सड़क परिवहन और राजमार्ग मंत्रालय

Ministry of Road Transport and Highways

सत्यमेव जयते

POLICY FOR DATA SHARING

from the National Transport Repository

Table of Content

1. Introduction

Ministry of Road Transport and Highways (MoRTH) maintains critical data related to Vehicle Registration Certificates (RCs) and Driver Licenses (DLs) collected through the VAHAN and SARATHI respectively, along-with the data recorded at time of generation of e-Challan or eDAR (Electronic Detailed Accident Report) and National Electronic Toll Collection (NETC)- FASTag data. This data is collectively referred to as the National Transport Repository (NTR). NTR is a centralized repository that holds record of over Thirty-Nine Crore vehicles, TwentyTwo Crore DL and data related to e-Challan, eDAR and NETC- FASTag.

The NTR is a unified central data repository maintained by MoRTH, required to be maintained *inter alia* under Section 25A and Section 62B of the Motor Vehicles Act, 1988 (MV Act). The demand for access from citizens, academics, private sector to this data in various forms continues to grow. Sharing data in a controlled manner can enhance services and benefit research and data driven decision making by government organizations, private sector and academia. Furthermore, State Governments are mandated to ensure electronic monitoring and enforcement of road safety under Section 136A of the MV Act. However, it is important to maintain appropriate safeguards from a security and privacy standpoint to prevent data leakage or breach.

MoRTH mandated the use of FASTag for all four-wheelers, irrespective of their date of sale, with effect from January 1st, 2021, through Gazette Notification G.S.R. 690(E) dated September 1st, 2020, amending Rule 138A of the Central Motor Vehicles Rules, 1989 (CMVR). Further, as per G.S.R. 1361(E) dated November 2nd, 2017, all motor vehicles in Category M (used for the carriage of passengers) and Category N (used for the carriage of goods), manufactured on or after July 1st, 2017, are required to be fitted with FASTag.

1.1. Purpose of this Document

As mentioned above, NTR serves as the central repository for the aforementioned records. Several government and enforcement agencies access this data for specific purposes. Given that this data includes personal and sensitive information, provision and sharing of data needs to be carefully managed through a governing policy document.

The recently enacted Digital Personal Data Protection Act, 2023 (DPDP Act) imposes obligations on the Data Fiduciary holding Personal Data. This policy outlines the procedures for data sharing while ensuring compliance with applicable laws and the implementation of necessary safeguards to benefit government, academia and to promote ease of living (EOL) and ease of doing business (EODB).

1.2. Key Objectives

The objective of providing access to data, while ensuring privacy and security of the data, is to enable the following:

	Smooth and controlled integration of external applications/systems with the Transport National Register, ensuring seamless access to authentic data for stakeholders.
	Increased operational efficiency by minimizing duplication of work and human intervention along-with furthering digital transformation.
	Improved services and benefits for citizens, academia/researchers, private sector, government and other stakeholders.
	Ensuring ease of living and doing business for all stakeholders.
	Provision of need-based data with user-specific variations.

1.3. Key Stakeholders

Data Fiduciary/Provider

- **Ministry of Road Transport and Highway:** MoRTH is the holder of the data and the primary Data Fiduciary of the NTR data (e.g., Vehicle Registration, Driving Licenses, e-Challan, eDAR, FASTag etc.). It is responsible for formulating the data-sharing policy and ensuring its proper implementation.
- **State Government:** The Transport Departments and Registering or Licensing Authorities are co-holders and co-Data Fiduciaries of State-level data. The data-sharing policy defined by MoRTH will also apply to States and Union Territories.

Data Recipients

Organizations that receive data from the NTR, under this policy, are referred to as Data Recipients and shall be implicitly considered as Data Fiduciaries as defined under the DPDP Act, who shall *inter alia* undergo audits and be liable for any data breach under the applicable law including Chapter VIII of the DPDP Act. These include:

1. **Police, Law Enforcement Agencies and National Security Agencies** will have complete access to all data parameters, including Personal Data, as required under the applicable law, including Section 7 (certain legitimate uses) and Section 17 (exemptions) of the DPDP Act.

2. **State Government or UT Administration:** The State Transport Departments will have complete holding of the transport data *inter-alia* comprising Vahan, Sarathi and e-Challan in respect of the concerned State or Union Territory. Regarding eDAR data, the stakeholders like Police, Transport, Health and Road-owning agencies will be the co-holders of respective data at the State level. The sharing of data with other departments or statutory entities of the State or Union Territory Government shall be approved by them as per the modalities or parameters of this policy. However, for sharing of data pertaining to other State(s) or pan-India data, the approval of MoRTH and consent of the respective State to which the data pertains, shall be mandatory.

3. **Government Agencies etc.:** Central or State Government Ministries or Departments and statutory entities or organisations owned or controlled by the Central or State Governments specifically mandated for the purpose by MoRTH, Central Government or State Government, as the case may be, will be provided complete access to the data, as required under the applicable law, including Section 7 (certain legitimate uses) and Section 17 (exemptions) of the DPDP Act. The said statutory entities or organisations shall be subjected to additional security measures to prevent data breach, in addition to the measures specified under Clause 6 of this policy. The sharing of data amongst State or Union Territory government entities will be subject to the applicable law including the DPDP Act.

4. **Academia and Research:** Data in aggregated or anonymized form will be shared with academia and private sector for promoting research, innovation and business purpose. This is in line with the National Data Sharing and Accessibility Policy (NDSAP), 2012. In general, aggregated and anonymized data will be made available on the open Government platform (https://data.gov.in).

5. **Citizen or Individuals:** Citizens or individuals can access their complete data related to their own vehicle/DL or e-Challan. Additionally, select parameters of these datasets can also 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 citizen through the open Government platform (https://data.gov.in) and also through public dashboards.

6. **Transport Service Providing Agencies:** To enable specialized services within the eTransport Ecosystem, relevant datasets will be shared with service providers based on their roles and data needs. Agencies such as insurance providers, banking gateways, HSRP vendors, smart card vendors, third party (TP) sales and Vehicle

Location Tracking Device (VLTD) vendors receive select data parameters as required for provision of their services. These entities shall execute a memorandum of data compliances (in the template provided in this policy) or an agreement with MoRTH or the State Government, as the case may be, on a case-by-case basis, in furtherance of ensuring compliance with law. These agencies shall be subjected to additional security measures to prevent data breach, in addition to the measures specified under Clause 6 of this policy.

7. **Private Sector Entities providing Authentication Services for Ease of Living and Ease of Doing Business:** 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. For instance, DL as an authentication service on similar lines as Aadhaar Authentication Service.

1.4. Sharing of Personal Data

Personal Data, as defined under clause (t) of Section 2 of the DPDP Act, means any data about an individual who is identifiable by or in relation to such data. MoRTH, as the primary Data Fiduciary, is responsible for determining how and when Personal Data is processed or shared.

The Personal Data of the DL holders or registered owners of motor vehicle, i.e. Data Principals, who are not in compliance with the provisions of the MV Act or any other rules made thereunder, shall be provided to the law enforcement agencies, transport service providers, insurance companies etc. in un-masked form, with reasonable safeguards. The data shall be shared for ensuring compliance with law or for the performance of functions under law.

2. Different Data Sets of the Transport Department

This Clause defines the data sets available for sharing, under this policy.

2.1. Vehicle Registration Data Sets (Source: Vahan Database)

A list of shareable data parameters available in the Vahan Database, categorized under the super heads listed below, is provided in Annexure VIII.

Vehicle Registration Related Data Set:

- Registration Details
- Purchase Details
- Vehicle Owner Details
- Vehicle Details
- Validity Norms
- Dealer Details
- Used Car Dealer Details
- Permit Details
- Insurance Details
- Hypothecation details
- NOC Details
- Non-use information
- e-Challan details

Note 1: Above is a superset of sharable data parameters. Individual agency needs to specify the required data with parameter-wise purpose and justification. The Personally Identifiable Information (PII) or other sensitive data parameters will be shared with the Data Recipients after due approval under this policy.

Note 2: The API facilitates search of any registered vehicle record by specifying one of the following input parameters:

- Vehicle Registration Number OR-
- Chassis Number OR-
- Engine Number

Note 3: In case of any duplicate record existing for same registration number, chassis number or engine number, the data will not be displayed. Rectification of Duplicate record is facilitated to RTO'S through De-Duplication Module.

2.2. Driving Licence Related Data Sets (Source: Sarathi Database)

A list of shareable data parameters available in the Sarathi Database, categorized under the super heads listed below, is provided in Annexure VIII.

Driving Licence Related Data Sets

- Driving Licence Details
- DL Holder's Details
- Validity
- International Driving Permit (IDP) Details
- PSV Details
- Adaptive vehicle Number
- e-Challan details

Note 1: Above is a superset of sharable data parameters. Individual agency needs to specify the required data with parameter-wise purpose and justification. The PII or other sensitive data parameters will be shared with the Data Recipients after due approval under this policy.

Note 2: Data of Driving License Holders can be searched through following input parameters viz.:

- Driving License Number AND
- Date of Birth

2.3. e-Challan related datasets (Source: e-Challan Database)

A list of shareable data parameters available in the e-Challan Database, categorized under the super heads listed below, is provided in Annexure VIII.

e-Challan Related Data Sets

- Challan Details
- Vehicle Details
- Challan Recipient Details
- Court Details
- Driving License details

2.4. eDAR related datasets (Source: eDAR Database)

A list of shareable data parameters available in the eDAR Database, categorized under the super heads listed below, is provided in Annexure VIII.

eDAR Related Data Sets

- Accident Details
- Vehicle and Driver Details
- Vehicle Passenger Details
- Pedestrian Details

2.5. NETC- FASTag related datasets (Source: Toll Database)

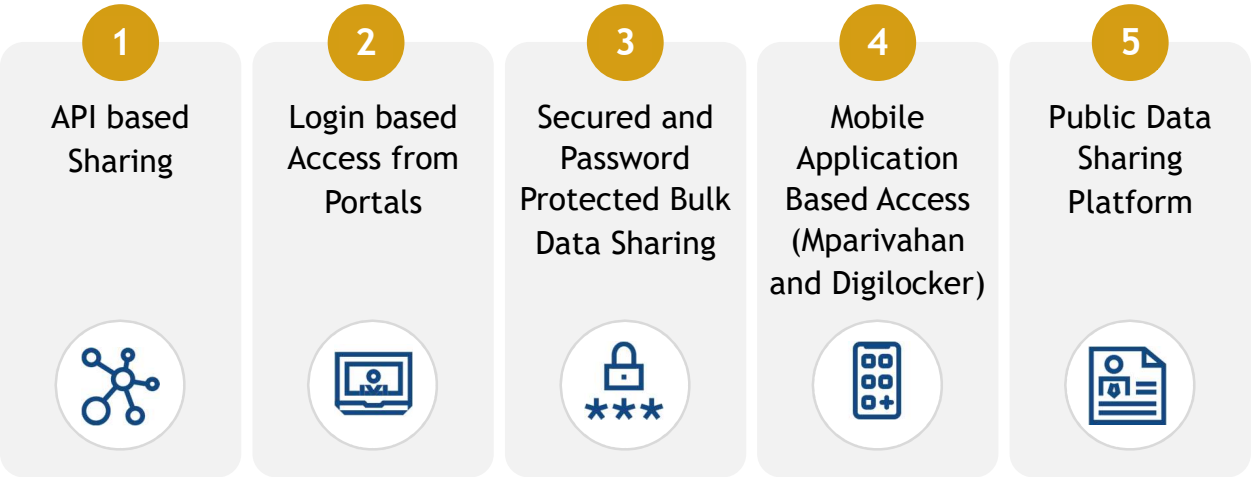
A list of shareable data parameters available in the NETC database, categorized under the super heads listed below, is provided in Annexure VIII.

NETC- FASTag Related Data Sets

- Vehicle Details
- FASTag Details
- General Details
- Bank Details
- Transaction Details

3. Modes of Sharing of Data

Under this policy, data sharing can be allowed through various modes depending on the category of users and type of data. The following modes are available:



3.1. API based Sharing

API-based sharing, which facilitates machine-to-machine data access will be the preferred mode of data sharing. APIs are published via the NIC API Exchange Gateway (NAPIX), and access is granted using security measures such as secret keys, user authentication, and IP whitelisting etc. Organizations desiring access to a specific set of data must submit 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, as outlined in Clause 6 of this policy.

In API based access, PII parameters will be masked for data shared with Data Recipient except (a) Police, law enforcement, national security agencies and (b) any entity specifically granted full data access by MoRTH, subject to the provisions of the DPDP Act.

3.2. Login based Sharing from Portals

This mode of data sharing shall be applicable to the following:

For Government Organizations:

These agencies will be given access to the data parameters of Vahan and Sarathi by logging into NTR Portal using secured credentials. Additionally, two-factor authentication will be introduced for additional security. The users will be required to

make Aadhaar authenticated OTP-based system, in addition to login/password-based access.

For Private Sector for EODB or EOL:

The data shall be shared with private sector stakeholders to strengthen the transportation ecosystem and to ensure EODB and EOL, thereby strengthening the economy, subject to consent of the Data Principal being obtained through the consent mechanism. Private Sector entities can access datasets from the NTR, subject to approval from MoRTH.

MoRTH shall fix a daily data access limit as specified on the concerned portal, from time to time, and specific to the type of Data Recipients. The above services will be subject to data limitation and consent mechanism, if applicable.

Such Data Recipient may include insurance companies with valid IRDAI licenses and Scheduled Commercial Banks regulated by the RBI, transporters, State Transport Undertakings, Automobile Manufacturers, Component Manufacturers, motor vehicle aggregators and private sector associations such as ACMA, SIAM etc.

Personal Data and PII may be provided under the condition that a Data Recipient obtains user consent through an Aadhaar authenticated OTP-based system linked to the mobile number on the concerned portal. If a mobile number is not available in the records, the user must update it via Aadhaar authentication before giving consent.

For Citizen:

Citizen/individuals can also have limited access to information on any Vehicle or Driving license through NTR portal. Only select, non-sensitive, non-PII parameters regarding Driving License or Vehicle Registration Certificate of any citizen may be shown. Moreover, user has to authenticate through mobile OTP and number of accesses per day will be restricted limited to three (3).

3.3. Secured and password protected bulk data sharing

Bulk data will only be provided on an exceptional basis to select organisations. Full data will be shared on one-time basis, with incremental updates on monthly, quarterly or half-yearly basis, as the case may be. Bulk data will be shared through portable password protected hard disk drive and collected physically by authorised personnel of the concerned organisation. Alternatively, a Secured FTP link may be set up for the Data Recipients to download the incremental data through secured network. For incremental data sharing, this mode shall be preferred.

The dataset will be provided to agencies as per their specific requirements.The data being shared with such organisations shall be subject to satisfaction of tenets under the DPDP Act, including Section 7 and Section 17 thereof.

3.4. Mobile App based Access

Citizen/individuals can also have limited access to information on any Vehicle or Driving license through NTR portal. Only select, non-sensitive, non-PII parameters regarding Driving License or Vehicle Registration Certificate of any citizen may be shown. Moreover, user has to authenticate through mobile OTP and number of accesses per day will be restricted limited to three (3). The following data parameters are provided:

A. Registration Certificate

- Vehicle number: Non-Masked
- Owner number: Masked
- Registering Authority: Non-Masked
- Vehicle class: Non-Masked
- Fuel type: Non-Masked
- Emission norm: Non-Masked
- Hypothecated: Non-Masked
- Registration date: Non-Masked
- Insurance valid up to: Non-Masked
- PUCC valid up to: Non-Masked
- Vehicle status: Non-Masked

B. Driving License

- DL number: Non-Masked
- DL holder's name: Masked
- Issue date: Non-Masked
- Licence validity (Non-Transport): Non-Masked
- Licence validity (Transport): Non-Masked
- Licensing Authority: Non-Masked

However, for their own DL or RC, citizens can access complete information/ status through the mParivahan and Digilocker mobile apps. There is a facility to create virtual RC and virtual DL for the concerned user by pulling data from the Vahan/ Sarathi databases through API. MoRTH has already notified the virtual DL and RC available in these two apps as legally valid documents.

However, MoRTH will make aggregated and anonymised data from its core applications, such as Vahan, Sarathi, e-Challan, eDAR, and FASTag, available through internal and external dashboards. These dashboards will feature key performance indicators, trend analyses, and reports to support informed decision-making. Requests for additional dashboard APIs would be entertained from an academic institution which requires such information for research and analysis purpose, for which a request signed by the designated officer of the academic institution would be necessary.

In line with the National Data Sharing and Accessibility Policy 2012 (NDSAP), anonymized datasets will be regularly published on 'data.gov.in' for public, academic, and research use. All internal portals, such Vahan, Sarathi, e-Challan, eDAR, and FASTag, are integrated to ensure seamless data sharing and efficient digital service delivery across platforms.

4. Datasets and the Mode of Sharing specific to the Data Recipients:

4.1. Sharing of NTR datasets with the State Government or UT Administration

Every State is the co-holder and co-Data Fiduciary of its own transport related data pertaining to Vahan, Sarathi, e-Challan, eDAR etc. Each State has been provided access to NTR database on read-only basis through secured VPN based access and access credentials are provided for Vahan and Sarathi to Transport Officers as approved by the concerned State Transport Authorities. However, this access is limited only to the State-specific data. This is to facilitate States to have view of their own data and also run ad-hoc reports or queries as per their need.

4.2. Sharing of State-level data with Government Agencies by State Transport Authorities

The State Transport Departments will have complete holding of the data pertaining to their jurisdiction and sharing of data with other agencies shall be their prerogative as per the modalities of this policy and subject to the applicable law, including DPDP Act. This access shall be provided preferably through secure API-based systems. However, for sharing of data pertaining to other State(s) or pan-India data, the approval of MoRTH with the consent of the respective State, under this policy, shall be necessary. The Recipient shall execute a memorandum of data compliances or an agreement with the State Government, on a case-by-case basis, in furtherance of ensuring compliance with law.

The data will be available in any of the modes mentioned under Clause 3, except for protected bulk data sharing. However, the preferable mode for sharing of data shall be through API access.

4.3. Sharing of NTR datasets with Police, Law Enforcement Agencies and National Security Agencies

As stated above, Police, Law Enforcement Agencies and National Security Agencies will have complete access to all data parameters, including Personal Data, as required under the applicable law, including Section 7 (certain legitimate uses) and Section 17 (exceptions) of the DPDP Act.

The data will be available in any of the modes mentioned under Clause 3. Additionally, when only specific data parameters and/ or from a specific time period, are required, they shall be provided on case-to-case basis. However, the preferable mode for sharing of data shall be through API access.

4.4. Sharing of NTR datasets with Government Agencies etc.

As mentioned before, the Central or State Government Ministries or Departments and statutory entities or organisations owned or controlled by the Central or State Governments specifically mandated for the purpose by MoRTH or State Government, as the case may be, will be provided complete access to the data, as required under the applicable law, including Section 7 and Section 17 of the DPDP Act.

In view of the same, the data will be available in any of the modes mentioned under Clause 3, except for protected bulk data Sharing. However, the preferable mode for sharing of data shall be through API access.

4.5. Sharing of NTR datasets with Academia and Research

As stated before, the aggregated or anonymized data will be shared in with such entities for research innovation and business purposes.

In view of the same, the data will be available through Dashboard/Reporting portals and OGD Platform as mentioned in the modes of sharing under Clause 3, except for protected bulk data sharing. Academia and Research entities can request additional select datasets from the NTR, subject to approval from MoRTH.

4.6. Sharing of NTR datasets with Citizen or Individual

As stated before, Citizen/ individuals, in addition to complete information of their own vehicle/Driving License details, can also have limited access to information on any Vehicle or Driving license through NTR portal. The user will authenticate through mobile OTP and number of accesses per day will be restricted limited to three (3).

4.7. Sharing of NTR datasets with Transport Service Providing Agencies

Transport service providing agencies shall execute a memorandum of data compliances or an agreement with MoRTH or the State Government, as the case may be, on a case-by-case basis, in furtherance of ensuring compliance with law. The provisions of DPDP Act, including Section 6 (consent), shall be applicable to such agencies and the preferred mode of data sharing shall be through API. In addition to the security measures outlined in Clause 6 of this policy, additional security measures to prevent

data breach will be imposed on these agencies from time to time and on case-to-case basis. Furthermore, Data Recipients shall be liable for any data breach under the applicable law including Chapter VIII of the DPDP Act.

Additionally, transport service providing agencies like banks, insurance companies, transporters, OEMs etc. may also be provided anonymised data along-with authentication services to strengthen the transportation ecosystem and facilitate EODB, subject to approval from MoRTH. This access will be subject to data limitation and consent mechanism, as applicable.

The State Governments or UT Administration shall onboard all such transport service providing agencies on NTR before commencing of data-sharing.

Some of the aforementioned entities are specified below:

A. Vehicle registration and Driving License data shared with Card/Smart-card vendors:

When a new vehicle is registered or a transaction (such as Renewal, Duplicate, Change of Address etc.) is done on an existing vehicle which necessitates issuance of a Registration Certificate in the form of PVC Card/Smart Card, then data will be made available to the State-authorized Card/Smart-Card vendor through API to issue the DL/RC as a Smart Card.

Similarly, when a new Driving License is being issued or a transaction (such as Renewal, Duplicate, Change of Address etc.) is done on an existing DL which necessitates issuance of a Driving License in the form of PVC Card/Smart Card, then data is made available to the State-authorized Card/Smart-Card vendor through API.

The approval for such data sharing shall be accorded by concerned State Transport Authority for the authorized agency/vendor.

For both aforementioned purposes, complete data for RC or DL (as specified in the relevant forms of CMVR) is made available to the authorized vendor for printing/embedding of the data in the card/smart-card.

B. Vehicle registration data shared with HSRP vendors:

When vehicle needs to get affixed with HSRP number plates– either during registration of a new vehicle or existing registered vehicle or when a vehicle requires replacement of registration plates, then data is made available to the OEM-authorized (in case of new vehicle) or State-authorised (in case of old vehicle) HSRP vendor through API. The following parameters are shared through API:

- Registration number
- Registration date
- State code
- Office code
- Vehicle manufacturer
- Vehicle type
- Vehicle category
- Fuel
- Emission norm
- HSRP front laser code
- HSRP rear laser code

C. Vehicle related select parameters shared with IIB & Insurance Companies:

Insurance Companies issue third-party insurance policies to every vehicle during registration of a new vehicle and also during renewal of insurance policy. Insurance Information Bureau verifies the issued insurance policy. The following parameters are shared through API:

- Registration Number
- Chassis Number
- Engine Number
- Manufacturer Name
- Model Name
- Vehicle Category
- Vehicle Class

D. VLTD Information to the Vehicle Location Tracking System Implementation Agencies in states:

The implementation agencies in the States or UTs authorized by concerned State Transport Authorities for setting up and maintaining the Vehicle Location Tracking System back-end system (Command and Control Centres). The following parameters are shared through API:

- VLT Device serial number
- Registration number
- Registration date

- Chassis number
- Engine number
- Vehicle class
- Owner name
- Manufacturer name of the VLTD
- Fitment Centre
- IMEI number
- ICC identification
- Type Approval Certificate Number
- Device Activation Status

E. Data Sharing with third-party for e-Challan implementations:

The Central Government, State Governments and UT Administration have implemented their own version of e-Challan and require select parameters of Vahan, Sarathi and e-Challan data for verification and reconciliation of data, in the interest of prevention, detection, investigation or prosecution of any offence or contravention. The State Governments and UT Administration shall onboard such third-parties on NTR or notify them, before sharing any data with them. Select data parameters will be shared with such third-parties in deference to the principle of data minimization and purpose limitation.

F. Data sharing with payment aggregators licensed by the Reserve Bank of India:

Payment related data for transactions in NTR and various other applications/ services are exchanged with the concerned payment gateway/ integrator as authorized by concerned authority to collect payment on its behalf for, amongst other things, providing benefit, service, certificate, licence or permit under Section 7(b) of the DPDP Act.

States or UTs have assigned their own payment gateways for collection of payments. These are used for collecting all payments for transactions related to transport services w.r.t. NTR. The options adopted by some States or UTs are:

i. Banks designated as payment gateway/integrator on behalf of state.

ii. Treasury of State.

iii. Payment aggregator licensed by Reserve Bank of India for collection of e-Challan payment.

iv. Prepaid Payment Instruments authorised by the Reserve Bank of India under the provisions of the Payment and Settlement Systems Act, 2007.

G. Sharing with NETC-FASTag:

NETC-FASTag data is integrated with internal platforms such as VAHAN, e-Detection, and e-Notice portals to enhance enforcement mechanisms. Electronic notices are issued to vehicles that evade toll payments, using integrated data from VAHAN and the National Payments Corporation of India (NPCI). The following parameters are shared:

- Type of vehicle
- Class of vehicle
- Type of ownership
- Registration number
- FASTag identification
- Number of axles
- Axle description
- Axle weight
- Seating/sleeping/standing capacity
- Manufacturer of vehicle
- Model of vehicle
- Color of vehicle
- Fuel type
- Emission norms
- Unladen weight
- Gross vehicle weight
- National Permit
- National Permit valid up to
- National Permit date of issue
- All India Tourist Permit
- All India Tourist Permit valid up to
- All India Tourist Permit date of issue
- Vehicle height, width and length
- Stage Carriage Permit
- Stage Carriage Permit valid up to
- Stage Carriage Permit date of issue

- Contract Carriage Permit
- Contract Carriage valid up to
- Contract Carriage date of issue
- Private Service Vehicle Permit
- Private Service valid up to
- Private Service date of issue
- Goods Permit
- Goods Permit valid up to
- Goods Permit date of issue
- Temporary Permit
- Temporary Permit valid up to
- Temporary Permit date of issue
- Special Permit
- Special Permit valid up to
- Special Permit date of issue

H. Sharing of NTR datasets with Private Sector Entities providing Authentication Services for EOL and EODB

To support EOL and EODB, MoRTH will provide authentication services along-with anonymised data to private sector entities based on specific business needs. For example, DL verification can be offered as an authentication service similar to Aadhaar authentication. Anonymized data fields for authentication may be made available time to time, upon request, subject to approval and compliance with applicable data privacy and security regulations.

Such entities can request masked PII datasets from the NTR for authentication purposes, as an exception, subject to approval from MoRTH. Additionally, these entities shall also execute a memorandum of data compliances or an agreement with MoRTH or the State Government, as the case may be, on a case-by-case basis, in furtherance of ensuring compliance with law.

5. Request and Approval Process

5.1. API-based Data Sharing – Process and Prerequisites.

If any Government Department/Agency wants access data through API, the following steps shall be followed:

a. For Vahan/Sarathi/e-Challan data, the applicant may submit a request letter, on official letterhead, to the Deputy Secretary or Director (MVL), Transport Bhawan, 1 Sansad Marg, New Delhi-110001for accessing the required data through API based Access as per form given in Annexure-I. For eDAR data access, the application has to be submitted to Deputy Secretary or Director (Road Safety) or the concerned Stakeholders at the State level (being co-holder of the data). For FAStag data access, the application shall be submitted to Superintendent Engineer or Director (Toll)/ Member NHAI.

b. The request for data access may be made by an officer of rank/position as below:

- Govt. of India– Joint Secretary or equivalent.
- State Govt.– Administrative Secretary or equivalent.
- PSU/ Govt. Undertaking– Director or equivalent.
- Enforcement Agencies– Additional Director General of Police or equivalent.

c. As per the application form, contact details of one Authorized Government/ PSU Officer and one Authorised Technical Support Head from the requesting agency are to be provided in the form. **The Authorised Government Officer** will communicate with MoRTH for all administrative purposes, including original request and renewal etc. The Authorised Government Officer will be responsible for the safety and security of the data received through the API. Even if the API is used for an application developed/maintained by any third-party agency, the primary responsibility will still rest with the Government Officer in whose name the API has been approved. If there is any change of officer over the course of time, the same must be informed to MoRTH along with contact details of the new officer. Details of the **Technical Support Head** also needs to be stated in the application form. The Technical Support Head will coordinate with the NIC for API integration and other technical requirements. If there is any change of the Technical Support Head over the course of time, the same must be informed to MoRTH along with contact details of the new Technical Support Head.

d. The form should be accompanied by the required list of data parameters from Vahan/ Sarathi/e-Challan/eDAR/ FASTag with Parameter wise Purpose/ Justification.

e. The form should be accompanied by explanation for eligibility of such organisations to process the data under Section 7 of DPDP Act.

f. The request should be limited to such Personal Data as is necessary for such specified purpose to ensure data minimisation.

g. A memorandum of data compliance also needs to be attached regarding safeguards to be ensured regarding the shared data. The format of the Undertaking is attached in the annexure III.

h. After submission of the data access request by the applicant agency, MoRTH will examine the details through a due verification process. If approved, same will be communicated to NIC (if necessary, with specific instructions, fur further action and implementation.

i. Once approved, Client ID and access credentials will be created by NIC, and information will be communicated to the applicant's official email ID. The API integration document and other technical details will also be shared. The process will be as below:

Allocation of Credential –

- The Client ID will be communicated by NIC to the applicant's official email ID (same as mentioned on request application form).
- The applicant needs to provide the confirmation email from official email ID of receipt of Client ID to NIC.
- The Security Key will be communicated to the official email ID only after receipt of confirmation email from the user.

Testing Phase–

- Initially, only one client IP will be whitelisted for the testing phase and after successful testing, the same will be made live on production.

j. The approved Data Recipient or Data Fiduciary needs to submit a Website Security Certificate from CERT-IN empanelled security auditor for the application for which the required data access is being requested. This certificate should cover the application security audit, vulnerability assessment, penetration testing, configuration review and safe hosting clearance.

This certificate is also required at the time of annual renewal of the API access.

k. After data access is operationalized on the testing platform, log records from the system regarding data access particulars need to be maintained and shared with NIC. (Format attached in Annexure VI). Similar logs need to be maintained in the

production environment, which may be demanded in case of any security related investigation.

l. Once data access is operationalized, it will be valid for one year only. The access must be renewed every year, well in time before end of the tenure, so that there is no discontinuity of services. The same form as used in the initial application will be used for renewal also. Fresh audit of the Data Processor's system must be made available before the completion of the tenure. Two intimations/alerts will be sent by NIC to the Data Recipient or Data Fiduciary, first after completion of 10 months and second after completion of 11 months. The alerts will be sent to the specified email IDs of the Authorised Government Officer and Technical Support Head. The duly filled application with all pre-requisites will be reviewed and approved by MoRTH and services will be continued. If not renewed or if fresh audit certificate is not furnished, API access will then be blocked automatically at the end of the yearly tenure.

m. MoRTH reserves the right to suspend/discontinue the data access for any Data Recipient at any point of time if any data breach or other security incidence is reported. If necessary, MoRTH may also ask for access log and/or other documentation from the Data Recipient.

n. The Data Recipient will also be considered as a Data Fiduciary as per DPDP Act and will be liable for legal actions as per the Act in case of any breach or unauthorized disclosure of Personal Data of citizen.

5.2. Portal-based Data Sharing- Process and Prerequisites.

If any Government Department/ Agency wants access data through Portal, the following steps maybe followed:

a. For Vahan/Sarathi/e-Challan, the applicant may submit a request letter, on official letterhead, to the Deputy Secretary or Director (MVL), Transport Bhawan, 1Sansad Marg, New Delhi-110001 for accessing the required data through Portal based Access as per form given in Annexure-II. For eDAR data access, the application has to be submitted to Director (Road Safety). For FAStag data access, the application has to be submitted to Superintendent Engineer or Director (Toll)/ Member NHAI.

b. The request for data access may be made by an officer of rank/position as below:

- Govt. of India- Joint Secretary or equivalent.
- State Govt.- Administrative Secretary or equivalent.
- PSU/ Govt. Undertaking- Director or equivalent.

- Enforcement Agencies– Additional Director General of Police or equivalent.

c. The Authorized Officer may apply for himself/ herself or for any other officer/ staff of the organization working on regular basis not below the L-13 or equivalent pay scale. Further, the access request may be requested for a single user, or for an Admin User. Admin User can create multiple access credentials and allocate them to other users.

d. As per the application form, contact details of two representatives from the requesting agency are to be provided in the form. The Authorised Officer will communicate with MoRTH for all administrative purposes, including original request and renewal etc. The Authorised Officer will be responsible for the safety and security of the data received through the portal access. Even if the access is meant for any other officer/ staff of the organization, the primary responsibility will still rest with the Authorized Officer who has submitted the request. If there is any change of officer over the course of time, the same must be informed to MoRTH along with contact details of the new officer. Details of the Actual User – who will be issued the access credentials, also needs to be stated in the application form. This user may communicate with NIC for any technical requirements. If this is an Admin User, then he/she can create other users also. If there is any change of the user over the course of time, the same must be informed to MoRTH along with contact details of the new user.

e. The form should be accompanied by the required list of data parameters from Vahan/ Sarathi/e-Challan/eDAR/FASTag with parameter wise Purpose/Justification.

f. The form should be accompanied by explanation for eligibility of such organisations to process the data under Section 7 of DPDP Act.

g. In case of Personal Data, the request should be limited to such Personal Data as is necessary for such specified purpose to ensure data minimisation.

h. An memorandum of data compliance also needs to be attached regarding safeguards to be ensured regarding the shared data. The format of the Undertaking is attached in the annexure IV.

i. After submission of the data access request by the applicant agency, MoRTH will examine the details through a due verification process. If approved, same will be communicated to NIC (if necessary, with specific instructions, fur further action and implementation.

j. Once data access is operationalized, it will be valid for one year only. The access must be renewed every year, well in time before end of the tenure, so that there is no discontinuity of services. The same form as used in the initial application

will be used for renewal also. Two intimations/alerts will be sent by NIC to the Data Recipient or Data Fiduciary – two weeks before and 1 week before the end of the yearly tenure. The alerts will be sent to the specified email IDs of the Authorised Government Officer. The duly filled application with all pre-requisites will be reviewed and approved by MoRTH and services will be continued. If not renewed Portal access will then be blocked automatically at the end of the yearly tenure, with intimation to the authorised officer.

k. Only one Login ID/password will be issued to an organization. The organization may, in turn, create sub- user IDs and passwords, if required, for its constituents/branches etc. In this case, Admin option should be chosen. However, the Authorised Officer will be responsible for the act/ conduct of all the users created under the admin option.

l. The Data Recipient will also be considered as a Data Fiduciary as per DPDP Act and will be liable for legal actions as per the Act in case of any breach or unauthorized disclosure of Personal Data of citizen.

5.3. Bulk Data Sharing – Process and Prerequisites.

Bulk data sharing is an exceptional requirement and will be considered by MoRTH on case-by-case basis. So far only five Government agencies have been provided bulk data from Vahan/ Sarathi databases, comprising specified datasets as per user requirements.

There is no specified request form or process for this, however, some suggested points are stated as below. Further, the existing bulk data sharing status also may be periodically reviewed by MoRTH and necessary guidelines may be issued to MoRTH.

a. For Vahan/Sarathi/e-Challan data, the Applicant may submit a request letter, on official letterhead, to the Director(MVL), Transport Bhawan, 1 Sansad Marg, New Delhi-110001for accessing the required data. For eDAR data access, the application has to be submitted to Deputy Secretary or Director (Road Safety). For FAStag data access, the application has to be submitted to Superintendent Engineer or Director (Toll)/ Member NHAI.

b. The request for data access may be made by an officer of rank/position as below:
   - Govt. of India- Joint Secretary or equivalent.

c. Contact details of concerned officials are to be provided in the form. The Authorised Government Officer will communicate with MoRTH for all administrative purposes, including original request and renewal etc. The Authorised Government Officer will be responsible for the safety and security of the data received. Details of the nodal Officer also needs to be stated in the application form. This officer will coordinate with the NIC for operational aspects

of secure exchange of data and other technical requirements. The Name, Designation, Email ID, Mobile Number and Office Address of both these officers need to be submitted for record purpose. If there is any change of officer over the course of time, the same must be informed to MoRTH along with contact details of the new officer.

d. The request should be accompanied by the required list of data parameters from Vahan/ Sarathi/ e-Challan/ eDAR/ FASTag databases with detailed Purpose/Justification. The periodicity of incremental data is also to be specified, which may be in terms of Year/ Quarter/ Month.

e. An Undertaking also needs to be attached regarding safeguards to be ensured regarding the shared data. The format of the Undertaking is attached in the annexure V.

f. After submission of the data access request by the applicant agency, MoRTH will examine the details through a due verification process. If approved, same will be communicated to NIC (if necessary, with specific instructions, fur further action and implementation.

g. Once approved, the data sharing mechanism will be worked out by the Operational Support Officer of the Data Recipient or Data Fiduciary and NIC. If data is to be provided through portable hard disk drive, the agency will provide the same with appropriate capacity to authorized NIC officer/ staff. Required data will be extracted by NIC and copied to the device and handed over to the authorized officer/ staff of the agency as per due security protocol. Alternatively, if the data size permits and the concerned agency agrees, the bulk data can be shared through an SFTP link to be set up by NIC. Access credentials will be created by NIC, and information will be communicated to the applicant's official email ID. For incremental data also, similar exercise may be undertaken.

h. The Data Recipient will also be considered as a Data Fiduciary as per DPDP Act and will be liable for legal actions as per the Act in case of any breach or unauthorized disclosure of Personal Data of citizen.

6. Data Sharing Security Practices and Procedures

At present, MoRTH shares data through API and portal-based access with Data Recipients/Fiduciary, such as Government Departments, Enforcement Agencies etc. While, MoRTH and NIC facilitate the provision of data, it is critical to protect sensitive information and ensure compliance with the provisions of the DPDP Act by these Data Recipient or Data Fiduciary.

Data Security Guidelines for Government Organisations agencies requesting data:

1. Data access for pan India data will be provided to Government Organizations and Enforcement Agencies upon approval from MoRTH, subject to compliance with all prerequisites. As the data contains sensitive personal information, the designated government officer of the Data Recipient, named in the request application form shall be responsible for safeguarding the data. If the officer of the Data Recipient is transferred, retires, or is replaced, MoRTH must be notified immediately via official letterhead, duly signed and stamped by the Competent Government Officer, to update the records.

2. Data Recipient shall execute a memorandum of data compliances or an agreement with a Data Recipient or Data Fiduciary, on a case-by-case basis, in furtherance of ensuring compliance with law. Data Recipients shall be Data Fiduciaries as defined under the DPDP Act.

3. Where a consent given by the Data Principal is the basis of processing of Personal Data and a question arises in this regard in a proceeding, the Data Recipient i.e. Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal in accordance with the provisions of the DPDP Act and the rules made thereunder, as provided under Section 6(10) of the said Act.

4. State-level data sharing may be approved by the respective State Transport Authority, who is the co-holder of the State-specific data. Approval can be granted by the State Transport Secretary or Commissioner, but only for State-specific data. National-level data sharing requires MoRTH approval.

5. A set of prerequisites, such as ensuring its completeness, accuracy and consistency must be met before implementing API-based data sharing.

6. Data Recipient must submit a Security Audit Certificate issued by a CERT-IN empanelled security auditor for the application in which API access is requested. The certificate should cover application security, vulnerability assessment, penetration testing, configuration review, and safe hosting clearance. Details on

certified consultants are available on the CERT-IN portal (https://cert-in.org.in). Additional audit may be required from time to time and on case-to-case basis.

7. The approval will be granted for only one year at a time and needs to be renewed every year. Further, the Security Audit must be carried out every year, and the certificate needs to be submitted to MoRTH annually. Agencies will receive two alerts or notifications before the renewal date. If the renewal of the data access is not done and updated audit certificate is not submitted to MoRTH in time, service access will be discontinued.

8. API access is granted for a specific application, with a maximum of four IPs (two for Production Servers and two for Development/Testing Servers) whitelisted. Separate approvals are required for each application requesting API access.

9. API credentials must remain confidential and must not be shared with any third party. Sub-granting of the API is not permissible.

10. Data Recipient must 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.

11. Log records of data access must be maintained, for at least one year, in the production environment and made available upon request for any security investigation.

12. Data Recipient must keep portal access credentials confidential. Passwords must be changed immediately after receipt and regularly thereafter to maintain security.

13. All accessed data must be processed and stored on servers located within India. Data must not be transferred or stored on servers outside India.

14. Data Recipient must specify the required data parameters with a detailed purpose and justification. MoRTH will grant approval based on this justification, ensuring that only necessary data is shared in compliance with the principles of the DPDP Act.

15. Data Recipient are prohibited from disclosing, reproducing, selling, distributing, or transferring any shared data or Personal Data. The data cannot be used for any purpose other than what was originally requested. A fresh application is required for any additional purposes.

16. Data Recipient must maintain up-to-date operating systems, robust cyber security measures, and conduct regular audits to safeguard data and prevent breaches.

17. Data Recipient must enforce private sector-standard managerial, technical, and physical safeguards to prevent unauthorized data processing or access.

18. Data Recipient Sare advised to implement and enforce strong password policies, including Multi-Factor Authentication (MFA), to enhance security and reduce the risk of unauthorized access.

19. In the event of a data breach involving personal or sensitive information, Data Recipient must immediately notify MoRTH and the affected individuals. Breaches must also be reported in compliance with the DPDP Act.

20. Failure to comply with these guidelines or the DPDP Act may result in debarment from further data sharing, along with legal action or monetary penalties under applicable laws.

21. An Undertaking outlining data protection and privacy responsibilities must be submitted by the Data Recipient prior to data sharing. This undertaking will be reviewed, updated, and renewed annually.

Annexure I

Application Form for API-based Data Sharing

1. **Name of Applicant Organisation:** _____
2. **Name of Authorised Government Officer**: _____
3. Designation: _____
4. Department: _____
5. Mobile number: _____
6. Office Phone number: _____
7. Official Email ID (Should be. nic/.gov domain): _____
8. Office Address: _____
9. **Name of the Technical Support Head**: _____
10. Designation: _____
11. Organisation: _____
12. Mobile number: _____
13. Email ID: _____
14. **Current/ prior access credentials (in case of renewal):** _____

    _____
15. **Required Client IP (2 Production & 2 Development API):** _____

    _____
16. **Required List of parameters from the Vahan/ Sarathi National Register with Parameter wise Purpose/Justification to be attached:** _____

    _____

Note: A platform for handling requests from all Data Recipient or Data Fiduciary and approval by MoRTH will be developed. It will facilitate Data Recipient or Data Fiduciary to apply online and allow the verifying and approving authorities to carry out the required action online. Until the online application for the request or approval is developed, manual form will be used by the applicant and communicated through eMail.

Annexure II

Application Form for Portal-based Data Sharing

1. **Name of Applicant Organisation:** _____
2. **Name of Authorised Government Officer**: _____

   Designation: _____
3. Department: _____
4. Mobile number: _____
5. Office Phone number: _____
6. Official Email ID (Should be. nic/.gov domain): _____
7. Office Address: _____

   Option: ☐ **Self/ Other user** ☐ **Admin Role required?**

8. **Name of the Actual User**: _____
9. Designation: _____
10. Mobile number: _____
11. Email ID: _____
12. Address: _____
13. **Current/ prior access credentials (in case of renewal):** _____

    _____
14. **Required List of parameters from the Vahan/ Sarathi National Register with Parameter wise Purpose/Justification to be attached:** _____

    _____

Note: A platform for handling requests from all Data Recipient or Data Fiduciary and approval by MoRTH will be developed. It will facilitate Data Recipient or Data Fiduciary to apply online and allow the verifying and approving authorities to carry out the required action online. Until the online application for the request or approval is developed, manual form will be used by the applicant and communicated through eMail.

Annexure III

MEMORANDUM OF DATA COMPLIANCES

(For API data sharing)

I hereby provide this undertaking in connection with "API based NTR data sharing" As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I will keep API credentials, Secret Key etc. confidential and not share them with any third party.
2. I understand that API access is granted only for a specific application/app, and a maximum of four IPs (2 IPs for Production Servers and 2 IPs for Development Servers) of the user system are whitelisted for access.
3. I will tightly bind API access to the approved application (Mobile App/Web Application) through appropriate access control mechanisms such as secret keys, user-id/password authentication, IP whitelisting, a token exchange mechanism, etc., ensuring that no third party can access the service through the application/APP.
4. I will submit Security Audit Certificate from CERT-IN empanelled security auditor for the application/app for which the required data access is being requested.
5. I will submit a similar Audit certificate to MoRTH every year at the time of annual renewal. Failure to do so gives MoRTH the right to discontinue the data sharing service.
6. I undertake that after the data access is operationalized on the testing platform, log records from the system regarding data access particulars shall be maintained and shared with NIC.
7. I undertake to be responsible for the safety and security of the data received through access. If I am transferred, retired, or released, the details of the new incumbent on the official letterhead, duly signed, and stamped, shall be shared with MoRTH for updating the records.
8. I undertake to use the shared data only for the purpose justified in the request form.

9. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.

10. I undertake not to use, display, or exchange any shared data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from MoRTH.

11. I undertake that all shared data shall be processed and stored on servers or Data Centres residing in India. The data at any point shall not be transferred, processed, or stored on a server outside India.

12. I undertake to develop and maintain strong policies enforcing strong passwords (password management) and the use of multi-factor authentication (MFA).

13. I undertake to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.

14. I undertake that, upon the request of MoRTH, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.

15. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

16. The Data Recipient or Data Fiduciary shall comply with the applicable law including Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

I have signed and executed this undertaking on this _____ day of _____, 20 at _____. I hereby declare that I have provided this undertaking willingly, without any undue influence or duress, and that the foregoing statement is true and correct. I commit to abiding by and complying with all the terms of this undertaking.

Name of Applicant Organisation: .....

Name of Authorised Government Officer/
Data Recipient or Data Fiduciary: .....

.....

Designation: .....

Department: .....

Mobile number: .....

Office Phone number: .....

Official Email ID: .....

Office Address: .....

Signature: _____

Name: _____

Seal

Annexure IV

MEMORANDUM OF DATA COMPLIANCES

(For Portal-based data sharing)

I hereby provide this undertaking in connection with "Portal based NTR data sharing" As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake to keep the Portal credentials confidential and not share them with any third party.
2. I undertake to change the password immediately after receiving it and thereafter, update the password as frequently as possible.
3. I undertake to be responsible for the safety and security of the data received through the Portal access. If I am transferred, retired, or released, the details of the new incumbent on the official letterhead, duly signed, and stamped, shall be shared with MoRTH for updating the records.
4. I undertake to use the shared data only for the purpose justified in the request form.
5. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.
6. I undertake not to use, display, or exchange any shared data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from MoRTH.
7. I undertake to comply with password policy and guidelines of the portal and the use multi-factor authentication (MFA).
8. I undertake to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.
9. I undertake that, upon the request of MoRTH, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.
10. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake

to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

11. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this _____ day of _____, 20 at _____. I do hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Name of Applicant Organisation: ……

Name of Authorised Government Officer/
Data Recipient or Data Fiduciary: ……

……

Designation: ……

Department: ……

Mobile number: ……

Office Phone number: ……

Official Email ID: ……

Office Address: ……

Signature: _____

Name: _____

Seal

Annexure V

MEMORANDUM OF DATA COMPLIANCES

(For Bulk data sharing)

I hereby provide this undertaking in connection with "Bulk NTR data sharing" As a 'Data Requester/ Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake the responsibility for the safety and security of the NTR bulk data received through a portable hard disk drive or Secured FTP (SFTP) link.

2. I commit to using the Shared Bulk Data only for the Purpose/Justification mentioned at the time of data requisition and shall not disclose, reproduce, sell, distribute, or transfer any Shared Data or portion of such data to any third party for any other purpose, without the prior written consent of the MoRTH.

3. I commit not to use, display, or exchange any Shared Bulk Data in any write-up, paper, presentation, discussion forums, or messaging applications without prior approval from the MoRTH.

4. I commit that all Shared Bulk Data shall be processed and stored on servers or Data Centres residing in India. The data at any point shall not be transferred, processed, or stored on a server outside India.

5. I commit to always keep up-to-date Operating Systems (OS), robust Cyber-Security systems, including encryption, intrusion detection systems, other application Software, and employee training, to safeguard the systems and data.

6. I commit that, upon the request of MoRTH, I will stop using/processing the data accessed through this mode and shall erase any personal as per the Digital Personal Data Protection Act, 2023.

7. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

8. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this _____ day of _____, 20 at _____. I hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Name of Applicant Organisation: ……

Name of Authorised Government Officer/
Data Recipient or Data Fiduciary: ……

……

Designation: ……

Department: ……

Mobile number: ……

Office Phone number: ……

Official Email ID: ……

Office Address: ……

Signature: _____

Name: _____

Seal

Annexure VI

MEMORANDUM OF DATA COMPLIANCES

(For Citizen sharing)

I hereby provide this undertaking in connection with NTR data sharing. As a 'Data Recipient or Data Fiduciary', I am fully aware of the terms and conditions outlined in the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023 of the Government of India. As a Data Requester/ Data Recipient or Data Fiduciary, I hereby undertake the following:

1. I undertake to keep the Portal credentials confidential and not share them with any third party, (if applicable).
2. I undertake to change the password immediately after receiving it and thereafter, update the password as frequently as possible (if applicable).
3. I undertake to be responsible for the safety and security of the data received.
4. I will not disclose, reproduce, sell, distribute, or transfer any shared data or portion of such data to any third party.
5. I undertake that, upon the request of MoRTH, I will stop using/processing the data accessed through this mode and shall erase any Personal Data as per the Digital Personal Data Protection Act, 2023.
6. I undertake that failure to comply with the requirements of these guidelines resulting in any data breach will lead to discontinuation of the service. I undertake to report data breach in accordance to the Digital Personal Data Protection Act, 2023. Further, this may entail legal action and monetary penalties as per Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023.
7. The Data Recipient or Data Fiduciary shall comply with the Information Technology Act 2000 and Digital Personal Data Protection Act, 2023.

This undertaking has been signed and executed by me on this_____ day of _____, 20 at _____. I do hereby declare that this undertaking has been given by me of my own volition without any undue influence or duress and that the foregoing statement is true and correct. I undertake to abide by and comply with all the terms of this undertaking.

Signature:_____

Name: _____

Annexure VII

Log Record Format

API audit logs are critical for tracking and recording actions and events related to API usage, ensuring security, compliance, and monitoring. All agencies granted API-based data access are required to maintain detailed logs for every API access. These logs must be preserved for a minimum of one year and provided to MoRTH either annually or upon request.

Request Timestamp	Request Method	Request URL	Request Headers	Request Body	Response Status Code	Response Headers	Response Body	Response Time	Client IP Address	Server IP Address	User Agent

Annexure VIII

Data Sets

A. Vahan Data Sets

- **Registration Details**
  - Registration Number
  - Registration Date
  - Registering Authority
  - Vehicle Status
  - Vehicle Blacklist Status
- **Purchase Details**
  - Purchase Date
  - Sale Amount
- **Vehicle Owner Details**
  - Owner's Name
  - Ownership Serial Number
  - Owner's Address
  - Permanent Address
  - Present Address
  - Owner's Father Name
  - Owner Mobile Number
  - Vehicle Owner History
  - Owner Category
  - Ownership Type
- **Vehicle Details**
  - Maker Name
  - Model Name
  - Chassis Number
  - Engine Number
  - Vehicle Colour
  - Vehicle Body Type
  - Wheelbase

- Vehicle Manufacturing Month/Year
- Vehicle Class
- Vehicle Category
- Vehicle Type(T/NT)
- Fuel Type
- Emission Norms
- Unladen Weight
- Laden Weight
- Number of Cylinders
- Vehicle Cubic Capacity
- Seating Capacity
- Sleeper Capacity
- Standing Capacity

- **Validity Norms**
  - Registration Validity
  - Fitness Validity
  - PUCC Validity
  - MV Tax Validity
  - Passenger tax validity
  - Goods tax validity

- **Dealer Details**
  - Dealer Name
  - Trade Certificate Number
  - Dealer Address

- **Used Car Dealer Details**
  - Dealer Code
  - Dealer Name

- **Permit Details**
  - Type
  - Number
  - Validity
  - Issuing Authority

- **Insurance Details**
  - Validity
  - Company Name
  - Policy Number
- **Hypothecation details**
  - Financer Name
  - Financer Address
  - Hypothecation type
- **NOC Details**
  - Reference Number
  - Date
  - State To
  - Transport Office To
- **Non-use information**
  - From Date
  - To Date
  - Reason
- e-Challan **details**
  - Date & Time
  - Place
  - Offence
  - Challan Number
  - Challan Amount

B. Sarathi Data Sets

- **Driving License Details**
  - Driving License Number
  - DL Issue Date
  - Issuing Authority
  - DL Category
  - Type of License
  - Class of Vehicle details
    - Description

    - Category
    - Issue date
  - Old Driving License Number
  - Last Endorsement Authority
  - Last Endorsement Date
  - Last Completed Transaction
  - Current License Status

- **DL Holder's Details**
  - License Holder's Name
  - Date of Birth
  - Photograph
  - Gender
  - Address
  - Permanent Address
  - Present Address
  - Previous addresses (if any)
  - Blood Group
  - Organ Donor Consent
  - Educational Qualification
  - Contact Number
  - E-Mail ID
  - Identification Marks
  - Son/Wife/Daughter of*

- **Validity**
  - Non-Transport Validity
  - Transport Validity
  - Hazardous Validity
  - Hill Validity

- **International Driving Permit (IDP) Details**
  - IDP Number
  - Issuing Authority
  - Issue Date
  - Validity

- **PSV Details**
  - Badge Number
  - Issue Date
  - Issued By
- **Adaptive vehicle Number**
- **Challan details**
  - Challan Number
  - Challan Source Type
  - Enforcement From Date
  - Enforcement End Date
  - Enforcement Remark
  - DL Intermediate Stage
  - RTO Action

C. e-Challan **Datasets**

- **Challan's Details**
  - Challan Number
  - Challan Date Time
  - Challan Location
  - Challan Location Lat-Long
  - State Name/Code
  - Circle/Area/Police Station
  - Challaning Authority Office
  - Challaning Officer Name
  - Department Code (TRAFFIC/TRANSPORT)
  - List of Offences
  - Challan Amount
  - Challan Status
  - Receipt No of Disposed Challan
  - List of Impounded Documents
- **Vehicle Details**
  - Vehicle Registration Number
  - Class of Vehicle

- **Challan Recipient Details**
  - Name (Challan recipient Name)
  - Father Name (Challan recipient Father Name)
  - Vehicle Owner Name
  - Vehicle Owner's Father Name
  - Driver Name
  - Driving Licence Number
- **Court Details**
  - Sent to Court Date-Time
  - Court Name
  - Court Address
  - Court Status of Challan
  - Date of Proceeding in Virtual Court
  - Fine Imposed in Virtual Court
- **Driving license Details**
  - Driving License Number

D. eDar datasets

- **Accident Basic Details**
  - Accident Id
  - Accident Date and Time
  - Accident Location
  - Point of Interest
  - Landmark Name
  - Severity of the Accident
  - Number of Vehicles Involved
  - Police Station
  - District
  - State
  - Driver
  - Passengers
  - Pedestrian
  - Road Classification
  - Road Name

- Collision Type
- Collision Nature
- Weather Condition
- Light Condition
- Visibility
- Initial Observation of Accident Scene
- Traffic Violation
- Accident Description

- **Vehicle and Driver Details**
  - Accident ID
  - Vehicle Damage
  - Vehicle Id
  - Vehicle Category
  - Hit and Run
  - Accused or Victim
  - Vehicle Type
  - Load Category
  - Skid Mark
  - Education
  - Occupation
  - Cellphone while driving
  - Severity
  - Injury Type
  - Seatbelt/Helmet
  - Drunk and Drive
  - Pedestrian Action

- **Vehicle Passenger Details**
  - Accident Id
  - Vehicle Id
  - Gender
  - Education
  - Occupation
  - Severity
  - Injury Type

- Mode of Hospitalisation
- Hospitalisation Delay
- Passenger Position
- Passenger Action
- Helmet/Seatbelt

- **Vehicle Pedestrian Details**
  - Accident Id
  - Vehicle Id
  - Gender
  - Education
  - Occupation
  - Severity
  - Injury Type
  - Mode of Hospitalisation
  - Hospitalisation Delay
  - Pedestrian Position

E. FASTag Datasets

- **Vehicle Details**
  - Vehicle Classes (VC1, VC2 etc)
  - Vehicle registration number
  - Vehicle exemption code
  - Commercial vehicle
  - Automatic vehicle class

- **FASTag Details**
  - FASTag id
  - Unique number printed on tag
  - TagCode

- **General Details**
  - Weight in motion
  - Lane Id
  - Lane Direction
  - Unregistered Flag (F/T)(1/0)

- Financial Year

- **Bank Details**
  - Merchant NETC code
  - Merchant Type (TOLL/Parking etc) we only receive plaza data
  - Merchant Sub Type (National/State)
  - Issuer Bank id in the NPCI system
  - Acquired bank id

- **Transaction Details**
  - Transaction seq. no. generated by NPCI for each txn.
  - Transaction no./id generated by acquirer bank
  - Transaction id generated by merchant/toll.
  - Transaction time captured by acquirer bank
  - Transaction type (Credit/Debit/Non-fin)
  - Original transaction id
  - Time at which the transaction was captured by reader
  - Transaction status:
    - Accepted,
    - Deemed Accepted,
    - Declined,
    - Pending.
  - Transaction Amount
  - Final settlement amount
  - Time at which transaction was received by NPCI
  - Transaction last updated at NPCI
  - Month of Transaction

Annexure IX

Abbreviation	Full Form
MORTH	Ministry of Road Transport and Highways
NIC	National Informatics Center
RC	Registration Certificate
DL	Driving License
eDAR	Electronic Detailed Accident Report
DPDP	Digital Personal Data Protection
NR	National Register
NTR	National Transport Repository
EODB	Ease of Doing Business
POI	Proof of Identity
NDSAP	National data Sharing Accessibility Policy
CAG	Comptroller and Auditor General of India
IRDAI	Insurance Regulatory and Development Authority of India
IIB	Insurance Information Bureau
GSTN	Goods and Services Tax Network
CBI	Central Bureau of Investigation
IB	Intelligence Bureau
NIA	National Investigation Agency
NATGRID	National Intelligence Grid
CBIC	Central Board of Indirect Taxes
SPG	Special Protection Group
OTP	One time password
API	Application Programming Interface
NGO	Non-Government Organisation

Abbreviation	Full Form
PII	Personally Identifiable Information
PUCC	Pollution under control certificate
MV Tax	Motor Vehicle Tax
T/ NT	Transport/ Non-Transport
NCRB	National Crime Record Bureau
NOC	No Objection Certificate
RTO	Regional Transport Office
IDP	International Driving Permit
PSV	Public Service Vehicle
PVC	Polyvinyl Chloride Card
OEM	Original Equipment Manufacturer
HSRP	High Security Registration Plate
VLTD	Vehicle location tracking Device
ICCC	Integrated Command Control Centre
VLTS	Vehicle location tracking system
IMEI	International Mobile Equipment Identity
CSC	Common Service Centre
DGQI	Data Governance Quality Index
NAPIX	NIC API Exchange Gateway
IIT	Indian Institute of Technology
MFA	Multi factor Authentication
IP	Internet Protocol
CERT-IN	Computer Emergency Response Team
OS	Operating System