
How to Get Your
HOTEL PCI AND GDPR
COMPLIANT

TABLE OF CONTENTS

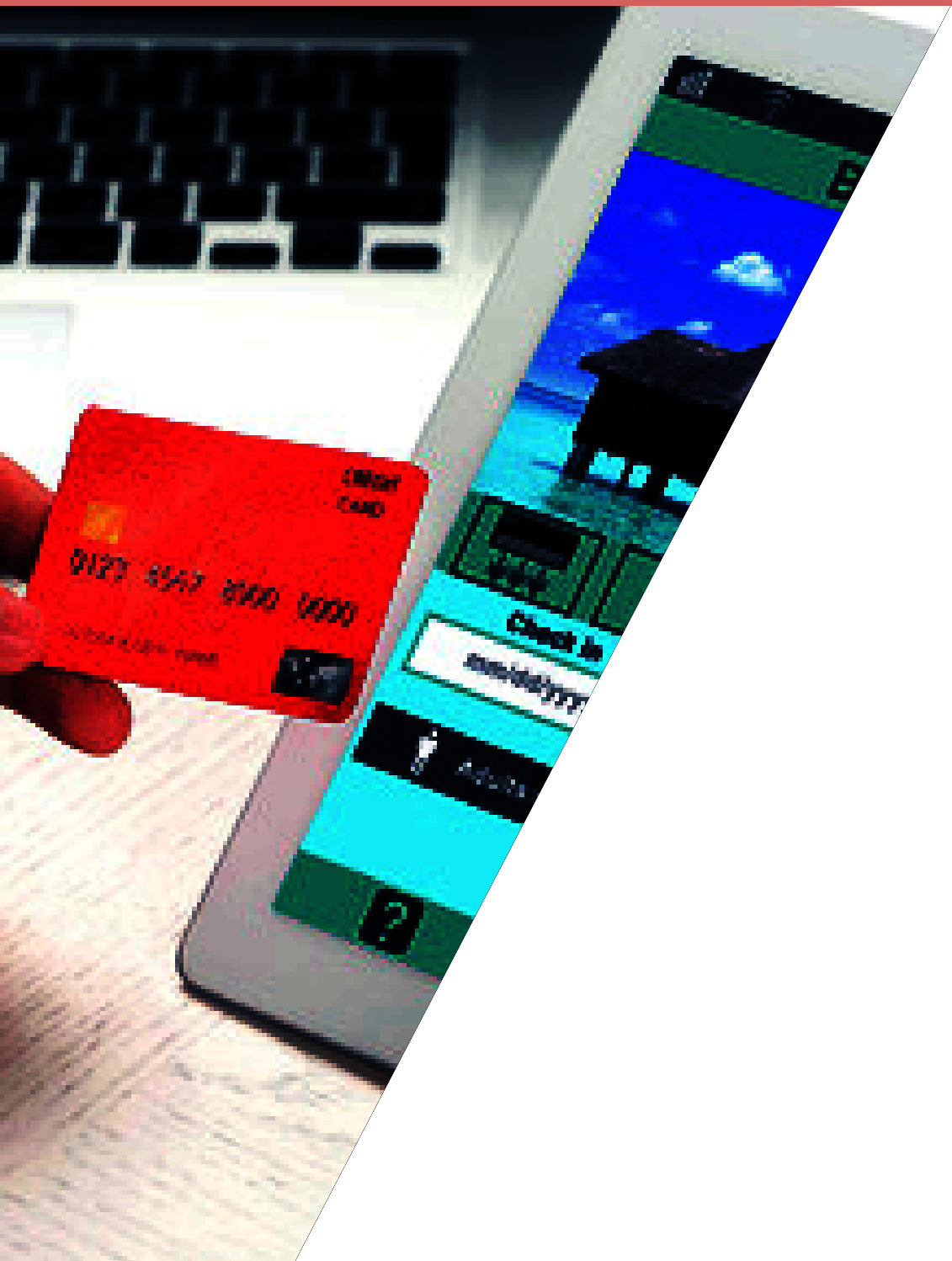
1

INTRODUCTION

The hospitality sector over the years has been the number one recipient of attacks and data security breaches. An estimated 14% of data related incidents have happened in or around the hospitality industry. The increased attacks are most likely associated with the increased use of digital systems.

Hotels use a number of databases and media that involve their customers signing in with their personal details. Customers use online bookings; while others use mobile location utilities, and text messaging applications, all of which entail guests handing over a good chunk of personal information.

Intrinsically, hotels have a responsibility to safeguard all this data at whatever cost. In this era of digital technology, protecting customers' data that has been entrusted through the aforementioned connections involves sticking to strict guiding principles that can be drafted under two specific classes: PII which means (Personally Identifiable Information) and PCI that refers to (Payment Card Industry) compliance. These two terminologies are most of the times used together or in combination with one another even though individually, each one of them is an extensive sector of compliance by itself.



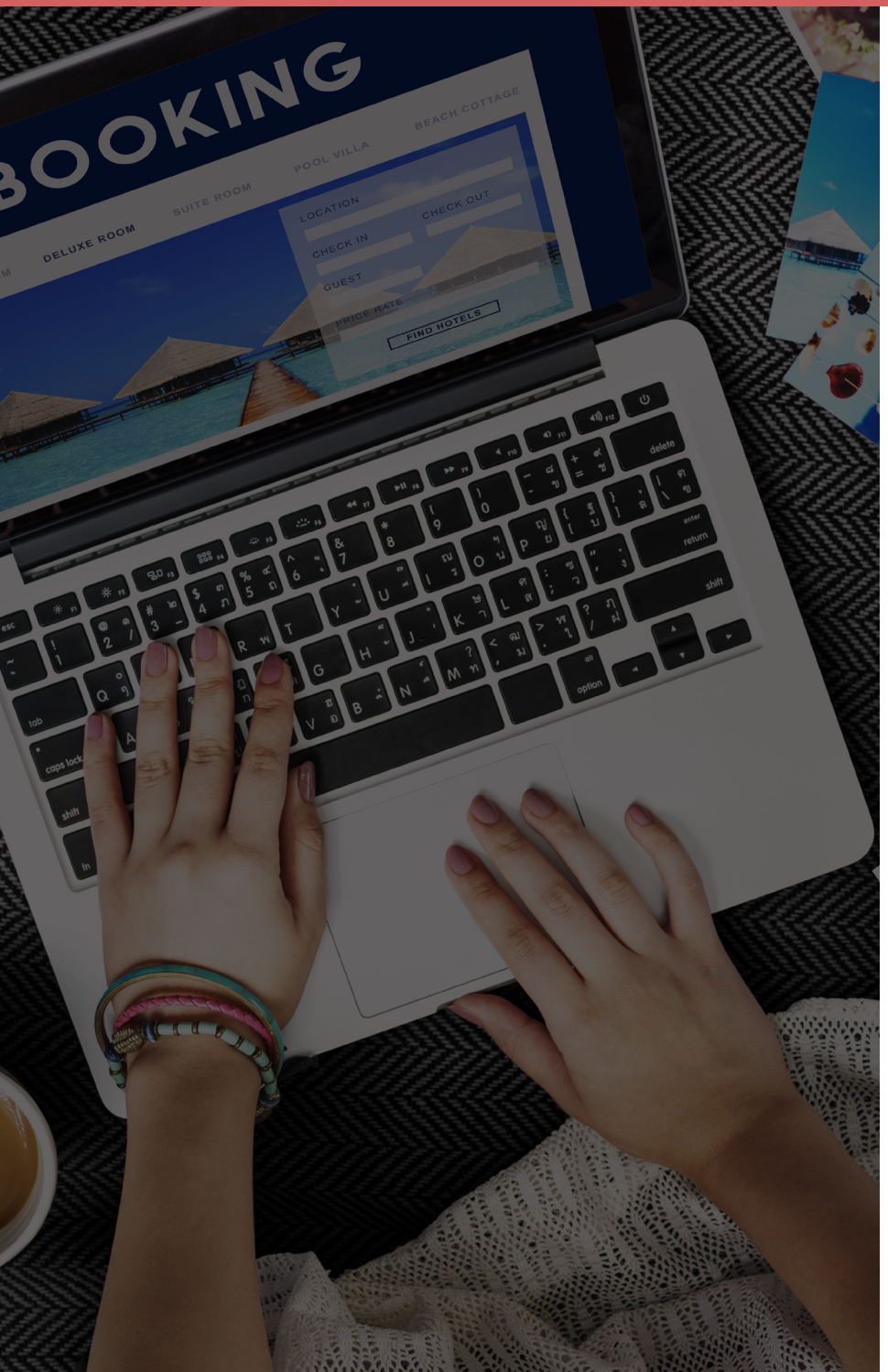
D. PCI COMPLIANCE

Any business which deals with information based on or derived from credit cards (as well as providing storage, processing, and even conveying the cardholder information) ought to be compliant to PCI. In order to make sure that the credit card information remains as with the best protection available, the PCI Data Security Standard also known as PCI DSS, has adopted a strategy that has 12 centrally located security areas—which have been acknowledged as the least possible level of safety procedures that organizations have to adopt and adhere to.

PCI compliance consists of a prescribed contract with the acquiring banks, and some of the U.S. states have brought in some essentials of PCI compliance and adopted them into their identifiable bylaws. In due course, the obligation for any type of breaches that may come up is heaped on the hotel.

Smaller hotels, for most of the time, may absolutely lack the expertise and input of a committed top-ranking department or officer to deal with compliance. A greater percentage of properties can still meet the set PCI compliance standards by following a few simple steps.

mycloud HOSPITALITY



II). PII COMPLIANCE DEFINITION

PII, otherwise known as (Personally Identifiable Information) refers to any data that can be manipulated to expose a particular person`s identity. This list is comprised of details such as:

a) *The name of a person*

b) *Birthdate*

c) *Email address*

d) *IP address*

e) *Phone number*

f) *Bank account details*

g) *Passport number*

h) *Address*

i) *Identification number*

j) *Social security number*

While compliance to PCI applies only to the protection of details pertaining credit card information, PII has a much wider area of coverage. In addition to this, it is also an area which hotels should be aware of especially with the increase in guest information being collected via a number of sources which include the likes of loyalty programs, profiling in social media and online bookings.

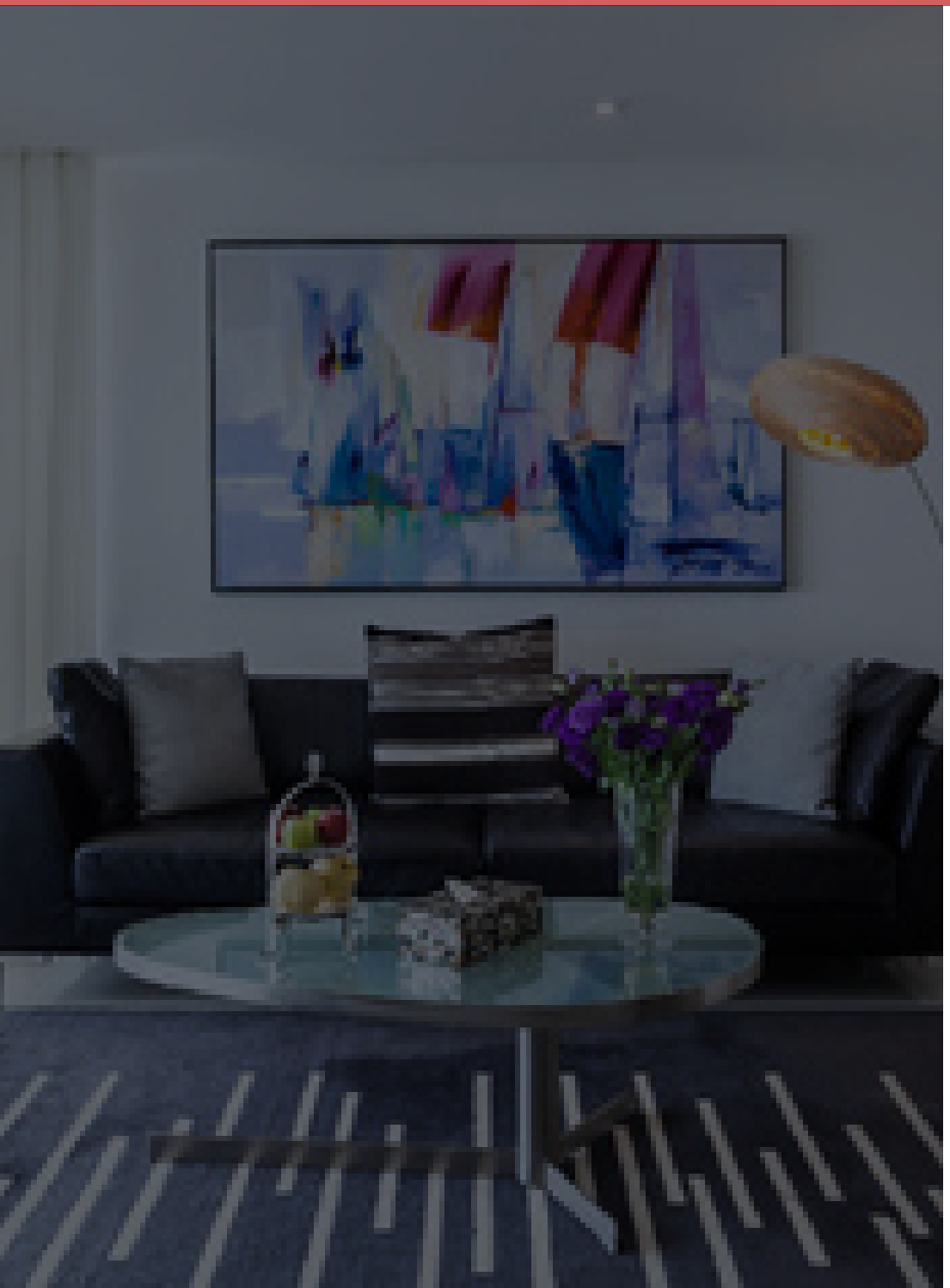
Just as it is dictated in PCI compliance laws, all businesses that fail to protect a person`s PII are liable to being given significant financial penalties, needless to mention the immense damage that it will have on the brand`s reputation.

III). GENERAL DATA PROTECTION REGULATION

From May 2018, there will be stricter laws that will be put in place by the new GDPR, with heftier financial penalties being stipulated for anyone found guilty of failure to comply with their laws. One of the key changes is an increase in the law`s scope of coverage. The GDPR is wrongly thought to apply only to companies in the European Union. However, the truth of the matter is that all companies around the globe that do any business with consumers from the EU are said to be subject to these rules.

Consent forms for data usage cannot be in the form of illegible pages that are ridden with legalese instead of easily accessible and intelligible language any longer. They should basically be composed of plain and clear language and in addition to this; they should be just as easily withdrawable as they are easy to give.

A General description of GDPR from EU GDPR portal



"mycloud PMS runs at its best to ensure the smooth efficiency of our front office department; it also keeps an accurate track record of statistics for the management team in order to make vital decisions. In addition, its POS system helps enhance food and beverage sales."

ALEX BRESSERS

MANAGING DIRECTOR | BYD LOFTS BOUTIQUE HOTEL & SERVICED APARTMENTS

www.bydlofts.com

mycloud HOSPITALITY

2

HOW A HOTEL CAN PROTECT INFORMATION IN CASE OF PCI

PCI compliance should be one of the top priorities of any organization. Any business operations that handle sensitive customer's data should be fine-tuned as this is too delicate to be manhandled. A hotelier should incorporate even software vendors. They are in a position to help in managing storage, processing and transmission of sensitive data. Sourcing for alternative solutions is advised if your current solution is not compliant. Organizations that go against GDPR are at risk of facing fines in the region of 4% of the organization`s global turnover!

3

HOW SHOULD A HOTEL HANDLE GDPR AND KEEP PCI SAFE AND ACCESSIBLE TO GUESTS

There are myriads of steps that hotels can take to ensure that their clients` personal data is under foolproof protection. Reviewing the security policies in place and pseudonymizing and encrypting data are examples of these strategies. However, it is vital for you to note that without adopting privacy measures by design, it is almost impossible to keep PCI safe. For you to achieve success, you should always prioritize data protection whenever you are coming up with a new service or designing a new process.

It is also important for you to note that hotels need to ensure that they have asked their guests for permission to communicate with them. This means that as a hotelier, you should see to it that you provide your hotel`s guests with an option of agreeing to communicate with the hotel whenever they are making reservations be it on an offline or online basis. In addition to this, when taking their phone numbers and email addresses, you are required to provide them with the option of a "forget me post guest departure". Both the forget me and opt-in options should be acknowledged as well as completed by the guests while they`re still in reservation.

On top of the above, you should always see to it that guests have been provided with an option where they can request the hotel for data stored in their software databases. With this information, the guests should be given the power to change communication preferences, to mark as opt-out or even ask the hotel to delete the data in its entity. Hotels are also required to maintain logs of the data shared with guests and their opt-in preferences. This should be done with an aim of preventing communication with guests that have not opted in for such communication.

Due to the fact that hotel systems usually talk to multiple systems, the primary system owner/provider should see to it that the flow of information to any third party system is closely monitored and has strict restrictions according to communication rules and guest preferences. In addition to this, there is a need for clear privacy policies as well as encryption of data in the hotel`s systems so as to see to it that whenever a breach takes place, the data is of no use to the hacker.

It is also of essence for hoteliers to also ensure that the systems they put in place can allow for easy accessibility to customers. Whenever a customer submits a subject access request, the system should be able to provide a comprehensive report concerning all the data that the hotel has on the customer within no more than 30 days.

HOW DO YOU WORK WITH TECHNOLOGY VENDORS ON INFORMATION SECURITY?

It is common knowledge that a vast majority of hotels have a tendency of outsourcing the technological bit of their hotel systems. In regards to this, it is easy to assume that the data protection responsibility is passed to the technology`s vendor. However, it is of essence to know that ultimately, whenever something negative ensues, the hotel is bound to be responsible for it.

Every time that you are implementing technological systems in your hotel, ensure that you give your system vendors a summary of your most pressing security requirements. See to it that communication remains clear and open with enough emphasis being laid on the expected features and how information is protected both on the vendor`s side and on the hotel`s side. You should also ensure that you indicate the kind of protocols to be followed in case of a breach or cyber-attack.

Also, you should note that consistent security evaluations as well as staff training sessions are vital if you want to see to it that a hotel is updated concerning the latest rules. By so doing, you could avoid being overwhelmed by dark and illegal compliance issues. On top of this, you will also be reducing the probability of getting legal fines as well as the repercussions that are linked to them. It is crucial for hotels to cultivate a culture of only using software`s that are GDPR and PCI compliant. Regarding this, hoteliers should not merely believe software vendors until they see these systems in action and try to establish whether they provide all the necessary compliances.

mycloud HOSPITALITY

5 STEPS TO PCI AND GDPR COMPLIANCE

PCI Compliance Steps

1) Limit the User Rights of Guest Data

When it comes to user rights, it is imperative that boundaries are set up in order to govern the number and kind of people that will have access to guest data. In most PCI compliant systems, there is an option of adding certain user rights levels. This is done to enable the hoteliers to see to it that the only people that have the power to access this data are staff members that are responsible for handling credit card data.

2) Offline Storage of Details Pertaining Credit Cards

For a hotel to adhere to the proper PCI compliance standards, it is of essence for the hotel to also take into account the storage of non-digital data. The hardcopy documents that store credit card details and guest data should also be stored securely and have strictly regulated access as mentioned above.

3) Online Transaction Codes

There are times when you are in the process of accepting digital transactions and there arises a need for extra verification from the card holder which is otherwise referred to as the CVC code. The only time that you are allowed to request your guests to provide you with this code is when you comply to PCI-DSS rules.

4) Encrypt any Data

It is important for you to see to it that the website you will use to inquire about your guests` credit card data is secure (https://). In the event that you store guest cards, you should see to it that the cards` numbers are encrypted and complete data is not stored in one place. Instead, you should split it up in order to ensure that there is no easy access to it.

On top of this, you should secure your primary network and warrant that it gets audited on a regular basis. Also, you should make sure that you have placed network firewalls in your hotel systems and secured all ports.

mycloud HOSPITALITY

GDPR Compliance Steps

1) Understand the Law

The hotelier should always be aware of the hotel`s obligations according to the set GDPR rules. All these obligations should be in regard to the processing, collection and storage of data.

2) Create a Map

You should then create a framework that you will use to perform discovery of information and enable the documentation of details such as; decisions, research findings and also the risks that come with being in possession of such data.

3) Find Out Which Data Should Be Regulated

You should then determine the information that should fall under the special GDPR categories. This should be followed by classifying the people that have authorization to access the various types of data, the people that are allowed to share the data and the type of applications that are authorized to process the data.

4 Risk Mitigation

You should ensure that your hotel assesses the various risks to security and privacy that could hurt your clients. This should then be followed up by demonstrating that you are mitigating them. This can be achieved via:

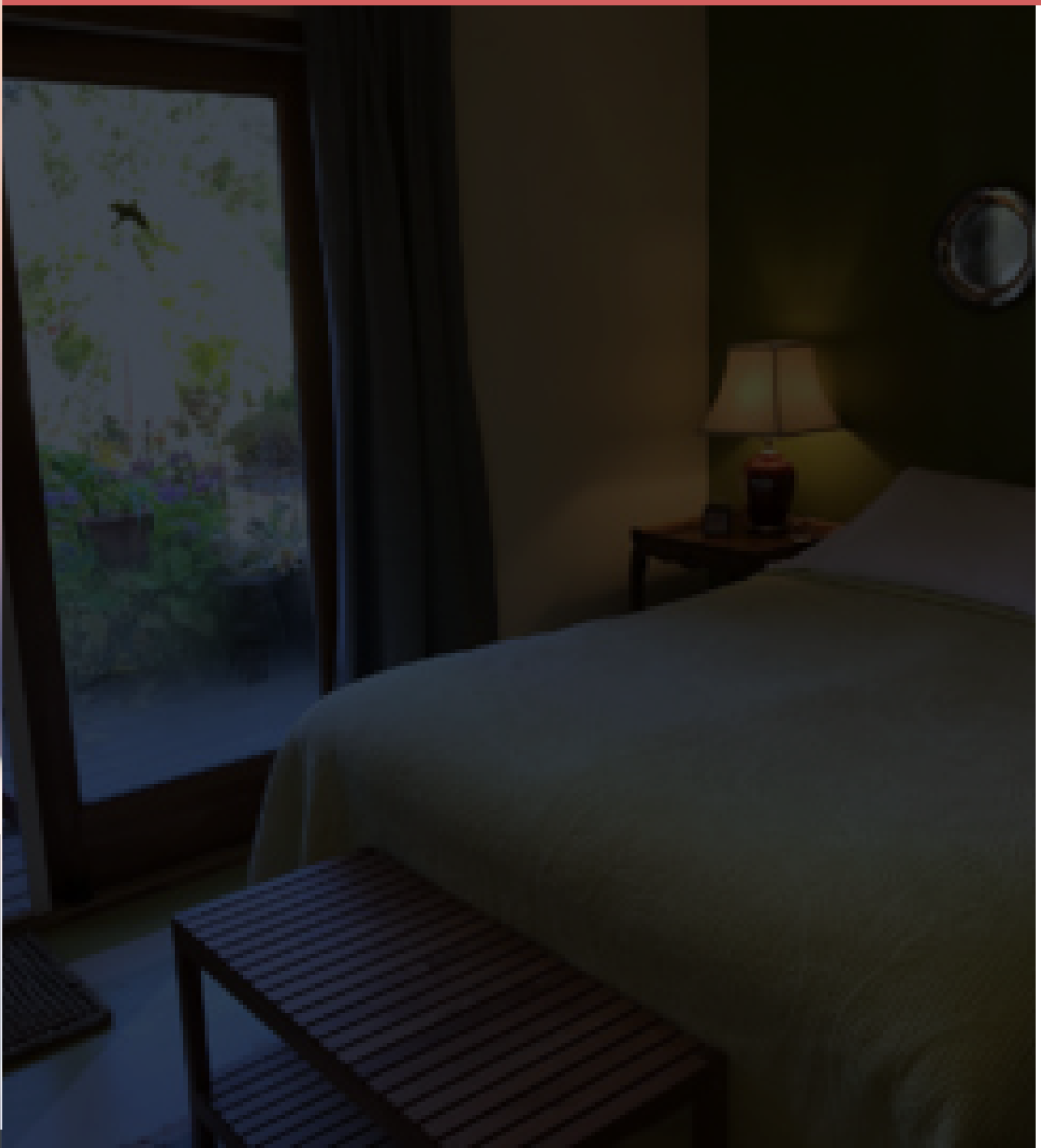
- Conducting a complete risk assessment exercise
- Implement foolproof measures to demonstrate and assure compliance
- Proactively assist partners and third-party customers to comply
- See to it that you ask guests for opt in for all communications while asking for phone numbers and emails.
- Provide guest access to request for their data and provide same in least amount of time.
- Make sure that your software is GDPR compliant and provides you with an option of anonymizing guest data.
- Store logs of all communications and whenever communication preferences are changed or information is deleted.

6

CONCLUSION

It is true that PCI DSS and GDPR are two entirely separate and different standards of compliance. However, it is vital to note that both of them are primary intersections which warrant deep scrutiny of the security of a client`s personal information as used by various industries such as hotels.

In order for a hotelier to ensure that he/she is developing a foolproof approach to GDPR compliance, it is vital for them to hire professionals in this industry such as technology vendors. Above is an in-depth insight on all the aspects that you need to know about ensuring that your hotel is tailored to meet all the GDPR and PCI compliance standards.



Overall, I am pleased with mycloud PMS and e-distribution solution. With a small operation, it is critical that our rates and availabilities are kept intact and with 'mycloud' we have succeeded in doing this. 'mycloud' is doing the job that it is supposed to and I am happy with it. I am also pleased to mention that I have been able to customize the booking engine as per my choice and it helps me a lot in getting direct bookings, thus saving us the commissions that we pay to third parties, mycloud is showing us its worth."

https://www.wisteriaguesthouse.com/

LEN (Owner)

mycloud HOSPITALITY

About mycloud hospitality

mycloud was developed by Prologic First, an independent, private company with over a decade and a half's experience delivering end to end technology solutions to the hospitality industry across the UK, Asia, Africa and the Middle East. One of the biggest barriers to adoption and usage that legacy systems face is the license and implementation cost which can run into thousands of pounds and is a big deterrent for hotels in adopting new technology. Looking at the current trend in technology in the hospitality sector, cloud computing is considered to be the biggest disruptive technology and changer. We you with an easy to learn, state of the art integrated solution for your hotel management needs as well as providing an online presence at a much lower cost. In fact, mycloud may very well be at a lower cost than the cost of maintaining your legacy systems when you also take into account the loss of revenue due to errors and inefficiencies to which legacy systems are prone.

Schedule a Hotel PMS Demo

(Our online demo takes about 30-60 minutes and you would need a desktop or laptop with microphone, speakers and Internet connectivity. Time shown here is in EST (Eastern Standard Time, -5:00 GMT)

***Award-winning hotel solution** by financesonline.com, hotel owner technology 2017, softwaresuggest.com, softwareadvice.com & getapp.com with capability user rating by 4.39.*

Resources:
http://www.traveltripper.com/blog/hotel-data-security-understand-the-difference-between-pci-and-pii-compliance/

mycloud HOSPITALITY