german cooperation
DEUTSCHE ZUSAMMENARBEIT

Published by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Ministry of Housing and Urban Affairs
Government of India

Green Urban Mobility Partnership

5

CREATING FRAMEWORK FOR MOBILITY AS A SERVICE (MaaS) IN INDIAN CITIES

LEGAL AND REGULATORY FRAMEWORK

Published by
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Integrated and Sustainable Urban Transport Systems
for Smart Cities (SMART-SUT)
GIZ Office
B-5/2, Safdarjung Enclave
New Delhi-110029
INDIA
T +91 11 49495353
F +91 11 49495391
I http://www.giz.de/india
E giz-indien@giz.de

As at
October 2021, New Delhi

Prepared by
SMART-SUT (GIZ), Cities Forum and CoE-UT, CEPT
Reasearch and Development Foundation (CRDF)

Officer responsible for the commission
Juergen Baumann
Project Head, SMART-SUT (GIZ)

Project Advisor
Laghu Parashar
Deputy Project Head, SMART-SUT (GIZ)

Project Coordinator
Narendra Verma
Technical Expert, SMART-SUT (GIZ)

Project Team
Cities Forum: Shailendra Kaushik, Sonal Ahuja,
CoE-UT, CEPT Reasearch and Development
Foundation (CRDF): Shaily Gandhi

Design by
Chitrapat Ideas Foundry

Editing support
Appurva Chauhan

Contact
GIZ is responsible for the content of this publication on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ)

ABOUT THIS REPORT

This report has been prepared as a part of bilateral technical cooperation project “Integrated Sustainable Urban Transport Systems for Smart Cities (SMART-SUT)” commissioned by the German Federal Ministry for Economic Cooperation and Development (BMZ) and jointly implemented by Deutsche Gesellschaft fuer Internationale Zusammenarbeit (GIZ) GmbH and Ministry of Housing and Urban Affairs (MoHUA), Government of India. The objective of the project is to improve the planning and implementation of sustainable urban transport in selected Indian cities. The project also supports the Green Urban Mobility Partnership (GUMP) between the governments of India and Germany.

Indian cities selected under National Smart Cities Mission are planning, designing, developing, and implementing various urban mobility projects. All these projects, after implementation, produce a huge amount of data. Thus, the management of the mobility data is at centre of increasingly complex urban transport challenges in these cities. The mobility data generated from various sources and in various forms could be used for providing an integrated journey experience to the commuters which is known as ‘Mobility as a Service or MaaS’. Though providing such a service to commuters would require developing standard data collection and management protocols, strong institutional and regulatory framework, interventions related to urban mobility data policies and so on. With this objective in mind, SMART-SUT initiated the study titled “Creating Framework for MaaS in Indian Cities”.

The study aims to explore opportunities for implementing MaaS in Indian cities and identify a structured approach towards developing a smart mobility ecosystem which is required for developing such a solution by leveraging the real value of mobility data. The study outlines a stepwise approach and set of recommendations towards implementing a MaaS solution in the Indian context, a series of reports have been compiled as an output of this study covering various aspects of MaaS. The recommendations from these reports would assist Indian cities embarking on developing various data-driven mobility solutions like MaaS by integrating different transport modes.

ACKNOWLEDGEMENT

The project team would like to thank all the individuals, experts and organisations who have provided continuous guidance and support during the course of this study and preparation of various reports.

The team would like to acknowledge contributions from the various city representatives during stakeholder consultations that took place in various stages throughout the study. We would like to thank Ms V Manjula, Commissioner, Directorate of Urban Land Transport (DULT), Mr Shamanth Kuchangi (DULT), Mr G P Hari, Additional General Manager (Urban Transport), Kochi Metro Rail Ltd (KMRL), Mr Vishal Khanama, General Manager, Ahmedabad Jan Marg Limited (AJL) and other representatives of DULT, KMRL, AJL for their support and knowledge contribution.

Our sincere thanks to Prof Shivanand Swamy, Director Emeritus, Centre of Excellence in Urban Transport, CEPT University, Mr Ravi Gadepalli (Public Transport Expert and Independent Consultant) and Mr Rishi Kothari (World Bank) for providing their valuable feedback and unbiased perspective on challenges and opportunities of MaaS ecosystem in Indian context during the focused group discussions (FGDs) organized by SMART-SUT. Additionally, we would like to appreciate and value the discussions and feedbacks received from all the participants during the consultation.

We would also like to thank Mr Amit Gupta, Mr Harshal Gupta and Mr Jaideep Kapani (Yulu), Mr Arjit Soni, Mr Ajaysinh Solanki and Mr Mufish Saiyed (Mybyk), Ms Anudeepika Jain (Uber), Mr Anish Michael and Mr Roshan Toshniwal (Ola Mobility Institute) for sharing their perspective on operational concerns in MaaS ecosystem from the viewpoint of private sector service providers.

We are also thankful to Mr Shirish Mahendru (Technical Expert, SMART-SUT, GIZ) and Mr Amegh Gopinath (Technical Expert, SMART-SUT, GIZ) for providing their valuable suggestions during internal group consultations.

Special thanks to Mr Yale Wong (ANZ Market Lead, Cities Forum) for peer review of various study outcomes, Mr Dipu Joy (Senior Transport and Regulatory Expert, Cities Forum), Mr Jaime Ruiz and Ms Zeina Nazer (Co-Founders Cities Forum) for providing expert inputs on various aspects of MaaS ecosystem.

We would also like to thank Mr Khelan Modi, Ms Nikita Bhakuni and Ms Sangeetha Ann from Center of Excellence - Urban Transport (CoE-UT), CRDF for assisting the project team with data collection and analysis.

The team would like to acknowledge the contribution of Mr Arpit Kanv and Ms Ronika Postaria (Associate Consultants, Cities Forum), Ms Madhura Kawadkar (CoE-UT, CRDF) for providing extensive support to the project team during report preparation. We would also like to acknowledge the contribution of Mr Deepak Bhardwaj (Cities Forum) in development of web based MaaS toolkit.

During the course of study, the project team had interactions with global industry partners and MaaS experts who provided their advice on technical details of MaaS solution. We are thankful to the contributions of Mr Adrian Ulisse, Mr Satinder Bhalla, Mr Walid Ward, Ms Lina Al Shnaikat and Mr Meshack Ochieng in this regard.

The team is hopeful of the study outcomes being a useful guide for deploying the MaaS ecosystem in Indian context.

CONTENTS

LIST OF TABLES

LIST OF FIGURE

DEFINITIONS

S.No.	TERMS	DEFINITIONS
1	Data Principal	A "data principal" is the natural person to whom some personal data relates.
2	Data Fiduciary	A "data fiduciary" is any person - including the state, a company, or a juristic entity-who, either alone or with others, determines the purpose and means of processing the personal data.
3	Data Processor	A "data processor" is any person who processes data on behalf of a data fiduciary; however, it does not include an employee of a data fiduciary.
4	Social Media Intermediary	"Social media intermediary" is any entity that enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
5	Consent Manager	A "consent manager" is a data fiduciary registered with the authority and enables a data principal to gain, withdraw, review and manage their consent.

1 BACKGROUND

India is going through a rapid digital transformation in the transport and mobility sector. It is estimated that with the current pace of access to internet-enabled smartphones, the internet user base in the country will rise to 829 million people by 2022. Approximately, 97 percent of the internet users across India have access to internet through mobile devices. The user base for these smartphones is expected to cover almost 60% of the population[1].

Smartphones with high-speed internet and various sensor technologies can now generate, record and store a high volume of useful data in phones and applications that feed on personal information. While this data can help solve many mobility problems, it builds on a high potential to overlook privacy issues and personal data exploitation, for commercial purposes.

Hence, it is essential to comprehend how this 'smart' transport data is being generated and managed and decide as to which data can be used to develop mobility solutions. Further, mechanisms for data sharing by the government and mobility companies need to be established so that this could be leveraged to provide innovative travel solutions. In this process, it is critical that the privacy of the users must be ensured under the existing legal frameworks.

Mobility as a Service (MaaS) is an emerging smart mobility service that provides access to integrated journey options across different transport modes in a city using a single travel booking and payment platform to its users. With multimodal transport system in the city, MaaS provides commuters with seamless travel options, ascertaining a comfortable journey. The key aspect that enables this solution is the data sharing between different modes and service providers. The study titled "***Creating Framework for Mobility as a Service (MaaS) in Indian Cities***" aims to identify measures that are required for developing a MaaS solution. The objective of the study is :

- To develop a framework for an effective implementation of "Mobility as a Service (MaaS)" in Indian cities.
- To recommend the requisite data and system specifications for implementing MaaS in Indian cities.
- To design an effective policy and a regulatory framework by contextualizing issues related to data sharing in India.
- To develop a capacity-building toolkit for a better understanding of MaaS and facilitating the decision-making process for its successful implementation in Indian cities

Following reports have been compiled and documented* as an output of this study covering various aspects of MaaS :

i. Basics of MaaS and Learnings from Global Case Studies
ii. MaaS Readiness Tool
iii. Urban Mobility Data Policy
iv. Mobility Data Standards and Specifications
v. Legal and Regulatory Framework
vi. System Architecture and Technical Requirements.
vii. Reference 'Scope of Work' Document for MaaS Project

This report outlines the requisite legal and regulatory framework for implementing MaaS projects in India.It provides a detailed snapshot of the regulatory frameworks related to MaaS around the world,focusing on the legislation in different countries that have outlined the guidelines for commercial use of personal user data.

It explores different aspects of MaaS ecosystem, in particular the role of associated data requirements and the current legislation in India related to personal data protection. Finally, it

[1] https://icea.org.in/wp-content/uploads/2020/07/Contribution-of-Smartphones-to-Digital-Governance-in-India-09072020.pdf

*All the reports can be accessed via https://www.maastoolkit.org/ which has been developed as a web-based capacity building toolkit and an open source knowledge resource for all the stakeholders and government agencies planning to implement MaaS in Indian cities.

summarises the complexities and associated gaps with current data sharing ecosystem and lays out required regulatory framework to fulfil the identified gaps in line with ongoing initiatives of the Government of India in this direction.

2 MaaS: AN EVOLVING CONCEPT

The definition of mobility as a service (MaaS) is rather new. It may be considered a principle (a modern way of thinking about mobility), a pattern (occurring as new behaviours and technology emerge), or a new form of transportation (which merges the different available transport modes and mobility services). In summary, MaaS is a versatile, customised, and on-demand mobility service model in which a service provider offers the consumer all of their transportation needs on a single platform[2].

The primary catalyst for MaaS is the availability of an internet based or smartphone based application where the MaaS operator does not own any vehicle fleet but provides demand-responsive mobility to its users through this application. The definition envisions a seamless mix of all modes of transportation and a 'mobility aggregator' that collects and sells all services into a single mobile app, allowing for integrated fare payment and one-stop billing[3].

The mentioned single payment can be made only through a registered account with the user's personal details. With this registration and a monthly subscription, the user can choose "pay-as-you-go" or "pre/post-pay" payment options. By adding user details and travel choices, subscription helps personalise and frame the accessibility systems around user's interests helping the user travel conveniently. The current public transport systems do not provide this comfort of combining various modes according to the users' interests and needs, thus, potentially shifting people to private modes for this customisation[4].

One of the key components of this customisation in MaaS is Information and Communications Technology (ICT) which enables the data gathering, transmission, processing, and presentation to determine the best mode of transportation for the user's needs. This is possible due to the technical advancements, the collaboration between multiple carriers, and the bundling of various modes of transportation.It often aids knowledge integration and convergence between customers, suppliers, and facilities[5]. Moreover, mutual customisation/personalisation benefits both the consumers and the transport suppliers by tailoring packets to the heterogeneous needs of subscribers (i.e. preference in mode choice[6]).

2.1 ROLE OF DATA AND ASSOCIATED REGULATIONS

Data is considered as the engine of MaaS and Intelligent Transport System (ITS) the backbone of data collection. Therefore, to use the data efficiently for MaaS, ITS is crucial. The European Union directive defines intelligent transport systems in their "ITS Directive" (Directive 2010/40/EU) as "systems in which information and communication technologies are applied in the field of road transport infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport".

To support the decision-making process, governments across the globe emphasise on making their transport systems intelligent to capture and make use of data. Therefore, these cities plan (short and long term) strategies for meeting their mobility demand efficiently and sustainably using innovative business concepts like MaaS.

[2] Hietanen, S. (2014). "Mobility as a Service"—The new transport model? Eurotransport, 12(2), 2–4

[3] CIVITAS. (2016). Mobility-as-a-Service: A new transport model. Retrieved from http://civitas.eu/content/civ itas-insight-18-mobility-service-new-transport-model.

[4] Atasoy, B. et al. (2015) 'The concept and impact analysis of a flexible mobility on demand system', Transportation Research Part C: Emerging Technologies, 56, pp. 373–392. doi: 10.1016/j.trc.2015.04.009.

[5] Nemtanu, F., Schlingensiepen, J., Buretea, D., &Iordache, V. (2016). Mobility as a Service in smart cities. In A. Zbuchea& D. Nikolaidis (Eds.), Responsible entrepreneurship—Vision, development and ethics: Proceedings of the 9th International conference for entrepreneurship, innovation and regional development. June 23-24, 2016 Bucharest, Romania (pp. 425–435). Bucharest, Romania: Comunicare.ro.

[6] Hietanen (2014); Hietanen, S. (2014). "Mobility as a Service"—The new transport model? Euro transport, 12(2), 2–4)

i. Need for collection of data

With the advent of newer technologies and an app-based transport mobility marketplace driven by location based user and infrastructure information, the data flows from various ITS systems deployed by city authorities.

Some of the priority areas from where the information and data flow are -

- Adaptive traffic control systems – to provide priority to road-based public transport vehicles, freeway management and information systems to reduce delays due to traffic incidents,
- Electronic fare collection systems – to improve the convenience of public transport travel and reduce system costs,
- Electronic tolling, vehicle location and scheduling systems – to reduce theft, improve roadside service, and the efficiency of freight movement,
- Advanced traveller information systems – to improve users' understanding,the efficiency of public transport systems, and congestion management in the cities.

These systems generate a huge quantum of data, and such data is fed into MaaS to provide the services to transport users. While the data is exchanged between various companies, its privacy and security have become a critical concern that needs to be looked into for any MaaS application development.

ii. Factorising users' rights

According to Warwick Goodall, MaaS depends not only on a combination of heterogeneous components but also on a strategic policy of balance between the private sector and public interest, and most importantly, on the involvement of people. Thus, users become an inevitable part without whom the system cannot function. Since data is the key factor of MaaS, establishing clear and fair rules for controlling information is crucial, especially the users' private data. Thus, from a legal perspective, ITS raises several questions concerning the control of information, specifically about the security of the technological platform where it is managed, the protection of personal data, the accuracy of data concerning roads, traffic and travel, and the transparency and accountability of all processes involved.

iii. Striking a balance

As mentioned above, transparent rules are needed to control users' information. Achieving and maintaining a balance between the public and the private institutions in terms of protecting the user's rights is vital to evolve technology-driven data collection and further MaaS as an ecosystem. Any legal and regulatory factor thus needs to focus on striking a balance between the data usage and users' rights.

3 DETAILS OF MaaS ECOSYSTEM

3.1.CHARACTERISTICS OF MAAS ECOSYSTEM

Mobility as a Service comprises various components and have certain core characteristics, as summarized in table 1:

Table 1- Characteristics of the MaaS ecosystem

S.No.	Characteristics	Description
1	Bundling of Modes	The core objective of the Mobility as a Service concept is to integrate various modes in a city and provide a combination of multiple modes to the users with the ease of single payment. These modes can be public transportation, taxi, car-sharing, ridesharing, bike-sharing, car-rental, on-demand bus services, etc.
2	Single Platform	MaaS integrates different modes, services, and transport operators under a single platform (an internet-based application). This enables the user to plan their journeys conveniently and in advance with a single payment. A single platform also helps in effective communication and interaction between different stakeholders involved like mobility users (e.g., private users or business customers), Third-party service providers, local government (as the regulatory body or direct owner of transportation modes), data storage telecommunication, private transportation services, etc.

S.No.	Characteristics	Description
3	Use of Technology	The concept of MaaS evolved with the advancements in technologies. Some of these technologies are – mobile computers and smartphones that acquire data; a secure mobile internet network (WiFi, 3G, 4G, LTE); GPS; e-ticketing and e-payment system; database management system; and integrated infrastructure of technology.
4	Demand Orientation	The effectiveness of MaaS is based on providing the best combination of transport services from the customer's perspective through multimodal trip planning and the inclusion of demand-responsive services like a taxi and other private services.
5	Registration Requirement	The user needs to create an account and provide their details with travel choices, which helps to provide the best possible combination (of transport services) options for their journeys. The payment methods can also be saved at the time of registration for an easy online payment option.
6	Customisation of Interface	End users can choose from the available service options suggested based on their needs through customisation. To better achieve their desired travel experiences, they can freely compose a unique chained trip or create multiple mobility packages with varying transportation mode choices. Such attributes can increase the appeal of MaaS to the users.

3.2. BUILDING BLOCKS OF MAAS

The fundamental building blocks of MaaS are infrastructure, technology and financial transactions[7]. An overview of a MaaS data ecosystem is presented in figure 1[7], which provides the tentative data representation from the demand and supply side, i.e. the consumer and the provider, shared with the third party MaaS operator to run MaaS effectively.

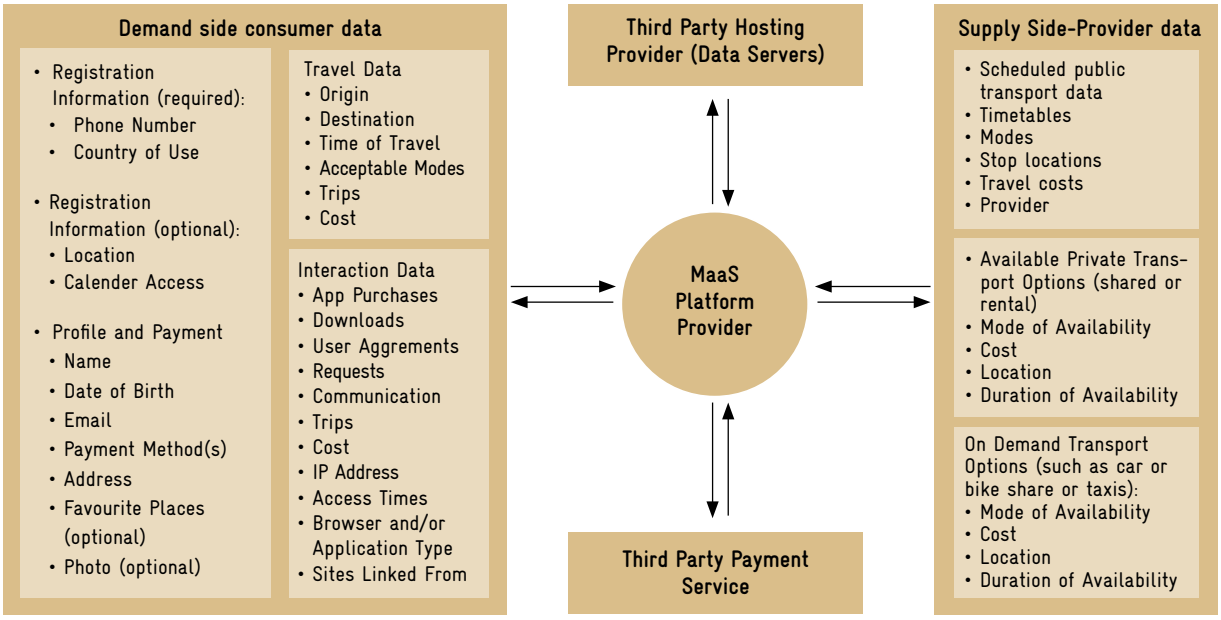


Figure1 MaaS ecosystem with data representation on both demand and supply-side along with the representation of stakeholders [7]

[7] Cottrill, C. D. (2020) 'MaaS surveillance: Privacy considerations in mobility as a service', Transportation Research Part A: Policy and Practice. Elsevier, 131(xxxx), pp. 50–57. doi: 10.1016/j.tra.2019.09.026.

The three major components of the MaaS ecosystem[8] are mentioned below -

3.2.1 Infrastructure

- A data-sharing platform for MaaS
- Data centre for storing and collecting data securely
- Data transmission infrastructure for fast interaction between different stakeholders and planning journey dynamically

3.2.2 Technology

- Integration of all transport modes and access through a unified interface
- Providing service byusing data analytics and real-time planning

3.2.3 Financial Transaction

- Ticketless transactions – use of smart card/e-wallets
- Unified payment interface (UPI) for interoperability of all payment systems

3.3 USER DATA REQUIREMENT ASSOCIATED WITH THE MaaS

Continuous data exchange between various stakeholders of the MaaS ecosystem is an essential component for successful implementation. To understand the type of data requirements for this exchange from the user ('data principal'), and to allow proper functioning of a MaaS platform, three international MaaS data platforms were analysed:

3.3.1 Whim App

Whim is run by MaaS Global. The app user can access various transportation modes like public transport, bike share, rental cars and taxis. The application suggests ways for the users to successfully reach the destination.It learns from user preferences and incorporates intelligent suggestions of mode choices and transfer location to reach the destination. The scope of this app is limited to Helsinki city.

Following are the details of user data collection by Whim app[9] -

- Data requirement by Whim app – basic and personal details include a telephone number, name, email address and street address. devices, home country, language, credit card details and other payment details
- Data requirement for information verification– personal identification number or photo or driving license details
- Positioning and location data– these technologies can entail sharing the location data, as well as specific computer and telephone, Wi-Fi, or other network-related identifiers with MaaS Global. When travellers use location-based services and features, such as location-based search, navigation, routing, or request map data, the location data is sent to MaaS Global to serve you with the appropriate content, which may also include and support location-specific services.
- Travel data – The travel data includes the trip start and end location with travel times.

3.3.2 Moovel App

In Stuttgart and Hamburg, travellers can pay for public transportation using their phones. Moovel is operated by Daimler; the services for the app are available in Germany and Helsinki. It's a single app to find, book, and pay for rides from car2go, mytaxi, and Deutsche Bahn.

[8] Mobility-as-a-Service (MaaS): Need of the Hour for India | BusinessMaaS.com (no date). Available at: https://www.businessmaas.com/apps/mobility-service-maas-need-hour-india/ (Accessed: 31 May 2021)

[9] WHIM SERVICE TERMS Effective date: 18. June 2019; Web Address- https://whimapp.com/terms/); Accessed on 20th May 2021

Following are the user data requirement in Moovel app[10] -

- Data requirement by Moovel app – name, email address, phone number, date of birth, country of residence, language, and time zone.
- Specific information of users' devices – specific information about and across users' devices, such as the product model, serial number, operating system, device settings, device performance, internet service provider, IP address and other unique identifiers.
- Positioning and location data– the Moovel app collect and process data about travellers' location if approved by the user. We tailor our services to best support you and our transit partners when we have your location details.

3.3.3 Bridj App

Bridj is a smartphone based on-demand commuter shuttle service that allows passengers to ride a shuttle between home and work during commuting hours. Bridj optimises pick-ups and drop-offs on demand using a fleet of flexible cars, resulting in a 40–60 percent more effective trip than conventional transit. Bridj is run by Bridj Inc.,and the scope of services for the app is limited to commuters in Boston, Kansas city, and Washington,D.C.

Following are the type of data collected by the Bridj app -

- Name and contact details (including email address and phone number);
- Past searches on the Bridj app and traveller location at the time of those searches;
- Trip and payment history;
- Payment details (such as your credit card or direct debit details);
- Feedback and ratings on your past trips;
- Device information and the operating system of your device; and
- IP address

3.3.4 User's Data Summary

Studying the operations and data requirements of Whim, Moovel and Bridj MaaS smartphone based applications, it can be understood that there is multi-level data interaction and exchange between the user and company operating the MaaS platform. At the time of registration,the requirement of some basic information like name, age, gender, date of birth, email address, residence address, home country, language, etc., is common -

- Another level of information and data acquired by the applications is at the time of verification of the information entered. The user has to submit a photo identification ID, for example, a driving license.
- Data related to trips stored by the application includes the origin and destination, along with the start and end time of the trips. The ratings are given to different stakeholders by the user
- Also, as the payment gateway is attached with the MaaS application and is, in most cases, operated by third-party operators, there is a certain level of information exchange between the smartphone application, including details of credit card and other information related to payments. The application also uses the transaction histories and other details attached to the payment.
- The MaaS platform operators list two major reasons for storing the detailed data information from travellers -

  a. Improvement of the application platform and adding capabilities to the current version

  b. For running commercial advertisement targeting travellers with specific behavioural interests

[10] MOOVEL NORTH AMERICA, LLC; privacy policy; Web Address- https://www.moovelus.com/privacy-policy/), Accessed on 20th May, 2021

4 REVIEW OF PERSONAL DATA PROTECTION REGULATIONS

For determining India's approach to data protection,especially considering the mobility marketplace, it is instructive to look at practices followed in other jurisdictions, particularly recent models that have emerged. A review of several case studies demonstratethat there are two distinct models in the field of data protection –the EU and similar models; and theAmerican model. In this report. A review of these models in the context of mobility service products was done.

Around 80 countries in the world have enacted data privacy laws. This report summarises and recommends the privacy protection laws that must be used for MaaS projects. Many countries have set precedents that other countries follow. The European Union: General Data Protection Regulation was studiedin detail and the key features of other personal data protection laws were summarised in table 2 for simplicity of understanding. Following is the list of global personal data protection laws summarised in this report -

i. European Union: General Data Protection Regulation (GDPR) – (presented in more detail as its particularly relevant to MaaS in India)
ii. USA: California's Consumer Privacy Act (CCPA)

In addition, a comparative summary has been provided along with the following countries:

- Brazil: General Data Protection Law (LGPD)
- Japan: Act on the Protection of Personal Information (APPI)
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

4.1 EUROPEAN UNION: GENERAL DATA PROTECTION REGULATION (GDPR)

4.1.1 When Was GDPR Enacted?

The General Data Protection Regulation (GDPR) is a revision of the 1995 Data Protection Directive 95/46/EC, sometimes known as the DPA. The GDPR came into effect on May 25, 2018. It has been highly significant and received more attention than any other data protection regulation in history. The GDPR was implemented to reflect developments in technology and consumer behaviour.

4.1.2 Who Is Affected By GDPR?

Organisations that collect, retain, distribute, or handle data that might be used to identify a person from an EU state is subject to GDPR. It impacts businesses of all sizes and types, regardless of where they are located in the world. However, documentation standards are less stringent for businesses with less than 250 workers.

4.1.3 What Data Is Covered By GDPR?

GDPR is all about personal data. The law classifies data into two types:

Personal data: Any data that can be used directly or in an aggregated form to identify an individual. Examples include name, address, date of birth, IP address, and financial information.

Sensitive personal data: If data is deemed "sensitive" under GDPR, more stringent measures will be applied to its protection. Sensitive data includes genetic data, biometric data, and data on life preferences, e.g., religious, racial or ethnic origin.

4.1.4 Basics of the Data Privacy Law

The law has been written to represent a legal framework for data processing. For instance, "consent" is regarded as a legal foundation for data usage. As a result, consent has become a key legal phrase, with companies being required to get "explicit and affirmative consent" before processing data. The GDPR establishes eight fundamental rights for individuals, sometimes known as "data subjects" -

- Right to be informed (about personal data use)
- Right to access (data)

- Right to data rectification (if errors in data are found)
- Right to data erasure (data deletion)
- Right to request the restriction of data processing
- Right to data portability (between services and platforms)
- Right to object to use of data
- Right to say no to automated decision-making, including profiling

The GDPR establishes the terms “data processor” and “data controller.” Depending on their function in data handling, each has different compliance obligations.

4.1.5 Fines and Other Important Points of the GDPR

The GDPR established two tiers of penalties, both of which are taxing.

Level 1: 2% of yearly worldwide income, or ten million euros, whichever is greater. Issues concerning data breaches, failure to undertake a Data Privacy Impact Assessment (DPIA), and inadequate record-keeping are all examples of non-compliance.

Level 2: 20 million euros or 4% of annual global income. Non-compliance in areas such as failing to get consent or safeguarding consumer rights under GDPR standards.

4.1.6 Compliance Requirements of MaaS As Per GDPR

For MaaS to work in a european context, it must be responsive to GDPR requirements related to privacy by design, consent, protection, and security. It must, in short, respond to an environment that both demands data revelations and protects them as per the following provisions -

- GDPR is applicable to personal data and sensitive personal data. Under this, personal data is defined as, *“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference toan identifier such as a name, an ident fication number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*[11]

Under the EU GDPR, the supervisory authority[12] set up in every member state has the power to investigate complaints relating to the breach of any of the rights of the data subject. The supervisory authority has a wide range of investigative powers and corrective powers. A ‘data subject’ may file a complaint with the supervisory authority regarding the processing of personal data that infringes the EU GDPR.

Also, it is evident from GDPR rules that MaaS service provision will include both “data controllers and data processors”. The supervisory authority has the power to impose an administrative penalty on the data controller where the latter has breached the provisions of the EU GDPR.

To summarise, some of the key points to be codified from GDPR while adapting to MaaS are as follows -

a. Clarity in language that adequately represents the practices by relevant service proviers while taking consent from users
b. Incorporation of privacy in the design principles of the system architecture, particularly in instances where the sharing of data between processors is necessary for service provision or utilisation
c. Regulate data collection as well as duplicity of data collected from different sources
d. Establish uniform compliances to all stakeholders, including government agencies
e. Appoint fiduciary and make them accountable for data (both collected and disseminated)

Thus, all cities across Europe, like Madrid, Barcelona, Berlin, Helsinki, etc., have a varying degree of GDPR framework when it comes to data security and privacy protection without losing the essence of GDPR regulations.

[11] 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. Official Journal of the European Union (OJ) 59, 1–88

[12] White Paper Of The Committee Of Experts On A Data Protection Framework For India, pp 13 authority[12]

4.2 UNITED STATES

In contrast to the EU privacy laws, in the USA, privacy protection is essentially a "liberty protection",i.e. protection of the personal space from the government. Thus, the American understanding of the "right to be let alone" has come to represent a desire for as little government intrusion as possible. US courts, however, have collectively recognised a right to privacy by piecing together the limited privacy protections reflected in the US constitution[12].

In addition to the common law (at thefederal level), most states have their own statutory framework. Hence, when it comes to a legal framework for MaaS, in the USA, different states have different frameworks for users' data protection and privacy concerns, the prominent ones being in Los Angeles and Oregon.

4.2.1 City of Los Angeles Department of Transportation (LADOT)

Amongst other data frameworks, a notable one is that of LADOT's Mobility Data Specification (MDS) format introduced in 2018. MDS is a set of Application Programming Interfaces (APIs) focused on dockless e-scooters, bicycles, mopeds and car share. APIs help get data to and from the user's mobile device to the backend system of a mobile service the user might be using. MDS consists of three APIs: provider, agency, and policy; each of them adheres to best practices for privacy standards, commits to data collection transparency, and above all else protects citizen privacy as its first principle. For this, MDS uses particular vehicle IDs – pretty much as IP address to a website owner – but here, the geolocation related data is masked. Thus, the agency & authority do not have direct access to the users' data unless requested through a warrant from a court of law.

4.2.2 Oregon Department of Transport (ODOT):

In May 2020, ODOT published a working paper on the implementation of MaaS in Oregon city[13]. For data privacy and geolocation policy, data has been identified as 'Personally Identifiable Information' (PII), indicating its sensitivity. ODOT's policy, ADM 08-01, guides the agency's collection and use of passive electronic data in a way that is transparent and ensures protection of the privacy and sensitive information of the public, including collected personal information. This policy can inform potential legislation that expands protections beyond the data collected by ODOT. After conducting the OReGO project, a pilot project on data collection for road usage charges, the legislature provided strong provisions to protect PII, including the fact that the public records advocate (in this case, the fiduciary) should function separately and independently from any other state agency, giving more responsibility and autonomy to fiduciary.

4.2.3 Comparative Summary of Privacy Regulations

Table 2 Key features of international privacy laws

	Canada: PIPEDA	Japan: APPI	Brazil: LGPD	European Union: GDPR	California: CCPA
Year of Implementation	2004	2017	First published in 2018	2018	2020
Scope of Application	PIPEDA only applies to private sector organizations when they are engaged in "commercial activity." Public sector bodies are subject to another law, the Privacy Act.	APPI applies to companies that offer goods and services in Japan both located within the country and with offices outside of Japan.	Processing data of persons who are in Brazil's territory, regardless of where the data processor is situated in the globe, No minimum threshold	European residents, No minimum thresholds	California residents, minimum thresholds

[12] White Paper Of The Committee Of Experts On A Data Protection Framework For India, pp 13

[13] https://www.oregon.gov/odot/Planning/Documents/MaaS%20White%20Paper%20Final%205-13-2020.pdfhttps://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

	Canada: PIPEDA	Japan: APPI	Brazil: LGPD	European Union: GDPR	California: CCPA
Year of Implementation	2004	2017	First published in 2018	2018	2020
Definition of Personal Information or other relevant term	Any data that can be used to identify an individual is deemed to be "personal information.".	Personal information: Identifying data such as name, address and biometric data but also includes driver's license numbers and similar.	Personal data: From the LGPD: "information regarding an identified or identifiable natural person".	• Uses "Personal Data" • Refers to identified or identifiable natural person	"Identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"
Definition of Sensitive personal information or other relevant term	Not legally defined term in PIPEDA. However, some personal information is regarded as being "sensitive" in the non-technical sense and requires additionawl care. This includes medical records, income records and information about sexual orientation	"Special care-required" personal information: This is deemed to be data that could be used for discrimination or prejudice. Typical data that sits in this category are medical information, marital status, "creed," social status, criminal records and so on.	Similar data is contained in this sub- category as in the same sub- category in GDPR, including racial or ethnic origin, religious belief, political opinion, health data and sexual preferences.	Sensitive data includes genetic data, biometric data and data on life preferences, e.g., religious, racial or ethnic origin.	Sensitive information such as personal characteristics, behavior, religious or political convictions, sexual preferences, employment and education data, financial and medical information
Individual Rights	Acesss to data copies, rectification of errors, right to deletion / right to be forgotten, right to object to processing, right to data portability, right to withdraw consent, right to complain to the relevant data protection authorities	Right to disclosure, correction, add or delete data, stop the use of data, erasure and stopping provision to third parties.	• Access, confirmation, rectification, consent in data portability • Respond within 15 days	• Access, delete, rectification, data portability, object • Respond within 30days	• Disclosure, access, delete, opt out of sale of information • Respond within 45 days
Fines	An organization found to be in non- compliance with PIPEDA, can be fined up to CAD $100,000 per violation	It may be subject to imprisonment of up to one year, or a fine of up to 500,000 yen (Id. Article 83).	Range from simple warnings to fines of up to 2% of the organization's revenue in Brazil, limited to BRL$ 50 million per violation.	•Up to 4% global turnover or €20 million	• Civil fines: $2,500-$7,500 • Private right of action: for data breaches if failure to maintain reasonable security. Statutory damages $100-750
Key Terminologies	• Commercial activity • Organisations • Breach of security safeguards etc	• Data controller • Datap rocessor • Principal etc	• Data Controller • Data Processor • Data Subjectetc	• Data subject • Controller • Processor etc	• Consumer • Business • Service Provider • Third Party (not a business or service provider for example may be an entity that was sold data from the business)

4.3 CURRENT STATE OF PERSONAL DATA PROTECTION IN INDIA

4.3.1 General

Though India is not a signatory to any data protection convention, the conditions of operation, existence of multimodal mobility players and federal structure of the Indian states make the situation comparable to the EU, where the GDPR or the Data Protection Directive is applicable. Other international declarations and conventions that recognise the right to privacy, such as 'Universal Declaration of Human Rights' and 'International Covenant on Civil and Political Rights', have been adopted by India or to which it is a member[13].

India does not have a stand-alone personal data protection law to protect personal data and information shared or received in a verbal, written, or electronic form.Though protections are available, they are contained in a mix of statutes, rules, and guidelines. Majority of the provisions only apply to 'sensitive personal data and information' collected through 'computer resources'. These provisions are restricted to corporate entities undertaking the automated processing of data, and consumers are only able to take enforcement action in relation to a small subset of the provisions.

The Information Technology Act (2000) ("IT Act"), which was amended by the Indian legislature to include Sections 43A and 72A, provides indirect data protection to a certain extent. The IT Act includes a right to reimbursement for wrongful disclosure of personal information and specific rulings of the Supreme Court of India in their judgements.

The primary law in India dealing with electronic commerce and cybercrime are contained in the Information Technology Act, 2000 (as amended by the Information Technology Amendment Act, 2008), The Information Technology (Reasonable Security Practices) and "Procedures and Sensitive Personal Data or Information Rules, 2011" (SPDI Rules). SPDI rules do not cover data and information that is exchanged in non electronic or physical format. These rules are only applicable to any exchange of data that takes place in electronic format. This gap was addressed with the introduction of the Information Technology Bill, 2006 in the Indian Parliament that led to the Information Technology (Amendment) Act, 2008.The act came into force on October 27, 2009. section 43A, 72, 72A are the prime sections that deal with personal data, privacy, and its protection. However, these laws are not holistically applied to government agencies that collect and disseminate the data.

Based on the gaps in the IT Act 2000, due to advancement of technologies, a bill was introduced in 2018 as "Indian Privacy Codes 2018", which was then revised by the Ministry of Electronics and Information Technology (MEITY), as Personal Data Protection Bill, 2019 (the Bill), in the Lok-Sabha on December 11, 2019. The bill proposes to supersede the Information Technology Act, 2000 (Section 43-A).

The bill covers the following -

- Application of the act to processing of personal data
- Type of personal data
- Obligations of data fiduciary
- Restriction on transfer of personal data outside India
- Exemptions

4.3.2 Understanding Data Protection As Suggested In Section 43A of the IT Act

Under this section of the IT Act, the central government of India released the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Rules"). On August 24, 2011, a clarification to the above rules (the "Clarification") was released.

[13] https://www.oregon.gov/odot/Planning/Documents/MaaS%20White%20Paper%20Final%205-13-2020.pdfhttps://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

The rules place additional conditions on Indian commercial and business organisations relating to the collection and disclosure of confidential personal data or information, which are similar to the GDPR and the Data Protection Directive. A body corporate (including a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities) that possesses, deals with, or handles any sensitive personal data or information in a computer resource that it owns, controls, or operates is liable to pay damages to the person affected if there is a breach of the IT act's section 43A.[14][15][16][17]

4.3.3 Understanding Data Protection As Suggested In Section 72A of the IT Act-.

Section 72A of the IT Act provides for a criminal penalty for any person (including an intermediary) who, while providing services under the terms of a lawful contract, discloses personal information without the consent of the person concerned, with the knowledge that he or she will cause or is likely to cause wrongful loss or gain.[18][19]

4.3.4 Supreme Court of India Judgement on Right To Privacy

In India, some judgements by the courts have provided indirect protections based on common law, equity standards, and the law of loss of confidence. The Supreme Court of India recognised the right to privacy as a constitutional right under article 21 of the constitution as part of the right to "life" and "personal liberty" in a landmark judgment issued in August 2017 (Justice K.S Puttaswami & others Vs Union of India).

The court overruled that right to privacy is not covered in the constitution. Informational privacy has been recognised as a facet of the right to privacy, and the court has ruled that information about an individual, as well as the right to access that information, must be afforded privacy protection ("Privacy Judgment").[20][21]

Limitations of the present provisions[22] -

- The provisions of the IT act on data protection have a relatively limited scope and application in the context of personal data protection. The IT act's provisions do not name any single government entity that would be in charge of data protection in India. Further, no data breach penalties are mentioned.
- The IT rules are applicable only to electronically generated and transmitted information.
- Applicable to the limited scope of sensitive data, geolocation information is not covered under the definition of sensitive data by the IT act.In the absence of such provision, the information can be misused by the people who access it.

4.3.5 Personal Data Protection Bill (PDPB), 2019

With the current limitation of legislative coverage of personal data protection and to provide a robust

[14] https://www.oregon.gov/odot/Planning/Documents/MaaS%20White%20Paper%20Final%205-13-2020.pdfhttps://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

[15] The Information Technology act 2000, Web Address-(https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf); Accessed on 25th May 2021

[16] Dr. Mohan Deewan, Personal Data Protection Law India Web Address https://www.rkdewan.com/articledetails.php?artid=183; Accessed on- 25th May, 2021

[17] The Information Technology act 2000, Web Address-(https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf); Accessed on 25th May 2021

[18] The Information Technology act 2000, Web Address-(https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf); Accessed on 25th May 2021

[19] IN THE SUPREME COURT OF INDIA CIVIL ORIGINAL JURISDICTION, JUSTICE K S PUTTASWAMY (RETD.), AND ANR. Versus Union of India and ORS, Web Address- https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf; Accessed on 24th May 2021

[20] India's new data protection bill makes a good show of user rights — but can it deliver on its promises?; Business Insider India; Updated on 10th March 2021; Web Address- https://www.businessinsider.in/tech/news/indias-new-data-protection-bill-makes-a-good-show-of-user-rights-but-can-it-deliver-on-its-promises/articleshow/81422687.cms; Accessed on 24th May 2021

[21] India: Personal Data Protection Bill, 2019, Published on 13th January 2021, Web Address-https://www.mondaq.com/india/data-protection/1024292/personal-data-protection-bill

[22] Press Release, National Common Mobility Card; Web Address- https://www.cdac.in/index.aspx?id=edu_et_Press_Release_MoHUA; Accessed on 30th May 2021

framework for data protection legislation, a committee was formed to draft the statute on data protection.The government of India has issued the Personal Data Protection Bill 2019 (PDPB)[19] defines data in three categories[20] -

1. Personal data under the bill is defined as the data relating to a natural person with regard to the characteristic, trait, attribute or any other feature that helps identify that person. The bill also distinguishes between sensitive personal data and critical personal data.
2. Sensitive personal data includes financial data, health data, sex life, sexual orientation, biometric data, transgender status, caste or tribe, religious and political affiliations, etc.
3. Critical personal data means any such data that the central government notify as critical personal data.

Following are the key rights given to the data principal in the PDPB (2019)[19]

- The right to obtain confirmation from the fiduciary on whether their data has been processed.
- The right to seek correction of inaccurate, incomplete, or out-of-date personal data.
- The right to have personal data transferred to any other data fiduciary in certain circumstances
- The right to restrict continuing disclosure of their data to a fiduciary if no longer necessary or consent is withdrawn.

Offence and Penalty in PDPB

The following Table-3 enlist the key offence and respective penalties in PDPB, 2019

Table 3 : Offence and penalty as stated in the Data Protection Bill by the Government of India in: 2019[19]

Offence	Penalty
Processing or transferring personal data in violation of the bill	Fine of ₹15 crores or 4% of annual turnover, whichever is higher
Failure to conduct a data audit	Fine of ₹5 crores or 2% of annual turnover, whichever is higher
Re-identification and processing of de-identified data without consent	Imprisonment of up to three years, or fine, or both

4.4 KEY FINDINGS FROM THE REVIEW

In this section, different personal data protection laws in the world were evaluated. The current state of personal data protection in India and the laws involved in the same were also studied. In all the privacy protection laws discussed, data is categorised into two categories – a) Personal Information and b) Sensitive Personal Information.

Personal information includes the information through which a person can be identified, and sensitive personal information involves some indication of a person's behaviour and beliefs. For processing these types of data, companies/businesses must be registered and require a lawful basis.Regular audit and other types of inspections are suggested to monitor, regulate, and successfully implement these laws.

In India, until the personal data protection bill is passed in both houses of parliament and comes into force, there is no overarching law currently in place to protect the users' personal data. Although section 43A and section 72A of the IT Act makes the defaulters pay damages, they do not empower the individuals about their rights related to privacy. Therefore, for the protection of personal data involved in the MaaS ecosystem and secured data transactions between different stakeholders, there must be contractual provisions considering best practices and the current privacy protection laws in India under which MaaS data must be governed and regulated.

The current version of the personal data protection bill that is under review by the joint selection committee of both houses of parliament will address several challenges, and the provision of the bill must be considered in any MaaS project.

[19] India: Personal Data Protection Bill, 2019, Published on 13th January 2021, Web Address-https://www.mondaq.com/india/data-protection/1024292/personal-data-protection-bill

5 MaaS ECOSYSTEM AND DATA CHALLENGES IN INDIA

5.1 CURRENT REGULATORY STRUCTURE

For understanding MaaS data challenges in India, it's also important to understand the current situation and challenges on data initiatives of MaaS implementation in India. The rapid adoption of cashless payment systems, as well as the increasing smartphone penetration (over 300 million users, with a CAGR of 23 percent through 2018), should encourage MaaS adoption. The adoption of MaaS will also be supported by the promotion of ITS in public transportation[23].

For effective implementation of MaaS, India requires standards to enable these technologies to communicate with one another. There have been a few government measures to standardise technical specifications in public transport, such as AIS 140 which identifies necessary elements for effective implementation of ITS in public transport vehicle operation and Urban Bus Specifications (UBS-II) which focuses on passenger safety and convenience. Standards like these can help synergize vehicle compliance for public transport vehicles under the MaaS service..

However, there is still a need for a multimodal, unified technology framework that would allow easy integration and publishing mobility data on an open platform to ensure data-driven mobility services growth. The time has come to capitalise on current government initiatives and begin developing a new architecture that will create a MaaS offering by providing data exchange channels and appropriate infrastructure for using 4G/5G networks for real-time data transfer.

Without an integrated payment interface across all modes of transportation, the MaaS offering will be incomplete, allowing for ticketless travel while still maintaining safe payments. If used by public transportation authorities, the government's latest initiative under Digital India, Bharat Interface of Money (BHIM) – an aadhar-based mobile payment application – will serve as a popular forum for the Unified Payment Interface (UPI).

The important legislation governing official public transportation and privately operated shared transportation services in India are summarised in table 4 below. The list of agencies in charge of their governance illustrates the variety of decision-making authorities, resulting in each mode designing its services and fares. Because of this lack of integration, shared modes frequently plan for services that compete with each other for ridership in high-demand routes, leaving lower-demand areas underserved. This is in contrast to the NUTP (2006)'s integrated multimodal public transportation system, which calls for public transportation to be available across the city[22]

Table 4 Important legislations governing public transportation and privately operated shared transportation services in India[22]

Mode of Transport	Legislation	Agency in charge of Governance
Bus	Motor Vehicle Act (1988), Road Transport Corporation Act (1960)	State Transport Undertaking (STU)/ Special Purpose Vehicle (SPV)
Metro	The Metro Railways (Construction of Works) Act, 1978	Special Purpose Vehicles (SPV)
Suburban Rail	Indian Railway Act	Indian Railways
Paratransit/Intermediate Public Transport (IPT)	Motor Vehicles Act	Road Transport Authority
New Mobility Services (app-based aggregators/ride hailing services)	Motor Vehicles Act, Taxi Guidelines by MoRTH	Road Transport Authority

Institutional structures such as the formation of Public Transport Authorities (PTA) in Indian cities are needed to oversee the integrated governance and regulation of shared means of transportation.

[22] Press Release, National Common Mobility Card; Web Address- https://www.cdac.in/index.aspx?id=edu_et_Press_Release_MoHUA; Accessed on 30th May 2021

[23] National Common Mobility Card; Web Address- https://www.cdac.in/index.aspx?id=pe_vlsi_One_Nation_One_Card; Accessed on 25th May, 2021

For coordinated decision-making across agencies, certain Indian cities have already established Unified Metropolitan Transport Authorities (UMTA). In the few places where they are operational, the role of UMTAs has been limited to infrastructure planning and finance choices. There are hardly any integrated urban mobility models that link detailed activity-based patterns of the people, their disaggregate mobility needs, and their socio-economicbehaviour to land use plans. There is hardly any sort of term or operational mobility plans, and real-time models are non-existent.The regulatory elements of shared mobility have not received much attention.

5.2 NATIONAL COMMON MOBILITY CARD (NCMC)

Despite the above-mentioned challenges, the Government of India has been successful in creating a fully indigenous interoperable payment platform. Recently, the government launched 'One Nation, One Card'– a single mobility card for seamless travel through different modes of transport systems. National Common Mobility Card (NCMC) is India's first indigenously developed payment platform[24]. The whole payment ecosystem consists of NCMC Card, Automatic Fare Collection (AFC) System, Access Gate, and Card Reader/Validator.

NCMC is a bank-issued debit/credit/prepaid card product platform. The customer can use the single card for payments across all segments, including metro, bus, suburban railways, toll, parking, and retail.

The National Informatics Centre (NIC), the Centre for Development of Advanced Computing (C-DAC), the Bureau of Indian Standards (BIS), the National Payment Corporation of India (NPCI), and the Ministry of Finance formed a committee to develop a vendor-agnostic interoperable ecosystem for NCMC, including an indigenous AFC system and banking interface.

NPCI was tasked with creating the card and terminal specifications to support the NCMC environment. The committee proposed an EMV-based open loop card with stored value as NCMC based on best worldwide practices and market conditions in India. On the other hand, the responsibility of finalising the NCMC specification for the AFC system, including the interface with the bank server,

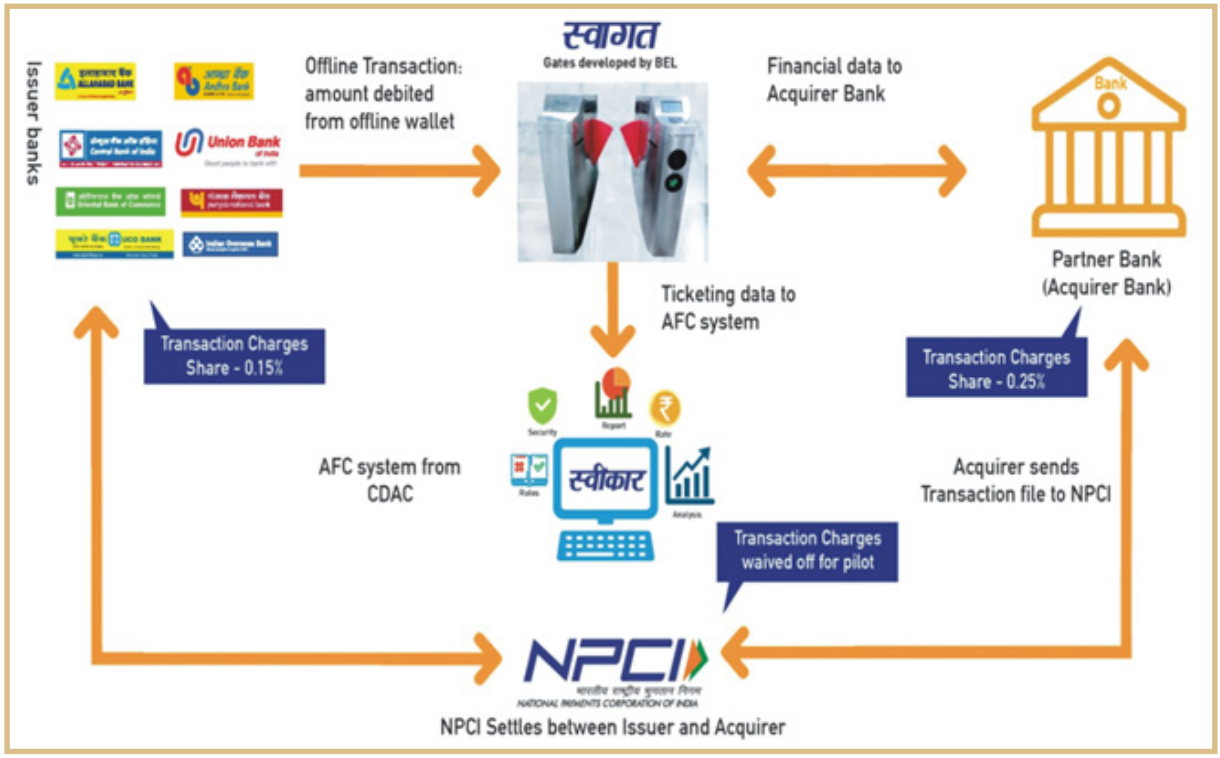


Figure2- NCMC ecosystem[24]

[24] Data Smart city document by Ministry of Housing and Urban affairs

was assigned to CDAC. This activity was completed in partnership with NPCI by CDAC. Following that, BEL was enlisted to create gates & readers.

The first level trials for the whole payment ecosystem have been completed in collaboration with CDAC, BEL, NPCI and SBI. The AFC systems have been installed at Delhi Metro Rail Corporation (DMRC) across a few stations for field testing purposes to exhibit the whole NCMC ecosystem for digital fare collection. NCMC-compliant gates have been installed at several DMRC stations, and cards have been distributed to customers by numerous banks as part of this test.

5.3 INDIAN URBAN DATA EXCHANGE

As a Government of India initiative under the Smart Cities Mission, IUDX (India Urban Data Exchange) has been established in the smart cities as an open-source software platform that allows for the safe, verified, and controlled exchange of urban data in India. Third-party data from multiple data platforms that have been validated and authorised, can be accessed by the other data providers, and data consumers through this database. The system is proposed to be operating at city level and then scaled up across cities finally to reach a national scale, consistently and smoothly. The platform is proposed to provide data owners complete control over what data to expose and to whom. It will be able to link with payment gateways using the built-in accounting procedures, laying the groundwork for a data marketplace. By establishing open APIs and data scheme templates (formats for understanding data), the entire platform will be developer-friendly, resulting in the creation of a new application ecosystem[25]. Below, figure 3 gives an overview of the IUDX platform, figure 4 shows the IUDX architecture, and figure 5 shows the key design principles.

IUDX architecture, however, needs to be integrated with the NCMC and be brought under the regulatory framework of the PDPB. One of the biggest challenges to MaaS data available under the current IUDX system is the lack of end-to-end complete trip chain or mobility data that can be used for planning and optimising MaaS and urban mobility plans. Without the creation or understanding of end-to-end trip patterns, the planning and implementation of MaaS and public transport and logistics networks of the city will always be sub-optimal and incomplete, as it will always have incomplete information about goods and people's mobility.

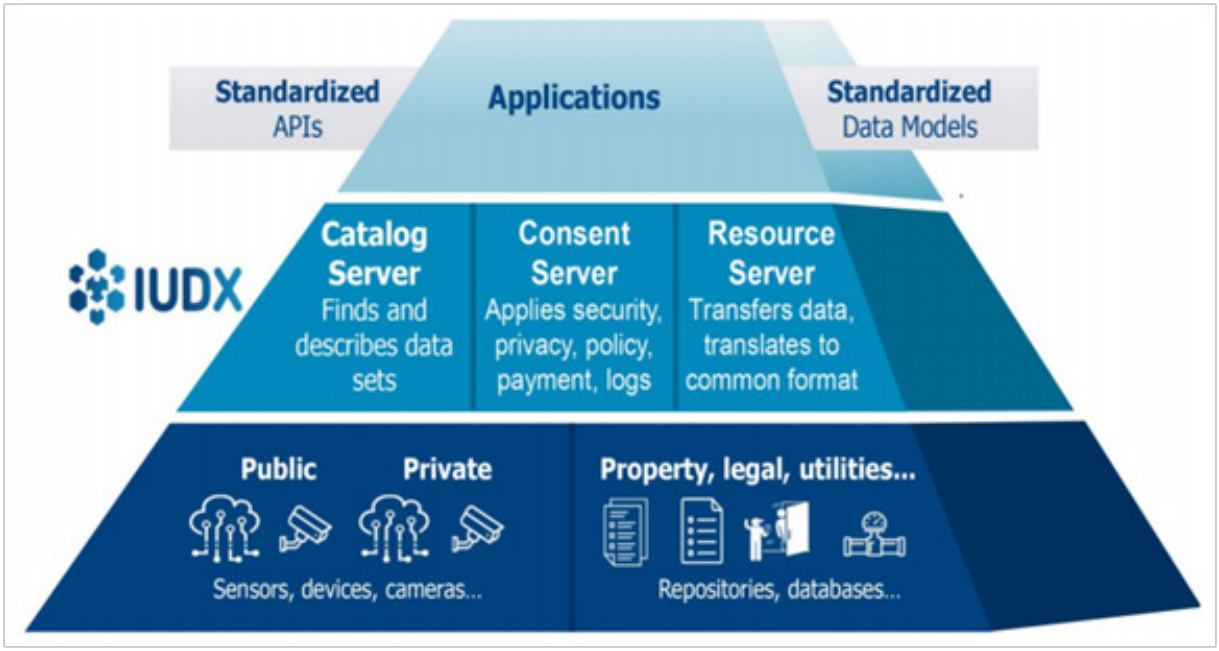


Figure 3- IUDX overview[25]

[25] Indian Urban Data Exchange booklet, Ministry of Housing and Urban Affairs and Ministry of Electronics and Information Technology. Access URL- https://nudm.mohua.gov.in/wp-content/uploads/2021/02/IUDX-Booklet-FINAL.pdf

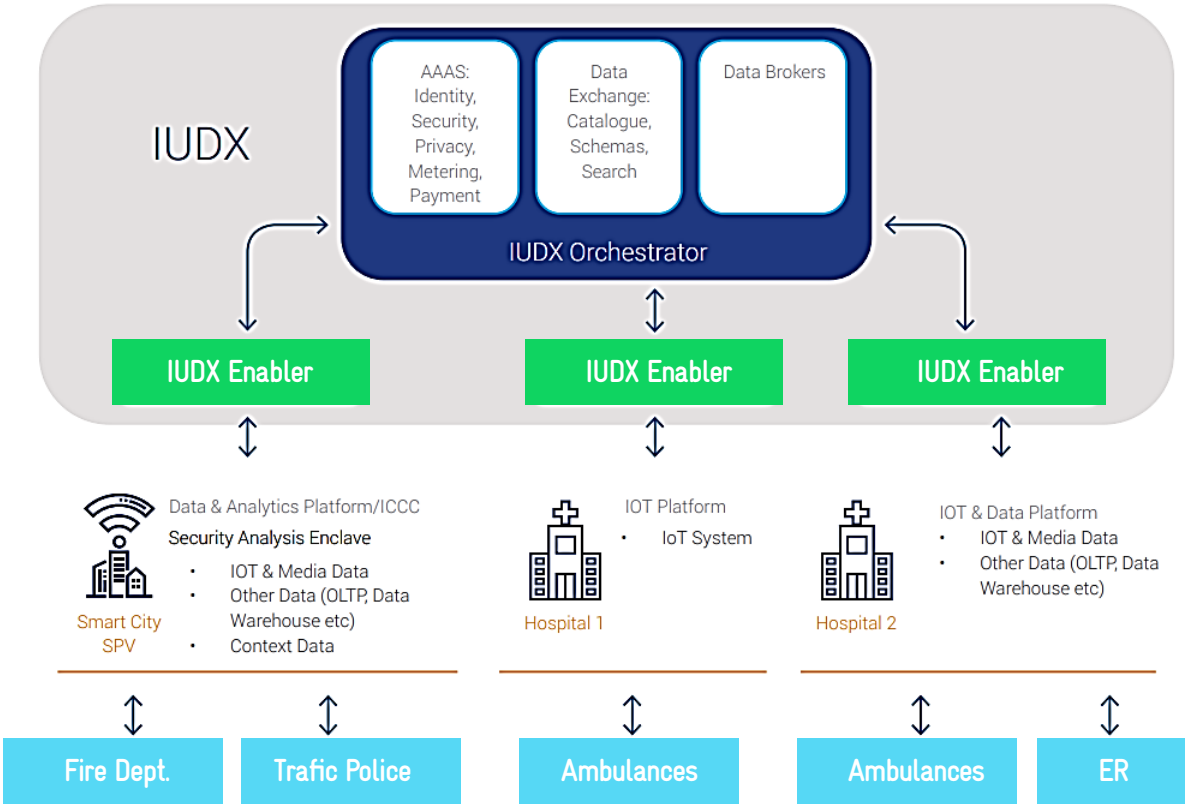


Figure 4- IUDX architecture[25]

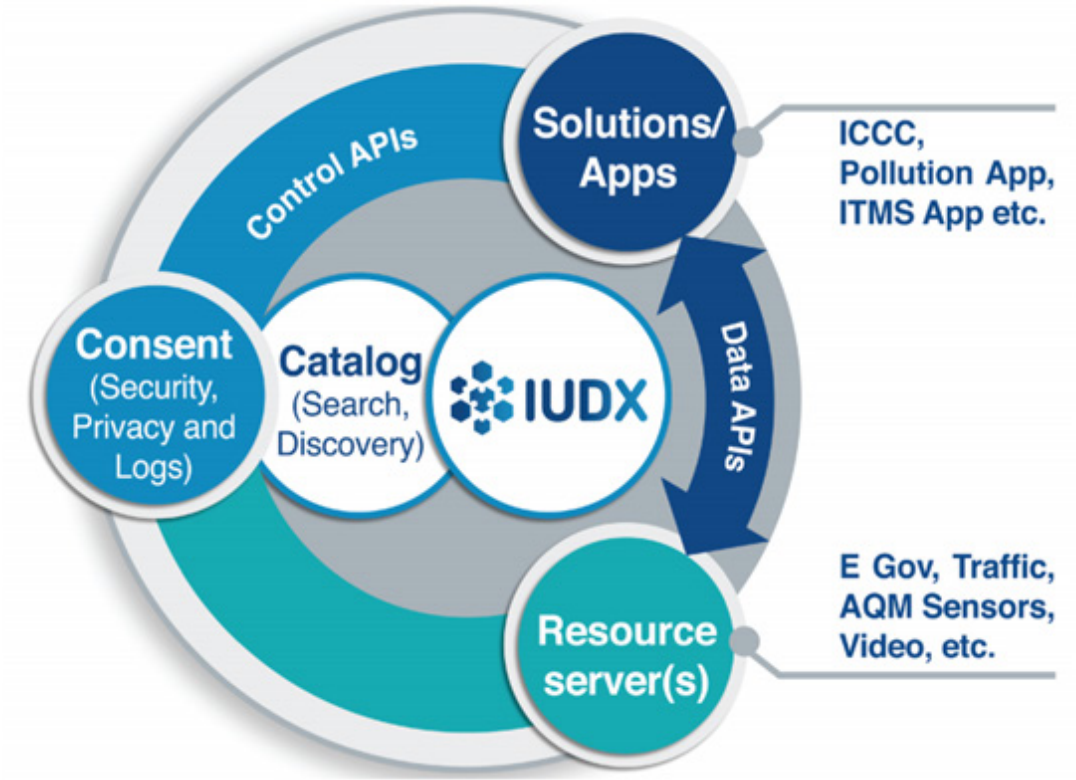


Figure 5 Key design principles[25]

[25] Indian Urban Data Exchange booklet, Ministry of Housing and Urban Affairs and Ministry of Electronics and Information Technology. Access URL- https://nudm.mohua.gov.in/wp-content/uploads/2021/02/IUDX-Booklet-FINAL.pdf

As a part of the data exchange ecosystem, the concept of protected data bank is recommended (figure 6). Here. the mobility data could be stored in the servers under the IUDX mission, and processing of raw data can be done using a third-party specialised institution or any one of the Centre of Excellence in Urban Transport. The anonymous consolidated data can then be published on an open data portal for meeting various data requirements.

Apart from the data storage part of the system, financial infrastructure development is proposed to be done in collaboration with NPCI and stakeholders data sharing, and communication interfaces can be developed in collaboration with C-DAC.

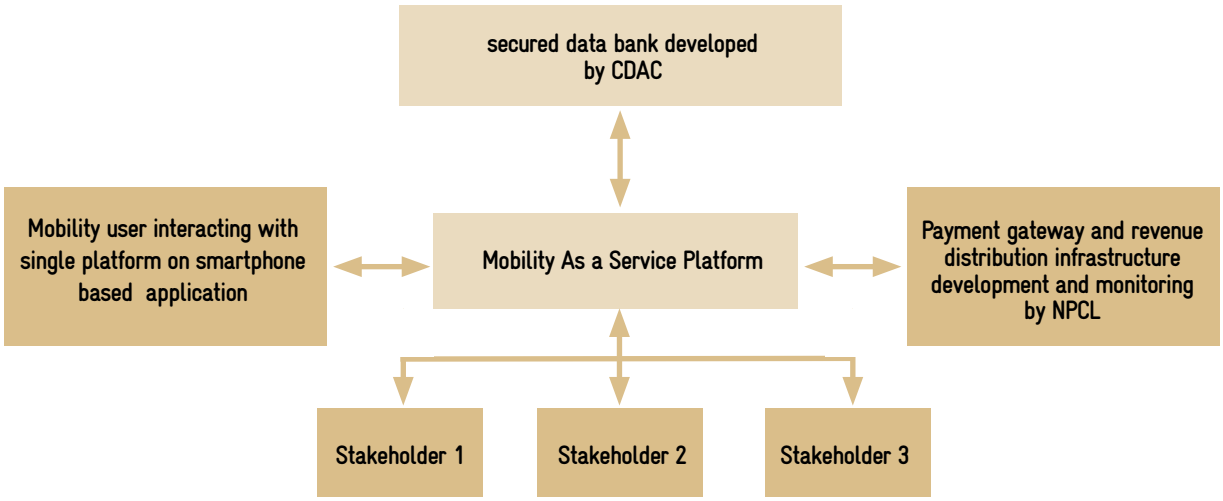


Figure 6- Suggested ecosystem for data exchange in MaaS

5.4 FUTURE OF MOBILITY AND DATA USAGE

5.4.1 Smartphone Based Application And Mobility Planning Surveys

The mobility landscape is rapidly changing, increasing diverse lifestyles. With new and emerging modes of transport, MaaS can meet the less predictable travel demand and activity patterns. In today's rapidly changing environment, transport planners and service providers require more accurate, detailed, and up-to-date behavioural data that could be captured via a common mobility mapping application. One such application is developed by MIT Boston- the mobile market monitor, which provides a previously unobtainable range of human mobility and activity insights in a secure way, taking into consideration the personal data protection issues of its users.

Getting accurate travel demand data has always been a challenge for any transport planning and modelling process. Journey patterns of individuals are often multimodal based on people's dynamic needs that conventional travel demand surveys fail to capture in total journey patterns. How do we predict travel demand in a fast-changing social, economic, and technological landscape? The next-generation approach for measuring and monitoring human mobility and activity is through smart phone-based applications. These data processors use consumer data with their full consent and data sharing approval to determine anonymised activity-travel behaviour. This type of software eliminates the data quality issues commonly experienced with travel surveys and enables measurement of:

- Day to day variation in travel and activity patterns
- The precise start and stop times
- Route information
- All trips including first/last mile, work-based sub-tours
- Richer activity patterns with greater detail on leisure and out-of-work activities

One such service provided is mobile market monitor,with which a mobile phone based application known as X-ING that can be used to collect, store, and analyse MaaS's interlinked mobility data across various mobility operators in an integrated way.

5.4.2 Real-Time Prediction Using Real-Time Traffic Data

Mobility problems in a city continuously increase due to haphazard growth in the urban population which in turn increases vehicular congestion, time on the road, emissions, and cost (both environmental and personal). The advancements of technology, availability of data from the Internet of Things (IoT) and the traffic simulation technology makes optimisation of city traffic network and Mobility as a Service based on AI-based real-time modelling to a real possibility with MaaS. With the advancement of technology advent of traffic problems and data coming in from the IoT mobility authorities around the world have started calling tenders for real-time traffic simulation-based forecast of the current traffic and public transport states with customised reliable KPIs customized KPIs for forecasted evaluation and decision making -

- For travellers real-time simulation-based prediction
- For transport and MaaS operators in terms of real-time information analysis, forecast and decision support

Figure 7 shows the current problems faced by the cities, figure 8 shows the data coming in from the Internet of things in the traffic operator room or control room and figure 9 shows the advanced decision support ecosystem.

MaaS data ecosystem hence provides both challenges and opportunities for mobility users to optimise their journeys in a seamless least cost or disturbed way while reducing congestion and sustainability for all.

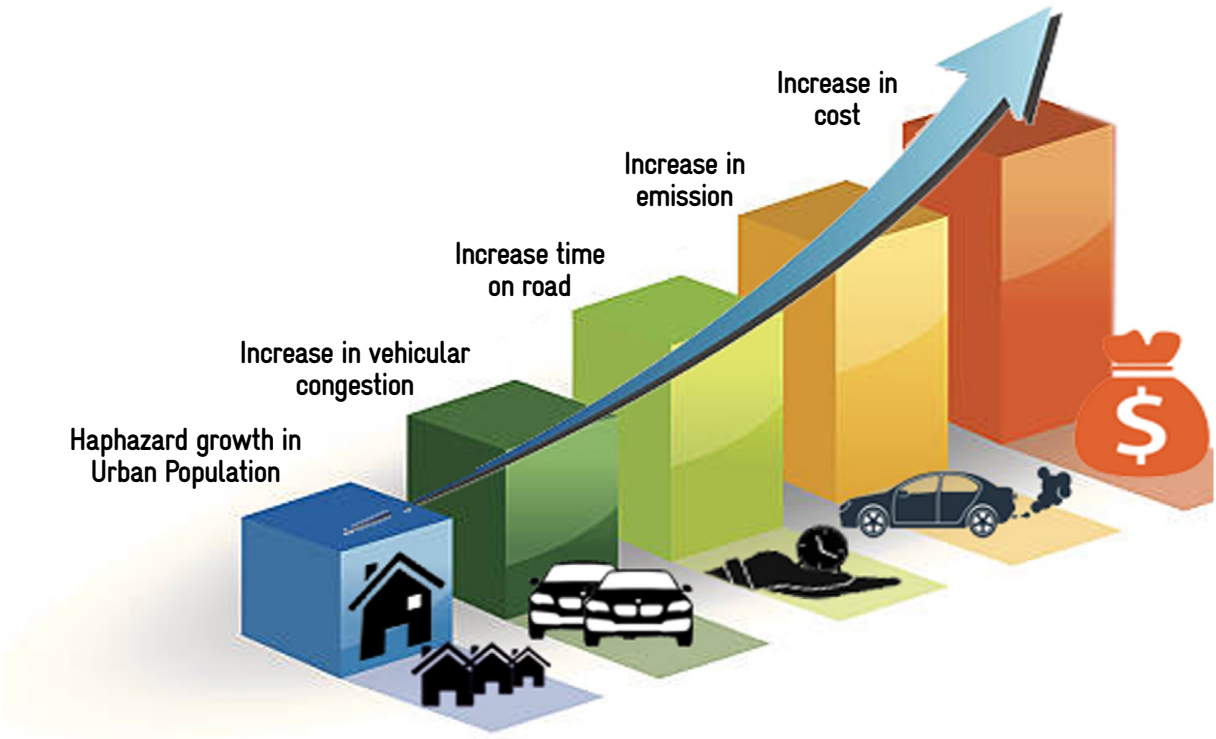


Figure 7- Current mobility problems in cities

As advance decision support system has been adopted there has been many fragmented approaches taken by various departments. Due to lack of data sharing legal framework for mobility data interdepartmental data sharing has been challenging. This leads to multiple agencies working on collecting similar data. However, it would be very useful for all the agencies to join hand to come up with a collective approach and reduce the repetitive effort of data collection.

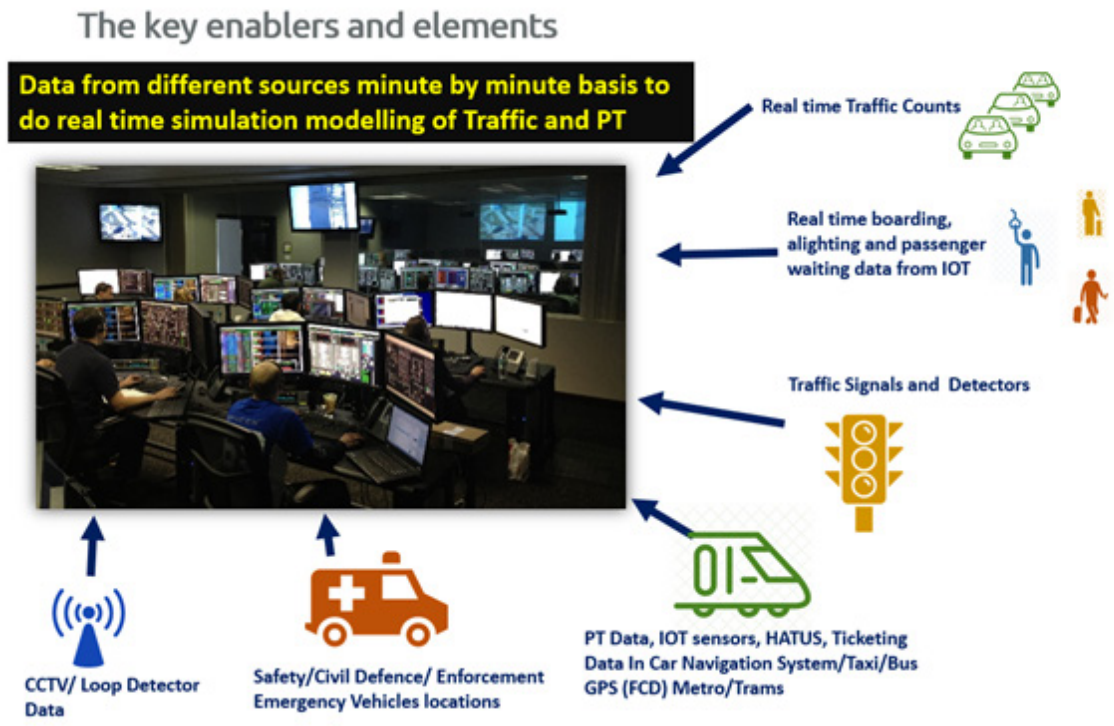


Figure 8- Real-time data coming from the Internet of Things

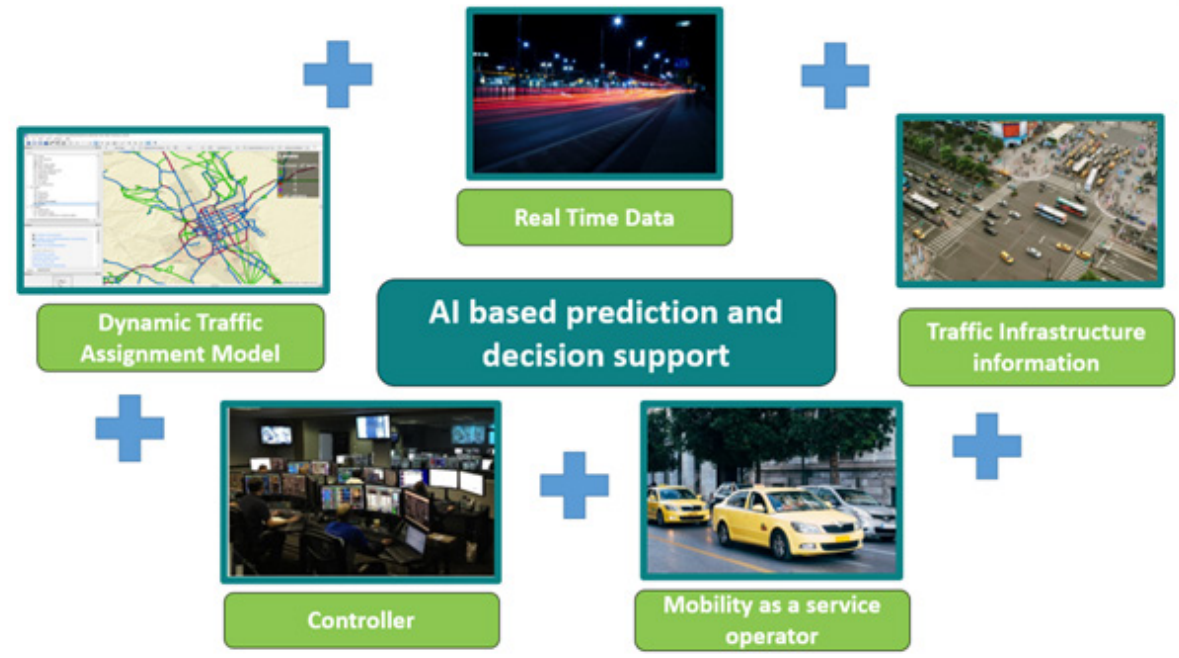


Figure 9- Decision support ecosystem

6 PROPOSED MaaS LEGAL FRAMEWORK

6.1 GENERAL

MaaS data protection laws govern the privacy and security of users' personal data shared within the MaaS ecosystem.The presence of a legal framework reduces breaches in personal data

security and deters the misuse of collected user data. In any country protection of personal data cannot be outside the framework of the existing privacy protection law. Currently, India does not have a dedicated data privacy protection law. While the Personal Data Protection Bill 2019 is still under review,several initiatives are being taken in Indian cities to develop efficiency and resilience in the urban infrastructure. Under the Smart Cities Mission of India, digital intervention both for themanagement of cities and transportation systems are being implemented. For such initiatives to be sustainable, India needs to ensure burgeoning digital innovations and entrepreneurship in the smart cities industry. This could only be realised if India ensures its users their privacy as well as protection of users' data, which, in turn, shall be the prime foundation for fostering an ecosystem for intelligent cities and transport systems. Considering Indians mobile users, who are depending ona myriad of mobile applications for their day to day activities, it is important to have a firm and robust legal framework that takes care of user interest without deviating from the fundamental principles laid down in the Indian constitution.

Therefore, in this section, in this section, the outline of the legal framework of the MaaS data protection in line with the suggested Personal Data Protection Bill is presented. Additionally, an outline of a broad understanding on the aspects of challenges faced, for the implementation of MaaS from the legal framework perspective is also covered.

As discussed in the above sections for the proper function of MaaS ecosystem different level of data exchange needs to be facilitated between multiple stakeholders involved in the ecosystem. The primary source of data is from the travellers' (data principal) smartphones, therefore, the applicability of privacy protection must be in understanding of the MaaS ecosystem complying with the existing legal framework and keeping in mind the Data Protection Bill, 2019.

6.2 CONSIDERATIONS IN THE PROPOSED LEGAL FRAMEWORK

While the transition to a digital city is underway, the processing of personal data has already become ubiquitous in both the public and private sectors. Data is valuable per se and more so when it is shared, leading to the creation of considerable efficiency. In the reality of the digital environment today, almost every single activity undertaken by an individual involves some sort of data transaction or the other. Something as simple as hailing a taxi now involves the use of a mobile application that collects and uses various types of data, such as the user's financial information, their real-time location, and information concerning her previous trips. To transform the concept of mobility into a service, it should become more necessary for the user to share their real-time data to MaaS operator and with many functionalities build into mobility marketspace at level 4 of MaaS projects, users personal profile and preferences shall be known to a MaaS operator and necessitate the required data security regulations. This can only be achieved by having an appropriate legal framework in place.

(i) Risks associated with data sharing

Pooled datasets allow quicker detection of trends and accurate targeting. Often these data are collected without the knowledge of the user, at an extremely basic level, whether it be the exact coordinates or the specific heart rate of an individual at any given moment. The real possibility that the user could not onlybe profiled but also "singled out" has raised many concerns in MaaS due to the increasing number of interconnected databases.

(ii) Risks due to location based navigation data

MaaS is a location-based service (LBS) navigation that uses real-time geo-data from a mobile device to provide user's location and other information. It is important to note that by collecting data on users' location, MaaS service providers or application developers can deduce many types of personal information in addition to locationthiswill included religious believes, political affiliation, social interaction etc. To give an example, if a person visits for worship regularly or goes to a liquor bar, conclusions can be drawn about that person's religion or lifestyle preferences,which may or may not be correct. Because many privacy-protected attributes are uniquely associated with places or events, collecting data that shows a person frequently visits

a place or attends a particular event represents a powerful means to draw a comprehensive picture of an individual. Under article 4 of the EU data privacy law (GDPR), location data is expressly mentioned as a factor by reference to which a person may be recognised as an 'identifier' of personal data.

(iii) Risks due to breach of data

In MaaS, data are provided by different sources, that may be using different protocols and platforms (e.g., transport operators), or externally leased or open-sourced protocols and platforms. Such complexity raises issues not only concerning the "quality of information" processed, but also regarding the division of responsibility among the service providers, "controller" and "processor" whenever a breach of data occurs. Unless a strong framework exists that assigns fiduciary responsibilities to data custodians and data stewards for collated data, risk due to breach or leakage of data cannot be enforced by law.

(iv) Risks due to storage & protection of data

The low costs for storing and processing information and the ease of data collection have resulted in the prevalence of long-term storage of information as well as the collection of minute details about an individual which allows an extensive user profile to be created. The principle of storage limitation is reflected in most data protection laws; however, it may not be feasible to prescribe precise time limits for storage of data since the purpose of collection will be the determining factor.

(v) Failures of masking data

Researchers at MIT recently analysed a pseudonymised dataset consisting of 15 months of spatial-temporal mobility coordinates of 1.5 million people ofaterritory within a radius of 100 km. The study showed that 95% of the population could be singled-out with four location pointsand that just two points were enough to single-out more than 50% of the data subjects(one of such points is known, being very likely "home" or "office") even when if the individuals' identities were pseudonymised by replacing their true attributes with other labels. In another instance, a famous re-identification experiment was conducted on the customers' database of the video content provider Netflix. The data was analysed using the geometric properties of the database consisting of more than 100 million ratings on a scale of 1-5 on over 18,000 movies, expressed by almost 500,000 users, even after masking data,the analytics engine was able to uniquely identify every customer with an accuracy of 99%.

(vi) Data Leakage

India is one of the hotspots of data leakage due to lack of data security measures despite having a very high internet and mobile penetration. A 2019 survey found that 69% of Indian companies haven't set up reliable data security systems; 44% have experienced at least one breach already.

6.3 PROPOSED FRAMEWORK

All the personal data collection and processing in India is currently addressed by the indirect provision of the IT Act section 43 A and 72 A and the Personal Data Protection Bill (PDPB), 2019 which is still in review. The basic aim of this report is to enforce the fact that the MaaS data protection regulation must be in line with the specification of PDPB so that when the bill comes into effect as an act, it resonates with PDPB and requires minor amendments .

The MaaS and mobility data protection framework must be based on the following seven principles-

6.3.1 Technology Agnosticism

The MaaS data storage,usage, and retrieval system must be technologically agnostic, there must be unbiased use of different technology tools to solve different mobility problems. Generally, the more the data environment is heterogenic, i.e., there is a multitude of interfaces with different data standards, technologies and supporting capabilities, the more complex is the data handling process

to integrate the data into the multimodal MaaS platform. The frameworks should be technologically agnostic so that it is flexible enough to take into account changing technologies and standards. The advent of newer technologies such as big data, data analytics, and the Internet of Things (IoT) may challenge the relevance of the purpose limitation principle, which states that data collected for one specified purpose should not be used for a new, incompatible purpose. Various applications of these technologies have demonstrated that many potentially valuable and innovative uses of data develop outside the scope of the purpose specified at the time of data collection. Data may be repurposed and used in an entirely different context irrespective of the stated original purpose.

6.3.2 Holistic Application

The role to integrate various services for MaaS platform could be taken by different actors such as the public transport authority, any transport operator, a MaaS operator, or companies from the banking, telecommunications, or other sectors.

The definition of service providers is quite ubiquitous but still equivocal and can include many categories ranging from different taxi hailing apps, car-share, travel ticketing and booking portals, entertainment apps for travellers, information, and search engines / apps, which may be a public or private sector entity. It also include agencies that runs and manages the payment gateways, banking applications, credit card facilities, etc. Service providers can also be a network providers, MaaS platform operators, Application Programming Interface (API) providers who facilitate their open-source protocol to provide seamless connectivity for both users and data providers. Thus, the legal framework to be framed shall be equally applicable to all its stakeholders irrespective of the degree of participation or whether they are public or private participant.

Moreover, the framework shall be applicable to all per sonnel of the entities within India as well global company doing business in India, who collects, receives, analyses and disseminates the data of the Indian public.

6.3.3 Informed Consent

The consent for data collection, storage and its use must be taken from the users. Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful. Any MaaS platform must ensure that consent meets the aforementioned criteria. The questions related to the consent on behalf of a minor who opts to choose the services, needs to be answered adequately within the framework.

6.3.4 Localisation of Data

Personal data should be stored in a secure and protected server as it has sensitive information like GPS locations of the individuals, trips starting and ending points, credit card details, other sensitive personal information like name, email address, residential address, age, photo identification verification,etc.

Data localisation requires companies to store and process data on servers physically located within national borders. Several governments, driven by concerns over privacy, security, surveillance, and law enforcement, have been enacting legislation that necessitates localisation of data. For example, the recent ban of Chinese apps by the Indian government, which manipulated and stored the data outside the country. MaaS projects within India are required to store data on physical servers on the premises of authority or a cloud based server in India.

6.3.5 Appointment of a Fiduciary

The MaaS operator that collects, store and process the data must be responsible for its security and privacy. The framework for MaaS shall allow the MaaS operator to appoint a fiduciary that can ensure transparency as well as accountability while collecting and disseminating personal data. The fiduciary shall, from time to time, be responsible to give notices and inform both users as well as service providers on their rights in a transparent manner with respect to the laws framed. Fiduciary shall also make sure that data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible

purposes beneficial for the data subject. Data fiduciary must also validate the age and obtain parental consent when processing sensitive personal data for minors who are using the MaaS services.

6.3.6 Structure Enforcement

Enforcement of the system must be from the high-powered statutory body. Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity. This must coexist with appropriately decentralised enforcement mechanisms. City authority should take a lead role on system enforcement.

6.3.7 Deterrent Penalties

Penalties on wrongful processing must be adequate to ensure deterrence. Additionally, the MaaS contract should clearly state the penalties in case of data security breach.

6.3.8 Other Provisions

- Personal data should be processed with responsibility to protect the privacy of data principal.
- Collection of personal data should be limited to the data that is necessary for processing; data should be processed only on the grounds detailed as per the existing law of the land.
- In case of data requirement of MaaS platform, the processing should be limited for the platform to suggest the best route and combination of modal choice for the traveller as per the requirement selections made by the traveller/user of the platform. This data can be used for development and planning purposes by city authorities but proper anonymised aggregation of the same should be ensured.
- Processing should only be for the purposes specified, or other incidental purposes that the data principal would reasonably expect the personal data to be used for.
- The data related to travel pattern of people from one area to another in a city is very important and is used for transportation planning, for developing a decision support system and for developing a priority platform for infrastructural projects.The personal data should be anonymised and aggregated from individual information to collective origin-destination information in particular areas.
- The MaaS platform should ensure that the personal data processed is complete, accurate, not misleading, and updated.
- The MaaS platform should not retain personal data in addition to the duration it is required, also the data principals should have all the privacy protection rights as per the law of the land.
- As the MaaS platform requires the processing of GPS location of the data principal for making suggestions, this can be treated as sensitive personal data and the requirement of explicit consent for the same should be mandatory for MaaS operators.
- The appointment of a data protection officer should be mandatory for MaaS platform operators.

6.4 ENSURING RIGHTS OF DATA PRINCIPAL

Data principal in case of MaaS will be the travellers or people who have registered on the MaaS platform and whose personal informationhas been taken in the application. They should have the right to see, check, rectify, or update their data, as well as obtain it in regularly used formats. The “right to be forgotten” will empower data controllers to prohibit the disclosure of personal data if it is no longer required or has fulfilled its purpose, or if the permission that allowed the disclosure has been revoked, or if the disclosure is done in violation of existing laws.

Common minimum mobility data related to anonymised use of modes, fares, travel times, modes, locations must only be stored and used for planning and optimisation of mobility network.

The common platform facilitating the whole process of planning the trips and bundling different modes together for travellers could well be a mobile phone-based application.The application will collect data from the user and suggest the optimum trip path and other alternatives as per user requirements.This platform can also track the real-time location of traveller to modify the trip journey

accordingly. The information collected by this platform includes both personal and sensitive personal information therefore the platform needs to come under the framework of privacy protection law (which is yet to be passed in houses of parliament in India).

MaaS platform operator should be required to designate at least one individual as the Data Protection Officer (DPO) to oversee data protection responsibilities and ensure compliance with the privacy protection law and other rights of the data principal. The responsibilities of the data protection officer should be but not limited to as mentioned below -

- Ensuring compliance with the existing framework of privacy protection in India when developing and implementing policies and processes for handling personal data.
- Fostering a data protection culture among employees and communicating personal data protection policies to stakeholders.
- Managing personal data protection related queries and complaints.
- Alerting management to any risks that might arise concerning personal data.

7 CONCLUSION

This report provides an in-depth understanding of the various concepts and functionalities of Mobility as a Service (MaaS).Inferring from global trials and the project experts experience. MaaS has various definitions but precisely it is an ecosystem with extensive possibilities to integrate multiple services that comprise multiple stakeholders, bundling of modes and associated trips to create a most optimised trip for the user with one-stop payment solutions by the third party secured payment gateways. The integrated multimodal singular systems that provide single point of contact for data and payment collection with all the stakeholders, travellers and payment gateway are the ideal MaaS ecosystem that many cities have started to develop and implement.

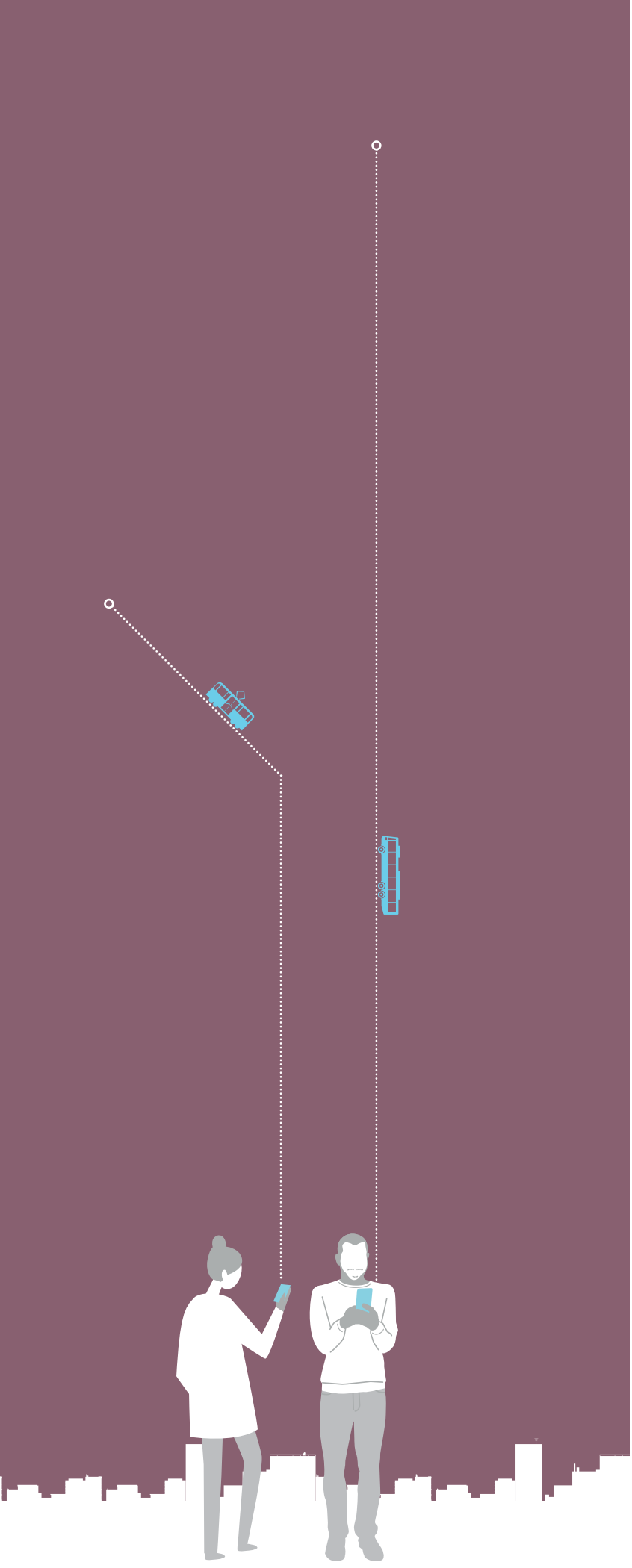
Various MaaS platforms currently operating in the world collect MaaS data for the operation and optimisation of their platforms but do not share any of this data with the city authorities who can greatly benefit from this data. This is one of the biggest challengesto the integrated public transport planning of the mobility networks. Current MaaS platforms take in the personal information of the users along with sensitive details like payment credentials,real time location that may be constantly collected or stored without user's explicit consent.

For understanding the personal data protection laws and regulations, internationally prevalent laws from around the world are studied for this report. The existing legal framework for personal data protection in India was also analysed and it was found that currently although the indirect protection to the users is provided by the section 43A and 72A of the IT act, these laws are not intended specifically to protect personal data and therefore are not sufficient. The introduced Personal Data Protection Bill, 2019 which is yet not approved as an act has the required provision for personal data protection and provides the right to the data principal with a detailed description of different provisions.

The MaaS ecosystem and data challengesare identified particular to mobility operators in Indiawhere different public transport authorities are controlled by different government bodies .Thereis a need fora unifying central body to facilitate the MaaS data collections, storage, and analysisfor planning and optimisation of mobility networks along with creating the MaaS decision framework under one mobility umbrella.

The strengthening government initiatives like the National Common Mobility Card and Indian Urban Data Exchange, where different stakeholders are brought on the same platform were also analysed. Based on the study the legal, regulatory and implementation framework for MaaS data protection in India are suggested which shall bebe included in PDPB.

Finally, the current state of art technological advancements in the mobility data mapping sector and the use of AI-based predictive modelling systems that be used for further expansion of successful implemention of MaaS and smart city technologies are also discussed.



Ministry of Housing and Urban Affairs (MoHUA) and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH are jointly implementing the technical cooperation project "Integrated Sustainable Urban Transport Systems for Smart Cities (SMART-SUT)", commissioned by the German Federal Ministry for Economic Cooperation and Development (BMZ). The project works with the three Smart Cities of Bhubaneshwar, Coimbatore, and Kochi and respective state governments of Odisha, Tamil Nadu, and Kerala to promote low carbon mobility planning, and to plan and implement sustainable urban transport projects.

As part of the Indo-German bilateral cooperation, both countries have also agreed upon a strategic partnership – Green Urban Mobility Partnership (GUMP) between Ministry of Housing and Urban Affairs (MoHUA) and Federal Ministry for Economic Cooperation and Development (BMZ). Within the framework of partnership's technical and financial cooperation, the German government will support improvements in green urban mobility infrastructure and services, strengthen capacities of national, state, and local institutions to design and implement sustainable, inclusive, and smart mobility solutions in Indian cities. As part of the GUMP partnership, Germany will also be supporting expansion of public transport infrastructure, multimodal integration, low-emission or zero-emission technologies, and promotion of non-motorised transport in India. Through this strategic partnership, India and Germany intend to jointly achieve effective international contributions to fight climate change.