ÖSTERREICHISCHE HOTELIERVEREINIGUNG

LEITFADEN

BARGELDLOSES BEZAHLEN

IMPRESSUM

Medieninhaber und Herausgeber:

ÖSTERREICHISCHE HOTELIERVEREINIGUNG I Hofburg, A-1010 Wien
T: +43 (0)1 533 09 52-0 I office@oehv.at I www.oehv.at
www.facebook.com/hoteliervereinigung

vertreten durch: Dr. Markus Gratzer, ÖHV-Generalsekretär

Koordination: Oliver Wolf

Grafik, Design:

Birgit Rieger I www.br-design.at

Zur besseren Lesbarkeit haben wir Begriffe, die sich zugleich auf Frauen und Männer beziehen, in der männlichen Form angeführt. Dies soll jedoch keinesfalls Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

ÖSTERREICHISCHE HOTELIERVEREINIGUNG

BS PAYONE

VORWORT

Viele Touristiker wissen es längst: Der Anteil bargeldlos getätigter Zahlungen steigt stetig. Inzwischen liegt er in Österreich fast gleichauf mit Bargeldzahlungen. Für die Hotellerie bringt dieser Trend beides: neue technische und organisatorische Herausforderungen ebenso wie spannende Potenziale.

Mit dem starken Wachstum des bargeldlosen Zahlungsverkehrs werden die Rahmenbedingungen für optimierte Bezahlprozesse immer wichtiger für den Hotelier. Hier hat sich in den letzten Jahren sehr viel getan. Die neue Zahlungsdienste-Richtlinie PSD2 (für engl. Payment Services Directive) soll Zahlungsdienste und Zahlungsdienstleister in Europa regulieren, Nichtbanken die Teilnahme am Payment-Markt ermöglichen und die Nutzer von Zahlungsdiensten besser schützen.

Viele technische, gesetzliche und branchenrelevante Neuerungen also, die Hoteliers im Blick haben müssen, um ihre Zahlungsprozesse optimal zu steuern:

Welcher Zahlungsarten-Mix passt zu uns und unseren Gästen? Wie setzen wir die PSD2 für unser Haus um? Wie erreichen wir maximale Sicherheit im Zahlungsverkehr, für unsere Gäste ebenso wie für unser Haus? Wie schaffen wir Zahlungsflexibilität, gerade auch angesichts des wachsenden Anteils ausländischer Gäste mit unterschiedlichsten Zahlungsgewohnheiten? Wie erschließen wir mit Bezahlverfahren, bei denen die Kreditkarte nicht physisch im Hotel vorliegt (z.B. Online-Buchung, MOTO-Transaktionen), neue Vertriebskanäle? Wie interagieren wir optimal mit Buchungsportalen? Wie nutzen wir den Bezahlprozess zur Verbesserung des Gästeerlebnisses?

Antworten, Einblicke und Tipps zu diesen Themen liefert Ihnen dieser vom Zahlungsdienstleister BS PAYONE in Zusammenarbeit mit der Österreichischen Hoteliervereinigung (ÖHV) erstellte Leitfaden.

INHALT

1. Vor Ort, Online, Multichannel – die Payment Trends

Ihre Gäste buchen und bezahlen heute da, wo es ihnen am besten passt: Daheim auf dem Sofa, unterwegs im Zug oder am Flughafen, auf Ihrer Website oder online bei einem Buchungsdienstleister. Ein kundenzentrierter Payment-Mix ermöglicht es Ihnen, diesem Buchungs- und Bezahlverhalten gerecht zu werden. Je einfacher es für Ihren Gast ist, bei Ihnen zu reservieren und zu bezahlen, desto eher hat das positive Auswirkungen auf Kundenzufriedenheit, Kundenbindung und die Bewertungen Ihres Hauses.

Doch gerade weil das Bezahlen ein Thema ist, mit dem der Gast am liebsten nicht behelligt werden möchte und das unauffällig nebenbei geschehen sollte, stellt sich Ihnen als Hotelier eine zentrale Frage: Wie kann ich den Bezahlvorgang für meinen Gast vereinfachen und noch komfortabler gestalten? Und welche Gewohnheiten und Wünsche haben meine Gäste?

Generell gilt:

Kunden zahlen immer weniger mit Bargeld und immer mehr mit Bank- und Kreditkarten. Das Mobile Payment per Smartphone wird in Zukunft eine immer größere Rolle einnehmen. Für Österreich wird eine Verdoppelung der Nutzung innerhalb der kommenden fünf Jahre erwartet. Schon heute tätigen bis zu 20 Prozent der Hotelgäste ihre Transaktionen via Mobile Payment. Parallel dazu gewinnen lokale, alternative Zahlungsmethoden an Bedeutung. Wenn viele Ihrer Gäste aus dem Ausland kommen, kann es sich für Sie lohnen, alternative Zahlungsmethoden (wie z.B. Alipay, Apple Pay oder Google Pay, siehe auch Info-Box auf S.7) anzubieten, die Ihre Gäste auch daheim nutzen. Zusätzlich wächst das bargeldlose Bezahlen im Fernabsatz, also online abgewickelte Zahlungen, rasant.

Die aktuelle Herausforderung für einen Hotelbetrieb besteht darin, einen auf die eigenen Gäste ausgerichteten Multichannel-Ansatz aufzusetzen, um Online (also die Buchungen über Ihre Webseite und über Buchungsplattformen) und Offline (Ihr stationäres Geschäft) optimal zu kombinieren.

Unabhängig von den einzelnen Bezahltechnologien und den Trends im Payment lassen sich heute im täglichen Hotelbetrieb grundsätzlich zwei Vorgänge unterscheiden: **Präsenzzahlung** (am Kartenterminal, so genannte „card present"-Transaktionen) und **Fernabsatzzahlung** (Online/MOTO/etc., so genannte „card not present"-Transaktionen). Diese wollen wir Ihnen im Folgenden vorstellen und Ihnen und Ihrem Team Hilfestellungen bei der Umsetzung geben.

2. Wenn die Kreditkarte physisch vorliegt (card present)

Wenn Ihr Gast bei Ihnen im Hotel nächtigt, werden, je nach Buchungsweg, die Logis und die getätigten Umsätze vor Ort bezahlt. Bei den stationären Bezahlmöglichkeiten steht neben Barzahlung vor allem die Kartenzahlung als häufigste Bezahlform im Vordergrund.

Für Sie und Ihr Team ist es daher wichtig, die Zahlungsabwicklung bei physisch vorliegender Kredit-/ Bezahlkarte sicher zu handhaben, ganz gleich, ob der Gast die Karte direkt nutzt oder sie über ein anderes Interface, z.B. Google Pay oder Apple Pay oder kontaktloses Bezahlen mittels NFC, zur Bezahlung einsetzt. (siehe Info-Box auf Seite 7).

2.1. Sicherheit durch Unterschrift oder PIN

Liegt die Kreditkarte oder das NFC-fähige Gerät physisch vor, wird die Zahlung meist über den EMV-Chip oder kontaktloses Bezahlen (per NFC) mit der Eingabe einer PIN durch den Gast bestätigt. Abhängig von der Kartenart kann es auch vorkommen, dass der Gast die Zahlung per Unterschrift freigibt. Achten Sie bei der Unterschrift stets auf den Abgleich der Vor-Ort-Unterschrift mit der Unterschrift auf der Karte! Der Name des Gastes muss auch mit dem Namen auf der Karte übereinstimmen.

Heben Sie alle Transaktionsunterlagen mindestens 180 Kalendertage auf, um im Falle von möglichen Rückbuchungen (sog. Charge-Backs) einen Beleg zu haben. So lange haben die kartenausgebenden Banken ab dem Zeitpunkt der Abrechnung im Regelfall Zeit, um eine Kreditkartentransaktion zu reklamieren. Beachten Sie zudem, dass die Genehmigungsnummer keine Zahlungsgarantie bedeutet. Der Autorisierungscode bestätigt lediglich, dass das Kartenkonto zum Zeitpunkt der Autorisierungsanfrage nicht gesperrt ist und über genügend Kreditrahmen verfügt. Viele Charge-Backs basieren nicht auf fehlenden Autorisierungen – viel häufigere Auslöser sind sogenannte „No Shows“, also das Nichterscheinen des Gastes, bei denen er versäumt hat, seinen Aufenthalt rechtzeitig zu stornieren. Die anfallenden Gebühren will der Gast nicht zahlen und weist seine Bank an, den gezahlten Betrag zurück zu buchen. Oder der Karteninhaber war nicht zufrieden mit seinem Aufenthalt und fordert über seine Bank den fälligen Betrag oder Teilbeträge zurück.

Apple Pay, **Alipay** und **Google Pay** sind sog. Wallets, die es dem Kunden ermöglichen, Bezahlkarten (meist Kreditkarten) digital zu speichern und damit an kontaktlosen Terminals zu bezahlen. Beim Bezahlvorgang wird auf eine digitale Version der Bezahlkarte zurückgegriffen. Um Zahlungen über Apple Pay entgegenzunehmen, benötigen Sie als Hotel lediglich ein NFC-fähiges Kartenlesegerät: Apple Pay ist die digitale Version einer Bezahlkarte. Über einen digitalen Code, den sogenannten Token, werden die Karteninformationen auf dem Smartphone oder der Smartwatch gespeichert. Damit können Zahlungen wie mit einer Kontaktloskarte getätigt werden – ohne weitere technische Konfigurationen handelsüblicher Terminals. Technisch gesehen ist der Bezahlvorgang dann eine NFC-Zahlung per Visa oder Mastercard (je nach dem welches Kartenprodukt der Gast in der Apple Pay App hinterlegt hat). Ein weiteres optisches Mobile-Payment-Bezahlverfahren ist beispielsweise Blue Code. Dabei wird die Zahlung durch den Scan eines optischen Codes abgewickelt.

Blue Code ist eine speziell für Smartphones entwickelte Bezahltechnologie die einen direkten Bezahlvorgang vom Bankkonto auslöst. Die Einrichtung der Blue Code App ist nur für Kunden mit einem Online-Banking-Zugang möglich. Mit Blue Code kann bereits in Geschäften an der Kasse (in 85% aller Lebensmittelgeschäfte in Österreich), via Bluetooth an Automaten oder via Scan App in der Hotellerie & Gastronomie bezahlt werden.

Gäste öffnen dazu die Blue Code App, geben ihren PIN ein und schon wird ein blauer Barcode auf dem Display des Smartphones dargestellt. Dieser wird an der Kasse eingescannt. Ist der Bezahlvorgang erfolgreich, ertönt ein Bestätigungston. Zum Zeitpunkt der Zahlung kann das Smartphone auch offline sein.

Vorteile sind: Attraktive Transaktionsgebühren, schneller Bezahlprozess an Kassen, höchste Sicherheit und Zahlungsgarantie.

Gerade unter asiatischen Gästen sind optische Bezahlverfahren, wie beispielsweise Ali-Pay, weit verbreitet. In Österreich ermöglicht die Kooperation zwischen AliPay und Blue-Code den Bezahlvorgang an hiesigen Kassen.

NFC (Near Field Communication) ist international wie auch in Österreich eine der gängigsten neuen Methoden für mobiles Bezahlen mit dem Smartphone. Dabei handelt es sich um eine Übertragungstechnik, die über kurze Distanzen den kontaktlosen Austausch von Daten zwischen zwei NFC-fähigen Geräten und Karten (z.B. einem NFC-fähigen Kassenterminal [erkennbar am NFC-Logo] und einem NFC-fähigen Smartphone oder einer Karte) ermöglicht.

QR-Bezahlcodes sind eine optische Mobile Payment-Variante. Hierbei erstellt eine App einen Strichcode, den der Gast an der Kasse über ein entsprechendes Kassengerät einscannt. Über den QR-Code entschlüsselt das Kassenterminal die in der App hinterlegten Zahlungsdaten (z.B. PayPal oder Kontodaten) und bucht den fälligen Geldbetrag ab.

2.2. Flexibel kassieren – mobil und stationär

Wenn Ihre Gäste bei Ihnen ausschließlich an der Rezeption oder an der Bar bezahlen, bieten sich stationäre Kartenlesegeräte an. Bei diesen Geräten erfolgen Stromversorgung und Datenübertragung über feste Anschlusskabel. Mobile Terminals ermöglichen dagegen mobiles Bezahlen überall im Haus, zum Beispiel an jedem Tisch im Restaurantbereich, und bieten zahlreiche Vorteile gegenüber stationären Geräten. Verfügt Ihr Haus über einen Gastronomiebereich sollten Sie die Anschaffung eines mobilen Terminals über WLAN in Erwägung ziehen. Der Gast schätzt es, wenn er die Möglichkeit bekommt auch direkt am Tisch bezahlen zu können. Hat Ihr Haus zusätzlich einen Gastro-Außenbereich, Wellness- oder Outdoor-Anlagen, dann müssen Sie einen größeren Bereich versorgen können. Hier helfen Ihnen Terminals mit GPRS-Verbindung Ihre Gäste flexibel bedienen zu können und die Servicewege Ihrer Mitarbeiter zu reduzieren.

2.3. Schnell und komfortabel – Flexibilität garantiert Kundenzufriedenheit

Optimaler Dienst am Gast erfordert eine hohe Flexibilität bei der Buchung und Zahlung von Services. Insbesondere wenn Sie rund um die Uhr für Ihre Gäste im Einsatz sind, müssen Ihre Terminals viel leisten. Moderne Terminals bieten Hoteliers und ihren Gästen eine große Bandbreite von Zahlungsoptionen: Abwicklung mit Karte und Identifikationsnummer (PIN), mit Unterschrift, Kontaktloszahlung via NFC (siehe Info-Box S.7) oder Zahlung über das Smartphone des Gastes. So sichern Sie schnelle Zahlungen und bieten Ihren Gästen gleichzeitig maximalen Abwicklungskomfort.

2.4. In Österreich daheim, in der Welt zuhause

Österreich wird als Reiseziel immer attraktiver: Der Anteil ausländischer Gäste, nicht nur aus Europa, sondern aus der ganzen Welt, wächst stetig. Damit steigen auch die Anforderungen an Ihr Zahlwesen. Nach wie vor zählen neben nationalen Bankkarten die internationalen Kreditkarten Mastercard und Visa zu den wichtigsten Zahlungsmitteln. Aber je nach Herkunftsregion bevorzugen Ihre Gäste zum Teil sehr unterschiedliche Bezahlverfahren und Karten. Darauf sollte Ihr Zahlungswesen vorbereitet sein:

- Gäste aus China nutzen häufig **UPI (UnionPay International)**-Karten. Sehr verbreitet in Asien ist auch das Zahlen über **Wechatpay** und **Alipay** mit optischen QR-Codes. Bei diesen beiden Zahlungsverfahren handelt es sich nicht um Kreditkartenverfahren. Ähnlich wie bei PayPal sind die Accounts direkt mit dem Bankkonto des Nutzers verbunden. Offene Beträge werden direkt vom Konto abgebucht.
- **Visa Electron** ist in Osteuropa und Lateinamerika verbreitet.
- Europäer zahlen gerne mit **Debitkarten**, z.B. mit **V-Pay**, der **Debit Mastercard** oder der **girocard**. Damit ihre Gäste im Ausland keine zweite Karte brauchen, setzen regional agierende Banken häufig auf das sogenannte Co-Badging, also eine Partnerschaft mit einem global agierenden Anbieter, in der Regel mit **V-Pay** oder **Maestro**.

Grundsätzlich gilt: Gäste schätzen es, wenn sie mit der Karte ihrer Wahl zahlen können. Je flexibler das bargeldlose Bezahlen bei Ihnen Haus ist, umso höher wird die Kundenzufriedenheit sein.

2.5. Bezahlen mit Mehrwert

Payment ist aber mehr als nur Bezahlen. Nutzen Sie den Bezahlvorgang Ihres Gastes, um ihm attraktive Einkaufserlebnisse zu bieten und gleichzeitig zusätzlichen Umsatz für Ihr Haus zu generieren.

Mit **DCC** (Dynamic Currency Conversion) zeigen Sie Gastfreundschaft an der Kasse: Die **dynamische Währungsumwandlung** ermöglicht es dem Gast, in seiner Heimatwährung zu zahlen.

Wenn Sie einen Hotel-Shop haben, ist auch die **Tax Free-Funktion** der Terminals attraktiv für Ihre Gäste: Das Gerät erkennt automatisch, ob Ihr Gast zum steuerfreien Einkauf berechtigt ist und druckt auf Wunsch vollautomatisch einen Erstattungsbeleg für ihn aus. Diesen Beleg kann er einfach und komfortabel an allen Global-Blue-Schaltern, zum Beispiel am Flughafen, zur Auszahlung vorlegen.

Ein weiteres starkes Plus von Terminals ist die **Bargeldauszahlungs-Funktion**, die Ihr Bezahlterminal gleichzeitig zu einem Geldautomaten macht: Statt extra einen Bankauto-

maten suchen zu müssen, kann Ihr Gast direkt beim Bezahlen Bargeld abheben. Dies bedeutet auch weniger Aufwand für Sie: Geringere Bargeldmengen im Haus reduzieren Ihre Handling-Kosten.

All diese Zusatz-Services machen den Bezahlprozess noch transparenter für Ihren Gast und geben ihm das Gefühl, bei Ihnen gut aufgehoben und versorgt zu sein. Zudem profitieren Sie von attraktiven Nebeneffekten: Services wie DCC generieren Zusatzerträge durch Provisionen für Sie als Anbieter.

2.6. Kosten – Bezahlen Sie nur, was Sie brauchen

Bezahlterminals werden in der Regel auf monatlicher oder jährlicher Abrechnungsbasis gemietet. Der Mietpreis variiert je nach Länge der Vertragsdauer inklusive aller erforderlichen Netzbetriebs- und Systemkosten. Achten Sie darauf, dass Zusatzkosten, wie beispielsweise zusätzliche Service- oder Wartungsgebühren, transparent und ersichtlich in Ihrem Mietvertrag aufgeführt sind. Die erstmalige Aktivierung sämtlicher Funktionen ist bei den meisten Anbietern für den Hotelier kostenfrei. Der Großteil der Kosten ist an die Transaktionen gekoppelt. Die Transaktionskosten setzen sich aus Kosten für die Nutzung der Zahlungsinfrastruktur und Kosten für die Abwicklung von Bezahlvorgängen zusammen. Der Zahlungsdienstleister berechnet dem Hotelier für die Abwicklung bargeldloser Bezahlungen eine Gebühr. Ein Teil dieser Gebühren wird für die Nutzung der Infrastruktur an Kreditkartenunternehmen abgeführt.

2.7. Safety First – der richtige Umgang mit Kartenterminals

Moderne Kartenlesegeräte bieten höchste Flexibilität und gleichzeitig Zahlungssicherheit. Hierbei sollten Sie folgende wichtige Faktoren im Blick haben:

2.7.1. Sicherheitssiegel gegen Betrug

Überall wo Daten übertragen und verarbeitet werden, sind Manipulationsversuche möglich. Namhafte Terminalhersteller und professionelle Zahlungsverkehrsdienstleister schützen Sie davor. Sie statten die Geräte mit einem Hologramm-Sicherheitssiegel aus. Versuche, das Gehäuse zu öffnen oder das Siegel abzulösen, führen zur sofortigen Zerstörung des Hologramms. Achten sie daher immer auf ein unversehrtes Sicherheitssiegel.

2.7.2. Passwörter und Terminals schützen

Eigentlich eine Selbstverständlichkeit, insbesondere wenn es um „geldwerte“ Daten geht: Wählen Sie ein **sicheres Passwort** und geben Sie es nur an berechtigte Mitarbeiter weiter.

Händigen Sie Terminals nur an geschulte und autorisierte Mitarbeiter aus und achten Sie darauf, dass Terminals **niemals unbeaufsichtigt** herumliegen. So verhindern Sie unbefugten Zugriff auf hochsensible Daten. Führen Sie **Wartungen der Terminals** nur nach vorheriger Absprache mit Ihrem Dienstleister durch. Verweigern Sie wegen vorgeblicher Störungen unangemeldet auftauchenden Technikern jeglichen Zugriff auf Ihre Terminals.

TIPPS BEIM KASSIEREN

Lassen Sie die Gäste immer den Betrag kontrollieren und überprüfen Sie ihn auch selbst noch einmal, um Tastatureingabefehler vor Abschluss der Kartenzahlung zu vermeiden.

- Stellen Sie sicher, dass Ihre Gäste PIN oder Geheimzahl unbeobachtet eingeben können.
- Bewahren Sie Belege grundsätzlich mindestens 180 Tage sicher auf. Danach entsorgen Sie alte Kartenbelege so, dass Daten darauf nicht in Besitz Dritter gelangen können. Achten Sie jedoch auch darauf, die gesetzlichen und die von der Kartenorganisation abhängigen Aufbewahrungsfristen für Belege einzuhalten.
- Gewähren Sie keinen unbefugten Personen Zugriff auf das Terminal und geben Sie nicht genutzte Terminals entweder beim Empfangsteam oder an einem abschließbaren Ort in Verwahrung.
- Melden Sie jeden Manipulationsverdacht umgehend der Polizei oder Ihrem Zahlungsdienstleister.

2.7.3. Karte gut – Zahlung gut

Hologramme, Prüfnummern und der EMV Chip – dank zahlreicher von den Kartenherausgebern installierter und sichtbarer Sicherheitsmechanismen zählen Bezahlkarten zu den fälschungssicheren Zahlungsmitteln. Gerade die sichtbaren Merkmale erlauben die Gültigkeit der eingesetzten Karten zu kontrollieren.

Gültigkeitsprüfung
Achten Sie darauf, dass das Gültigkeitsdatum auf der Karte nicht überschritten ist.

Karteninhaberüberprüfung
Vergewissern Sie sich, dass Name des Karteninhabers und Geschlecht des Zahlenden übereinstimmen.

Kartenprüfnummer
Diese Nummer wird abgefragt bei E-Commerce-Bestellungen. Die dreistellige Nummer darf nicht gespeichert werden.

Unterschriftenvergleich
Vergleichen Sie, ob die Unterschrift auf dem Beleg mit der Unterschrift auf der Karte und dem Namen übereinstimmt.

TIPP

Lesen Sie Hinweise über aktuelle Entwicklungen und Sicherheitstipps auf den Webseiten der großen Kreditkartenorganisationen Visa (www.visaeurope.at) und Mastercard (www.mastercard.at). Weitere Informationen finden Sie auch auf der Website www.bspayone.at.

3. Wenn Ihr Gast nicht vor Ort ist (card not present)

Je einfacher Sie es Ihrem Gast machen, bei Ihnen zu buchen und zu bezahlen, umso wahrscheinlicher ist es, dass er sich für einen Aufenthalt in Ihrem Haus entscheidet und es zu keinem Abbruch im Bezahlprozess kommt. Mit einer Kombination aus mobilen Zahl-Terminals und einer ePayment-Plattform sind Sie optimal gerüstet, Ihren Gästen Buchungskomfort und maximale Zahlungsflexibilität zu bieten – egal ob stationär oder online.

Dabei ist die ePayment-Plattform das Herzstück Ihres Online-Payments. Sie macht einerseits Ihre internen Prozesse effizienter und ermöglicht einen sicheren, regel- und gesetzeskonformen Zahlungsprozess.

3.1. ePayment-Plattformen – flexibel, sicher, kundennah

Die Einrichtung einer ePayment-Plattform im Hotelbetrieb zahlt sich gleich mehrfach aus. Sie ermöglicht Ihnen als Hotelier nicht nur die optimale Abwicklung kartenbasierter Bezahlverfahren, sondern gewährt Ihnen auch direkten Zugang zu weiteren, insbesondere klassischen und elektronischen Zahlverfahren. Der größte Vorteil für den Hotelier ist jedoch die hohe Sicherheit, die die ePayment-Plattform in allen Zahlungsprozessen bietet. Zusätzlich können über Zusatzservices der ePayment-Plattform zahlreiche kaufmännische Vorteile realisiert werden, z.B. die Einsparung von Zeit und Kosten durch die Automatisierung von Back-Office- und Buchhaltungsprozessen. Die Integration einer ePayment-Plattform in Ihre Strukturen ist dabei wenig aufwendig. Da ein Großteil der Kosten transaktionsgebunden ist, ist der finanzielle Aufwand zuverlässig planbar. Damit lohnt sich die Investition auch für kleinere Hotelbetriebe.

Die ePayment-Plattform wird über eine technische Schnittstelle (API) direkt in Ihre Hotel-Webseite integriert, egal ob Sie ein eigenprogrammiertes oder ein standardisiertes Buchungs-System haben. Bei Letzteren ist eine Payment-Schnittstelle meist schon integriert, ansonsten unterstützt Sie Ihr Zahlungsdienstleister bei der Integration. Die Schnittstellen regeln den zur Abwicklung der Bezahlprozesse erforderlichen Datenaustausch. Dabei können Sie das System nach Ihren individuellen Bedürfnissen aufsetzen:

Zahlungsarten

Je nach Ihren Präferenzen können Sie in Ihrem ePayment-System verschiedene Zahlungsarten anbieten, z.B.:

- **klassische Zahlverfahren** (Zahlung per Rechnung und Überweisung)
- **kartenbasierte Zahlverfahren** (z.B. Zahlung per Kreditkarte oder girocard)
- **elektronische Zahlungen** (z.B. PayPal, paydirekt, Sofortüberweisung etc.)

Zusätzliche Online-Services

Eine ePayment-Plattform unterstützt Sie zudem, Ihre internen Buchhaltungsprozesse effizienter zu gestalten:

- Aufeinander abgestimmte **Debitorenbuchhaltungsprozesse** und **automatisch korrekt verbuchte Zahlungsvorgänge** erleichtern Ihnen die praktische interne Abwicklung Ihrer Zahlungen.
- Auf Wunsch unterstützt Ihr Zahlungsdienstleister Sie auch im **Forderungsmanagement**: Bei Zahlungsversäumnissen oder Rückbelastungen wird er automatisch aktiv und wickelt die Forderung für Sie ab – von der ersten Mahnung bis hin zum Inkasso.
- Dank automatischer Mahnsperren, Mahn- und Inkassovorschlagslisten haben Sie jederzeit Hoheit über Ihre Prozesse.

3.2. Mehr Sicherheit mit PSD2

Die Zahlungsdienste-Richtlinie PSD2 (für engl. Payment Services Directive) ist eine EU-Richtlinie zur Regulierung von Zahlungsdiensten und Zahlungsdienstleistern, deren grundlegende Ziele es sind:

- die Sicherheit im Zahlungsverkehr zu erhöhen,
- den Verbraucherschutz zu stärken,
- Innovationen zu fördern und
- den Wettbewerb im Markt zu steigern.

Die PSD2 gilt für Zahlungen in EU/EWR-Währungen zwischen im EU/EWR-Raum ansässigen Zahlungsdienstleistern. Teilweise findet sie auch Anwendung auf Zahlungen in Nicht-EU/EWR-Währungen (z.B. US-Dollar oder britische Pfund).

Darüber hinaus führt die PSD2 (eigentlich ab dem 14. September 2019 gültig, nun nachdem Beschluss der Europäischen Bankenaufsicht mit einer verlängerten Umstellungsphase bis zum 31.12.2020) die Verpflichtung der sogenannten „starken Kundenauthentifizierung“ ein. Dies bedeutet mehr Sicherheit im Zahlungsverkehr. Online- und Kartenzahlungen müssen nun grundsätzlich durch zwei unabhängige Merkmale aus den Kategorien Wissen, Besitz und Inhärenz bestätigt werden. Durch PSD2 sind sowohl Verbraucher als auch Sie als Hotelier besser gegen Missbrauch oder Betrug bei Kartenzahlungen geschützt.

Die neuen PSD2-Vorgaben fordern mehr Transparenz: Reserviert ein Gast z.B. ein Zimmer in Ihrem Hotel und Sie wollen für diese Zimmerbuchung einen bestimmten Betrag auf dem Kartenkonto reservieren und vor der Anreise abbuchen, so bedarf diese Zahlung oder dieser „Block“ des Betrages nun der expliziten Zustimmung des Gastes.

In den Schnittstellen moderner ePayment-Plattformen sind die neuen Sicherheitsstandards für Online-Zahlungen gemäß PSD2 bereits umgesetzt. Die **PSD2-Richtlinie** gilt insbesondere für elektronische Bezahlverfahren, die speziell für das Bezahlen im Internet entwickelt wurden, z.B. die Zahlungsarten PayPal, Sofortüberweisung oder Online-Kreditkartenzahlungen.

Ihre ePayment-Plattform unterstützt Sie als Hotelier bei der Umsetzung der in der Richtlinie geforderten **starken Kundenauthentifizierung** (auch SCA genannt, englisch für Strong Customer Authentication) bei Online-Buchungen in Ihrem elektronischen Zahlungsverkehr. Dabei werden elektronische Zahlungen durch eine **Zwei-Faktor-Authentifizierung (2FA)** abgesichert. Zur Freigabe einer Bezahlung muss der Gast mindestens zwei unabhängige Faktoren aus den drei Kategorien Wissen (z.B. Passwort oder PIN), Besitz (z.B. Karte oder Smartphone) oder Inhärenz (z.B. Fingerabdruck oder Gesichtserkennung) angeben. Damit wird sichergestellt, dass es sich beim bezahlenden Gast auch tatsächlich um den Kontoinhaber handelt.

Zwei-Faktor-Authentifizierung bei Kreditkartenzahlungen

3D Secure, Identity Check, J/Secure und SafeKey sind Verfahren der kartenausgebenden Banken für mehr Zahlungssicherheit. Die Zwei-Faktor-Authentifizierung erhöht die Sicherheit von Online-Kreditkarten-Zahlungen und reduziert Betrugsrisiken oder Zahlungsausfälle durch Kartenmissbrauch. Wenn der buchende Gast im Bezahlprozess seine Kreditkartennummer eingibt, wird automatisch eine Verbindung zum Kartenherausgeber hergestellt. Der fordert den Gast auf, seine Identität mittels eines Codes zu bestätigen. Erst nach korrekter Authentifizierung wird die Kreditkartenzahlung ausgeführt. Sie als Gastgeber profitieren dabei von einem deutlich verbesserten Schutz vor Kartenmissbrauch. Gleichzeitig findet eine Haftungsumkehr auf der Bank statt. Gäste können nicht mehr so einfach das Argument „Transaktion nicht durchgeführt“ für eine Zahlungsrückgabe ins Feld führen.

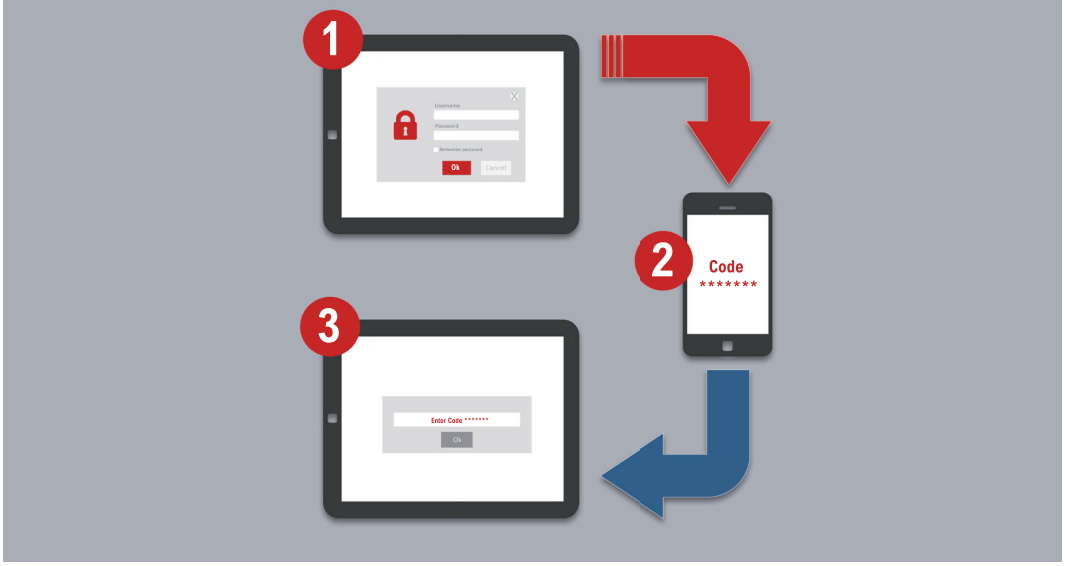
Vorteile 3D Secure

- Schutz vor betrügerischem Kartenmissbrauch
- Erhöhung der Zahlungssicherheit
- Einfache Integration
- Plugin zur sicheren Datenübertragung an die Kartenorganisation / kartenausgebende Bank

Zwei-Faktor-Authentifizierung bei Kreditkartenzahlungen

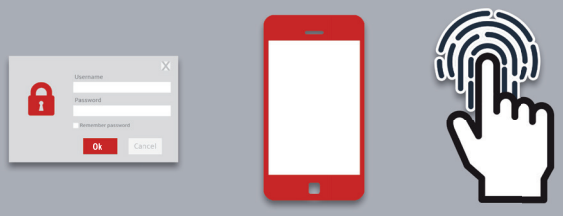
Gültig ab dem 14.09.2019, umzusetzen bis spätestens 31.12.2020

Neuerungen



Details

Betätigung mit 2 Faktoren aus 3 verschiedenen Bereichen.



Wissen | Besitz | Inhärenz

Ziel:

Mehr Zahlungssicherheit

Höherer Verbraucherschutz

3.3. Deposit- und Anzahlungsmanagement

Mittlerweile nutzen viele Hotels die Kreditkarte zur Absicherung von Stornierungen oder nicht angetretenen Aufenthalten. Wird ein Zimmer für einen längeren Zeitraum gebucht, kann der Hotelier ein **Deposit** verlangen. Auch bei Frühbucherraten wird die Kreditkarte bereits zum Zeitpunkt der Buchung belastet. Alternativ kann die Kreditkarte auch als **Sicherheitsleistung** bzw. **Anzahlung** dienen. Dabei wird der Betrag vom jeweiligen Kreditkartensystem reserviert, aber noch nicht belastet. Wichtig ist auch hier, bereits bei der Anreise die Karte durch das Terminal zu ziehen und die PIN abzufragen, und nicht erst beim Check-Out.

Im Umgang mit **Deposit und Anzahlungen** sollten Sie als Hotelier auf die umfassende Information des Gastes achten. Denn laut der PSD2-Richtlinie müssen Sie in solchen Fällen ausdrücklich Ihre Gäste darauf hinweisen und brauchen deren Zustimmung, bevor Sie einen Betrag blocken können.

Bei der Buchung über Website, Telefon oder E-Mail sind daher der Deposit- bzw. Anzahlungsbetrag, die Stornobedingungen einschließlich des letztmöglichen Zeitpunktes für eine kostenlose Stornierung, sowie anfallende Kosten nach Ablauf der Stornierungsfrist zu kommunizieren. Bestätigen Sie dem Gast seine Anzahlung schriftlich innerhalb von drei Tagen, zusammen mit einem Buchungsbeleg. Damit sichern Sie sich auch bestmöglich gegenüber eventuellen Charge-Backs ab.

3.4. Online Vertriebswege

Buchungstool auf Ihrer Website

Eine eigene Hotel-Webseite über die Ihre Gäste bequem buchen, reservieren und bezahlen können, bietet nicht nur Ihren Gästen viele Vorteile, sondern unterstützt Sie auch in Ihren eigenen Prozessen und macht Sie unabhängiger von großen Buchungsportalen.

Mit einem guten Mix an Bezahlverfahren bieten Sie Ihren Gästen maximale Zahlungsflexibilität. Das dazu notwendige Zahlungssystem kann in das hoteleigene Website-Design integriert und mehrsprachig dargestellt werden. Im Verlauf des Buchungsprozesses gelangt der Gast in das Zahlungsportal, wo er seine Bezahldaten eigenständig eingibt. Im Onlineportal getätigte Transaktionen können Sie im Administrationsbereich der Software schnell und unkompliziert bis zu drei Monate lang bearbeiten.

Moderne Systeme erlauben Ihnen, das Buchungstool mit integriertem Zahlungssystem optimal zu konfigurieren. So kann zum Beispiel das Buchungstool über entsprechende Schnittstellen mit Ihren anderen Systemen (Hotelsoftware oder Property Management System, Buchhaltungssoftware, etc.) verknüpft werden. Mehrere etablierte Anbieter unterstützen Sie passgerecht dabei, inklusive Integration der an Ihren Bedürfnissen ausgerichteten und PCI DSS-konformen (siehe Info-Box, Seite 18) ePayment-Plattform.

Der Payment Card Industry Data Security Standard (PCI DSS)

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein strenger globaler Sicherheitsstandard für den sorgfältigen und geschützten Umgang mit Kreditkartendaten. Der Standard, der von den fünf großen Kreditkartenunternehmen American Express, JCB, Mastercard, Discover Financial Services und Visa ins Leben gerufen wurde, umfasst Sicherheitsanforderungen für die Verarbeitung, Speicherung und Übertragung von Karteninformationen, die maßgeblich Kreditkartenmissbrauch, Betrug und Cyber-Diebstahl vorbeugen sollen.

Bei **Kreditkartenzahlungen im Fernabsatz** (also über Ihre Website) liegt für Sie als Hotelier ein „card not present" Szenario vor. Hier sichert heute in den meisten Fällen das sogenannte 3D Secure-Verfahren (siehe Box: Zwei-Faktor-Authentifizierung bei Kreditkartenzahlungen, Seite 15) mit vorgeschriebener Passwort und PIN-Eingabe im Internet die Zahlung. Bei Problemen trägt der Karteninhaber die Beweislast.

! BITTE BEACHTEN SIE:

Die elektronische Speicherung von Kreditkartendaten ohne entsprechende PCI-DSS-Zertifizierung ist nicht zulässig. Eine Speicherung der Daten trotz fehlender Zertifizierung kann zu unangenehmen Rechtssituationen führen. Im Falle eines Datenlecks oder Hacker-Angriffs drohen neben Image- und Vertrauensverlusten erhebliche Strafgebühren, Einschränkungen oder sogar ein Verbot der Abwicklung von Kreditkartenzahlungen. Falls Sie Kreditkartenzahlungen elektronisch erfassen und verarbeiten möchten, empfiehlt sich eine Tokenisierung von Zahlungsvorgängen. Dabei werden sensible Daten, wie zum Beispiel Kreditkartennummern, durch alphanummerische Referenzwerte ersetzt – die sogenannten Tokens. In den Buchungs- oder Kassensystemen werden also nur verschlüsselte Daten und keine sensiblen Karteninformationen verarbeitet – so dass keine PCI-DSS-Vorgaben verletzt werden.

MOTO-Zahlungen

MOTO steht für **Mail-Order & Telefon-Order**. Bei **Zahlungen per Telefon oder E-Mail** erfolgt in vielen Hotels immer noch die Eingabe der Kartennummer manuell in das Terminal. Dieses vermeintlich kundenfreundliche Vorgehen ist nicht mehr zeitgemäß und zudem auch noch gefährlich, denn Sie können die Daten nicht sicher verifizieren und haben als Hotelier keine Zahlungsgarantie. Ihr Gast könnte jederzeit sein Geld mit dem Argument zurückfordern, er habe die Buchung gar nicht getätigt oder seine Kartendaten seien missbräuchlich verwendet worden. Auf die eigenen AGBs oder die nationale Gesetzgebung können Sie sich dabei nicht unbedingt verlassen, da bei Unstimmigkeiten rund um die der-

art getätigten Zahlungen in der Regel das übergeordnete Recht des Kartenherausgebers und seines eingetragenen Gerichtsstandes greift. In diesem Fall müssen Sie also Forderungen gegenüber Ihren Gästen aus dem Ausland in deren Herkunftsland juristisch einfordern (siehe Fallbeispiel).

99 % Zahlungssicherheit stellen Sie bei MOTO-Transaktionen nur her, indem Sie mit einem **Bezahllink** arbeiten. Das funktioniert so: Der Gast bucht telefonisch oder per Mail und erhält von Ihnen eine Bestätigungsmail mit einem Bezahllink. Um die Buchung abzuschließen, klickt der Gast auf diesen Link, gibt seine Kartendaten ein und bestätigt so seine Buchung.

Für solche MOTO-Transaktionen empfiehlt sich eine **MOTO-Software bzw. ein virtuelles Terminal**, das die Online-Eingabe der Kartendaten ermöglicht. Dadurch werden diese Daten PCI DSS-konform unmittelbar in Ihrem Online-Portal erfasst und auch Risikomanagementprüfungen finden wie bei einer Online-Zahlung Anwendung.

FALLBEISPIEL „MANUELLE EINGABE“:

Ein Mann reserviert telefonisch in der Hauptsaison zwei Zimmer für vier Personen und der Hotelier trägt die ihm am Telefon genannten Kreditkartendaten manuell am Terminal ein, um den Logispreis zu reservieren. Doch statt der anreisenden Familie kommt am Anreisetag die Stornierung der Reise. Das Hotel beruft sich auf die Stornobedingungen und bucht den nach den AGBs fälligen Stornobetrag manuell ab. Die Reaktion der nicht erschienenen Gäste: Sie rufen den abgebuchten Betrag zurück (Charge-Back). Trotz vorliegender und vom Gast rückbestätigter Reservierung ist der Hotelier machtlos. Denn der Mann hat angegeben, die Reise nie gebucht zu haben. Seine Rückbelastung ging ohne Weiteres durch, weil seine Bank den angegebenen Grund akzeptiert hat und auch nicht überprüfen musste. Weil der Gast zudem aus den USA stammt, müsste der Hotelier einen aufwendigen zivilrechtlichen Prozess im Heimatland des Gastes anstrengen, um sein Recht einzuklagen. Damit verliert der Hotelier die gesamte Stornogebühr zuzüglich des darüber hinaus angefallenen Preises für die nicht belegten Zimmer mitten in der Hauptsaison.

Das hätte der Hotelier tun sollen:

Im obigen Szenario hätte der Hotelier auf eine Anzahlung (per Zusendung eines Bezahllinks, damit der Gast seine Daten eingibt und die Zahlung über 3D Secure autorisiert) bestehen sollen und dem Gast nach Eingang der Zahlung die Buchung bestätigen sollen. Aufgrund der Haftungsumkehr hätte dann der Gast beweisen müssen, dass er nicht gebucht hat. Mit einer ePayment-Plattform lassen sich solche Prozesse bereits im Vorfeld sauber aufsetzen und automatisieren, so dass Fälle wie der obige von vorneherein mit optimaler Sicherheit gesteuert werden können. Auch „garantierte Buchungen“ (es wird keine Anzahlung getätigt. Durch die Angabe einer Kreditkarte und Bestätigung mittels SCA wird die Buchung gesichert und ggf. mit einer Vorautorisierung belegt) können abgewickelt werden.

FALLBEISPIEL „ÜBERWEISUNG AUF EIN ANDERES KONTO“:

Bei einem Hotel geht eine Buchung per E-Mail ein. Das Hotel bearbeitet die Buchung und belastet die angegebene Kreditkarte mit den Kosten für die Hotelübernachtungen. Einige Tage bevor der Gast anreist, bittet er das Hotel per E-Mail aufgrund eines persönlichen Schicksalsschlages, seine Buchung zur stornieren – soweit ein Routinevorgang. Aber der Gast wünscht eine Überweisung des Betrags direkt auf sein Konto – statt einer Gutschrift auf die zuvor belastete Kreditkarte. Das Hotel kommt dem Wunsch nach und überweist das Geld – ein fataler Fehler, wie sich später herausstellt!

Denn Wochen später erfährt das Hotelmanagement, dass es einem Betrug zum Opfer gefallen ist: Die kartenausgebende Bank hat für die getätigte Kreditkartentransaktion eine Rückbelastung veranlasst. Denn der vermeintliche Hotelgast hatte bei seiner Buchung missbräuchlich erlangte Kreditkartendaten angegeben und der rechtmäßige Karteninhaber wurde inzwischen auf die unrechtmäßige Buchung aufmerksam. Die Konsequenz: Ein Totalausfall für das Hotel, neben dem Charge-Back der Kreditkartentransaktion wurde zusätzlich noch auf das Bankkonto des Betrügers überwiesen.

Durch Beachtung einfacher Regeln, kann man das Betrugsrisiko erheblich senken. Unter den Betrugsmaschen ist der oben beschriebene Vorfall mittlerweile ein Klassiker. Entscheidend ist der richtige Umgang mit Reservierungen, Buchungen und Stornierungen!

BITTE BEACHTEN SIE:

- Bestehen berechtigte Zweifel bei einer Zimmerreservierung, sollten alle Fragen im direkten Dialog mit dem Gast geklärt werden. Sollte bei einer Reservierung z.B. mehr als eine Kreditkartennummer angegeben werden, ist äußerste Vorsicht geboten! Wurde die Reservierung auch vom berechtigten Karteninhaber durchgeführt? Erkennt das Hotel diese Betrugsform, ist in jedem Fall die Sicherheitsabteilung des zuständigen Kreditkarten-Akquirers einzuschalten.
- Nutzen Sie Bezahllinks um PSD2-konform Zahlungen, Anzahlungen oder Reservierungen abzuwickeln. Weiters können virtuelle Terminals für die Transaktion genutzt werden, Dieses Terminal macht es dem Händler möglich, Zahlungen ohne Unterschrift des Zahlenden anzunehmen und zu verifizieren.
- Eine Zahlung muss immer über den gleichen Weg storniert werden, wie sie erfolgt ist. Das heißt bei einer Kreditkartenzahlung muss die Gutschrift auch auf dieselbe Karte erfolgen – führen Sie keine Barauszahlungen oder Banküberweisungen durch.
- Lassen Sie sich beim Check-In eine Kreditkarte vorlegen und reservieren Sie den Betrag, nehmen Sie weitere formelle Prüfungen vor, etwa über eine Unterschrift des Gastes oder durch Vorlage von Legitimationsdokumenten (z.B. Personalausweis).
- Lesen Sie beim Check-Out die Kreditkarte im Kartenterminal aus (card present-Transaktion) und belasten Sie dann die Kreditkarte endgültig. Mit einer Pin-Eingabe bestätigt der Gast die Zahlung.

Buchungen über intermediäre Plattformen wie Booking.com, Expedia oder HRS

Wenn Sie mit Buchungsplattformen wie Booking.com, Expedia, HRS oder anderen zusammenarbeiten, müssen Sie entscheiden, ob der Gast über das Buchungsportal zahlt, welches Ihnen nach Abzug der Gebühren den Logispreis überweist, oder die Zahlung direkt bei Ihnen erfolgt. Die Buchungsplattformen bieten unterschiedliche Möglichkeiten für die Bezahlung, die Sie als Hotel (je nach Plattform) festlegen können:

- **Zahlung vor Ort (klassische „card present“ Transaktion):** Die Zahlung erfolgt bei Anreise oder Abreise direkt im Hotel. Für Anzahlungen oder die Absicherung bei No Shows werden die Kartendaten des Gastes per Formularservice via E-Mail oder über ein Extranet der jeweiligen Plattform an das Hotel weitergeleitet („card not present“). Diese Kartendaten sollten über ein virtuelles Terminal eingegeben und abgerechnet werden. Mit der schrittweisen Umsetzung der PSD2 wird eine manuelle Buchung am Kartenterminal vor Ort zukünftig nicht mehr möglich sein.
- **Zahlung im Voraus und Abrechnung über die Plattform:** Hier ist der gesamte Zimmerpreis zum Reservierungszeitpunkt fällig. Der Gast gibt dazu seine Kreditkartendaten auf der Buchungsplattform ein, diese erhält den Betrag direkt vom Gast und sendet dem

Hotelier eine virtuelle Kreditkarte zu, welche mit dem gleichen Betrag beladen ist. Der Hotelier gibt die Kreditkartendaten in sein Terminal ein und erhält den Betrag gutgeschrieben. Das Kartenprodukt, das hier genutzt wird, ist eine Commercial Card, welche mit höheren Kosten vergebührt wird.

3.5. Riskmanagement und Betrug

In jüngster Zeit häufen sich in der internationalen Hotellerie leider verschiedene Arten von Betrugsfällen bei Buchungen und Zahlungen. Als Hotelier sollten Sie und Ihr Team auf Ihr gesundes Bauchgefühl und Ihre Praxiserfahrung setzen. Denn bei 100 Fällen sind normalerweise nur 1 oder 2 auffällig und fühlen sich falsch an. Diese sollten dann genauer geprüft werden.

Wenn ein Gast beispielsweise 3 Kreditkarten angibt, die alle nicht funktionieren ist Vorsicht geboten und Sie sollten auf sichere, alternative Zahlungsarten wechseln. Auch eigenartige Kombinationen in den Daten des Gastes gilt es zu hinterfragen. Wenn zum Beispiel ein russischer Gast mit Wohnsitz in London eine Schweizer Kreditkarte nutzt und sich über eine Ukrainische E-Mail bei Ihnen meldet, ist dies auf jeden Fall sonderbar und sollte Ihnen Anlass geben auch hier auf für Sie sichere Zahlungswege zu bestehen. Bei Unsicherheiten hilft es auch manchmal den Gast mit seinem Namen einfach mal zu googeln, um einen Plausibilitätscheck zu machen. Natürlich gilt es Augenmaß zu bewahren. Auch wenn nur der Eigentümer der Karte für die Zahlungsabwicklung akzeptabel ist, kann es vorkommen, dass zum Beispiel der Ehemann die Karte seiner Ehefrau nutzt oder umgekehrt. Vorsicht geboten ist dagegen immer bei Zusatzleistungen, die der Gast wünscht und mittels Rechnung oder Karte begleichen möchte. Alles was zum normalen Hotelbetrieb gehört ist legitim, aber Sonderwünsche, wie z.B. der Erwerb von Elektronikartikeln oder ähnlichem, sollten Sie dringend an Partner oder Dienstleister vermitteln.

Seien Sie auch wachsam bei Reservierungsanfragen bei denen der Gast auf Vorabbezahlung besteht. Hierbei werden teilweise gestohlene Kreditkarten genutzt. Und kurz vor der geplanten Anreise wird die Reise mit Verweis auf einen Unglücksfall abgesagt (wie im Fallbeispiel beschrieben). Die Betrüger erklären sich großzügig mit einer Rückerstattung von 70 oder 80 Prozent des bereits gezahlten Betrags einverstanden, allerdings unter der Bedingung den Betrag einem anderen Konto oder einer anderen Kartennummer gutzuschreiben. Wer dieser Bitte nachkommt verliert sein Geld.

Wenn Sie und Ihr Team stets aufmerksam sind werden Sie kaum Probleme haben, denn auch Betrüger haben Blacklisten und meiden Häuser, bei denen es eine sorgfältige Prüfung aller Zahlungsvorgänge gibt.

Darüber hinaus bietet Ihr Zahlungsdienstleister auf Wunsch zahlreiche weitere Services an, z.B. Identifizierung eventueller Betrugsversuche anhand von Transaktionsmustern, Abgleich von Reservierungsdaten mit den bei der kartenausgebenden Bank geführten Daten, Security Check bei der kartenausgebenden Bank, Betrugsmuster-Überwachung von Sales Channels etc.

Folgende Handlungsempfehlungen ergeben sich:

1. Sprechen Sie mit Ihrem Acquirer, Zahlungsdienstanbieter, Payment Service Provider und Ihrem Partner bei Direktbuchungen (Buchungsmaske bzw. Web Booking Engine) um Zahlungsprozesse vor Ort (card present) und vor allem Online-Zahlungen oder die Absicherung einer Buchung mit Kreditkarte (card not present) an die neuen Vorgaben anzupassen.
2. Bereiten Sie Ihre Website auf die Neuerungen vor und lassen Sie 3D Secure Verfahren mithilfe Ihres Zahlungsdienstanbieters integrieren. Die Nutzerfreundlichkeit sollte hier im Fokus stehen, um erhöhte Abbruchquoten zu vermeiden. Am besten Sie informieren sich bei Ihrem Acquirer auch über die Möglichkeiten der PCI-konformen Paymentlinks. Diese Links zu virtuellen Terminals verschicken Sie einfach direkt per E-Mail und Ihre Gäste können schnell, sicher und unkompliziert bezahlen.
3. Möglicherweise sind auch Ihre Datenschutzerklärungen zu aktualisieren, nachdem Sie mit Ihrem Zahlungsdienstleister gesprochen haben. Es gilt abzuklären welche Gastdaten für den Zahlungsvorgang verarbeitet werden. Diese Daten dürfen nicht zu Marketingzwecken verwendet oder gespeichert werden.

4. Fazit

Der Gast bewegt sich heutzutage nahtlos zwischen off- und online Welt. Deshalb sollten Sie ihm parallel unterschiedliche Wege zu Ihrem Angebot über verschiedene Kanäle ebnen. Wenn Sie das schaffen, gewinnen Sie den Gast und das Rennen mit dem Wettbewerb.

Mit einer Kombination aus modernen, mobilen Zahl-Terminals für die Zahlungsabwicklung vor Ort und einer ePayment-Plattform zur Abwicklung aller onlinegestützten Zahlungen, bieten Sie Ihrem Gast ein durchgängig attraktives Payment- und Servicelevel und sind Ihrerseits optimal gerüstet für einen sicheren, regel- und gesetzeskonformen Payment-Prozess in Ihrem Betrieb.

Die ePayment-Plattform sollte dabei Ihre zentrale Schaltstelle zu allen Vertriebskanälen sein. In den Plattformen etablierter Dienstleister sind in der Regel alle neuen Sicherheitsstandards wie Zwei-Faktor-Authentifizierung bereits PSD2-konform integriert. Dadurch bietet Ihnen eine ePayment-Plattform vor allem folgende Vorteile:

- **Kanalübergreifendes Kundenerlebnis** bedeutet, sich konsequent an den Wünschen der Gäste auszurichten und die Kanäle so miteinander zu verknüpfen, dass der Hotel-Gast überall ein positives Erlebnis bekommt.
- **Haftungsumkehr:** Nicht der Hotelier muss aufwendig nachweisen, dass der Gast die Buchung getätigt hat. Die mit der Benutzung der Software verbundene Haftungsumkehr zwingt den Gast bei Diskussionsbedarf zum Nachweis.
- **Komfortable Integration** der ePayment-Software in gängige Buchungs- und Buchhaltungssysteme.
- **Zuverlässige und schnelle Abwicklung** von Zahlungen und nachgelagerten Prozessen.
- **Effizienzsteigerung**, z.B. durch vereinfachte Überwachung von Zahlungseingängen.
- **Reduzierung von Zahlungsausfällen** dank integrierter Sicherheitsverfahren.

So bieten Sie nicht nur Ihren Gästen optimalen Buchungskomfort und maximale Zahlungsflexibilität. Mit dieser Technologie machen Sie auch Ihre internen Prozesse sicherer und effizienter.

Die Integration einer ePayment-Plattform in Ihre Strukturen ist dabei weit weniger aufwändig als oft vermutet. Abläufe und Funktionen können optimal auf Ihre Bedürfnisse und Ihre Gäste sowie deren Herkunft ausgerichtet werden. Da ein Großteil der Kosten transaktionsgebunden ist, ist der finanzielle Aufwand zuverlässig planbar.

Die ÖHV und BS PAYONE als Payment Service Provider, helfen Ihnen, die für Sie passenden Bezahlmöglichkeiten für Ihr Unternehmen und Ihre Gäste zu treffen, effiziente und sichere Bezahlprozesse einzurichten und gleichzeitig neueste Trends im Payment zur Kundenbindung und -gewinnung zu nutzen.

Mit einer ePayment-Plattform sind Sie bestens gerüstet für die Zukunft der Hotellerie und die Zukunft des Bezahlens!

5. Glossar

3D Secure	Dies ist ein neuer Sicherheitsstandard für Online-Händler, der von Mastercard und Visa gemeinsam entwickeltet wurde. Dadurch werden die Risiken durch Betrug im E-Commerce-Sektor minimiert. Das Verfahren ermöglicht es Karteninhabern, sich während des Bezahlvorgangs mit einem persönlich vergebenen Passwort zu authentifizieren. Mit der Einführung des Sicherheitsstandards geht eine Haftungsumkehr („Liability Shift“) einher, womit ein vom Kunden reklamierter E-Commerce-Umsatz nicht mehr an den Händler zurückgegeben werden kann, wenn dieser die 3D Secure-Technologie unterstützt.
Acquirer/ Acquiring	Kreditinstitut oder im Auftrag eines Kreditinstitutes tätiges Unternehmen, welches Unternehmen für die Kreditkartenakzeptanz unter Vertrag nimmt und die Kreditabrechnung durchführt.
Autorisierung / Authorisation	Verfahren zur Genehmigung oder Ablehnung von Kartenumsatzanfragen. Die Umsatzanfrage wird durch das Händlerterminal an die Karten ausgebende Bank gerichtet. Die Antwort kann eine Genehmigung, eine Umsatzablehnung, Aufforderung zum Karteneinzug oder zur Legitimationsprüfung umfassen.
Card Not Present	Hier geht es um eine Zahlungskarten-Transaktion, bei der der Gast nicht am Point of Sale (PoS) anwesend ist und die Kreditkarte nicht physisch vorliegt. Der Kunde teilt seine Kartendaten telefonisch oder per Online-Eingabe mit.
Card Present	Eine Zahlungskarten-Transaktion, bei der der Karteninhaber und dessen Karte beim Händler vor Ort sind und die Karte am Point of Sale (PoS) physisch am Terminal eingelesen wird.
Charge-Back	Das Verfahren wird angewandt, wenn ein bereits abgerechneter Umsatz vom Karteninhaber aus Gründen reklamiert oder bestritten wird, für die ein Rückbelastungsrecht vorgesehen ist. Der Begriff "chargeback" bezeichnet auch den die Rückbelastung bewirkenden elektronischen Datenaustausch zwischen Issuer-Bank und Acquirer-Bank.

CVC2 (Card Verification Code)	Dieser Kartenverifizierungscode dient zur Sicherheit bei Mail-order- und Internet-Transaktionen. Der Karteninhaber wird vom Händler aufgefordert, neben der Kartennummer und des Gültigkeitsdatums auch noch die Kartenprüfnummer mitzuteilen. Die Kartenprüfnummer befindet sich auf dem Unterschriftsstreifen der Kartenrückseite.
DCC	Mit Dynamic Currency Conversion (dynamische Währungsumrechnung) bezahlt der Karteninhaber in seiner Heimatwährung. Bei einer korrekt durchgeführten DCC Transaktion wird der Kaufpreis von der Währung des Händlers automatisch in eine sogenannte Transaktionswährung umgerechnet, die der Währung des Karteninhabers entspricht. Dies geschieht direkt am PoS bevor der Händler den Kaufbetrag zur Autorisierung einreicht. Die Software des PoS Terminals erkennt automatisch anhand der Kartennummer das Herkunftsland der vorgelegten Karte und bietet das Bezahlen in der jeweiligen Währung an. Der tagesaktuelle Kurs der Währung wird täglich neu und automatisch an das Terminal übertragen und auf dem Terminal-Beleg ausgewiesen. Der Karteninhaber findet den von ihm unterschriebenen Betrag auf seinem Abrechnungsbeleg und der Händler erhält den Original-Transaktionsbetrag wie gewohnt in Euro.
Debit Card	Die Zahlungskarte ist mit einem Bank(giro)konto verknüpft. Jede Transaktion, die mit dieser Karte getätigt wird, führt zu einer sofortigen Kontobelastung des Karteninhabers.
Emittent / Issuer	Bank, die Zahlungskarten an ihre Kunden ausgibt, die Kartenkonten ihrer Kunden verwaltet, Kartentransaktionen autorisiert (entweder selbst oder über beauftragte Dienstleister) und der Acquirer-Bank gegenüber den Zahlungsausgleich für gültige Kartenumsätze garantiert.
EMV	Europay, MasterCard, Visa = EMV Die drei Kartenorganisationen haben sich zwecks Erarbeitung und Förderung globaler Standards für elektronische Finanztransaktionen abgestimmt. Das Kürzel "EMV" bezieht sich auch auf die von allen drei Unternehmen übernommenen technischen Spezifikationen zur Gewährleistung globaler Kompatibilität und Interoperabilität für Chipkarten, Chipterminals und den entsprechenden Datenformaten in der Transaktion.

Kartenprüfnummer	Für die Kartenprüfnummer wird häufig auch die Abkürzung CVC2/CVV2 verwendet. Hierbei handelt es sich um eine drei- oder vierstellige Sicherheitsnummer auf der Kreditkarte.
Liability Shift / Haftungsumkehr	Als Folge der Einführung der EMV-Chiptechnologie bzw. PSD2 (mit der "Strong Customer Authentication", SCA) muss diejenige Transaktionspartei (Issuer oder Acquirer) die Haftung für betrügerische Transaktionen tragen, die den Betrug durch die Nutzung der Technologie und/oder Karteninhaberverifikation mittels PIN hätte verhindern können. Bei der Haftungsverteilung wird damit eine Art Verursacherprinzip eingeführt. Ist entweder das Terminal oder die Karte bei einer Transaktion EMV-fähig bzw. kann eine SCA durchgeführt werden, trägt diejenige Transaktionspartei die Haftung für Schäden aus Kartenfälschungen, die nicht EMV/SCA-fähig war. Zudem trägt die EMV-Chiptechnologie entscheidend dazu bei, Kartenfälschungen und -kopien nachhaltig zu verhindern.
MOTO – Mail-Order und Telefon-Order	Die Bestellung der gewünschten Leistungen kann mündlich (z.B. per Telefon), schriftlich (z.B. per Email, Brief oder Fax) oder auch online (über die Website oder Vermittlungsportale) getätigt werden. Die anschließende Bezahlung kann per Kreditkarte erfolgen.
NFC	Near Field Communication (NFC) bezeichnet in diesem Zusammenhang das Bezahlen per berührungslosem Austausch von Daten über kurze Distanzen z.B. mit Bankomatkarte, Kreditkarte, Handy oder Smartwatch etc..
PAN	PAN steht für Primary Account Number. Diese Nummer ist eine Zahlungskartennummer, die Kreditkarten und Debitkarten eindeutig identifiziert.
PAN-Schlüsseleingabe / PAN Key Entry	Bezeichnet die manuelle Eingabe (über Tastatur) der Kartennummer in ein Terminal im Hotel statt elektronischer Einlesung über den Magnetstreifen.

PCI DSS	Um eine einheitliche Vorgehensweise bei der Umsetzung dieser Sicherheitsanforderungen zu ermöglichen, haben sich die Kartenorganisationen Visa und Mastercard auf gemeinsame Standards geeinigt. Diese tragen die Bezeichnung "Payment Card Industry Data Security Standards" und haben Gültigkeit für die gesamte Kartenzahlungsbranche.
Pharming	Pharming ist eine Weiterentwicklung der Internet-Betrugsmethode "Phishing". Bei Pharming wird der Internet-Nutzer nach Eingabe einer korrekten URL (Internet Adresse) auf eine gefälschte Seite umgeleitet, die der echten täuschend ähnlich sieht. Auf der gefälschten Seite wird der Kunde dann aufgefordert, Geheimzahl (PIN) oder Transaktionsnummern (TAN) einzugeben, mit denen die Kriminellen Geld vom Konto des Betrogenen abheben können. Da die Kriminellen oft ganze Server-Farmen mit gefälschten Websites betreiben, wird diese Methode "Pharming" genannt.
Phishing	Phishing ist ein Kunstwort aus Passwort und Fishing. Es bezeichnet ein Verfahren, bei dem mittels gefälschter E-Mails oder Webseiten unbemerkt persönliche Daten auf fremden Rechnern aus spioniert werden. Dabei erhält der Anwender eine seriös wirkende E-Mail, die den Empfänger darauf hinweist, sein Zugang bei seiner Bank würde verfallen oder bei einer Kreditkarte müsse eine Sicherheitsabfrage stattfinden. Um dies zu verhindern, müsse auf einen im Text enthaltenen Link geklickt werden. Diese Links führen jedoch nicht zur Bank oder zum Kreditkarten-Unternehmen. Stattdessen landet der Anwender auf Seiten, die populären Web-Anbietern wie eBay, Amazon oder Banken zum Verwechseln ähnlich sehen. Dort sollen sie dann vertrauliche Angaben wie Name, Passwort oder PIN-Codes eingeben, die Betrüger für Straftaten nutzen.
PIN – Persönliche Geheimzahl	Personal Identification Number oder Geheimnummer, die nur dem Karteninhaber bekannt ist und die Issuer-Bank (oder deren Dienstleister) in die Lage versetzt, die persönliche Legitimation des Karteninhabers zu überprüfen.

PoS	PoS steht für Point of Sale und beschreibt die Stelle, an der ein Verkauf stattfindet. Unter diesem Begriff wird häufig das Hotel/ das Resaurant/ das Geschäft beschrieben.
PSD2	Die Zahlungsdiensterichtlinie (Abkürzung PSD von englisch Payment Services Directive) – genauer die zweite Zahlungsdiensterichtlinie (EU) 2015/2366 (Abkürzung PSD2) – ist eine EU-Richtlinie der Europäischen Kommission im Zahlungsdiensterecht zur Regulierung von Zahlungsdiensten und Zahlungsdienstleistern in der gesamten EU und dem Europäischen Wirtschaftsraum (EWR). Ziel der Richtlinie war und ist es, den europaweiten Wettbewerb und die Teilnahme an der Zahlungsbranche auch von Nichtbanken zu erhöhen und durch die Harmonisierung des Verbraucherschutzes und der Rechte und Pflichten für Zahlungsdienstleister und Nutzer gleiche Wettbewerbsbedingungen zu schaffen. Bezahlvorgänge im Internet sollen dadurch bequemer, billiger und vor allem sicherer werden.
PSP – Payment Service Provider	Payment Service Provider sind Unternehmen, die sich auf die technische Anbindung und die Transaktionsabwicklung mit Finanzdienstleistern im E-Commerce Bereich spezialisiert haben und Webterminals für Online-Zahlungen anbieten. Für alle PSP ist es verpflichtend, sich nach einem international abgestimmten Sicherheitsstandard, dem Payment Card Industry Data Security Standard (PCI-Standard) zertifizieren zu lassen.
SCA	Mit Inkraftreten der PSD2 müssen Online-Kreditkartenzahlungen mit der sogenannten Zwei-Faktor-Authentifizierung oder auch Strong Customer Authentication (SCA) abgesichert werden. Dabei sind zur Freigabe einer Bezahlung mindestens zwei unabhängige Faktoren aus den drei Kategorien Wissen (z.B. Passwort, PIN), Besitz (z.B. Bezahlkarte, Smartphone) oder Inhärenz (z.B. Fingerabdruck, Gesichtserkennung) notwendig. Die SCA soll sicherstellen, dass es sich beim bezahlenden Nutzer auch tatsächlich um den Kontoinhaber handelt. Ziel ist die Reduktion von Kreditkartenbetrug.

SEPA	Die europäische Kreditwirtschaft arbeitet an der Realisierung eines einheitlichen europäischen Zahlungsverkehrsraums (SEPA). Ziel ist es, den Bürgern die Möglichkeit zu eröffnen, Zahlungsverkehrsdienstleistungen im Euro-Raum zu den gleichen Konditionen auszuführen zu können wie im Heimatland. Die Plattformtechnologie ist dabei EMV.
Token	Mit der Möglichkeit der "Tokenization" bei Kreditkartennutzung, ob nun online oder offline, werden Kreditkartenzahlungen sicherer, da Kreditkartendaten bei bargeldlosen Zahlungen verschlüsselt werden. Ein Gast bezahlt online mit Kreditkarte - Er gibt im Bezahlvorgang seine Kreditkartennummer (16 Ziffern) ein. Diese Kreditkartendaten werden nach der Übertragung vorerst an einen externen Server gesendet, auch Tokenization-Server genannt, der diese Daten wiederum überträgt und verschlüsselt. Diese verschlüsselten Daten nennt man Tokens. Sie werden zurück an die entsprechende Website gesendet. Durch die Speicherung der Daten auf einem externen Server trägt der Händler/ das Hotel keine Sorge mehr um die Sicherheitsrisiken.
Trace-Nummer	Die Trace-Nummer ist die Nummer einer Transaktion, mit der sich eine bargeldlose Kartenzahlung eindeutig identifizieren lässt.
Virtuelles-Terminal	Ein virtuelles Terminal ist ein Internet-Bezahlsystem, bei dem eine spezielle, vom Payment Service Provider bereitgestellte Webseite als Kasse genutzt werden kann. Dieses Terminal macht es dem Händler möglich, Zahlungen ohne Unterschrift des Zahlenden anzunehmen und zu verifizieren. Es kommt beispielsweise bei MOTO-Käufen oder bei CNP-Transaktionen zum Einsatz. Die Risikomanagementprüfungen finden wie bei einer Online-Zahlung Anwendung.

BS/PAYONE

JETZT KENNENLERNEN UND STAUNEN!

BEZAHL-LÖSUNGEN
PERFEKT SERVIERT

BS PAYONE GmbH | Wienerbergstraße 11 / 12a | A-1100 Wien, Österreich | +43 800 2957 68 | www.bspayone.com

Österreichische Hoteliervereinigung
Hofburg, A-1010 Wien

T: +43 (0)1 533 09 52-0 I F: +43 (0)1 405 25 84 I office@oehv.at I www.oehv.at

Für eine STARKE Hotellerie.