CEDR

Conférence Européenne
des Directeurs des Routes

Conference of European
Directors of Roads

Final Programme Report: CEDR Call 2022 Data

November 2025

Final Programme Report: CEDR Call 2022 Data

by

Risto Kulmala, Adewole Adesiyun, Ilkka Kotilainen, Scott Stephenson and Alan Walker

The report is an output from the CEDR Transnational Road Research Programme Call 2022: Data. The research was funded by the CEDR members of Belgium-Flanders, Denmark, Ireland, Netherlands, Norway, Sweden, Switzerland, and the United Kingdom-

Consortium Partners: DROIDS (Traficon Ltd, FEHRL, Haskoning, IFE, MAPtm, University of Warwick), PRESORT (AECOM, Haskoning, MAPtm, Traficon Ltd, Université Polytechnique Hauts-de-France, White Willow), and TIARA (AESIN, SINTEF, Traficon Ltd, Transport & Mobility Leuven TML)

ISBN: 979-10-93321-86-8

Executive Summary

CEDR set up the research call for data in 2022 to provide the NRAs a certain level of confidence in approaching the era of digitalisation, where collecting, managing and sharing the data from NRAs, third-party service providers and road users become vital to improve the safety, efficiency and sustainability of road transport. This Programme had the topics of:

a) Maintaining and sharing the digital road infrastructure
b) Improving the use of third-party data by NRAs
c) Integrity, Authenticity and Non-Repudiation (e.g. proof of the origin, authenticity and integrity of data) integrated in Trust Models for C-ITS applications.

The call resulted in the selection of three project consortiums for the specific topics a-c above. The consortiums set up the three projects of a) DROIDS (Digital Road Operator Information and Data Strategy), b) PRESORT (ImPRoving thE uSe Of third-paRTy data by NRAs), and c) TIARA (Trusted Integrity and Authenticity for Road Applications). The projects managed to work in close cooperation, which turned out to be very useful.

The DROIDS project looked at the evolving roles of the NRAs as they transform themselves into digital road operators. Special focus was given to new roles brought by digital road operation while changes foreseen about the existing roles for e.g. NRAs were addressed. Key results for NRAs included a priority list of use cases for digitalisation. assessment of integration of of the digital twins with the processes in the NRA core business and tasks, general definitions of digital models, shadows and twins for road operation, and the identification of the issues related to ensuring trust and security in the maintenance, sharing, and use of the digital road infrastructure.

The PRESORT project focused on the use of third-party data. PRESORT identified the most important gaps in the present use of data, and delivered a data catalogue of findings in the form of a spreadsheet of use cases for three key ecosystems: C-ITS, road safety, and road use charges and tolls. Furthermore, PRESORT investigated in detail the use of floating vehicle data, in-vehicle data, and eCall data resulting in lessons learned highlighting the importance of planning, robust procurement models, and continuous data quality assurance. The likely most valuable outcome of the PRESORT work was a guide for the NRAs with regard to the use of third-party data in three parts: 1) Use case identification and validation framework, 2) Data Acquisition and Quality Assurance Guidelines, and 3) Best Practices.

The TIARA project studied the elements that NRAs will need to understand before implementing C-ITS systems more widely: The key solution for trust and security is PKI (Public Key Infrastructure) deployment, and TIARA presented the likely solutions for the NRAs is setting up and supporting PKI. TIARA also found feasible methods to tackle the legal and ethical aspects of data use and provision including actions based on the principles of transparency, accountability, and fairness. To ensure privacy, TIARA proposed a structured roadmap reflecting a phased prioritisation on the short, medium, and long terms, derived from the privacy threats, attacker profiles, and mitigation strategies.

DROIDS compiled the key findings, outcomes and recommendations of the three projects in a Digital road operator data strategy. A major conclusion was that the NRAs and other road operators benefit from digitalisation and the use of digital models, shadows and twins. The development, operation, maintenance and use of the digital representations have high value for money. The implementation roadmap of the data strategy includes 11 action categories:

- Road operators:
  1. Provide education and enhance skills
  2. Implement interoperability and utilise standards
  3. Carry out stakeholder collaboration and prioritise use cases
  4. Develop and purchase data and services based on standards, guidelines and design principles
  5. Develop data governance and risk management framework
  6. Implement a change management process
  7. Implement a trust framework
- CEDR:
  8. Establish appropriate CEDR actions to support digital road operation
- Specific actions for the European Data Spaces
  9. Implement an EMDS-compliant data space supporting digital road operations
  10. Formalise the standards to be applied for digital road operations
  11. Implement a data governance framework and a data governance body

It is not expected that all NRAs would immediately commence the recommended actions. Each NRA is recommended to study the content of the actions and select the ones that best help them in carrying out their mission as NRAs to meet the national transport policy goals, to address their national transport related problems, and to give them the best value for money. The last point is especially relevant for the data strategy actions are expected to increase the efficiency of road operator processes to a considerable extent with benefit/cost ratios exceeding 10, and thereby assist the NRAs to carry out their road operation tasks in the world of diminishing budgets.

According to the projects, the use case-oriented approach would likely be the best way to go forward. Asset management was identified as a priority use case by most NRAs involved. Each NRA likely focuses on its own priority use cases and priority road networks when starting its data and digitalisation related actions. An important finding was that the priority of individual actions can also depend on the use case.

It is also clear that the maturity level of NRAs regarding digitalisation differ considerably. Thereby, lessons learned by high maturity NRAs could and should be utilised by those of lower maturity. In sharing the lessons learned and best practices related to data CEDR has a prominent role to play

The results of the three projects were presented during the CEDR Call 2022: Data Final Programme Conference on 14–15 October 2025 at Birmingham UK in parallel to the Highways UK 2025 conference. The final conclusions of the conference highlighted the extremely good timing of the Call with regard to global and European technology and policy developments. The conclusion was also that the project results are relevant for the NRAs. The final conference also agreed that data is fuel for NRAs in decision-making, innovation, and making NRA processes more efficient.

Table of Contents

1 Definition of the Issue

1.1 Purpose

NRAs face a challenge in understanding what they need to prepare and facilitate in order to ensure useful, trustworthy and secure data being collected and shared effectively by themselves, third-party service providers and road users. The digitalisation progress from digital roads to digital twins led by the NRAs is aiming for a greater improvement in asset management operations. These improvements could enable new construction projects to save time and money, reduce emissions across entire road networks, and be integrated with more sophisticated traffic modelling even before starting the construction works. In return, this generates a significant amount of data leading to the questions that the research needs to address such as what data should be collected, managed, processed and shared, and what kind of data infrastructure and regulations that the NRAs need to develop to help them improve safety and efficiency. (CEDR 2022)

For the reasons above, CEDR set up the research call for data in 2022. The purpose of this report is to describe the main outcomes of that call.

1.2 Scope

The aim of the programme was to provide the NRAs a certain level of confidence in approaching the era of digitalisation, where collecting, managing and sharing the data from NRAs, third-party service providers and road users become vital to improve the safety, efficiency and sustainability of road transport. The road users are gaining increasing benefits from new technologies and business models developed by third parties service providers thanks to the availability of data, however, to date this data has not been exploited to its full potential. Meanwhile good data shared by third parties service providers supports NRAs to plan, manage, operate and maintain their road infrastructure effectively and safely. Such data could be acquired e.g. from data aggregators, navigation system providers, fleet management systems and public transport via cooperative intelligent transport systems (C-ITS). This requires a robust and sustainable data infrastructure to enable the exploitation of data from existing and new data sources. As a result, this data is becoming more complex and challenging regarding its volume (real-time or long-time requirements), trustworthiness and security. (CEDR 2022)

This Programme had the following topics (CEDR 2022):

a) Maintaining and sharing the digital road infrastructure
b) Improving the use of third-party data by NRAs
c) Integrity, Authenticity and Non-Repudiation (e.g. proof of the origin, authenticity and integrity of data) integrated in Trust Models for C-ITS applications.

The call resulted in the selection of three project consortiums for the specific topics a-c listed above. The consortiums set up the three projects of a) DROIDS (Digital Road Operator Information and Data Strategy), b) PRESORT (ImPRoving thE uSe Of third-paRTy data by NRAs), and c) TIARA (Trusted Integrity and Authenticity for Road Applications).

1.3 Methodology

The final programme report has been produced on the basis of the deliverables of the three projects DROIDS, PRESORT and TIARA as well as the presentations, discussions and the conclusions made at the programme's final conference in Birmingham, England on 14-15 October 2025. The contents of the report have been validated by the Programme Executive Board of the programme.

The key documents behind this report have been the final reports of the projects DROIDS (Kotilainen, et al. 2025), PRESORT (Stephenson & Cowell 2025), and TIARA (Walker & Lockhart 2025).

2 Outcomes

2.1 Introduction

This chapter compiles the main outcomes of the three projects carried out in the programme. Detailed results and their description can be found in the deliverables of the project available at the CEDR web site. Key outcomes of the projects are the data strategy and the road map to implement that data strategy utilise the results of all three projects albeit being reported as deliverable of the DROIDS projects, which had the responsibility to compile these documents.

2.2 DROIDS

2.2.1 Approach

The Objective of the DROIDS project was to provide the National Road Authorities (NRAs) increased knowledge and support to reap optimal benefits from digitalisation as they evolve to become digital road operators operating the physical, operational and digital road infrastructures. As digital road operators, the NRAs will provide better road user services while improving road transport's safety, efficiency and sustainability. The overall governance approach of DROIDS is presented in Figure 1. Specific attention was given to maintain close contacts with other stakeholders in digital road operations via an advisory group containing representatives from private road operators, cities, vehicle manufacturers and their suppliers, digital map providers, service providers, and academia.

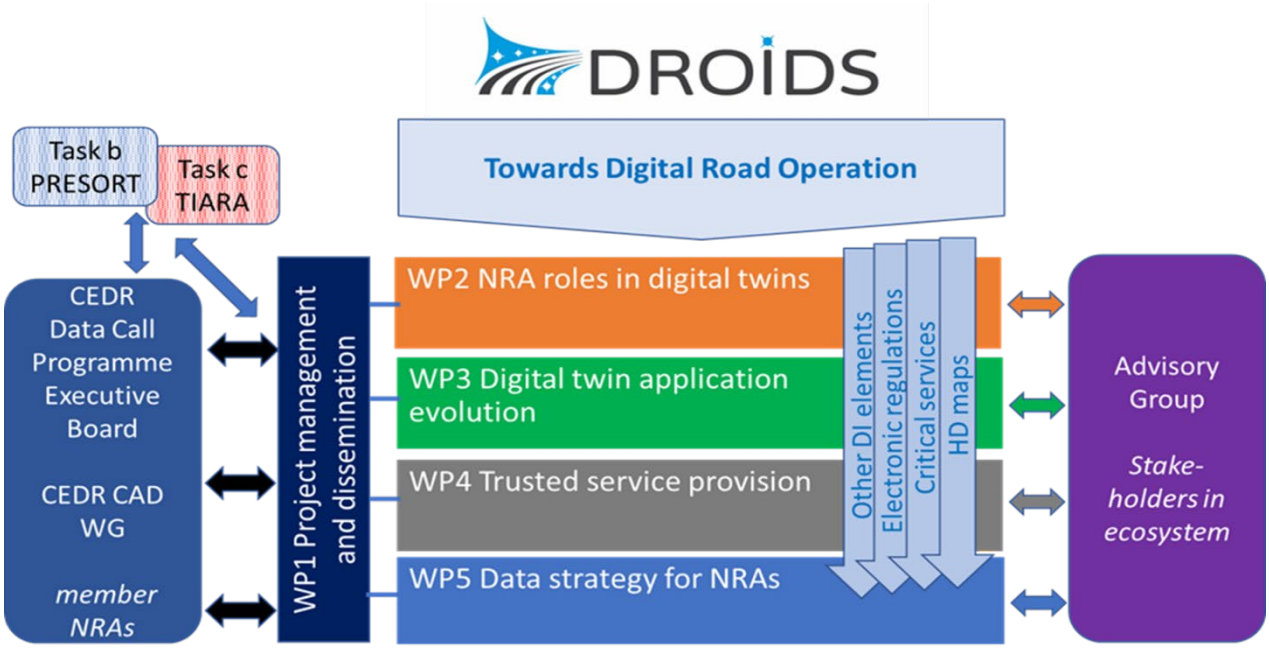

Figure 1. DROIDS project governance approach and stakeholders.

First, the DROIDS project looked at the evolving roles of the NRAs as they transform themselves into digital road operators. Special focus was given to new roles brought by digital road operation while changes foreseen about the existing roles were addressed. DROIDS paid specific attention

to the role evolution in different CEDR member countries with currently varying roles and digital maturity.

Secondly, the project studied the evolution of digital twins from road data banks to comprehensive real-time digital twins of the road transport system, including the infrastructures, traffic, land use, road environment etc. Here, the integration of the digital twins with the processes in the NRA core business and tasks was assessed.

Thirdly, trust has been identified as the key attribute for NRA-originated data/information concerning its use by private sector stakeholders such as vehicle manufacturers and service providers. Thereby, DROIDS also highlighted the issues related to ensuring trust and security in the maintenance, sharing, and use of the digital road infrastructure.

Finally, the work of DROIDS concluded an overarching data strategy for the physical and digital road operators taking on board the results from DROIDS and other ongoing projects (such as CEDR Data Call 2022 PRESORT and TIARA projects).

Literature studies, surveys, interviews, workshops and stakeholder collaboration were widely utilised in DROIDS.

2.2.2 Results

As a basis, DROIDS proposed a definition of a road transport digital twin: *"A Road transport Digital Twin is a virtual representation of the real-world physical road transport systems. The road transport Digital Twin includes digital representation of elements such as road infrastructure, traffic with vehicles and pedestrians, road environment and land use. The road transport Digital Twin has a bidirectional real-time data connection between the physical and the digital representation. It can support road operator decision making with dynamic monitoring, analysis, and predictive modelling capabilities of the road transport systems that enable road operators for instance to enhance traffic flow, road safety and infrastructure asset management or to facilitate automated driving."*

The data flow between the physical object and its digital representation determines whether the digital representation is a digital model (manual data flows), digital shadow (automatic data flow from the physical to the digital) or digital twin (automatic data flows).

<u>NRA role in digital twins</u>

NRA or road operator roles (public and private) in the larger ecosystem of digital twins for road infrastructure were analysed and presented. The analysis included digital representation role tables and role descriptions which included nineteen stakeholder roles in life cycle of road infrastructure digital representations. It was noted that the road operator role will evolve in collaboration with the ecosystem stakeholders depending on the use case and its requirements. The results are presented in Table 1.

Table 1 Summary of the road operator roles in digital representations use cases for road infrastructure.

Road operator roles	Life cycle of road infrastructure digital model/shadow/twin			
Use Case	Development	**Operation**	**Maintenance**	**Use**
Road planning and building (model)	A	A	A	A
Road maintenance (shadow)	A	A	A	A
Winter maintenance (shadow)	A	A	A	A
Asset management (model)	A	A	A	A
Common operational picture for traffic management (network level use case)				
➢ Traffic jam conditions and end of queue (shadow)	P	P	P	A
➢ Surface condition monitoring (shadow)	A - own	A - own	A - own	A
➢ Tunnel closure and management (shadow)	P/A - own	P/A - own	P/A - own	A
➢ Road works (shadow)	A - own	A - own	A - own	A
➢ Safety related incidents and incident management (model)	A/P	A/P	A/P	A
➢ Incident detection (shadow)	A/P	A/P	A/P	A
➢ Event management (model)	(A)	(A)	A	A
Electronic/Digital traffic rules/regulations				
➢ General traffic regulations (model)	P/A		A	A
➢ Speed limits (shadow)			A	A
➢ Access Control / UVAR (shadow)	A (road tolls)	A (road tolls)	A (road tolls)	A
Signal control (shadow / twin)	A/P	A/P	P	A
Hard shoulder running (shadow / twin)	A/P	A/P	P	A
Automated traffic enforcement (shadow)	P/A	P/A	P/A	P/A
HD Map (shadow / model)	A (DM) - own	A (DM) - own	A (DM) - own	A
Cooperative Connected and Automated Mobility (CCAM) – Distributed ODD attribute value awareness (shadow)			P/A	A

'A' means active (actually carrying out the task or commissioning it), 'P' more passive, '( )' means that the role is valid in some European countries only. 'A/P' refers to possible Active or Passive role, 'DM' refers to Digital Model, 'own' refers to possible responsibility to developing their own digital representation.

The analysis of the road operator roles indicated that road operators have an active role in many of the use cases life cycle stages. Natural active roles in digital representation full life cycle for road operators are in their core business of road maintenance and asset management as well as

in use of the digital models in road planning and building. In use cases where private industry provides products and services, such as HD maps, signal control and probe vehicle data, road operator may have a more passive role, depending on the national implementation and business models with the industry. The likelihood of deploying the various use cases is shown in Table 2.

Table 2 Road operators estimated likelihood of use case deployment by 2030 by at least three Member States. Results from the DROIDS project workshop and feedback of road operators.

Priority		Estimated likelihood of use case deployment by 2030 by at least three Member States?		
	Use case	Unlikely	Likely	Very Likely
	Common operational picture for traffic management (network level use case)			
	- Traffic jam conditions and end of queue	DT	DS	
	- Surface condition monitoring	DT		DS
9	- Tunnel closure and management	DT	DS	
3	- Road works	DT	DS	DM (static RW data)
9	- Safety related incidents and incident management	DT and DS (all stakeholders)		DM
4	- Incident detection	DT		DS
	- Event management	DT	DS (large events)	DM
8	Road maintenance	DT		DS
11	Winter maintenance	DT		DS
1	Asset management	DT	DS (high-risk assets)	DM
11	Road planning and building	DT (smart construction)	DS (smart construction)	DM
	Electronic/Digital traffic rules/regulations			
6	- General traffic regulations	DT	DS (dynamic)	DM
2	- Speed limits		DT (dynamic)	DS
4	- Access Control / UVAR		DT (dynamic)	DS
	Automated traffic enforcement		DS	DM
	Signal control		DT (dynamic)	DS
11	Hard shoulder running		DT	DS
11	HD Map	DT		DS
6	Cooperative Connected and Automated Mobility (CCAM) – Distributed ODD attribute value awareness		DT	DS

Asset management, digital information of speed limits, and road works were regarded as the digital representation use cases with highest priority. For most use cases, digital shadows would be the most likely type of digital representation deployed by 2030.

Evolution of digital twins

BIM information from design and construction phase can transition into asset information model which can be used by the road operators for asset management. However, to enable such integration, road operators must adopt common standards which will allow interoperability between different information systems. To improve information management and exchange throughout the project's lifecycle, it is essential to adopt ISO 19650 as the framework. This standard provides a structured approach for managing crucial project data and ensures consistency across all stages.

Another important aspect is developing or refining existing Building Information Modeling (BIM) standards and guidelines, which will specify the requirements for data exchange, level of detail, and format compliance. Using formats like Industry Foundation Classes (IFC) and openBIM standards will facilitate seamless communication and integration.

Creating or using a comprehensive Object Type Library (OTL) is also vital. This library defines the properties and attributes of each asset type, ensuring consistency and interoperability across various projects and organizations.

Fostering active collaboration and communication between internal stakeholders, such as BIM and Asset Information Management (AIM) departments, is crucial for mutual understanding of requirements and capabilities. Additionally, engaging with external stakeholders, including contractors, design and engineering firms, consultants, and technology providers, helps identify information requirements and ensures the needs of all parties are met.

Road operators should also focus on data governance models to understand the responsibilities behind information management. The following five recommendations for the road operators on how to collect, maintain and distribute the information in such a way that it is compatible with digital representations i.e. models, shadows and twins, were given in the study:

1. Identify road operator roles by use case
2. Utilise regulations and standards
3. Maintain trust
4. Exchange data with ecosystem stakeholders
5. Operate, evaluate and maintain

Standards provide services and data common technical solutions, interoperability, scalability and reduce cost risk, to mention few benefits, across European member states borders. For example, sharing of safety related traffic information or electronic traffic rules for human and automated driving system-controlled vehicles requires collaboration between public and private partners. Standards ensure a common approach and safeguard joint digital representation implementations, i.e. future proof solutions and services.

DROIDS made an inventory of the current state of BIM information maintenance among road operators. Road operators across Europe are increasingly adopting BIM to enhance project delivery, improve collaboration, and optimize asset management. Several common challenges hinder the effective maintenance of BIM information. These challenges include the lack of standardized data, difficulties in data sharing and integration, and resistance to change.

The utilization of OTLs for BIM information management varies significantly among road operators. Some have well-developed and integrated OTL systems. Some are creating data

dictionaries and OTLs, but policy implementation is still pending. There are also cases where road operators have not adopted OTLs at all. The focus of OTL extension also differs among road operators. This highlights the need for road operators to consider their specific needs and priorities when developing and extending their OTLs.

Road operators are increasingly recognizing the value of reusing BIM information throughout the asset lifecycle. Key challenges in BIM information reuse include integration and system compatibility, standardization, software dependency, and data quality. To address these challenges, road operators should prioritize standardization, training, and the adoption of flexible software solutions. By implementing these strategies, road operators can improve the efficiency and effectiveness of their asset management processes, leading to better-informed decision-making and long-term sustainability.

DROIDS studied in detail three digital representation use cases: digital transport regulations, opening new roads (BIM information reuse in HD maps), and automated lane level navigation. The stakeholder roles, prioritisation of efforts, and implementation issues were elaborated in detail. As an example, Figure 2 shows an example of the prioritisation of digitising traffic rules and regulations.

Figure 2 Priorities of various traffic rules and regulations for digitisation as indicated by stakeholders

Trusted service provision

For an organisation to be able to reap the true benefits of digitalisation, it needs to develop an appropriate level of trust to ensure correct use. DROIDS proposed that instead of treating trust as a monolithic construct to instead consider two forms of trust:

- Trust in the system
- Trust with the system

By system in this context, we refer to informational systems, as well as their components. “Trust in the system” means an organisation’s trust in the capabilities of the system or in the system’s ability to do what it is supposed to do. When applied to data this refers to trust that the data is accurate and correct for its intended purpose. “Trust with the system” means the user’s awareness or attitude towards the limitations of the system and their ability to adapt their usage of the system to accommodate the limitations of the system to deliver the expected benefit. This extends to ensuring that members of the organisation are aware of these limitations and are able to adapt to them. In the context of data, trust with it is the user’s awareness of its limitations and degree of

correctness, as well as the ability to ensure that the data can be used for its intended purpose. A DROIDS workshop completed during the study provided valuable insight into what issues NRAs are concerned with, along with potential solutions.

2.2.3 Outlook

The restrictions of public sector budgets in road infrastructure and its operations mean that the NRAs have to move towards digital road operation as all evidence supports the view that digitalisation makes also NRA operations more efficient with high benefit-cost estimates. At the same time the restricted budgets mean that digital representations cannot be realised for every use case at once. The conclusion thereby is that the NRAs need to focus on some use cases. The data strategy (Bokolo et al. 2025) proposes the following overall priority order for digitalisation for the next years:

- asset management (digital model/shadow)
- electronic traffic regulations – speed limits (digital shadow)
- road works (digital model/shadow)
- incident detection (digital shadow)
- access control/ urban vehicle access regulations incl. road tolls (digital shadow)
- electronic traffic regulations – general regulations (digital model)
- CCAM (Connected Cooperative Automated Mobility – distributed Operational Design Domain ODD awareness (digital shadow)

Each NRA likely selects the best use cases based on national policies, transport problems, available expertise, status of existing processes and the available resources.

To effectively utilise BIM representations throughout the full lifecycle of digital twins for road infrastructure, road operators can implement the process as outlined below:

- Define Objectives and Scope: Clearly define the goals and scope of BIM reuse, considering data availability, requirements, and stakeholders.
- Establish Standards and Guidelines: Develop and adopt BIM standards, ISO 19650, and OTLs to ensure consistency and interoperability.
- Establish Collaboration and Communication: Foster collaboration between BIM and AIM teams, engage stakeholders, and simplify processes.
- Identify Information Requirements: Define and prioritize information requirements aligned with OTL.
- Facilitate Data Exchange: Implement data governance, utilize CDEs, and establish data transfer protocols.
- Integrate BIM into Design Processes: Collect and standardize BIM data, incorporate BIM from early stages, and link BIM models to OTL.
- Ensure Data Quality: Implement quality control procedures, validate data against OTL, and conduct data audits.
- Integrate BIM with Asset Management Systems: Develop data migration strategies and integrate BIM data to enrich asset management systems.
- Data Management and Maintenance: Ensure continuous data updates, quality assurance, and effective change management.
- Monitoring and Evaluation: Conduct regular assessments, establish a feedback loop, and plan for scaling.

By following these steps and prioritizing change management, road operators can successfully reuse BIM information to enhance asset management and digital twin development.

Concerning the establishment of trust for NRA data and service provision in the future, DROIDS presented a set of recommendations. The “Trust in” recommendations were:

- Reputation-based trust
- Identify potential conflicts of interest with OEMs
- Independent or Third-Party Certification
- Ensure adherence to standards and participation in standardisation activities.
- Use of Standardised Data Formats
- System Auditing
- Data Authentication
- Maintain Access Control and Audit Trails
- Data Redundancy and Cross-Verification

The “Trust with” recommendations were:

- Transparency of Data Collection and Processing
- Develop clear requirements for data provisioning
- Assess risks associated with data
- Document Assumptions and Use Constraints
- Validate Data Against Ground Truth
- Encourage Use of Complementary Data Sources
- Define Baseline for Data Quality
- Periodic Data Quality Assessments
- Cross-NRA cooperation
- Training and Capacity Building for NRAs

The recommendations given are a collection of actions or policies formed through an analysis of the trust model in coordination with the workshop. The list of recommendations has been given in no particular order as the priority and importance of each will not only depend on the implementing organisation, but also on the application. While individual consideration is important, there are two types of recommendations that should take priority over others. The first type is recommendations that deal with compliance with legal requirements and standards. These have the potential to cause the most detrimental or beneficial effects and therefore should be given a high priority. The other type of recommendations that should be given priority are those that deal with information security and cybersecurity, as they can heavily influence public trust.

2.3 PRESORT

2.3.1 Approach

The PRESORT project set out to deliver an evidence-based decision support guide that can be used to enable National Roads Authorities (NRA) to make better decisions regarding how and when to acquire and use third-party transport data. It includes data from sources such as vehicle manufacturers, suppliers of in-vehicle technology, navigation and fleet management systems, private mobility providers, specialist road condition data including weather, and other environmental monitoring services.

The over-arching objectives of this project were to:

- **Capture** the current state of third-party data usage
- **Analyse** and understand what NRA's core business is and how it could enable the third-party service providers to generate crucially useful data for sharing
- **Deep Dive** to establish the use cases most likely to benefit from third-party data
- **Conclude** the work undertaken to produce an actionable and implementation guide
- Disseminate the Guide produced so all CEDR NRA member states can access.

These objectives correlated with the PRESORT work packages (Figure 3). PRESORT was built on earlier work such as the development of the C-ROADS platform for testing and implementing C-ITS services in light of cross-border interoperability, Building Information Modelling and the impact of CAD on safe smart roads, and National Highways (England) Digital Roads and Asset Management strategies.

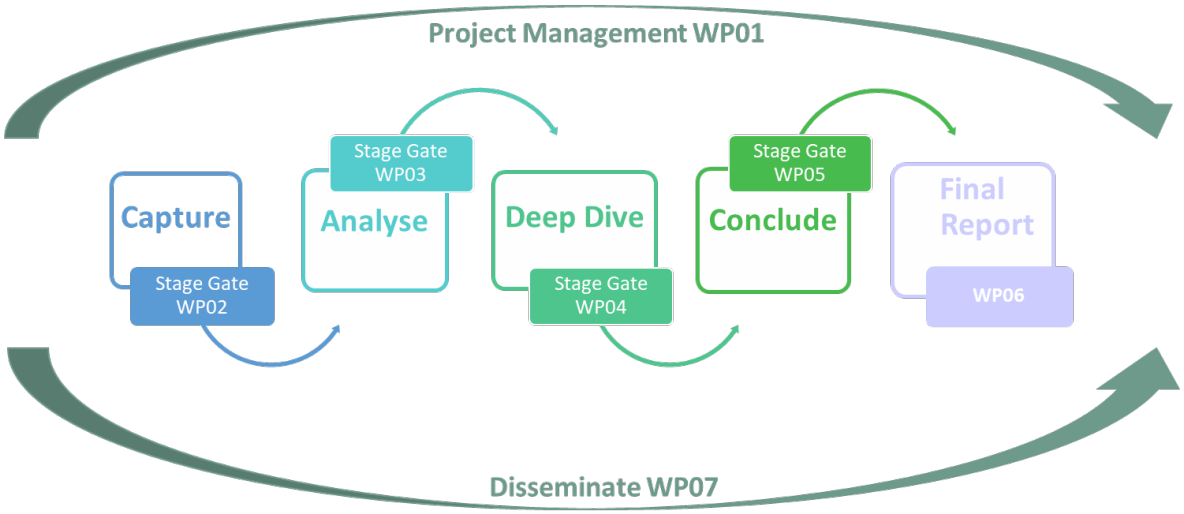

Figure 3. PRESORT project methodology.

The project used surveys, interviews, literature studies and workshops to gather the data required in addition to the consortium's expertise and experiences. Furthermore, it utilised an Advisory Group involving related stakeholders for the consultation and validation of the results.

2.3.2 Results

PRESORT analysed the data needs of NRAs and identified gaps between their current data resources and what is optimally required. It also explored challenges faced by NRAs and third-party data providers in acquiring, using, and maintaining data. The focus was on three key ecosystems namely: Cooperative Intelligent Transport Systems (C-ITS), road safety, and road user charging and tolls.

NRAs' concerns regarding accuracy, reliability, and privacy were explored, together with their programmes to address them through collaborative efforts, technological advancements, and clearer regulatory frameworks. Workshops with NRAs and interviews with third-party data providers were carried out to identify any potential gaps in their practices.

PRESORT identified three different categories of gaps in the present use of data. These were:

- Desirability – the analysis identified the different needs and incentives between NRAs and data providers. NRAs need individual vehicle data, whereas for data providers GDPR (General Data Protection Regulation) may be an issue. They are also more demanding of reliability and coverage.
- Technical fit – differences in fields of expertise exist between NRAs, with knowledge of the roads system, and data providers, with better data literacy and knowledge of protocols and standards.
- Business viability – gaps include uncertainties in business models and agreements, complex stakeholder dependencies, unclear data ownership and rights (leading to fears of losing control over data handling), mismatched cost expectations, and worries over long-term stability.

PRESORT also included delivery of a data catalogue of findings in the form of a spreadsheet of use cases for three key ecosystems: C-ITS, road safety, and road use charges and tolls. A data utilisation level dashboard was also created.

The Deep dive work selected three use cases for detailed investigation:

- Traffic Management using Floating Car/Vehicle Data (C-ITS): This explores the further potential of real-time vehicle data to improve traffic management, incident response, and asset management.
- Using in-vehicle data: How data from vehicles can enhance various aspects of road management beyond C-ITS, including asset management and safety.
- eCall data use for Road safety improvement: This focuses on leveraging eCall data to enhance road safety measures.

Investigation combined workshops and desktop research to discover practices and experiences as well as to generate use case findings and outcomes. It concluded with lessons learned regarding the procurement, implementation, and use of third-party data by NRAs. In each of these cases, lessons were drawn from five phases of a project: from Pre-procurement, Procurement, Implementation, Implementation, Maintenance and monitoring, and an overarching phase including the overall project strategy.

The lessons learned from the five phases highlight the importance of planning, robust procurement models, and continuous data quality assurance. By incorporating these lessons, NRAs can effectively reference, make informed decisions and embark on navigating the complexities of third-party data usage to enhance traffic management, asset management, and road safety across Europe.

The research revealed that procuring third-party data needs a different approach from traditional infrastructure procurement. NRAs should focus on the purpose of the data once retrieved, the goal it is intended for and organisational and procedural impact it will generate.

PRESORT provided several recommendations for NRAs with regard to third-party data. The recommendations were the following on a general level:

- Establish a Shared Vision.

- Invest in Staff Education.
- Foster Collaboration and Innovation.
- Prioritise Data Coverage.
- Adopt a Use-Case-Centred Approach.
- Strategically Integrate AI and Sensors.
- Address Data Quality Concerns to ensure data reliability.
- Develop Standardized Frameworks and Agreements.

Likely the most valuable outcome of the PRESORT work was a guide (Laine et al. 2025) for the NRAs with regard to the use of third-party data. The guide, in the form of a slide deck, consisted of three sections:

- Deliverable 5.1. Use case identification and validation framework
- Deliverable 5.2. Data Acquisition and Quality Assurance Guidelines
- Deliverable 5.3. Best Practices

The first section provides NRAs guidance on how to assess the possibility of using third-party data as an input in their core business processes, before the actual decision has been made for proceeding to data procurement. This section's intended readership consists of e.g. NRA's core business owners, strategists and senior management who are responsible for the development of internal processes and data driven decision making within the NRA.

The second section provides a practical guideline how to successfully perform a third-party data acquisition process following the related European and national legislations. Guidance is also provided on how to monitor the agreed service-level, data quality and other requirements during the production phase. This section is primarily for technical experts responsible for defining requirements/specifications as well as for procurement staff responsible for running the actual procurement process.

The third section provides practical examples from three implemented third-party data procurement processes on how NRA's have in practice designed their procurement process and how they have set the selection and quality criteria that have led to a successful outcome of the procurement. This section should be read together with section 2.

Two example slides from the guide are shown in Figures 4, 5 and 6.

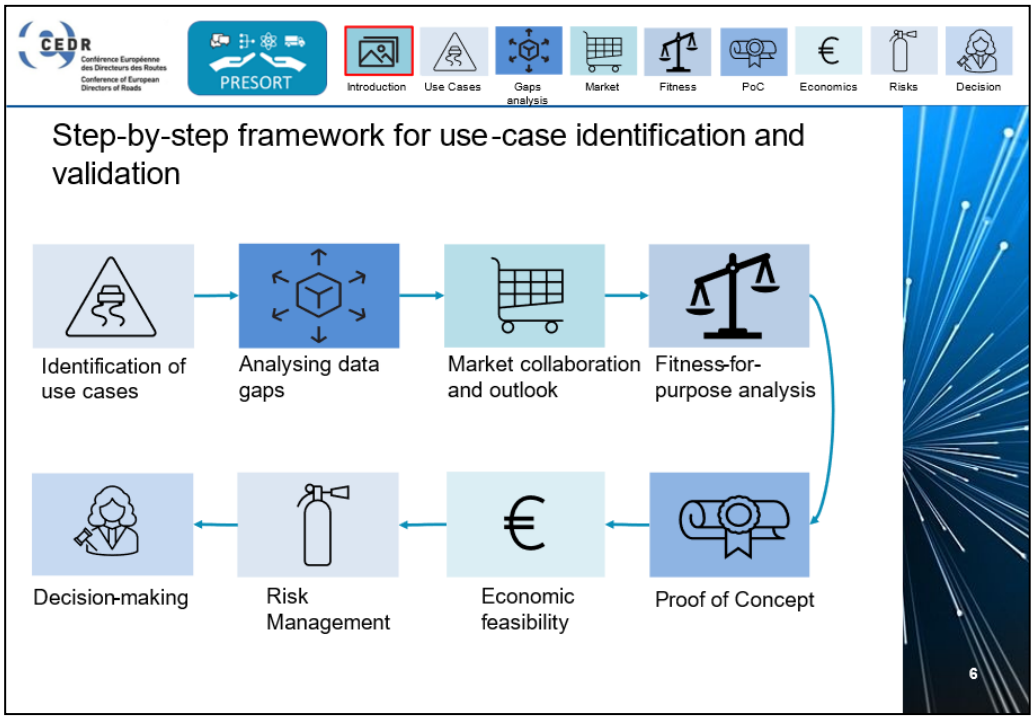

Figure 4. A page from the step-by-step guide for all phases of the process of acquisition and use of third-party data by NRAs.

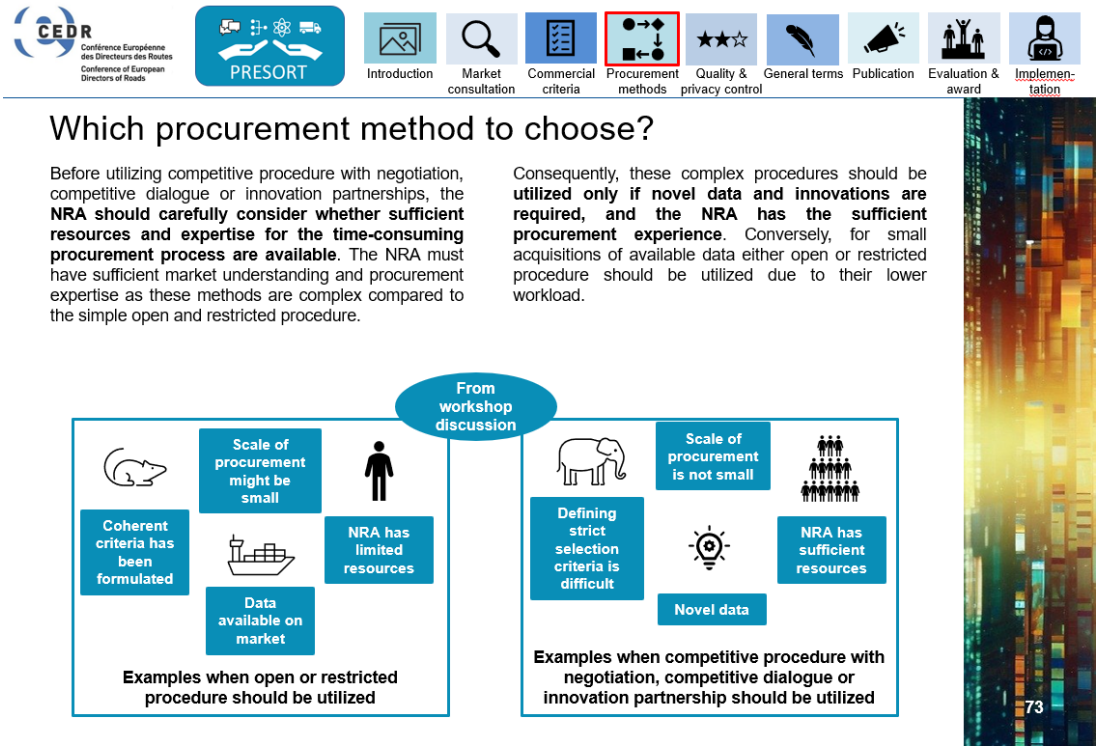

Figure 5. A page from the step-by-step guide for selection of advanced procurement methods.

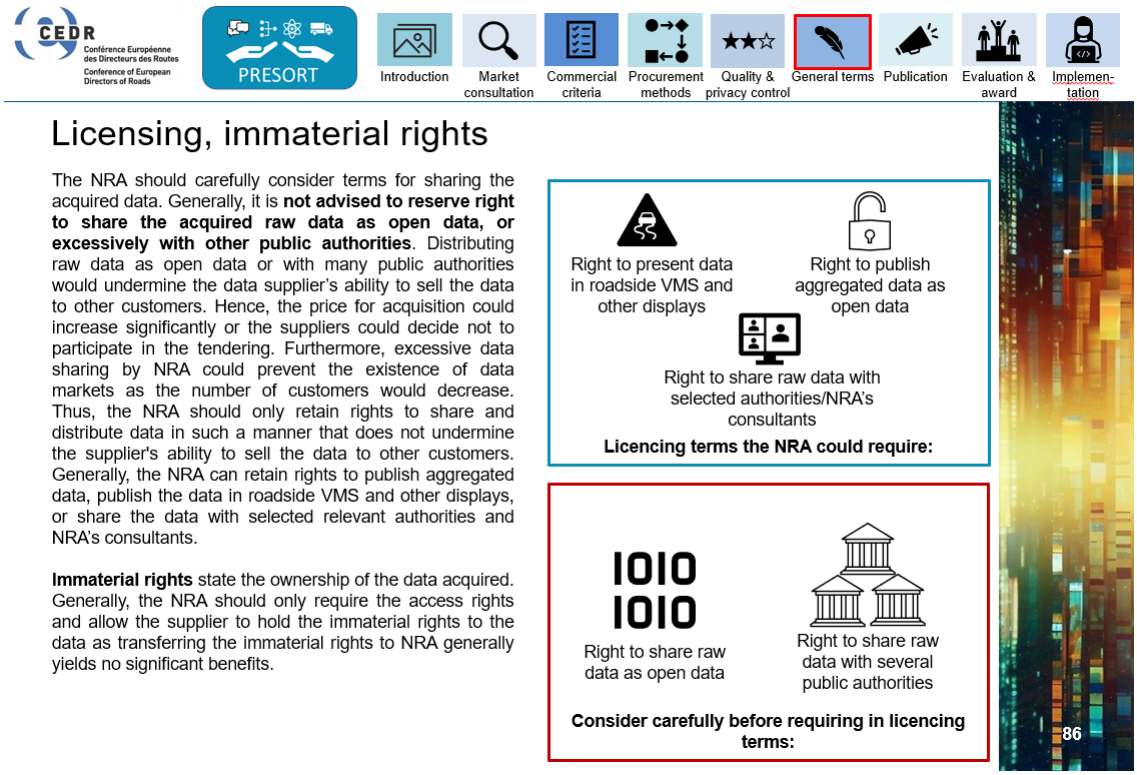

Figure 6. A page from the step-by-step guide for addressing licensing and immaterial rights.

2.3.3 Outlook

The PRESORT project's outcomes are highly applicable already now, for the following reasons:

1. Increased availability of third-party data:
    - Data from vehicles, mobile apps, and sensor networks is already being generated at scale.
    - PRESORT provides a roadmap for NRAs to begin responsibly integrating this data into operations like traffic management and road safety.
2. Support for policy and procurement decisions:
    - The project's step-by-step implementation guide helps NRAs navigate complex procurement, legal, and technical environments.
    - It enables more informed, efficient investment decisions using real-world use cases.
3. Immediate use cases identified:
    - The deep dives into traffic management, in-vehicle data, eCall, and road user charging provide practical templates NRAs can act on now.
    - Tools like the data catalogue and utilisation dashboard are ready for application.
4. Compliance and risk management:
    - Guidance on GDPR and licensing helps NRAs reduce legal risk while enhancing data-driven service delivery.

The PRESORT project's outcomes are applicable in the future for the following reasons:

1. Scalability and evolution with technology:
    - As AI, connected vehicles, and data-sharing standards evolve, PRESORT's frameworks are adaptable and forward-compatible.
    - Future NRA systems will require structured data procurement models and interoperability, which PRESORT anticipates.
    - NRAs are becoming more digital in operation and the highway technology is increasing digital demand, which PRESORT acknowledges.

2. Cross-border and cross-sector integration:
    - The framework supports future harmonisation across European NRAs and alignment with EU digital infrastructure goals.
    - Enables broader collaboration with industry, academia, and other government bodies.
3. Enabling a sustainable and resilient transport network:
    - By supporting the shift to data-informed decision-making, PRESORT contributes to CO_2 reduction, efficiency, and improved safety.
    - Its work also aligns with future mobility trends like autonomous vehicles and dynamic road pricing.
4. Capacity building and workforce development:
    - The emphasis on education and organisational change prepares NRAs to grow internal capabilities for long-term digital transformation.

PRESORT also identified several topics for further work. These included:

1. Broader dissemination and knowledge transfer
Extend outreach to more NRAs, especially in Eastern and Southern Europe, which were underrepresented in the project. Publish case studies and make training materials widely available to NRAs, academia, and industry. Engage professional networks (e.g., ITS groups, Connekt, ATEC) to spread awareness of the implementation guide and best practices.

2. Refinement of procurement models
Conduct comparative studies on procurement frameworks specific to third-party data. Test and validate the decision support system for data acquisition in real-world procurements across different jurisdictions.

3. Standardisation and legal framework development
Collaborate with EU and national bodies to develop standardized contracts, data-sharing agreements, and GDPR-compliant frameworks. Explore common licensing models that balance data access with provider rights and legal constraints.

4. Further technical and ecosystem research
Investigate interoperability standards across different transport data ecosystems (e.g., C-ITS, road safety, tolling). Explore the integration of AI, IoT sensors, and digital twins in data-rich applications for road planning and traffic control.

5. Use case expansion and impact assessment
Build on existing use cases by a) testing additional ones, such as weather-based maintenance, real-time emissions monitoring, or automated incident detection, and b) conducting quantitative impact evaluations on safety, congestion, emissions, and operational costs.

6. Workforce training and capacity building
Design and pilot training programs to upskill NRA personnel in data literacy, procurement of digital services, and AI-readiness. Partner with STEM initiatives and academic institutions to ensure pipeline talent understands transport data challenges.

7. Long-term monitoring and evaluation
Set up a longitudinal monitoring framework to track the uptake, usage, and ROI of third-party data by NRAs over time. Develop a PRESORT observatory or dashboard to collect and share updates, new insights, and case studies.

2.4 TIARA

2.4.1 Approach

Since the C-Roads Platform started its operation in 2016, several Intelligent Transport Systems (ITS) programmes have been rolled out and it has been identified that there are key elements that the NRAs will need to understand before implementing these systems more widely. The TIARA project was designed to address the two key areas of Trust and Privacy in C-ITS applications. The first subject, Trust, concerns an understanding of the implementation of trust models that could protect C-ITS data. The second subject, Privacy, concerns an understanding of the impact of processing user personal data, including location.

TIARA highlighted elements that road authorities will need to understand before implementing C-ITS systems more widely:

Roll-out of PKI (Public Key Infrastructure) systems

The PKI systems required for C-Roads and C-ITS systems are comparatively complex. Certificates are generated and loaded into a vehicle, and are regularly rotated for security and privacy reasons, meaning that there is a large throughput of certificates. The PKI needs to support this generation of certificates and needs to support the regular verification of messages. Road authorities need support and guidance to better understand how to implement the PKI systems required.

How NRAs' ethical and legal obligations change with connected road infrastructure

C-ITS systems represent an evolution of the role of the road authority, from building and maintaining roads, through traffic management technology, to directly transmitting data to the road user. This is a change in the responsibility of the NRA. The NRA needs to ensure that the data they provide maintains integrity, that the road user understands the data they are receiving, and how the collected data is being used. As such, NRAs must understand their ethical responsibilities to customers and other users of the data that they collect.

Privacy of road operators' customers' data

To ensure road users trust the lawful and sensible use of their data by road operators, road authorities must be open and transparent about the data that is collected and for what it is used or could be used. Opinion 3/2017 of Art. 29 Data Protection Working Party indicates that identifying the physical location of a road user can be sufficient to trace back to an individual in a population (taking account of regular travel patterns within certain precision). Several European Road operators process location data from road users to optimise signalised intersections (e.g., Flanders and the Netherlands) or to warn about slow moving vehicles. Measures must be implemented to make such re-identification more difficult, and road authorities should understand to what extent these measures are sufficient to make reidentification "reasonably" impossible.

Thereby TIARA created three work packages to deal with the above mentioned three topics while ensuring compatibility with the work of the other projects in the programme (Figure 7).

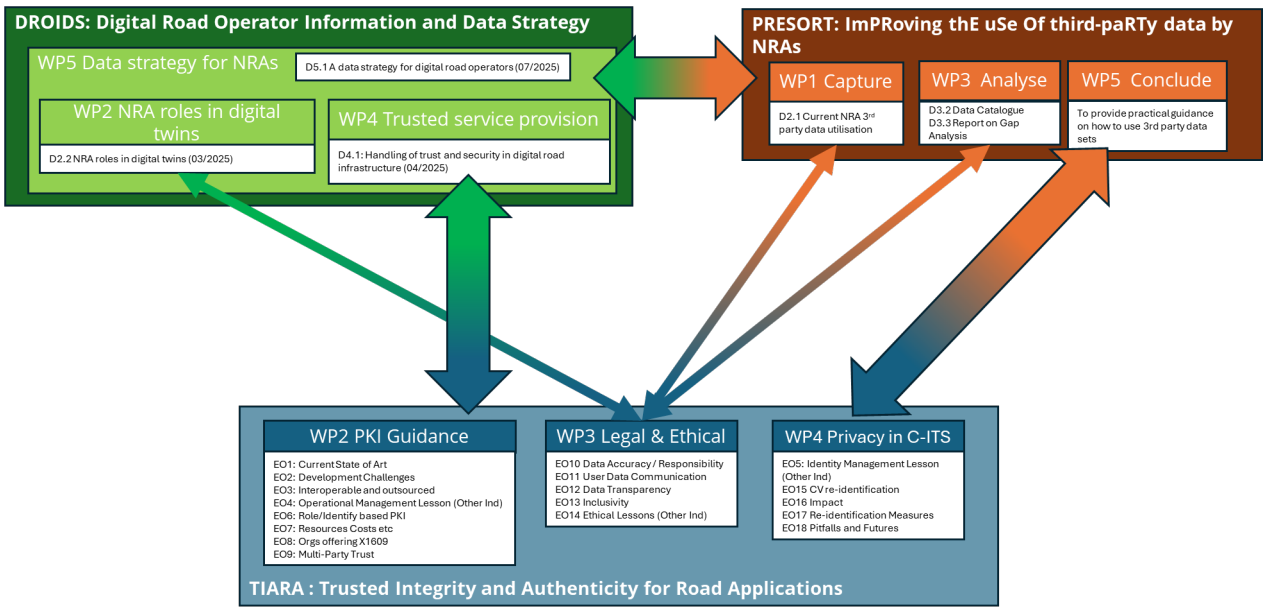

Figure 7: Linkages between scopes of the three CEDR research projects.

TIARA utilised surveys, interviews, literature studies and workshops to gather the data required in addition to the consortium's own expertise and experiences.

2.4.2 Results

TIARA work packages worked independently from each other and thereby the results are presented separately for each work package.

2.4.2.1 PKI (Public Key Infrastructure) guidance development

Digital certification is a cornerstone of trust, security, and interoperability in C-ITS. PKIs enable secure authentication and data exchange between C-ITS stations, such as vehicles, roadside units, and traffic management systems. A PKI ensures the trustworthiness of digital certificates through a defined framework of roles, policies, procedures, and secure infrastructure.

Operational deployments of C-ITS PKIs remain limited in Europe. Countries such as Austria, Germany and France have made notable progress to establish a significant C-ITS PKI and credential management nationally and locally. Compared with a European roll-out, the national system offers more control but can be less cost-effective. Other countries are pursuing limited demonstrations and pilots, although these focus more on functionality than security. Cross-border C-ITS services, such as related to safety, customs, or payments, are yet to be addressed or harmonised. Some NRAs are using existing PKI solutions from other operators, with the goal to be part of the harmonised, interoperable EU CCMS using the EU Root Certificate Authority (CA), with enrolment and authorisation currently operated by Eviden from France. More than 40 actors are currently connected to the EU Root CA.

To support a harmonised approach, the EC has introduced the EU CCMS (C-ITS Credential Management System), which defines a common trust hierarchy for CAs. Coordinated action of multiple parties, including OEMs, to adopt the EU Root CA and get their C-ITS services "approved", will be needed to succeed. Without managed transitions between different PKIs, seamless interoperable communication will not be achieved across borders and across different systems and brands. Maintaining compliance of hardware while regulations and protection profiles

evolve over years, yet legacy vehicles persist on the roads, adds cost and complexity. Operating costs dominate considerations.

NRAs are expected to serve as key trust anchors within the European trust model. Strict processes and significant expertise are required but these can be challenging to maintain consistently over time. Finding the required niche expert skills is difficult. Due to the high complexity and resource demands of PKI operations, most states think that the technical implementation of their PKI solution will be outsourced to specialised service providers responsible for implementation and operation, but that the state or NRA will be the solution owner.

Based on lessons from other sectors, the operational practices should reflect organisational structures. Avoiding hierarchical structures makes PKI more useful in real-world use cases. Too much focus on technology, and not enough on organisational aspects, particularly skills and resources to operate a PKI, can lead to an expensive and unsuitable PKI design.

There are many different PKI use cases, and C-ITS has specific/unique requirements which are not necessarily met by the most common PKI solutions. Purpose designed PKIs are more useful than one-size-fits-all. because different use cases have different needs and requirements, and unnecessary functionality should generally be avoided to reduce complexity.

The trust hierarchy defined in the EU CCMS appears to be a good foundation for the European C-ITS architecture, provided that the various stakeholders are assigned appropriate roles and responsibilities. The choice of trust model when dealing with inter-organisational PKIs is common to other sectors. C-ITS needs to move from "shell-based" protection to transaction-based protection, although over-engineering is likely before the adoption of standards is widespread. A shell-based solution secures the device (or system) itself, by creating a protective "shell" around the hardware or operating environment. This contrasts with transaction-based security, where individual transactions (such as sessions, API calls or financial transactions) are secured. Using short-lived pseudonym certificates instead of traditional revocation mechanisms can minimise complexity and avoid potential response time issues when checking certificate validity. Understanding the number of users and easily changing user credentials will be helpful.

Other issues include weak keys, unnecessarily long certificate lifespans, improper protection of private keys, and lack of policy consistency. Information technology, healthcare, finance, e-government, telecoms, education, maritime and aviation sectors highlighted fundamental PKI management challenges:

- Lack of skills and resources to operate a PKI.
- Lack of investments in modern PKI infrastructures, leaving outdated manual PKI management methods.
- Attackers will exploit weak credentials, too weak keys, unnecessarily long certificate lifespans, improper protection of private keys, lack of policy consistency.
- Poor key management practices and compromised/rogue CAs should fail PKI management and cryptography audits.
- Data theft, service disruption, and malware distribution are high risk.

Local private PKI is needed if a subset of roles is required, with different types of users, such as police vehicles, ambulances, maintenance vehicles, repair shops, etc. Different certificate roles may be required – e.g., permissions for local transit buses within one city, rather than for all transit buses nationally. C-Roads and C2C-CC are working to harmonise the more common use cases. The certificate validity management (revocation or short-lived) will also depend on the type of application/service and type of users.

Although there are several private companies providing PKI services, it is important to ensure that C-ITS specific needs are properly identified and met. A recurring challenge is the scarcity of PKI specialists in the transport sector. As a result, many NRAs and infrastructure operators are

expected to rely on outsourced PKI services. This shift necessitates robust outsourcing models, clear contractual frameworks, and close oversight to ensure compliance, reliability, and scalability. Ultimately, the success of C-ITS deployment in Europe will depend on strong cross-sector collaboration, alignment between technical and policy layers, and the ability to manage complexity while delivering secure, interoperable, and user-centric services. NRAs require this guidance when establishing and applying best practices.

Commercial and public organisations are offering X.509 and 1609.2 PKI functionality. Competition between short-range communication (ITS-G5), adopted by VAG, and long-range communication (C-V2X), adopted by other vehicle manufacturers, may lead to a hybrid solution, where both standards will be used, potentially with parallel PKI systems for different services according to the required speed of communication (1609.2 certification for ITS-G5 and X.509 certification for C-V2X).

Even though C-ITS is at an "early stage", there are already some providers that offer C-ITS PKI services, albeit prices are high and a hybrid short-/long-range solution may cost even more. For the most part, these providers have information security as (part of) their core business, but there are also a few actors from the automotive industry, such as VAG, who have decided to establish and operate their own PKI. Operating a PKI requires specific competence and resources. NRAs can therefore implement PKI by undertaking all activities themselves, or procure parts of the system, or procure the entire system as a package.

In the extension of the trust infrastructure across multiple parties, identifying how C-ITS applications will be monetised, i.e., who will benefit and who will pay, is probably the most challenging part. More data sharing between vehicle manufacturers and NRAs will be required for effective provision of high-quality relevant information according to the desired services. Other third parties should be engaged, such as maintenance companies to provide use cases involving road workers.

2.4.2.2 Legal and ethical aspects

Concerning data accuracy and accountability, there are no direct technical requirements outside of required data formats (e.g., DATEX II) related to ITS or C-ITS data accuracy nor quality in European legislation. However, Member States are required by the EU Real-time traffic information (RTTI) delegated act 2022/670 legislation to set up National Access Points (NAPs), make the data available, communicate inaccuracies, provide data quality parameters, and follow minimum quality requirements agreed with relevant stakeholders. These are further implemented in Member States, depending on legislation and policies, by the road operator or NRA. Other ITS and C-ITS relevant European legislation includes the EU Product Liability Directive (EU, 2024), which includes software and related services, where navigation systems providing traffic data are mentioned as an example of a product with safety liabilities.

It is important to know who the users are and what are their needs, so users need to be consulted throughout the data and service development life cycle to ensure inclusivity. The NAP and the national or regional interchange nodes or clouds are the main channels for data publication. Road operators should also inform data users about the quality of the data. The first user group contained different road user stakeholders referred to in the ITS Deployment directive (EU, 2010), such as vehicle owners or vulnerable road users. The second user group had specific needs, such as mobility impairment or disabilities.

TIARA gave the following recommendations for transparent and inclusive communication mainly based on UK Government (2020b) guidance and its workshop results:

- Follow legislation, rights and principles
- Explain importance of data quality communication
- Develop effective, bidirectional communication with users and stakeholders
- Make communication user-centric
- Make communication accessible and inclusive
- Practice transparent and reliable data quality and service communication
- Ensure privacy and data protection in communication
- Communicate in a timely and responsive manner
- Engage with data providers and users
- Provide education to users
- Provide communication guidelines for all communication
- Create a process for continuous communication monitoring and development
- Practice proactive risk management in communication

TIARA identified several recommendations on addressing road users' technical abilities:

- Human Machine Interface (HMI) development needs to reflect road users' technical abilities. Inclusive, universal, and usable principles make systems easy to use.
- No legislation or regulation directly relates to service development or HMIs. The ITS Deployment directive (EU, 2010) does contain indirect references for safe service deployment. Although in-vehicle systems have developed considerably since 2008, the EC's recommendations for safe and efficient in-vehicle information and communication systems (EU, 2008) are still valid and can be applied.
- Road operator responsibilities extend to their agreements and contracts with road maintenance contractors. For example, if a contractor is required to use a service or third-party application, the road operator needs to ensure the service usability.
- The barriers and opportunities identified included missing inclusive regulation, enhanced co-creation, and simplifying GDPR compliance messaging. Co-creation requires collaboration between road operators, private industry, and road users, to meet user needs. There is a lack of inclusivity or HMI regulation, but with sufficient collaboration this should not be needed.
- Inclusive services require extensive modelling, simulation, testing, and piloting with the road users. If road operators decide to develop their own services, they need to carefully consider if those services are core business priorities. Multisided business models could lead to high development and maintenance costs so discrepancies between potential services and road operators' responsibilities should be evaluated.

Concerning ethical data use, the data ethics framework of the UK Government (2020a) is recommended for road operators and contractors. The principles of transparency, accountability, and fairness guide road operators along with practical actions, which should be documented and shared with the community. It is ethical to provide data quality information with data and implement an organisational code of ethics.

Potential road users' data leakage and impact aspects include the following:

- Data and services delivered by NRAs or subcontractors are the NRAs' responsibility.
- Inclusive communication requires engagement with a wide range of user groups.
- Potential leakage risks and their potential impact need to be communicated to road users along with mitigation actions. NRAs need data ethics policies and processes.

2.4.2.3 Privacy in C-ITS applications

Reidentification or deanonymisation and preventive measures are essential for ensuring privacy. Privacy risks associated with C-ITS messages can reveal sensitive information about vehicle locations and user behaviours, even when anonymisation techniques are applied. There are suppression and generalisation strategies that enhance privacy protections to counter re-identification or deanonymisation threats. Technical preventive measures include differential

privacy, synthetic data generation, and encryption, while legal frameworks strengthening data protection represent non-technical preventions.

A balanced approach combining technical innovations with safeguards, and collaboration between governments, industry stakeholders, and privacy advocates, will be a pragmatic route to ensure an ethical and responsible implementation of private connected vehicle data.

The impact of processing users' personal data involves exploring the inherent risks of reidentification if leaked and the potential impact on individuals' privacy. Deanonymisation of connected vehicle data is the starkest risk. Studies consistently show that even pseudonymised or aggregated mobility datasets can be reverse engineered since just a few location data points suffice to uniquely identify individuals within large datasets.

The content transmitted in C-ITS message headers and payloads includes personal information such as vehicle location, speed, heading, etc. Correlating V2X attributes with personal data, it is possible to deduce personal information, such as home and work locations, travel habits, and real-time tracking capabilities, even uncovering daily schedules, driving behaviour, and personal preferences that may serve as unique biometric identifiers. Therefore, a structured risk assessment of privacy threats must consider attacker capabilities, attack types, and the estimated likelihood and impact. This indicates that many high-impact risks arise not only from well-equipped state-level actors but also from private entities with lesser capabilities, highlighting the broad attack surface and underscoring the need for targeted mitigation strategies.

In specific cases, some auxiliary information, such as aerial imagery or public datasets, could support inferences about vehicle identities. In these cases, contextual factors allow to overcome anonymity, given that the latter uses basic aggregation or pseudonymisation measures. Scenarios and examples of potential reidentification pitfalls are available, ranging from linkages between vehicle trajectories and home locations to correlations with external datasets such as tolling or mobile app usage, each illustrating how seemingly anonymised data can still be traced back to individuals when combined with sufficient auxiliary information.

TIARA identified several measures to prevent reidentification. Identifiability prevention strategies must avoid compromising the functional value (interoperability and usability) of the data. Mitigations cannot be reactive or generic, but rather proactive, especially in high-risk use cases involving longitudinal vehicle tracking or high-resolution geolocation. The effective strategies combine technical data protections with governance safeguards and public trust mechanisms. These include technical interventions (such as reduced spatial resolution, random perturbation, or differential privacy techniques) and organisational and procedural protection controls (such as access limitations, contractual clauses, and transparency obligations).

2.4.3 Outlook

With regard to PKI deployment and operation, TIARA gives the following recommendations:

- Combine specialist skills and trusted outsourced service providers to build expertise.
- Follow CCMS and ensure cross-border interoperability to align with EU trust model.
- Coordinate across NRAs, OEMs, telecoms, and cities to foster collaboration.
- Avoid vendor lock-in, promote open interoperable standards, support hybrid comms.
- Ensure robust security by continuous monitoring, readiness, and independent audits.
- Plan for flexibility and scalability, with modularity, and backwards compatibility.
- Share costs and responsibilities (with use of e.g. Public-Private Partnerships, automation, and long-term contracts).

- Focus on user trust and adoption by delivering reliable, high-quality services.

Furthermore, the NRAs should also focus on:

- Authenticating and controlling users,
- Managing the expiration of certificates,
- Reducing PKI infrastructure complexity, and
- Standardised use cases and message formats.

With regard to the legal and ethical aspects, TIARA gave the following guidance and recommendations for NRAs in the future:

- Embed legal, contractual, and ethical responsibilities for data accuracy in operations.
- Identify road users, communicate and involve in real-world service development.
- Acquire expertise on C-ITS services, use cases, and their limitations.
- Establish inclusive and transparent communication.
- Develop inclusive services using human-centred design principles.
- Apply ethical principles and processes for data use.
- Carry out risk evaluation when communicating and developing ITS/C-ITS services.

With regard to privacy, no single technique provides complete connected vehicle deanonymisation privacy protection. While pseudonymisation and geo-obfuscation are practical short-term options, their limitations in advanced threat scenarios justify a longer-term inclusion of decentralised processing and dynamic consent models. To achieve meaningful privacy protection while ensuring interoperability and usability, a structured and phased approach is necessary. Our proposed structured roadmap reflects a phased prioritisation on the short, medium, and long terms, derived from the privacy threats, attacker profiles, and mitigation strategies. In the short term, privacy protection is based on governance and interoperability such that it can be implemented relatively quickly and easily. In the mid- and long-terms these measures are built upon enable stronger decentralisation and privacy-by-design protocols.

Subsequent reuse of data sets requires that road users trust road operators to continue using data in a lawful and deliberate manner. It is essential that road authorities strive to be open and transparent. Road authorities should understand the types of information, characteristics, behavioural patterns, etc., that can be inferred about road users from the connected vehicle data that is collected.

3 Recommendations

3.1 Digital road operator data strategy

The data strategy (Bokolo et al, 2025) builds on the outcomes of the three projects DROIDS, PRESORT and TIARA. The strategy is structured in five parts (chapters):

- European data strategy and recommendations (Chapter 3)
- Stakeholder roles and priority of use cases for road operators (Chapter 4)
- Information life cycle, maintenance and regulations (Chapter 5)
- Use of third-party data (Chapter 6)
- Trust in data and service provision (Chapter 7)

A major conclusion is that the NRAs and other road operators benefit from digitalisation and the use of digital models, shadows and twins. The development, operation, maintenance and use of the digital representations are estimated to have high benefit to cost ratios in most use cases.

European data strategy recommendation topics based on European data strategy and related initiatives such as operationalization of dataspaces to ensure safe, reliable, and trustworthy data sharing for NRAs and other stakeholders, were as follow:

- Recommendations on data governance
- Recommendations for a sovereign data sharing approach
- Recommendations on trusted data sharing and exchange
- Recommendations from deployment methodology for dataspaces
- Implementing skills and training

A conclusion is that in a multistakeholder European-wide digital ecosystem, liaison between stakeholders and data exchange according to the guidelines of the European mobility data space are essential for the NRAs and other road operators as this ensures interoperable and secure sharing of road transport data.

The role of the road operator for digital representations (model – shadow – twin) depends on the use case. It is important to bear in mind that the European NRAs have also other roles than the road operator depending on the national road transport system governance models. Thereby, many road operators have also the role of traffic managers, while some also have the role of traffic information service provider or road transport authority.

Typically, the road operator assumes an active role in development, operation and maintenance of the use cases directly connected to the primary tasks of the road operator. In addition, road operators tend to be the users of the digital presentations available for all use cases as this likely increases the efficiency of the road operators' own processes.

The restrictions of public sector budgets in road infrastructure and its operations mean that the NRAs have to move towards digital road operation as all evidence supports the view that digitalisation makes also NRA operations more efficient with high benefit-cost estimates. At the same time, the restricted budgets mean that digital representations cannot be realised for every use case. The conclusion thereby is that the NRAs need to focus on some use cases. The data strategy proposes the following overall priority order for digitalisation for the next years:

1. asset management (digital model/shadow)
2. electronic traffic regulations – speed limits (digital shadow)
3. road works (digital model/shadow)
4. incident detection (digital shadow)
5. access control/ UVAR incl. road tolls (digital shadow)
6. electronic traffic regulations – general regulations (digital model)
7. CCAM – distributed ODD awareness (digital shadow)

Many of the use cases are expected be realised as digital shadows, i.e. the digital representation is automatically updated whenever the status of the physical counterpart is changing. For asset management and road works, however, the very likely 2030 situation will be digital models. For most critical parts of the infrastructure such as vulnerable bridges and tunnels, the asset management should likely be utilising digital shadows.

As all the use cases are relevant for the NRAs, the NRAs should at the minimum liaise or otherwise agree with the active stakeholders in a use case, where the NRA itself is not actively involved in except for its use and providing support to its maintenance by providing information to it. In addition, the NRA should liaise with other stakeholders operating similar digital representations

as having an identical view of the physical aspects of the transport system is in every stakeholder's interest.

The road operators must standardise the information by adopting ISO 19650 and implementing an object type library from early phases of digital representation development in order to ensure interoperability. The road operators are recommended to pilot the usefulness of BIM and AIM information within HD maps in cooperation with HD map providers. At an early stage, road operators can focus on making sure that the information related to assets such as GIS information is organised, updated, and complete. It is questionable whether the HD maps would be NRAs core business even in the future, however.

Services and data that are typical and core business for an NRA as a road operator and often a traffic manager, and their operational services and common operational picture should be shared with the road traffic management ecosystem. These services and data can provide benefits for example on traffic safety and flow as well as reducing emissions. Important part of the benefits comes from OEMs and service providers who build their services by utilising the road operator and traffic manager data and services.

However, all data and services should not be shared. For example, data that has been bought from third-party service providers and data that is under ecosystem agreement are outside of sharing scope. Furthermore, data that is shared should not cause harm or damage. The damage can involve for example security or privacy related issues. Therefore, a risk analysis is needed to evaluate any privacy, security or other risks that the data and services provided by the NRAs could include.

Information life cycle, maintenance and regulations included the following recommendations for the digital road operators on information maintenance and availability:

- Identify use cases and define the scope/purpose
- Invest in skills and education
- Adopt Open Data Standards
- Align with National Standards
- Prioritize Major Projects for Information Management Upgrades
- Move Towards Integrated Asset Management Systems
- Phased Implementation
- Change Management

BIM representation for full life cycle of road infrastructure included the following recommendations to maintain the BIM information throughout the lifecycle of road infrastructure:

- Implement ISO 19650
- BIM standards: Create or adapt existing BIM standards and guidelines
- Develop and implement OTL
- Establish collaboration and communication

To reap the benefits of standardisation emerging from OTL implementation and possible extension, road operators could consider the following key components:

- Data Dictionary Foundation: Build upon existing data dictionaries to establish standard definitions and meanings.
- Leverage Open Sources: Utilize open-source libraries like bSDD and Uniclass to establish a solid foundation and ensure continuous updates.
- Extend with New Attributes: Incorporate new attributes to accommodate dynamic information and future needs.
- Collaborative Development: Involve multiple stakeholders to ensure the OTL meets diverse needs and facilitates data exchange.
- Continuous Adaptation: Regularly review and update the OTL to adapt to evolving requirements and technologies.

- Standardization and Interoperability: Ensure the OTL is standardized and interoperable with other systems and platforms.

- ISO Standards Implementation: Adopt ISO 19650 to provide a framework for information management and exchange.
- To improve the BIM information reuse, road operators should implement BIM standards within their organisation for information management and try implementing an OTL to provide structure to asset information.

The digital twin use cases of digital transport regulations, opening new roads, automated lane level navigation, included the following recommendations:

- Early engagement in standardization
- Local perspective and requirement sharing
- Phased digitalization of traffic rules
- Development of a clear digitalization strategy
- Uniform Traffic Regulation Order (TRO) processes
- BIM standardisation
- Ensuring high-quality infrastructure for Automated Driving Systems (ADS)

Third-party data usage recommendations for successful collaboration between NRAs and third-party data providers to fully utilise the potential of third-party data within NRAs were as follows:

- Establish a Shared Vision
- Invest in Staff Education
- Foster Collaboration and Innovation
- Prioritize Data Coverage:
- Adopt a Use-Case-Centred Approach
- Strategically Integrate AI and Sensors
- Address Data Quality Concerns
- Develop Standardized Frameworks and Agreements

Insights into the practical use of third-party data with in-depth overview of the outcomes and lessons learned by the selected NRAs in procuring, implementing, and utilising third-party data provided five main lessons learned included the following which are here summarised by main topic:

1. Pre-procurement phase
   a. Pre-studies
   b. Market consultation
2. Procurement phase
   a. Balancing quality and cost
   b. Setting minimum requirements and award criteria
3. Implementation phase
   a. Data integration: System operation and data extraction of procured data require ensuring compatibility with existing platforms and proper adaptation for smooth integration
   b. Understand the data that is procured
   c. Addressing data attributes
   d. Data access control for procured data and its derivatives must balance open access for public use and controlled distribution for private entities.
4. Maintenance and monitoring phase
   a. Ongoing data quality assurance and data understanding: Regular monitoring and validation of data quality are essential for maintaining effectiveness of third-party data.

   b. System flexibility: Adaptability in systems and data management processes is crucial for handling updates and changes in third-party data providers.
5. Overarching phase: Service Level Agreement (SLA), scalability, barriers/challenges, and risk
   a. SLA monitoring: third-party data providers meet the expected standards for data delivery and quality.
   b. Scalability challenges when aiming full-scale implementation with increased data coverage with accuracy and performance maintained.
   c. Risk mitigation

The strategy recommends the step-by-step guidance for all phases of the process of the use of third-party data from pre-procurement studies to the actual procurement phase and follow-up activities during the contract period as provided by the PRESORT project.

Trust in data and service provision recommendations start with an overview of the ongoing roll-out of the C-ITS PKI within the European NRAs, including overview of PKI roll-out, multiple PKIs and lessons from other sectors. Furthermore, guidance on the implementation of the C-ITS PKI includes guidance on procurement and costs as well as a roadmap.

The review of legal and ethical ramifications for NRAs when making use of ITS and C-ITS data, and of how these change the role of the NRA, included responsibility of data accuracy, ethical use of data, inclusive communication and development of ITS and C-ITS services to road users. For the forementioned topics, the recommendations for the NRAs are:

- The NRA should embed legal, contractual and ethical responsibilities for data accuracy in their operation.
- Identify the road users and involve them in communication and real-world development of the services.
- Understand and acquire expertise on C-ITS services, use cases and their limitations.
- Follow inclusive and transparent communication recommendations.
- Develop inclusive services by using the human-centred design principles.
- Apply basic principles and processes for ethical use of data.
- Carry out risk evaluation when communicating and developing ITS/C-ITS services.

Connected vehicle deanonymisation research review and impact study provided knowledge on the privacy impacts of the processed road user location data, as well as recommendations to improve the location privacy-preservation.

The strategy promotes following the trusted service provision recommendations of DROIDS for road operators as related to “Trust in the system“ as well as “Trust with the system“.

3.2 Implementation roadmap

The roadmap for implementing the data strategy (Kvalvik et al. 2025) compiled findings from the strategy as well as the outcomes of the DROIDS, PRESORT and TIARA projects. In all, the actions regarded as relevant for the roadmap included 94 separate actions. Many of the actions overlapped partly and were thereby compiled. The high-priority actions to be finally included into the roadmap were selected on the basis of the workshops (DROIDS Advisory Group, Programme Executive Board) held in June 2025.

The roadmap includes 11 action categories, which further comprise 15 actions for the digital road operators. The following paragraphs present the action categories and actions included for road operators, CEDR, and specific actions concerning the European Data Spaces. The following seven high-priority action categories for road operators were proposed in the roadmap:

1. Provide education and enhance skills
2. Implement interoperability and utilise standards
3. Carry out stakeholder collaboration and prioritise use cases
4. Develop and purchase data and services based on standards, guidelines and design principles
5. Develop data governance and risk management framework
6. Implement a change management process
7. Implement a trust framework

Table 3 High-priority action categories and actions for NRAs.

1. Provide education and enhance skills	
Action A1	A training programme tailored to different road operators and contractors for a particular country based on their digital readiness levels and high priority use cases should be developed. Besides traditional competence development, the programme should include more practical approaches, such as participating in pilots, smaller proof-of-concept activities, or use-case-driven training. The educational institutions should be involved in the training program. For example, the following curriculum could be established: (1) Procurement of digital tools, services and third-party data, including competitive dialogue and innovation partnerships. (Laine et al., 2025), (2) IoT, (3) Digital Twins, (4) HD Maps, (5) Digital trust (PKI) and security (6) C-ITS services, use cases and their limitations (7) BIM, (8) AIM, (9) Interoperability and standards, (10) Cyber security, (11) Data governance, (12) Data science, (13) WEB3 and (14) Data space technology
2. Implement interoperability and utilise standards	
A2	Utilisation of international and EU standards shall be prioritised, but where they do not exist, national standards should be used. Appointed ambassadors from the road operation domain should take part in different standardisation committees and forums. Standards and their implementation profiles need to be validated and implemented, e.g. C-ITS in C-Roads Platform. High-priority standards within the following areas should be prioritised: • Cooperative Intelligent Transport Systems (C-ITS PKI, C-Roads) • Real-time Traffic Information (RTTI delegated regulation, Datex II) • Road Infrastructure Data (OTL) • Privacy (GDPR, ePrivacy, ITS) • Road Infrastructure Asset Management (BIM, AIM, GIS).
3. Carry out stakeholder collaboration and prioritise use cases	
A3	By engaging stakeholders, road operators can ensure that data initiatives are closely aligned with the digital needs of road operations. This includes: • Deploy the most important and useful digital representation use cases about road operators' core business in a cost-effective manner The national road operators should outline real-world challenges and opportunities in prioritised use cases that promote the acquisition of new data sources. This can be achieved through early engagement with end-users by demonstrating selected use cases, pilots, and proof-of-concept activities.
A4	The road operators should develop a stakeholder strategy to engage with key data providers (e.g., road authorities, third-party data providers, citizens) to establish a shared vision on utilising data as an asset, ensuring comprehensive data coverage and fostering innovation (the CEDR PRESORT project, e.g. Laine et al. 2025). The national road operators should encourage collaboration between public administrations and private companies to share costs and expertise.

4.	**Develop and purchase data and services based on standards, guidelines and design principles**
A5	Data has become a new raw material for service provisioning and innovation in digital road operations (e.g., Digital Twins, AI tools, HD Maps). New, digital services and products should be developed, supporting data as an asset, by carefully considering the following: • Development of new digital services and products based on data, adhering to a set of recommendations for interoperability and standards (such as data formats and quality attributes), ownership and usage rights, laws, and regulations (GDPR, Data Act, Data Governance Act). • Focus on developing mature, well-functioning products that have undergone MVP verification, provide clear commercialisation opportunities • Leverage open data sources while safeguarding sustainability, quality and accuracy.
A6	A revised set of guidelines for purchasing data products and services must be incorporated into public procurement procedures (and supported by digital contract negotiations in data spaces). (e.g. Laine et al. 2025)
A7	Development and innovation of new services and products should integrate human-centric design principles and co-creation with relevant stakeholders.
5.	**Develop data governance and risk management framework**
A8	The national road operators should agree on a data governance framework that: • Define the data attributes that are align with the requirements early (e.g. accuracy, coverage) • Ensures the efficient and effective utilisation of information, including backwards compatibility and diversity • Covering areas such as data privacy, data security, data quality, data catalogues and metadata management, data in cloud and hybrid environments, data ethics, data governance tools, and data governance maturity. • Supports quality metrics with well-established and accepted measurement methods • Road operators should be mindful of potential data quality issues in less populated regions, where third-party data providers often operate. • The road operator should embed legal, contractual and ethical responsibilities for data accuracy in their operation • Aims to integrate data from various sources and systems to meet objectives (accuracy, consistency, coverage, other requirements), facilitating interoperability and ensuring that data across the stakeholders is compatible and usable. • Effectively managing compliance and mitigating risks in data handling (e.g., sensitivity, potential impact, and C-ITS services) requires a strategic approach, and data governance plays a pivotal role. • Work across sectors to align legal frameworks, technical standards, and operational practices. • Conduct regular security audits • Define clear consent models, especially for pseudonymised vs. personal data that communicates well with the consenter. • Integrate privacy-by-design into procurement rules and certification processes • Work with legal, procurement and audit to elevate data as a deliverable and communicate all data policies internally and externally • Introduce adaptive governance, allowing stakeholder-led audits

6.	**Implement a change management process**
A9	Implement a change management process that supports new processes, organisational changes or adoption of technologies to ensure smooth transition and acceptance.
7.	**Implement a trust framework**
A10	Apply adequate monitoring of PKI infrastructure to detect technical and security issues. Using the EU C-ITS PKI will allow for effective data exchange across borders

The key priority action for CEDR is to establish appropriate CEDR activities that support the evolution of road operators towards digital road operation. Such an activity can be a temporary working group, a workshop or series of them, or a research call, for instance. The actual format of the activity needs to consider the work topic, the needs of the road operators, and the urgency of the need for the activity. The actions related to the CEDR action category are presented in Table 4.

Table 4 High-priority action for CEDR

8.	**Establish appropriate CEDR actions to support digital road operation**
A11	Establish appropriate CEDR activities that support the evolution of road operators towards digital road operation. According to the road operators participating in the DROIDS workshops, the current list of possible topics for such a CEDR activity is: • Establishment of skills needed by road operators and their contractors in digital representations (models, shadows, twins) and related processes including cybersecurity. • Identification of the most important digital representation use cases and their types based on European, national and CEDR priorities as well as a socio-economic assessment of the different use cases in various deployment scenarios • Aim to ensure that road operators embed legal, contractual and ethical responsibilities for data accuracy or in general high data quality in their operation so that the society and key stakeholders can trust and thereby fully utilise the data from the road operators. • Use of open standards to reduce dependency on proprietary technologies and patents, ensure cross-member state harmonisation, improve data quality and transparency as well as preserve privacy. • Define the role and actions of the road operators in joining the European mobility data space promoted by the European Commission including the need of a European data governance body. • Development of a clear digitalisation strategy for road operators taking on board related European strategies, national priorities and the varying digital maturity of the road operators.

The following three high-priority action categories for specific actions for the European Data Spaces were proposed in the roadmap (Table 5) :

9. Implement an European Mobility Data Space compliant data space supporting digital road operations
10. Formalise the standards to be applied for digital road operations
11. Implement a data governance framework and a data governance body

Table 5 High-priority actions related to European data spaces

9. Implement an European Mobility Data Space compliant data space supporting digital road operations	
A12	Road operator should create a data space that is compliant with the common European Mobility data space (European Commission, 2023). Deployment of data spaces supporting road operations should comply with the data spaces design principles (Appendix 6.4), the step-by-step approach in the Co-Creation Method (Appendix 6.5) and the Deployment stages (Appendix 6.6) provided by Data Spaces Support Centre to engage stakeholders in the following key areas: (1) Developing use cases and identifying functional requirements, (2) Defining the governance structure (Technical and organisational), (3) Developing data products and services, and (4) Defining the architecture and the technical infrastructure.
10. Formalise the standards to be applied for digital road operations	
A13	The standards agreed on for digital road operations should be implemented as a data space "vocabulary service" (see chapter 1.3 Terminology) that acts as a central repository for standardised data models and their documentation, enabling semantic interoperability.
11. Implement data governance framework and data governance body	
A14	The data governance framework agreed by the road operators should be implemented according to the recommendations proposed for the Common European Mobility Data Space (Scholliers et al., 2025). Road operators should agree on a rulebook (governance model) for the data space.
A15	CEDR should agree up on the form for the data governance body (e.g. EU wide, Member state, Expert group) for digital road operations by reviewing the analysis performed by Directorate-General for Mobility and Transport (Scholliers et al., 2025)

The roadmap action implementation schedule differs between road operators, as it is dependent on two factors: first, the road operator's maturity level (or technical readiness level) in road operation digitalisation, and secondly, the priority of the action for the local road operator. Also, implementation of actions depends on combination of the local road operator ambitions and budget constraints.

Most of the actions were directed to the road operators. The actions directed to CEDR were fewer but still important, as several key actions and decisions by road operators require support from CEDR-initiated activities, including the sharing of best practices, identification of key digital representation use cases, and guidance to ensure trust in road operator data, among others.

3.3 Final Conference

The results of the three projects were presented during the CEDR Call 2022: Data Final Programme Conference on 14–15 October 2025 at Birmingham UK in parallel to the Highways UK 2025 conference. Each project presented their results, which were discussed among the participants. In all 25 persons participate in the conference. More than half of the participants were not members of the three project consortia.

Figure 8. A group of final conference participants at the end of conference.

The PRESORT presentation focused on the key outcome of the project, i.e. the Conclude report (Laine et al. 2025), that provides guidance to the NRAs with regard to dealing with third-party data.

The discussion pointed out that switching data providers requires significant system updates due to changes in algorithms and integration. To mitigate this, NRAs should develop adaptable in-house systems, schedule development time for compatibility updates, and ensure continuous operations through planned provider transitions. The discussion also concluded that given there are many CEDR members, the possibility of jointly procuring data across Europe instead of each NRA doing small procurements should be encouraged. This could particularly help smaller NRAs lacking sufficient experience for such procurement. In addition, current work in Europe with the common European mobility data spaces (EMDS), could offer potential help to navigate between data and providers.

The TIARA presentation covered all its three work areas i.e. 1) Public Key Infrastructures (PKI) and trust, 2) legal and ethical aspects, and 3) privacy issues related to C-ITS and other ITS.

Several points were raised in the discussion, especially related to trust. PKI implementation requires specialised skills. Thereby, it was recommended to build internal expertise for core governance but consider outsourcing day-to-day operations to specialised vendors.

To ensure interoperability between different communication technologies, (ITS-G5, C-V2X, cellular IP), certificates should work consistently across all technologies. Systems must avoid vendor lock-in and be designed for hybrid communication environments.

To keep end users' trust even when data or services differ between jurisdictions, the user experience must remain seamless across borders; inconsistent or unreliable services will erode public trust.

Concerning ethics related to acceptable data quality, it was agreed that 100% quality and accuracy are impossible to reach, and for this reason liability problems might arise. Thereby the ethically correct and also legally sensible approach is that the NRAs transparently announce the quality of the data and information provided. This naturally requires sound quality management and monitoring practises.

DROIDS presented it results with regard to NRA roles in digital models/shadows/twins, digital twin state of the art and evolution, trust assurance as well as the digital road operator data and information strategy.

Finally, a workshop was organised to evaluate top 3 digital road operator data strategy and roadmap action priorities when implementing two use cases of asset management and electronic traffic regulation speed limits.

The workshop participants answered a questionnaire individually and anonymously in two groups depending on their stakeholder group: either as a road operator or as a private industry member. The participants were instructed to consider them as being a road operator with low to medium maturity level digital road operation capability. After the questionnaire, the participants had an open discussion on the questionnaire results.

The asset management use case top 3 priorities for action categories to implement for both road operator and private sector members (n=17) were the following:

1. Carry out stakeholder collaboration and prioritise use cases
2. Provide education and enhance skills
3. Implement interoperability and utilise standards

The electronic traffic regulation speed limits use case top 3 priorities for action categories to implement for both road operator and private sector members (n=16) were the following:

1. Develop a data governance and risk management framework
2. Formalise the standards to applied for digital road operations
3. Implement interoperability and utilise standards

Most of the questionnaire answers by road operators and private industry members on top 3 priority actions to implement aligned which each other. Although the order of the answers in top 3 could slightly differ, the actions included in the top 3 were mainly the same. Road operator related actions were ranked high as well as Data spaces action to formalise the standards to be applied for digital road operation. CEDR action was mid-level priority, being a supportive action.

Discussion in the workshop based on the questionnaire results underlined the difficulties to compare the detailed actions with each other due to complex use case implementation environments where road operators' maturity levels can differ.

Based on the findings of the three projects, the conference paved the way for the NRAs to become digital road operators. This was proposed to be done in the following manner:

1. Focus on the national policies and transport problems requiring attention while working within the natural constraints (budgets, personnel resources, etc.)
2. Build up a national action plan utilising the Data Call 2022 results where and when relevant
3. Prioritisation is necessary as budgets are restricted while remembering that investments in digitalisation will save money
4. Invest on parts of road networks and use cases or processes where the deployments bring most value for money
5. Utilise lessons learned from more advanced NRAs utilising CEDR support.

The final conclusions of the conference highlighted the extremely good timing of the Call as the call coincides with the development and publication of the EU Data Strategy, European Mobility Data Space, and the rise of AI requiring Data as its fuel. The conclusion was also that the conference and especially the discussions during it proved that the project results are relevant for the NRAs.

The final conference also agreed that data is fuel for NRAs in decision-making, innovation, and making NRA processes more efficient. The results obtained so far from individual NRAs indicate benefit/cost ratios above 10 for digitalisation of NRA processes, which is also a necessity as most NRAs are experiencing continuously decreasing budgets.

The lessons learned during the two years of the project work included the vital importance of interaction with the PEB (Programme Executive Board). The experiences of the projects proved that active mutual cooperation with PEB representatives provided fruitful results while passive coexistence provided scarce benefits. The experiences with working with Advisory Groups were clearly positive bringing in the views of the other stakeholders in digital road operation.

During this call, the cooperation between the projects in the call worked very well and resulted in added benefits to the projects itself and also CEDR and its members. The resulting data strategy and its implementation road map fully took on board the findings, outcomes and recommendations from all three projects of DROIDS, PRESORT and TIARA.

4 Conclusions

The Data Call of CEDR's Transnational Road Research Programme was established in 2022 to support the National Road Authorities (NRAs) to address the challenges and to reap the benefits of digitalisation. The NRAs were seen to need to ensure useful, trustworthy and secure data being collected and shared effectively by themselves, third-party service providers and road users. The digitalisation progress in the various business areas of NRAs indicated great promises of increased efficiency in road operation domains from digital roads to digital twins led by the NRAs is aiming for a greater improvement in asset management operations.

The evolution of digitalisation during the lifetime of the Call's projects has proved the timing of the Call to be extremely appropriate. The launches of the European Data Strategy and European Mobility Data Spaces as well as the outburst of AI using data as its fuel have highlighted the crucial position of data in all domains of the society including mobility and road transport.

The call expected research work on three topics, and a project consortium was selected for each of the topics. The topics and their respective projects were:

a) Maintaining and sharing the digital road infrastructure - DROIDS
b) Improving the use of third-party data by NRAs - PRESORT
c) Integrity, Authenticity and Non-Repudiation (e.g. proof of the origin, authenticity and integrity of data) integrated in Trust Models for C-ITS applications - TIARA

Each project fulfilled the objectives set to them in the original description of research needs and the research questions set by CEDR. While the topics focused on specific aspects, the three projects identified and clearly mapped their commonalities, and managed to work closely together. This facilitated the development of a data strategy for NRAs (Bokolo et al. 2025) and an implementation road map (Kvalvik et al 2025) for that strategy utilising the outcomes and findings of all three projects.

The data strategy and its implementation road map describe 15 recommended high-priority actions to the NRAs and one action to CEDR. It is not expected that all NRAs would immediately commence the recommended actions. Each NRA is recommended to study the content of the actions and select the ones that best help them in carrying out their mission as NRAs to meet the national transport policy goals, to address their national transport related problems, and to give them the best value for money. The last point is especially relevant for the data strategy actions are expected to increase the efficiency of road operator processes to a considerable extent and thereby assist the NRAs to carry out their road operation tasks in the world of diminishing budgets.

All the projects also agreed that the use case-oriented approach would likely be the best way to go forward. Asset management was identified as a priority use case by most NRAs participating in the workshops of the Call. Each NRA likely focuses on its own priority use cases and priority road networks when starting its data and digitalisation related actions. As learned in the final conference, the priority of individual actions can also depend on the use case.

It is also clear that the maturity level of NRAs regarding digitalisation differ considerably. Thereby, lessons learned by high maturity NRAs could and should be utilised by those of lower maturity. In sharing the lessons learned and best practices related to data CEDR has a prominent role to play.

5 References

Bokolo, J. A., Kvalvik, P., Farbrot, J. E., Kotilainen, I. & Kulmala, R. (2025). Data strategy for digital road operators. CEDR Call 2022 Data, Digital Road Operator Information and Data Strategy (DROIDS) project, Deliverable 5.1. .

CEDR (2022). Description of Research Needs (DoRN). Call 2022 Data. CEDR Transnational Road Research Programme funded by Belgium-Flanders, Denmark, Ireland, Netherlands, Norway, Sweden, Switzerland, and the United Kingdom. October 2022. 15 p.

Kotilainen, I., Kulmala, R., Farbrot, J.-E., Kvalvik, P., Bokolo, A. J., Soni, S., Alkim, T., Adesiyun, A. & Dodoiu, T. (2025). DROIDS Final report. DROIDS Deliverable 1.5. 6 October 2025. 48 p.

Kvalvik, P., Bokolo Jr, A., Farbrot, J. E., Kulmala, R. & Kotilainen I. (2025). A roadmap for implementing the data strategy. Deliverable D5.2. CEDR Call 2022 Data, Digital Road Operator Information and Data Strategy (DROIDS) project. Version 1.0.

Laine, T., Isoranta, V., Kulmala, R., Kotilainen, I., Cowell, D., Graham, A., Soni, S., Huisken, G., Stephenson, D., Ayaida, M. (2025). Report on WP5 Conclude. PRESORT Improving the use of third-party data by NRAs,Final !7 April 2025. 108 p.
https://www.cedr.eu/docs/view/682daa0e2fa30-en

Stephenson, S. & Cowell, D. (2025). PRESORT: Final report. CEDR Call 2022 Data. May 2025. 27 p.

UK Government (2020a). Data Ethics Framework: Glossary and methodology, Guidance updated 16 September 2020. https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, accessed 24 October 2025.

UK Government (2020b). Data Quality Framework: guidance, Guidance published 3 December 2020. https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework-guidance, accessed 24 October 2025.

Walker, A. & Lockhart, P. (2025). TIARA Final report. TIARA Deliverable D1.2. Date 30/09/2025. 25 p. https://www.cedr.eu/docs/view/68e93e1d518e8-en

Ref: CEDR Contractor Report 2025 / Final Programme Report: CEDR Call 2022 Data

ISBN: 979-10-93321-86-8

Conference of European Directors of Roads
Avenue d'Auderghem 22-28
1040 Brussels, Belgium

e-mail: information@cedr.eu
Tel.: + 32 (0) 2 771 2478