pay2sender

Data Protection in the Hotel Sector
The payments challenge

In this whitepaper we explore how new Data Protection rules (the GDPR) challenge some of the standard ways hotels collect guest payments. GDPR represents a positive opportunity for hotels to review their payment processes and improve security and customer experience.

Hotels and other hospitality businesses are working hard to comply with GDPR across their customer transactions, internal processes and supply chains. GDPR is proving costly in terms of upskilling and ongoing resource requirements, and businesses are understandably wondering if there is ever going to be any return on this investment.

To comply with GDPR, hotels are required to do the following:

1

Have secure procedures for collecting personally identifiable information from customers ('data subjects') such as credit card information, addresses, etc.

2

Be able to demonstrate a valid reason for customer data retention and inform customers for what purpose and for how long the data will be retained.

3

Build and maintain marketing relationships with customers on the basis of active 'opt in', thus permitting storage of information based on valid consent.

4

Keep detailed records to support procedures for data retention.

About GDPR

GDPR (the General Data Protection Regulation) is the biggest change to data protection legislation in over 20 years. It officially starts on 25th May, and whilst this comes as no surprise, preparing for the new legislation has been a challenge for the hospitality industry. Businesses may be subject to fines of up to €20 million or 4% of total worldwide annual turnover (whichever is greater).

On the positive side, GDPR offers an opportunity to fix processes that were already broken, and the resulting improvements will ensure that risks are mitigated and customer experience improves.

Data Breaches in The Hotel Sector

The Trustwave Global Security report 2018 examines data breaches worldwide. The report shows that the hospitality industry (hotels, food & beverage) accounted for 21.4% of all data compromises worldwide. Card Not Present accounted for 18% of fraud in 2017. This is down from 29% in 2006 indicating that business are tightening up controls already. However 40% of breaches in the hospitality industry occurred within their internal corporate networks meaning that it is critical for them to minimise storage of, and access to sensitive customer data.

GDPR Challenges

One of the biggest risks for hotels is insecure handling of credit cards, and this is where a strong focus on GDPR and PCI compliance will pay dividends.

Payments over the Phone

Collecting card data over the phone is a long-established practice for hotels; whether for a room booking, a bottle of champagne for a friend's suite, a wedding deposit, or a round of golf.

Asking callers to visit the website to complete their payment isn't really a valid solution, as there is no way to ensure they'll get the deal they agreed on the phone and every moment that goes by puts the sale at risk.

While phone payments may be the default solution for hotels to deal with 'card not present' scenarios, it is inconvenient for the customer, and the disadvantages to the business include increased no-shows, chargebacks and card fraud.

Furthermore, it treats customer data in an insecure way whilst failing to provide any security of funds due to the potential for chargebacks.

While it is inevitable that a high proportion of personal service business, such as hospitality, will continue to be concluded via phone, it is far less secure than card present or online.

Charge-to-card Payments

Hotels often store and reuse cards from their most trusted visitors – regular business travellers who expect a more personal level of service and familiarity on their return. The hotel is trusted to process payments using those cards without the need for the customer to authorise each time.

This is no longer secure and hotels must find better ways to process payments from these valuable customers that protects both parties from possible card fraud.

Card-Not-Present Fraud is Growing

Since the introduction of chip and pin in the UK, card fraud has moved to card not present, growing as a share of all fraud, and in real terms by almost 50%.

Hotels taking phone payments are particularly vulnerable to card testing – where a fraudster books a room purely to establish whether a stolen card is still active. Adding 3D Secure to a remote payment will greatly reduce this risk.

Type	2007	2016
CNP Fraud	**54%**	**70%**
Stolen card	11%	16%
Account takeover	6%	6%
Card cloning	27%	6%
Card not delivered	2%	2%

Source: Financial Fraud Action UK

The Pay2Sender Solution

Pay2Sender provides a faster, more secure way for hotels to request and accept card payments. Instead of taking card details over the phone, staff can simply send customers an SMS or email, each containing a unique link to a personalised online form that the customer can use to complete payment quickly and securely.

Get Paid Faster

Pay2Sender accelerates guest payment collection. You can stay on top of all payment communications and payments received and issue reminders and refunds at the touch of a button. Unlike manual payment collection by phone, you can send multiple payment requests and receive multiple payments simultaneously.

Secure & Compliant

With Pay2Sender no card details are passed between you, your customers or your staff, therefore the risks of card numbers being inadvertently stolen or compromised are greatly reduced. 3D Secure can also be applied to further minimise the fraud risk. A GDPR-compliant opt-in is included as a single click activation, so you can ask the customer to consent to your ongoing marketing messages in a fully compliant manner.

Stored Card Payments

Pay2Sender's Autocharge feature is a more secure and convenient solution for stored card payments. Because the customer card details are tokenised and stored with your payment gateway, there is no need to view or store the card details locally. Autocharge enables your hotel to charge extras such as room service, spa treatments, and any other items to your guests' card while eliminating the risk of compromising sensitive card data.

More Time For You & Your Guests

Avoiding taking card payments over the phone frees up your staff's time to spend on more productive activities - like making your guests feel even more welcome! Your guests will save time too: with Pay2Sender they can complete your payment request at a time that is most convenient time for them.

What is Card Tokenisation?

Given the inherent risks associated with capturing customer card data, either via an external booking site, from group head office, or over the phone, no hotel can afford to store that data on site. Tokenisation is the process of replacing the customer's card number (PAN) with a unique reference which cannot be related back to the original card number. Pay2Sender stores a tokenised reference for your customer's card with your payment processor to enable features such as Autocharge, Express Checkout and Recurring payments.

Case Study

The Só Hotel Group is a dynamic, modern group of Irish family-owned hotels, delivering accessible luxury in elegant, guest-focused surroundings. Their properties include Castletroy Park Hotel Limerick, Lough Rea Hotel and Spa Co. Galway, Charleville Park Hotel Co. Cork and Killeshin Hotel Portlaoise.

Challenge

The Só Hotel Group understood there was a need to make improvements to their payments processes in order to become fully compliant with the emerging GDPR legislation changes.

Solution

The Só Hotel Group use Pay2Sender to ensure that they no longer request customer card details over the phone and do not store card details within their business.

Implementing Pay2Sender has allowed them to automate much of the reservations process and as a result, they are now able to reduce the number of staff involved.

The group also utilise Pay2Sender's ability to attach a standard hotel invoice giving the customer a full breakdown of charges ensuring a customer is always aware of what they are paying for.

Pay2Sender provides the Só Hotel Group with a secure and intuitive web interface so staff can see which payments have been successful and automates the process of sending follow up requests to those who have not yet paid.

Results

The Só Hotel Group is no longer taking payments over the phone and is instead putting payments through the secure Pay2Sender solution, resulting in a quicker, safer customer experience which is totally compliant with GDPR legislation, and a more streamlined reservations process overall.

> **”We wanted to secure our customers' data and ensure that we were fully compliant with GDPR in 2018. We found a solution that achieved that, but which also helped us to streamline our reservations process”**

Lisa O'Farrell
Reservations Manager, Castletroy Park Hotel.

Pay2Sender is the smart way to request and receive payments from your customers quickly, conveniently and securely using SMS and email. We help organisations of all sizes save time, reduce costs and get paid faster.

Contact us for a Demo
tel: +353 1 4995090

or visit us online at
www.pay2sender.com

pay2sender