zurück und storniert die betreffende Transaktion.

10.8. PAPIERROLLEN FÜR POS-TERMINALS

Wenn Sie ein elektronisches Terminal betreiben, vergewissern Sie sich, dass Sie über genügend Papierrollen verfügen und den korrekten Rollen-Typ für Ihr Zahlungsterminal ausgewählt haben.

10.9. ERSTELLUNG IHRER EIGENEN WERBUNG

Wenn Sie Ihre eigenen Werbeunterlagen erstellen möchten in denen den Kunden mitgeteilt wird, dass Sie Zahlungskarten als Zahlungsform akzeptieren, fordern Sie bei uns bitte ein Paket mit den relevanten Bildmaterialien an.

In diesem Paket sind detaillierte Informationen enthalten – unter anderem auch wie die Logos der Kartenorganisationen vervielfältigt werden können.

Bitte denken Sie daran, dass folgende Regeln gelten:

- Die Kartenlogos wurden als geschützte Marken registriert und sind entsprechend der Anleitung zu verwenden, welche im Paket mit den Bildmaterialien enthalten sind.
- Im Rahmen der Werbung dürfen die Kartenlogos nicht in einer Weise verwendet werden, durch welche angedeutet werden kann, dass die Kartenorganisationen Werbung für Ihre Leistungen oder Ware machen.
- Sie sind verpflichtet, uns alle Werbe- oder Verkaufsunterlagen zur Genehmigung vorzulegen, in denen unser Unternehmen oder etwaige Kartentypen erwähnt sind.
- Auf Ihrer Internetzahlungsseite muss das betreffende Logo der Kartenorganisationen vorhanden sein.

Wenn Sie das Logo von Global Payments auf Ihrer Webseite oder in Werbeunterlagen verwenden möchten, müssen Sie eine Lizenzvereinbarung über eine geschützte Marke abschließen. Für weitere Informationen wenden Sie sich bitte an uns (die Kontaktdaten sind auf S. 33 angegeben).

Alle Ihre Geschäftsstellen und Verkaufsorte müssen in den betreffenden Werbeunterlagen klar identifiziert werden.

10.10. WIR HALTEN SIE AM LAUFENDEN

Wir senden Ihnen regelmäßig aktuelle Informationen zu diversen Angelegenheiten und Sachverhalten, welche Auswirkungen auf die Art der Akzeptanz und Bearbeitung von Transaktionen mit Kredit- und Debitkarten haben.

Es ist sehr wichtig, dass Sie diese aktuellen Informationen lesen und unseren Empfehlungen nachkommen, vor allem jenen, welche von den Kartenorganisationen selbst geforderte verpflichtende Änderungen betreffen. Wenn Sie weitere Hilfe und Unterstützung benötigen oder befürchten, diese Informationen nicht erhalten zu haben, wenden Sie sich bitte an uns (die Kontaktdaten finden Sie auf S. 33).

11. WICHTIGE KONTAKTE

Wenn Sie uns telefonisch kontaktieren, halten Sie bitte immer Ihre Händlernummer/Terminalnummer/UID bereit. Damit können wir Sie schneller identifizieren, was den Ablauf beschleunigt.

Die Gespräche werden teilweise überwacht und aufgezeichnet. Dies dient der Verbesserung der Serviceleistungen die wir für Sie erbringen. Alle Aufzeichnungen verbleiben ausschließlich in unserem Eigentum.

HELPDESK/TELEFONNUMMER DES SUPPORTS VON GLOBAL PAYMENTS:

Unsere Aufgabe ist es, Sie mit Rat und Tat zu unterstützen. Zögern Sie nicht, sich jederzeit telefonisch oder per E-Mail an uns zu wenden.

Helpdesk und Service – rund um die Uhr für Sie da!

Tel.: +43 1 266 11 00, E-Mail: helpdesk@globalpayments.at

- Reklamationen
- Hilfe beim Storno von Transaktionen und Rückbuchungen
- Nachberechnung von Transaktionen
- Betrugsverdacht
- Telefongespräch mit „Code 10“
- Datenmissbrauch von Zahlungskarten
- Datenschwund

pci@globalpayments.at:

- Verdacht auf Datenmissbrauch von Zahlungskarten
- Verdacht auf Datenschwund

Oder schreiben Sie uns unter:

Global Payments s.r.o. Zweigniederlassung Österreich
Am Belvedere 1
1100 Wien
Österreich

Global Payments s.r.o. Zweigniederlassung Österreich
Am Belvedere 1
1100 Wien
Österreich

Tel.: +43 1 266 11 00
www.globalpayments.at



In Zusammenarbeit mit



globalpayments.at

SERVICE. DRIVEN. COMMERCE