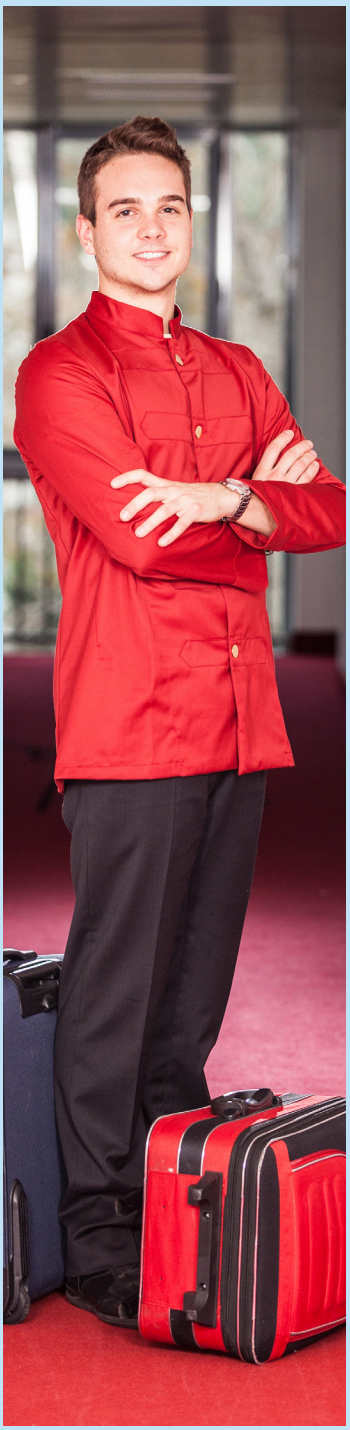
VIEW POINT

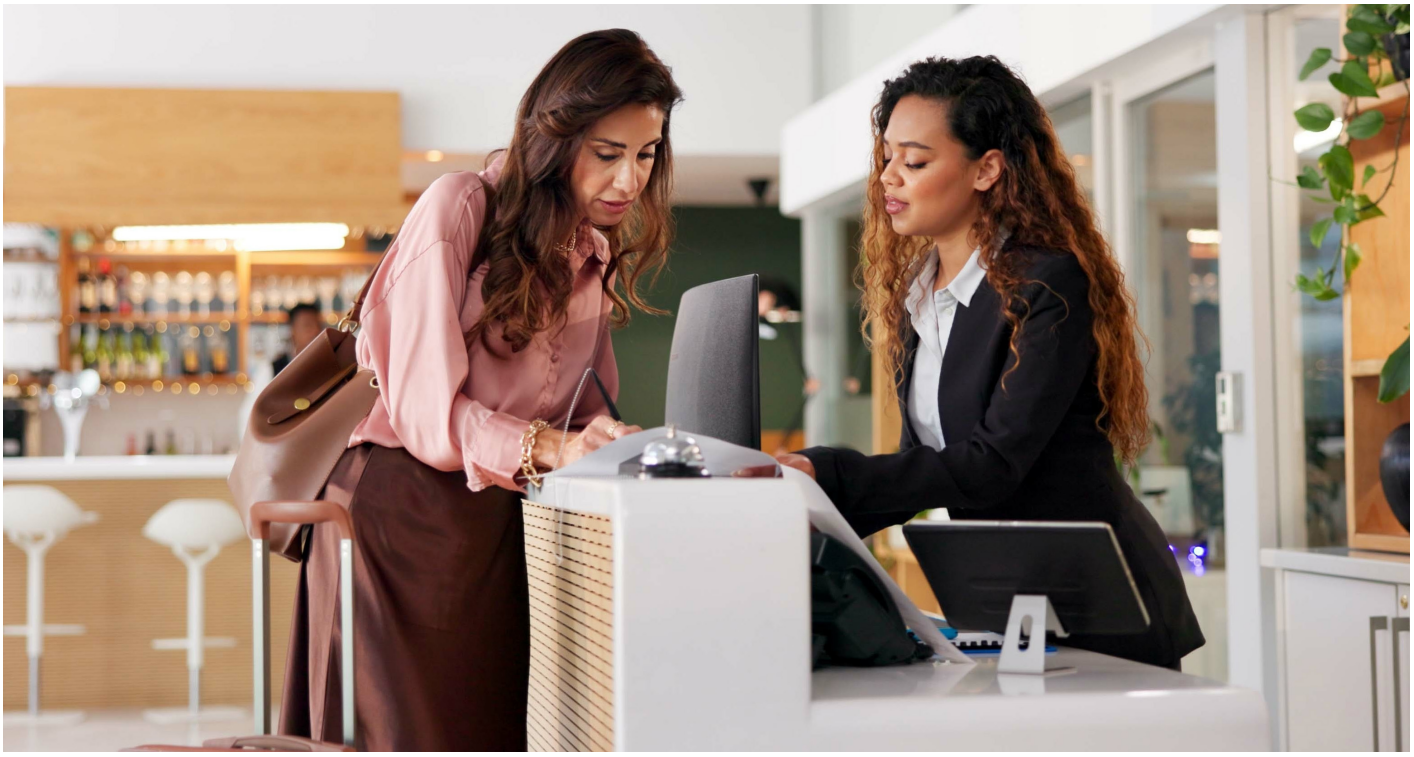


BALANCING DATA PRIVACY WITH PERSONALISATION IN HOSPITALITY

Abstract

Personalised customer service in the hospitality industry serves to build relationships, drive loyalty, and outdo the competition. To do so, hotels collect guests' dining, room, travel, check-in, and check-out preferences, and several other forms of personal data. They use it to tailor the guest experience and run analytics on a larger dataset to optimise service delivery. However, ensuring the security of data and guest privacy is crucial in this process. The hospitality industry must use the technology, systems, and methods to find the right balance between personalisation and privacy.

Infosys®
Navigate your next



Rapid technological advances and innovations are driving operational efficiency, better customer experience, and personalisation in hospitality. However, it also accompanies unique challenges, one of which is ensuring data privacy and security without compromising personalisation.

According to a report by a leading management consulting company, 71% of customers want a personalised service across industries, and 61% are willing to spend more for it. In general, data privacy is essential, and 85% of the customers want to know the company's privacy and data protection policies. By managing their concerns proactively, hoteliers show their commitment towards data privacy in the hospitality industry.

This article discusses service personalisation in the hospitality sector, why the data is prone to cyber-attacks, ways to personalise services, privacy by design, and the steps you can take to honour hotel guest privacy rights.

71%

Customers want a personalised service across industries.

61%

Customers are willing to pay more for personalised services.

85%

Customers want to know the company's privacy and data protection policies.

Why is customer data in hotels prone to cyber-attacks?

Customer data in hotels contains Personally Identifiable Information (PII), such as date of birth, passport numbers, phone numbers, addresses, credit card numbers, and travel and shopping patterns. Luxury hotels that receive high net worth guests are highly prone to cyber-attacks because of the potential to sell this data at a higher price. This makes hospitality data ripe for cyber-criminals. Reports show that 89% of hospitality businesses face multiple breaches in a year.

Another study shows that 65% of five-star hotels have witnessed identity theft, and 12% have faced debit card or credit card fraud. To protect guest interests and to continue personalising the service, 83% of hospitality businesses have allocated 4% to 20% of their IT budget to cybersecurity.

89%

Hospitality businesses face multiple breaches in a year.

65%

Five-star hotels have witnessed identity theft.

12%

Customers have faced debit card or credit card fraud.

Balancing personalisation and data privacy in the hospitality industry

The statistics above show that customers want personalisation in hospitality and are willing to pay more for the service. However, data security is their concern, and by collecting too much information or tracking the customer's location, you can push them away.

These practices can come across as an infringement on the guest's right to privacy. According to research, 55% of respondents fear that their data will fall into the hands of fraudsters and 30% worry about foreign governments and advertisers. Collecting data without transparent policies and customer consent can spoil a hotel's reputation rapidly. Hotels should collect data only to the extent necessary to provide personalisation while respecting the guests' boundaries.

Lastly, the more data a hotel collects, the more susceptible it becomes to cyber-attacks. Integrated digital environments that connect systems such as the CRM, Point-of-Sale (POS), and booking front-end have multiple points that a cyber-criminal may compromise. This reinforces the need to balance personalisation and data privacy in the hospitality industry.

55%

Respondents fear that their data will fall into the hands of fraudsters.

30%

Respondents worry about foreign governments and advertisers.

How to personalise hospitality service while maintaining guest trust?

If a hotel assures the guests that their data is safe, they will have no apprehension about sharing it. Here are some of the ways to reassure them:

Allow the guests to choose what they want to share

Informed consent and transparent communication establish trust with the customers. The process to get guest consent for collecting data should be simple. It should state the purpose of collecting and the process of handling the data.

Once the guests know that their data is secure, they feel comfortable to share it with the hotel. As part of the consent, the hotel must provide an option to opt in or out to demonstrate their commitment towards the guests' privacy preferences. Guests can also tailor or choose the information they wish to share and that which they want to withhold.

By following this practice, the hotel builds and maintains a strong reputation for data protection and guest privacy while ensuring personalised services.

Use anonymous guest data

Anonymous data is devoid of PII to protect the guests' privacy. This data helps hotels understand broader trends and preferences. By understanding the client pool better, you can offer personalised customer service in the hospitality industry. Examples of anonymous guest data are:

Room preferences

Use anonymous data to understand the room preferences, such as the category, bed type, view, and temperature according to the season and guest nationality. Using this data, you can assign the rooms based on the guest's past choices and provide a tailored experience as they check-in.

Tailored recommendations and amenities

Based on the guest's information, you can provide recommendations such as restaurants, tourist attractions, and activities in the city. You can deliver this through targeted messaging, an in-room digital information guide, or through email/mobile apps. This information can also help you provide personalised services such as sparkling instead of still water, extra towels, specific beverages in the refrigerator, etc.

Easy check-in and check-out

Anonymous guest data helps hotels streamline the check-in and check-out process. For example, if too many guests are raising complaints about delayed billing, the hotel can clear this bottleneck by optimising the process.

Personalised Offers

Through emails and mobile apps, the hotel can push personalised offers, such as discount coupons on spa treatments, preferred dining experiences, and room types. This leaves a customer delighted and builds long-term loyalty.

The balancing act is about finding the sweet spot where you provide personalised service without violating guest data privacy in the hospitality industry.

Avoid data collection through excessive guest tracking

It can be tempting to over-personalise the hospitality services by collecting excessive guest data. However, rather than building trust, it can leave the customer feeling spooked, irritated, and betrayed. For example, a digital room key that tracks a guest's location in the hotel and sends offers on WhatsApp based on their whereabouts would make them feel spied on.

According to a study, 74% of respondents perceive push notifications as invasive and a violation of their privacy. Hotels can improve their personalisation efforts by regularly gathering guest feedback and measuring it against their data privacy metrics. This helps create a balance between personalisation and data privacy in the hospitality industry.

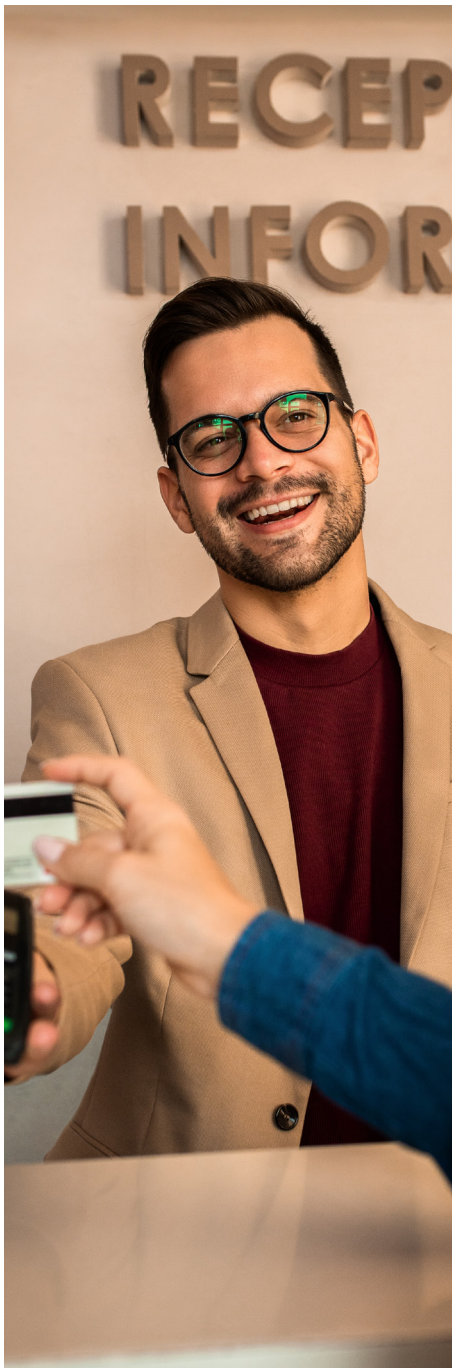
Privacy by Design

This approach considers data protection and privacy an essential component right at the outset rather than an afterthought. It builds data security and privacy practices into the system and process, making it a part of day-to-day operations.

For example, various data management policies, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), govern different geographies. By building these policies into the system at the design stage, you can manage how long you retain guest data. You can also protect it better from cyberattacks and unauthorised access.

Steps to improve customer data privacy in the hospitality industry

To proactively mitigate the risk of privacy violations, hotels must plan for and prevent security incidents. These best practices help the hospitality businesses personalise service while protecting customer data.



Data Governance

A comprehensive data governance framework has well-defined policies for data collection, processing, and storage. It establishes robust access control and limits the number of people with the credentials. Effective data governance can enhance data security and ensure transparency, compliance, and privacy. It supports responsible data management for guests.

Data Encryption

Cybersecurity protocols such as multifactor authentication protect personal data during storage and transmission from breaches and unauthorised access. A software and cloud infrastructure that follows the Payment Card Industry Data Security Standard (PCI DSS) and GDPR compliance for hotels safeguards personal and sensitive guest information.

Staff training

According to a study, 77% of organisations perceive a need for better training and qualification for their staff. Employees play a crucial role in implementing data security because they handle a guest's data and must undergo regular training on the critical aspects of privacy. The training may include mock security audits and simulation of use cases.
As hotels move towards a unified ecosystem for greater efficiency, personalisation, and seamless guest experience, they can consider uniform data formats and security protocols to ensure interoperability and ease of staff training.

Onboarding a trusted technology partner

Digital solutions and technologies are pivotal for providing personalised customer service in the hospitality industry. Examples include keyless room access, IoT-based sensors, artificial intelligence (AI), analytics, and machine learning (ML).
The hospitality industry must engage with the solution provider on using systems that comply with security standards. Additionally, the solution provider needs to provide an adequate training plan for the staff to safeguard the integrity of guest data.

Conclusion

While guests appreciate personalised customer service in the hospitality industry, they also expect the business to respect their privacy and honour data security. It is the responsibility of the business to walk the tightrope and strike a balance in partnership with a trusted travel and hospitality digital transformation partner.

This is not only an ethical obligation but also crucial for building a brand reputation in a competitive market. Comprehensive personalisation strategies that blend with guest data privacy drive repeat business and put you several steps ahead of the competition.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next