



# WHY AIRLINES AND HOTELS CANNOT AFFORD TO IGNORE BIOMETRIC DATA PRIVACY LAWS

## Abstract

Biometric technologies are transforming travel and hospitality by enabling faster, safer, and more personalised experiences. However, this shift raises critical concerns about the ethical use of biometric data and associated biometric data privacy laws. Airlines and hotels must adopt ethical, transparent practices and comply with evolving regulations to harness innovation while protecting guest trust, security, and legal standing.

The travel and hospitality industry is under growing pressure to deliver speed, security, and seamless guest experiences. Biometric technologies – facial recognition, iris scans, and fingerprinting – have emerged as game changers, eliminating lengthy documentation checks, slashing wait times, and reducing fraud. From automated airport check-ins

to smart hotel room access, biometrics are transforming travel. The travel and hospitality industry is set to generate a major chunk of revenue from biometric digital identity technologies. However, this transformation also brings risks. For example, rapid adoption places a heavy responsibility on businesses to comply with biometric data privacy laws.

As convenience increases, so do concerns around data misuse, surveillance, and regulation. Ignoring the evolving legal landscape could cost companies more than reputational damage; it could result in severe penalties and loss of customer trust.

## Biometric identity in practice in the travel and hospitality industries

Biometric technology has gained serious momentum across travel and hospitality, with the push for contactless services post-pandemic, combined with rising fraud and identity theft, accelerating the adoption. Guests and travellers now prioritise hygiene and minimal contact. Biometric systems such as facial recognition and iris scanning reduce physical touchpoints, making them ideal in a post-COVID world,

while also delivering faster services. They also provide a more reliable and secure way to verify identity, mitigating fraud risks. Moreover, convenience is no longer a value-added but an expectation. Whether skipping queues during check-ins and check-outs or unlocking hotel rooms with a face scan, biometric tech enhances personalisation and efficiency. Oracle's

Hotel 2025 report found that 62% of consumers believe their experience would improve with biometric services, while 41% said they would visit more often if these were available. However, these systems collect vast amounts of personal data, making adherence to biometric data privacy principles essential to avoid potential breaches and associated legal backlash.

As the adoption of biometric technologies continues to grow, here are some of the most common use cases of biometric identity transforming the travel and hospitality industry:



### Streamlining check-ins

Whether at a hotel or an airport, biometric systems allow travellers to breeze through the check-in process. Facial recognition kiosks can verify identity in seconds – without the hassle of verifying paperwork – and cut queues.



### Strengthening surveillance and access security

Security checkpoints at airports leverage biometrics to monitor unauthorised access and track suspicious activity. However, this can raise serious privacy concerns if stringent legal frameworks are not in place for data management.



### Simplifying hotel access

Hotels are using biometrics for keyless room access and simplifying access to hotel amenities. This creates a seamless experience, especially for digital-native travellers.



### Enhancing workforce management

Biometrics streamline staff attendance, tracking, and payroll by eliminating manual logging and proxies. However, storing and handling such data requires transparency and compliance with [biometric data regulations in hospitality](#).



### Streamlining reservations and bookings

Integrating biometric technologies with booking platforms links guest profiles to preferences, enabling faster, personalised bookings while reducing the risk of fraud. This ensures smooth transactions and operational efficiency but requires ethical data handling to enhance guest trust.

Some of the real-world examples of biometric identification systems making an impact are:



**Hamad International Airport (Qatar)** uses iris recognition at immigration and security checkpoints, speeding up passenger processing while tightening border control.



**Disney Experiences** uses fingerprint and facial recognition to streamline guest tracking and simplify billing across their properties.




**Canadian airports** employ iris scans to authenticate airport staff and limit access to secure zones, enhancing safety without slowing operations.


These use cases demonstrate the potential of biometric data, but they also underline the need for clear governance and a delicate balance between convenience and transparency. As more travel operators embrace these tools, airlines and hotels must not overlook the implications of biometric privacy laws.

## Benefits of biometric identity technologies for airlines and hotels


Biometric identity technologies are playing a pivotal role in digital transformation in travel, offering efficiency, security, and personalisation at scale. The key benefits it can offer include:

**Speeding up service delivery**


Biometrics enable faster check-ins and identity verification, eliminating manual documentation.

**Scaling with flexibility**

Unlike traditional ID systems, biometric platforms can scale rapidly across regions and functions, adapting easily to varying demands without costly overhauls.

**Boosting employee engagement**

Biometric-based workforce management reduces manual input and human error, allowing employees to focus on guest interactions and improving morale and service quality across operations.

**Reducing operational costs**

Biometrics reduce manual processes and fraud-related losses, lowering labour costs and delivering higher ROI while maintaining high service standards.

**Strengthening security**

Real-time identity verification ensures dynamic risk management and enhances accountability, building trust among guests and regulators alike.

**Delivering personalised experiences**

Linking biometric data to guest profiles enables tailored services, allowing hotels to recognise returning guests and offer customised amenities. Such personalisation fosters loyalty, a key source of competitive advantage in hospitality.



### Maximising guest convenience

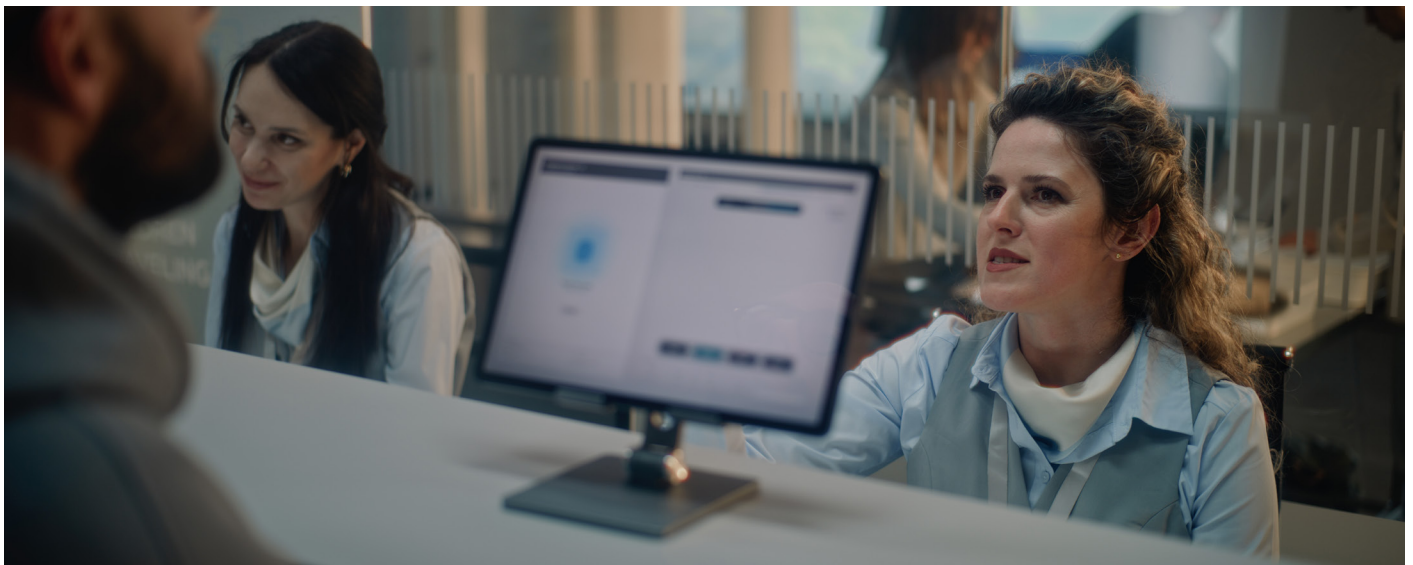
Eliminating the need for physical documents or keycards ensures a seamless travel journey, creating effortless and convenient experiences for the guests.

However, as adoption increases, so does the importance of operating within the boundaries of biometric data privacy laws. Without a clear compliance framework in place, legal and ethical pitfalls can overshadow the advantages of biometric data.

## Importance of biometric data privacy

Although biometric technology drives efficiency, it also raises serious ethical and legal concerns. This makes biometric data privacy a fundamental concern for any organisation in the travel and hospitality industry. As biometric technologies become mainstream, failing to align with biometric data privacy laws could result in reputational damage, regulatory penalties, and loss of customer trust.

Some of the key concerns businesses must address to safeguard themselves and their customers are:



### Navigating the data broker ecosystem

People often expect that their biometric data will stay where they have shared it. But that is often not the case, and data brokers can share it – directly or indirectly – with third-party vendors, analytics firms, and service providers. This creates a hidden data economy that raises questions about informed consent and the ethical use of biometric data. Without strict adherence to biometric data regulations in hospitality, businesses may unintentionally contribute to the exploitation of personal identity data.



### Addressing human rights in the digital age

Unethical use of biometric data – like biometric surveillance – can infringe on individuals' rights to privacy, freedom of movement, and freedom from discrimination, raising human rights concerns. This risk is even more pronounced in travel settings – where people are already vulnerable. Airlines and hotels must build systems based on regulatory frameworks like the GDPR and the EU AI Act to honour human dignity, not just for compliance with biometric data privacy laws.



### Prioritising guest privacy

Many contemporary biometric systems lack effective opt-in and opt-out mechanisms. Guests and travellers often do not fully understand what they are agreeing to or how the businesses will handle their data. Without transparent policies and consent protocols, even well-intended businesses can violate biometric data privacy laws and risk alienating customers and facing fines.





### Mitigating bias and discrimination

Biometric systems can inadvertently perpetuate bias as facial recognition technologies often perform unequally across age groups, genders, and ethnicities. This can result in false positives, discriminatory practices, or exclusion. Rigorous testing and inclusive design are critical, especially for hospitality brands that serve a global and diverse customer base.

In response to these risks, global bodies like the World Travel and Tourism Council (WTTTC), International Air Transport Association (IATA), International Biometrics + Identity Association, and World Economic Forum are shaping



### Preventing security vulnerabilities

Biometric systems are more vulnerable to attackers, and breaches can be catastrophic. Breaches involving facial scans or fingerprints are far more damaging than those involving usernames and passwords. Once compromised, it is impossible to reissue biometric credentials. This makes investment in encryption, secure storage, and access to protocols essential.

the guidelines for ethical biometric use. Biometric data regulations in hospitality are also growing more complex, with GDPR, the EU AI Act, and the US's Illinois Biometric Information Privacy Act (BIPA) setting strict restrictions on how



### Tackling emerging threats

The future also brings new threats. Deepfake technologies can mimic facial data, while spoofing tools can trick biometric sensors. Geopolitical concerns also emerge when it comes to data control, with some systems outsourcing processing to countries with weaker privacy laws. This can lead to what experts call “data colonialism”, which demands a proactive, globally aware approach to biometric data privacy.

businesses collect and use biometric data. Businesses must navigate these overlapping frameworks to stay compliant with biometric data privacy laws while leveraging biometrics to enhance guest experience.

## Future of biometric identity in travel and hospitality



The future of biometrics in travel and hospitality is bright, provided businesses navigate the risks responsibly. The demand for secure, seamless, and personalised travel will only grow, and organisations

must strike a careful balance between innovation and accountability. Complying with biometric data privacy laws is just a start. Placing biometric data privacy at the core of operations can help airlines

and hotels harness biometrics to deliver seamless, secure, and personalised experiences to today's digitally aware travellers. This includes:



### Building a responsible biometric ecosystem

Ethical practices like explicit consent, robust opt-out mechanisms, and privacy-by-design must guide all biometric data use.



### Turning compliance into a strategic asset

Leading with compliance can help businesses build trust, reduce legal risk, and stay ahead of regulations.



### Cautiously embracing the upside

The benefits of biometrics are clear, but businesses must prioritise biometric data privacy to effectively balance convenience with customer trust.

## End note

Biometrics are revolutionising travel and hospitality, offering speed, security, and personalised experiences for enhanced customer satisfaction. However, as these technologies drive efficiency and guest satisfaction, biometric data privacy has become non-negotiable. Compliance with biometric data privacy laws mitigates risks like data breaches and unconscious bias, ensuring customer and regulator trust. By embracing ethical data use practices, airlines and hotels can unlock the full potential of biometric data. The future of travel and hospitality will demand innovation balanced with responsibility and will belong to those who treat data privacy not as a hurdle but as a cornerstone of responsible innovation.

For more information, contact [infosysbpm@infosys.com](mailto:infosysbpm@infosys.com)

**Infosys**<sup>®</sup>  
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.