# Automotive & Mobility

## DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

*For vehicle manufacturers, ride-hailing platforms, EV charging networks, and micro-mobility services.*

## 1. Overview & Applicability

Connected vehicles, ride-hailing apps, and mobility-as-a-service platforms generate continuous streams of personal data — real-time location, driving behaviour, trip history, payment details, and biometrics. The automotive sector is rapidly becoming a data business. DPDPA requires mobility companies to obtain specific consent for each type of data collected, allow users to control their data, and implement strong security for vehicle telematics systems.

## 2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

| | |
|---|---|
| **Telematics Data** | Speed, braking, acceleration, engine data, location derived from connected vehicle systems — personal data when linked to the owner. |
| **Location Data** | Real-time GPS location of a vehicle or driver during a ride — highly personal. |
| **Driver Behaviour Data** | Harsh braking, speeding, cornering data — used for insurance telematics and fleet monitoring. |
| **Trip Data** | Origin, destination, route, duration, and fare — personal trip record. |
| **Biometric Driver Verification** | Facial recognition used by ride-hailing apps to verify driver identity — sensitive biometric data. |
| **EV Charging Data** | Vehicle ID, charging duration, location of charging, payment — personal data. |



## 3. Core Compliance Obligations

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

1. **Connected Vehicle Consent**
   In-vehicle data collection (telematics, location, driving behaviour) requires owner consent at vehicle registration or app setup. Clearly explain what data is collected and why.
2. **Ride-Hailing Trip Data**
   Trip data (origin, destination, route, payment) is personal data. Retain only for the period necessary for billing and dispute resolution. Delete thereafter.
3. **Driver Data Governance**
   Driver personal data (PAN, Aadhaar, vehicle documents) collected during onboarding must be encrypted, access-controlled, and not shared with third parties without consent.
4. **Insurance Telematics**
   Driving behaviour data shared with insurers for usage-based insurance requires explicit policyholder consent and a DPA with the insurance partner.
5. **EV Charging Network Data**
   Charging session data must be used only for billing and network management. Anonymise for aggregate analytics. Do not share with vehicle manufacturers without consent.
6. **Driver Biometric Verification**
   Facial recognition for driver verification is sensitive. Obtain driver consent. Delete biometric templates after verification. Do not build persistent biometric databases.

| | |
|---|---|
| 7 | **In-Vehicle Advertising**<br>Delivering targeted ads inside connected vehicle infotainment systems based on location or behaviour requires explicit user consent. |

## 4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all connected vehicle data flows — telematics, infotainment, location, and driver behaviour data.
- ☐ Implement granular in-app consent for each type of data — location during ride, trip history, driver behaviour.
- ☐ Encrypt all trip and driver data in storage and transmission.
- ☐ Execute DPAs with insurance partners, fleet management platforms, and EV charging network operators.
- ☐ Build a rider/driver rights portal — access trip history, manage data preferences, request deletion.
- ☐ Implement deletion schedules for trip data — retain only for billing and dispute resolution periods.
- ☐ Obtain driver consent for biometric verification — delete templates after each verification session.
- ☐ Review insurance telematics programmes — ensure policyholder consent is obtained separately.
- ☐ Appoint a Grievance Officer and display contact details in the app and on your website.
- ☐ Train driver onboarding teams on DPDPA obligations and driver data rights.
- ☐ Conduct a DPIA for any new AI-based feature using driver or passenger personal data.

## 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: Telematics Audit**<br>Map all data generated by connected vehicles and mobility platforms. |
| 2 | **Month 2: Consent Architecture**<br>Design in-vehicle and in-app consent flows for each data type. |
| 3 | **Month 3: Partner DPAs**<br>Execute DPAs with insurance, EV network, and fleet management partners. |
| 4 | **Month 4: Driver Rights**<br>Build driver and rider data portal; appoint Grievance Officer. |
| 5 | **Month 5: Security**<br>Implement encryption and access controls for all vehicle and trip data systems. |
| 6 | **Month 6+: DPIA**<br>Conduct DPIAs for all AI/ML features using personal data. |

📍 Location data from vehicles and ride apps is among the most sensitive personal data. It reveals home address, workplace, religious attendance, medical visits, and social connections. Handle it with the highest level of care.