
## Introduction

The Ministry of Road Transport and Highways (MoRTH) has issued a comprehensive "Policy for Data Sharing from National Transport Repository" dated 18 August 2025 (Policy). The National Transport Registry (NTR), a centralised repository, contains a range of data in the transport ecosystem such as vehicle registration (RC), driving license (DL), FASTag details, etc., which are collected from platforms like Vahan (vehicle registration), Sarathi (driving licenses), eChallan, EDAR (Electronic Detailed Accident Report) and FASTag. The Policy notes that the NTR contains data which are personal and sensitive in nature and thus requires careful management.

Consequently, the Policy is intended to formalise data sharing protocols to meet the demand from various stakeholders, including government agencies, academia and the private sector. This Policy is a significant step in the operationalisation of India's upcoming data protection regime and an innovative effort to balance the need for data consumption by various stakeholders to promote ease of living (EOL) and ease of doing business (EODB) at the same time protecting citizens' personal data while ensuring compliance with purpose limitation, data minimisation and security safeguards under the Digital Personal Data Protection Act, 2023 (DPDP Act).

## Key highlights of the Policy

1. Key Stakeholders: The Policy identifies MoRTH as the primary data fiduciary (i.e. a person who alone or in conjunction with other persons determines the purpose and means of processing of personal data) of the NTR data and State transport departments and registering / licensing authorities under each state government are co-holders and co-data fiduciaries of state level data. Additionally, the Policy also identifies organisations that receive data from NTR as "data recipients" and are considered as data fiduciaries as defined under the DPDP Act.

2. Access to data, including personal data: Access to personal data can be provided to the following data recipients:

    a. Law Enforcement Agencies, Police, National Security Agency: will have complete access to all data parameters as required under applicable law, including Sections 7 and 17 of the DPDP Act.

    b. State Government or Union Territory (UT) Administration: will have access to complete transport data such as from Vahan, Sarathi and e-Challan of their respective state/territories. Inter State / UT transfer or data pertaining to pan-India will require approval from MoRTH and consent of the respective State to which the data pertains.

    c. Central and State Government agencies: will have complete access to data required under applicable law, including Sections 7 and 17 of the DPDP Act. Notably, statutory entities / organisations have to implement additional security measures to prevent data breaches apart from the security measures provided under Clause 6 of the Policy. Further, any sharing of data amongst States / UTs will be subject to the applicable law.

d. Academia and research entities: will have access to data in aggregated or anonymised form.

e. Citizens or individuals: will have access to their own complete data. Only aggregated and anonymised data will be accessible to citizens through the open Government platform (https://data.gov.in) and also through public dashboards. Further, MoRTH will also provide access to certain data parameters for third-party verification of RCs and DLs. Citizens may access limited, non-sensitive, non-PII details of any vehicle or driving license through the NTR portal. Access requires mobile OTP authentication and is capped at three queries per day.

f. Transport service providing agencies: will have access to datasets which are relevant to the roles of such agencies and their data needs. Agencies like insurance providers, banking gateways, HSRP vendors, etc., can seek access to data relevant to their services upon execution of a memorandum of data compliance in the format provided in the Policy or an agreement with MoRTH or the relevant State Government. These agencies will be subject to additional security measures to prevent data breaches in addition to the data security practices provided under Clause 6 of the Policy.

g. Private sector entities providing authentication services for EOL and EODB: will have access to select data parameters required for verification / authentication purposes. For example, DL as an authentication service on similar lines as the Aadhaar authentication service.

3. Purpose limitation and data minimisation: These fundamental principles of the DPDP Act have been explicitly laid down in the Policy by MoRTH. For instance, the Policy mentions that "The request should be limited to such Personal Data as is necessary for such specified purpose to ensure data minimisation" for API based data sharing or portal-based data sharing. Further, the format of application provided under Annexures I and II of the Policy requires an applicant organisation to provide purpose / justification for the data parameters requested. Additionally, as per the format for "Memorandum of Data Compliances" provided in the Policy, the applicant organisation requesting data sharing must undertake to use the shared data only for the purpose justified in their application. Clause 6 of the Policy further emphasises purpose limitation.

4. Modes of sharing data: Data, including personal identifiable information (PII) or personal data, can be shared through API, portal, secured and password-protected bulk sharing, mobile app-based or through public data sharing platforms. Personal data and PII may be provided to a data recipient after obtaining user consent by them through an Aadhaar authenticated OTP based system linked to the mobile number on the concerned portal.

5. Statutory Compliance: All data recipients have been classified explicitly as Data Fiduciaries and are subject to the provisions of the DPDP Act, including the liabilities and potential monetary penalties for data breaches or unauthorised disclosure. The shared fiduciary responsibility creates a clear legal chain of accountability that extends beyond the government to external organisations. Additionally, to access personal data or PII, service providers must obtain consent from the data principals (i.e., individual to whom the personal data relates, and in case of a child or a person with disability, includes the parent or lawful guardian). Service providers can obtain consent via an Aadhaar authenticated OTP bases system linked to the mobile number on the concerned portal. Whether accessing through API or portal or bulk data request, agencies may have to comply with additional security measures (apart from security measures under Clause 6 of the Policy) that may be imposed on them from time to time to prevent data breaches.

6. Mandatory Security, Audits and Breach reporting: A central pillar of the Policy is the mandatory submission of a yearly security audit certificate from a CERT-In empanelled security auditor. The policy mandates that the data recipient implement appropriate access control mechanisms such as secret keys, user-id/password authentication, IP whitelisting, token exchange, etc., for API integration and to prevent unauthorised access. The data recipients must also enforce private sector-standard managerial, technical, and physical safeguards to prevent unauthorised data processing or access and maintain up-to-date operating systems, robust cyber security measures. Data recipients are required to report any breach to MoRTH in addition to Data Principals and the Data Protection Board under the DPDP Act. Further, the agency is required to implement access controls, including user ID/password authentication, IP whitelisting, and similar measures, to prevent any third party from accessing the API through its application.

7. Data localisation: The Policy categorically stipulates that all accessed data must be processed and stored on servers located within India. Any cross-border data transfer or storage is prohibited.

## Conclusion

The Policy is the first of its kind introduced by a central ministry that establishes a framework for sharing data in alignment with the DPDP Act. It balances transparency, research enablement, and public utility with stringent privacy and security safeguards, aligned with the DPDP Act. Access modalities (API, portal, bulk, and mobile) are tailored per recipient category, with rigorous security practices, localisation mandates, and annual audits. Clause 6 (data security practices) stands as the cornerstone of the Policy through which the Policy intends to ensure that personal data remains protected throughout its lifecycle, under well-defined accountability and enforcement mechanisms. Notably, this Policy has not provided any charges or fees that the data recipient is required to pay to access data from the NTR.

- Harsh Walia (Partner), Supratim Chakraborty (Partner), Shramana Dwibedi (Senior Associate) and Aadarsh Prakash (Associate)

## About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com