India's Digital Personal Data Protection Act, 2023 | Impact on Hospitality Sector

---

The hospitality sector, encompassing restaurants, hotels, and other hospitality establishments, is no stranger to handling vast amounts of personal data. From guest information, employee data to transaction records, this sector deals with a plethora of sensitive information on a daily basis. With the implementation of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") in India, the hospitality sector is presented with new challenges and opportunities for enhancing data protection practices. This article delves into how the hospitality sector can ensure compliance with the DPDP Act, considering its complex ownership structures and diverse data management systems.

One of the unique challenges in the hospitality sector is its intricate ownership structure. Restaurants, hotels, and other establishments often involve franchisors, individual owners or groups of owners, operator/management companies. Each entity may use separate systems to store and manage personal data, leading to the complex movement of information across these systems. This complexity can create vulnerabilities in terms of data protection.

Data Breach: A Costly Lesson

In its inaugural year, the European Union's General Data Protection Regulation (GDPR) recorded 281,000 reported cases, potentially subjecting companies to fines of up to €20 million or 4% of total worldwide annual turnover of the preceding financial year, whichever is higher.

An exemplary instance involves a prominent international hotel chain, which faced grave repercussions due to a data breach originating in 2014 but only detected in 2018. The breach compromised sensitive information, like credit card details and passport numbers, of over 300 million guests stored within the global guest reservation database of a brand acquired by this hotel chain.

This incident ranks among the largest data breaches in history, serving as a vivid reminder of the hospitality sector's susceptibility to risks. It underscores the criticality of data protection in this sector. To avert such consequences within the Indian hospitality landscape, businesses must proactively shield personal data from unauthorized access, usage, disclosure, and destruction by adhering to the provisions of the DPDP Act, the Information Technology Act, 2000, along with its rules and regulations, as well as follow directives from the Indian Computer Emergency Response Team (CERT-In) regarding "cybersecurity incidents" reporting obligations.

Applying the DPDP Act to the Hospitality Sector

The DPDP Act brings a significant shift in how personal data is managed and processed in India. Key features of the legislation, such as itemized notice, informed consent, purpose limitation, data processing

principles, and rights of data principals[1] (akin to 'data subjects'), impact every sector, including hospitality. Given the DPDP Act's prioritisation of itemized notice and consent as the fundamental foundation for data processing, enterprises within the hospitality sector must ensure the transparency of their data collection and processing methods. It is imperative that guests, employees any other entity from whom personal data is collected ("**Information Providers**"), are provided with comprehensive information regarding the utilisation of their data.

While many global hospitality businesses adhere to data protection laws like GDPR, this alone may not fully address handling Indian data principals' personal data. Notable differences between GDPR and the DPDP Act warrant a separate review of practices to ensure compliance with the latter.

There are several challenges posed by the complex ownership structures and data management, owing to which businesses in the hospitality sector need to take a holistic approach to data privacy compliance. This includes:

- **Fiduciary vs Processors** – The DPDP Act recognizes data fiduciaries[2] (akin to 'data controllers') and processors[3]. Data fiduciaries bear liability for DPDP Act compliance including in case of processing carried out by data processors on their behalf. In complex ownership scenarios, such as in hospitality, where ownership and operation entities differ, the entity determining processing purpose might not be the one executing it, necessitating clear responsibilities and agreements. Therefore, demarcating data fiduciaries and data processors within the structure and ensuring their DPDP Act compliance, especially through robust data protection agreements between such entities is vital.

- **Extraterritorial Applicability** - The DPDP Act has limited extra-territorial applicability and will extend to processing of digital personal data outside India, if such processing is in connection with an activity related to offering of goods or services to data principals within India.

- **Privacy Policies**: Given the interconnected nature of data flow within the hospitality sector, it is essential to establish privacy policies that all entities within the ownership structure adhere to. This ensures consistency in data handling practices and helps in complying with the new legislation's transparency requirements.

[1] The term "data principal" is defined under the DPDP Act as '*the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf*'

[2] The term "data fiduciary" is defined under the DPDP Act as '*any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data*'

[3] The term "data processor" is defined under the DPDP Act 'as *any person who processes personal data on behalf of a data fiduciary'.*

- **Data Mapping and Audit:** Businesses are required to conduct a thorough data mapping exercise to identify all touchpoints where personal data is collected, processed, and transferred. Regular data audits can help identify potential gaps in compliance and improve data protection measures. In fact, the DPDP Act mandates undertaking of data protection impact assessments for a certain class of data fiduciaries denoted as significant data fiduciaries.

- **Notice and Consent Mechanisms:** Implement clear and comprehensive notice and consent mechanisms as per the DPDP Act that provide Information Providers with a detailed understanding of how their data will be used. Consent should be freely given, specific, and informed, aligning with the DPDP Act's requirements. Once consent is obtained for processing of personal data for a specific purpose, businesses need to ensure that the same is not used for any other purpose. For instance, a leading hospitality business in France faced penalties due to GDPR violations. Their pre-checked consent box for newsletters was deemed invalid, and sending newsletters with unrelated services (for e.g., offers from third party partners) not limited to services 'analogue' to those already provided for the mentioned customers (hotel services) breached consent principles. This highlights the importance of accurate consent collection and purpose limitation.

- **Children's data** - Guests also include individuals under 18 years and in such cases, businesses need to ensure that secure 'verifiable consent' from parents or lawful guardians prior to data processing is obtained. Processing data that might harm a child's well-being is prohibited. Additionally, businesses need to refrain from tracking children's behavior or directing targeted ads at them as per the DPDP Act.

- **Data Security Measures**: With the DPDP Act's emphasis on data security, hospitality establishments must implement robust technical and organizational measures to safeguard guest information. Encryption, access controls, and regular security assessments are crucial to prevent data breaches. Businesses will also have to inform each affected individual in case of a personal data breach. Notably another leading hotel chain has been fined in the past *inter alia* for not disclosing information about breaches by the New York Attorney General.

- **Rights of Data Principals:** The DPDP Act grants data principals various rights, including right of grievance redressal, right of access, correction, updating and erasure of their personal data. The DPDP Act has also introduced the novel concept of 'consent managers' who will be persons acting as a single point of contact to enable data principals to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform. Hospitality businesses must establish efficient processes to address Information Providers' requests related to these rights and liaise with such consent managers.

- **Cross border data transfer** - In the global hospitality sector, data often moves across borders. The DPDP Act allows this, except to government-restricted territories. Businesses should prepare to relocate data from potential blacklisted territories and cease transfers there. If another law provides stronger data protection or transfer limits than the DPDP Act, it takes precedence. This applies notably to payment systems data, where regulations like the Reserve Bank of India's data localization mandate will supersede the DPDP Act.

The DPDP Act imposes substantial responsibilities on data fiduciaries in the hospitality sector. Businesses must proactively adopt appropriate technical and organizational measures to uphold data principal rights, ensuring compliance and avoiding significant penalties. Data protection is a shared responsibility and therefore all employees, trainees etc. from front-line staff to management, must be well-versed in the DPDP Act's provisions and the organization's policies. While the forthcoming rules under the DPDP Act will provide more guidance, current provisions emphasize the need for swift comprehension and alignment through thorough process review and decisive actions. With no specified transition period, organizations must begin preparations promptly.