



## Tax alert: Policy for sharing data from National Transport Repository

**1 September 2025**

The Ministry of Road Transport and Highways (MoRTH) has published a policy for sharing data from the National Transport Repository (NTR), establishing a structured framework for transport-related data to be shared with governmental bodies, enforcement agencies, academicians, citizens and the private sector, while ensuring compliance with applicable laws and with necessary safeguards. The policy seeks to balance data sharing and compliance with data protection laws, particularly the Digital Personal Data Protection Act, 2023 (DPDP Act).

### In a nutshell



- Provides structured access to authentic transport data under a controlled and secure framework.
- Aims to promote ease of living and ease of doing business.
- Aligns with the DPDP Act, 2023 principles of purpose limitation, data minimization, and consent-based processing.



- MoRTH & State RTOs identified as Data Fiduciaries.
- Law enforcement and government agencies provided full access to data sets, subject to exemptions under DPDP Act.
- Anonymized data sets to be provided for research/academia.
- Private sector to be provided with select parameters of datasets subject to agreement and DPDP Act compliance.



- Data to be shared based on approval by MoRTH/State RTOs via API integration, portal login, bulk secure transfer, and public platform.
- Data sharing approval valid for 1 year, renewable with security audit.
- All accessed data to be processed and stored on servers located within India data must not be transferred outside India.



Scroll down to read the detailed alert

## Key highlights of the Data Sharing Policy for the National Transport Repository (Data Sharing Policy)

- **Background of the NTR**

The NTR is a unified central repository consolidating data from multiple flagship transport platforms including VAHAN (vehicle registration), SARATHI (driving licenses), e-Challan, eDAR (Electronic Detailed Accident Reports), and NETC-FASTag, thereby covering over 39 crore vehicle records and over 22 crore driver licenses and other related data.

- **Objective of the Data Sharing Policy**

The Data Sharing Policy aims to provide access to data to eligible stakeholders under a controlled and secure framework and enables *inter alia*:

- Controlled integration of external applications/systems with NTR ensuring seamless access to authentic data.
- Ease of living and doing business through streamlined digital services and improved accuracy of information.
- Align transport data governance with obligations under the DPDP Act, 2023, including principles of purpose limitation, data minimization, and consent-based processing.

- **Key Stakeholders**

### Data Fiduciary/Provider

- As per the Data Sharing Policy, MoRTH will act as the Data Fiduciary, with the overall responsibility for policy formulation, oversight, and compliance. State Transport Departments / RTOs will function as Joint Data Fiduciaries for state-level data governance.

### Data Recipients

- **Law Enforcement Agencies & Government Agencies:** Complete access to all data parameters, including Personal Data, without obtaining consent of the Data Principal as permitted under Section 7 (certain legitimate uses) and Section 17 (exemptions) of the DPDP Act. However, statutory entities will be subjected to additional security measures for sharing data.
- **Academia and Research:** Data will be shared (upon approval) in an aggregated or anonymized form and shared with academia and private sector for promoting research, innovation and business purpose.
- **Citizens or Individuals:** Select parameters of datasets can be made available to any citizen for the purpose of verification of RC or DL etc. Additionally, aggregated and anonymized data will be accessible to citizens through the open Government platform (<https://data.gov.in>) and also through public dashboards.
- **Transport Service Providing Agencies:** Agencies such as insurance providers, banking gateways, HSRP vendors, smart card vendors, third party (TP) sales and Vehicle Location Tracking Device (VLTD) vendors can receive select data parameters as required for provision of their services. Such entities are, however, required to enter into a memorandum of data compliances or an agreement with MoRTH or the State Government, on a case-by-case basis.
- **Private Sector Entities providing Authentication Services:** Select data parameters or verification/authentication will be provided depending on specific business requirement in line with promoting EOL or EODB for availing authentication services from MoRTH.

- **Modes of Sharing Data**

The policy specifies multiple secure channels through which NTR data may be accessed, depending on the category of users and type of data, such as:

- **API-based access for authorised system integration:** Entities desirous of accessing a specific set of data must submit a request in specified form to MoRTH with relevant documentation, purpose for which such data is sought, disclosing their eligibility to process the data under Section 7 of DPDP Act, execution of a memorandum of data compliances, mandate security audit certificate and log records. In such cases personal data elements will be masked for all other recipients except law enforcement agencies, government agencies, or any entity granted full access by MoRTH (subject to provisions of the DPDP Act).
- **Portal-based login for authenticated users:** Government organizations will be given access to data sets using secured credentials including two factor authentication. Private sector stakeholders can access data sets on NTR portal subject to consent of the Data Principal being obtained.
- **Password-protected bulk data sharing:** Only to be provided on exceptional basis to select organizations on one time basis. Such bulk data is to be shared through portable password protected hard disk, or a SFTP link to download data through secured network. Data shared with such select organizations will be subject to satisfaction of tenets under the DPDP Act.
- **Mobile applications for individual/citizen-level access:** Citizen/individuals can also have limited access to information on any Vehicle or Driving license through NTR portal. Only select, non-sensitive, non-personal data parameters regarding Driving License or Vehicle Registration Certificate of any citizen may be shown.
- **Public platforms:** MoRTH will make aggregated and anonymized data sets available through internal and external dashboards. Moreover, anonymized datasets will be regularly published on 'data.gov.in' for public, academic, and research use.

- **Process for Approval**

Stakeholders seeking access must submit a formal application specifying the nature of data required, purpose of processing, and compliance with the DPDP Act. Stakeholders are required to submit a memorandum of data compliance regarding

safeguards to be ensured regarding the shared data. The approved data recipient or Joint Data Fiduciary will be required to submit Website Security Certificate from CERT-IN empanelled security auditor for the application for which the required data access is being requested. Access, once granted, is typically valid for one year and renewable upon submission of an updated security audit.

- **Security and Privacy Safeguards**

At present MoRTH shares data through API and portal-based access with Data Recipients/ Joint Data Fiduciary, such as Government Departments, Enforcement Agencies etc., however, to ensure compliance with the provisions of the DPDP Act by these Data Recipient or Data Fiduciary the Data Sharing Policy lays down following guidelines:

- Data access for pan India data will be provided to Government Organizations and Enforcement Agencies upon approval from MoRTH, for State specific data approval of State authorities will be relevant.
- Data Recipient shall execute a memorandum of data compliances or an agreement with a Data Recipient or Data Fiduciary
- Completeness, accuracy and consistency of data shall be ensured before API based data sharing

- Data Recipient must submit a Security Audit Certificate issued by a CERT-IN empaneled security auditor for the application in which API access is requested.
- Where consent given by the Data Principal is the basis for processing of Personal Data and questions arise in a proceeding, the Data Recipient will be obligated to prove that a notice was given by them to the Data Principal and consent was given by such Data Principal in accordance with the provisions of the DPDP Act.
- Data Recipient to implement appropriate access control mechanisms e.g., secret keys, user-id/password authentication, IP whitelisting, token exchange to ensure that no third party can access the API through their application.
- Data Recipient are prohibited from disclosing, reproducing, selling, distributing, or transferring any shared data or Personal Data.
- Enforce strong password protection policies, including Muti Factor Authentication.
- Immediately notify MoRTH and affected individuals in the event of personal data breach.
- All accessed data to be stored on servers located within India and data must not be transferred outside India.

### **Deloitte comments**

By creating a secure and uniform framework, the policy strikes a balance between enabling innovation in transport solutions and protecting citizens' privacy. From a compliance perspective, the framework embodies the spirit of the DPDP Act.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see <http://www.deloitte.com/about> to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.