Travel, Hospitality & Aviation

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For airlines, hotels, online travel agencies, tour operators, and visa/immigration service providers.

1. Overview & Applicability

Travel and hospitality entities collect some of the most personal information about individuals — passport details, travel itineraries, dietary preferences, health conditions, payment history, and loyalty programme data. Airlines share Passenger Name Records (PNRs) internationally. Hotels store guests' identity documents. Visa agencies process biometric and sensitive document data. DPDPA requires careful consent, strict retention limits, and clear cross-border data transfer policies.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Passenger Name Record (PNR)	Name, travel dates, seat, meal preference, contact details, payment — shared with international authorities.
Passport Data	Full name, nationality, date of birth, passport number — highly sensitive identity data.
Biometric Data	Fingerprints and facial scans collected for visa applications and airport immigration — sensitive data.
Loyalty Programme Data	Tier status, travel history, preferences — builds a rich personal profile.
Health Data	Dietary restrictions, medical conditions, special assistance requests — sensitive health data.
Cross-Border Transfer	PNR data shared with foreign immigration authorities — subject to approved country restrictions.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1	**Booking Consent** At booking, separate the consent for reservation processing from consent for marketing, loyalty programme enrolment, and analytics. Do not bundle all into a single checkbox.
2	**Passport & Identity Data** Minimise passport data — collect only what is legally required for the booking. Delete or securely archive after the journey. Encrypt all identity document stores.
3	**PNR Sharing** International PNR sharing with immigration authorities is a legitimate use — but document the legal basis and disclose in your privacy notice.
4	**Hotel Guest Data** Guest identity documents collected at check-in must be secured, accessed only by authorised staff, and deleted per hotel policy and government retention requirements.
5	**Health & Dietary Data** Meal preferences and medical conditions are sensitive — use only for the stated purpose (flight catering, accessibility). Do not share with third parties without consent.
6	**Visa Service Providers** Biometric data collected for visa applications must be processed strictly per the diplomatic mission's requirements and deleted

	thereafter.
7	**Travel Insurance** Health and travel data shared with insurers requires explicit consent — separate from booking consent.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all booking data flows — what is collected, stored, shared with airlines, hotels, car rental, insurance partners.
- ☐ Separate booking consent from marketing consent at all online and offline booking points.
- ☐ Implement encrypted storage for passport and identity documents across all booking systems.
- ☐ Review PNR sharing protocols with international authorities — document legal basis in privacy notice.
- ☐ Execute DPAs with airline GDS systems, hotel property management systems, and payment processors.
- ☐ Build a traveller rights portal — allow guests to access booking data, loyalty history, and request deletion.
- ☐ Appoint a Grievance Officer and display contact details on your website and at check-in counters.
- ☐ Implement retention schedules for guest data — delete identity documents after regulatory hold period.
- ☐ Review cross-border data transfers to international airline partners, hotel chains, and GDSs.
- ☐ Train front desk, call centre, and reservations teams on guest data handling and rights requests.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Data Map** Map all traveller data across booking, check-in, stay/journey, and post-travel stages.
2	**Month 2: Consent Redesign** Redesign booking flows to separate transactional, loyalty, and marketing consent.
3	**Month 3: Document Security** Implement encryption for all identity and passport data stores.
4	**Month 4: Partner DPAs** Execute DPAs with GDSs, OTAs, airlines, and payment gateways.
5	**Month 5: Traveller Rights** Build rights portal and grievance mechanism.
6	**Month 6+: Review** Annual PNR sharing and cross-border transfer compliance review.

✈ PNR data shared with foreign governments must be disclosed in your privacy notice. International data transfers require the destination country to be on the approved government list.

Disclaimer: *This handbook is for awareness and informational purposes only. It does not constitute legal advice. Please consult a qualified data protection lawyer for specific compliance guidance. | DPDPA 2023 · India*