Co-funded by the European Union

Digital Transport Infrastructure Upgrade Plan

DELIVERABLE D4.4

Version: Final

Project Acronym :	24-EU-TG-TISGRADE
Project ID:	101232828
Deliverable number:	D4.4
Deliverable name:	Digital Transport Infrastructure Upgrade Plan
Work package number:	WP4
Due date:	June 2026
Delivery date:	10 June 2026
Lead beneficiary:	PT_ARMIS
Main Authors:	André Rehberg João Montenegro Lígia Conceição Petr Bureš Sara Linhas

Table of contents

1 Introduction and context

1.1 Scope of task T4.3

Task T4.3 – "Improvements of digital transport infrastructure, data standards, DR compliance & cybersecurity" – is situated within work package 4 (WP4) – "NAP upgrades" –, whose overall objective is to support the upgrade of National Access Points (NAPs) towards at least the minimum level of service (LoS) defined by the NAPCORE project, thereby improving interoperability, accessibility, reliability, and usability of transport-related data and metadata across Europe. While NAPCORE focuses on harmonisation and coordination at a conceptual and policy level, TISGRADE's WP4 is explicitly concerned with practical implementation and deployment, translating agreed recommendations into concrete technical improvements on individual NAPs.

Deliverable D4.1 – "Roadmap for the implementation process" – is a product of task T4.1 – "Coordination & Mapping of IT infrastructure and architectures of NAPs" – and describes both WP4 and its place within TISGRADE in greater detail.

Within the above context, task T4.3 addresses the enhancement of the digital transport infrastructure (DTI) underpinning NAP operations, with a particular focus on back-office systems, data standards compliance, delegated regulation (DR) compliance, and cybersecurity. The task aims to strengthen the technical foundations of NAPs so that they can reliably support the publication, exchange, and reuse of transport data in line with evolving European legal, technical, and operational requirements.

The primary objectives of task T4.3 are to:

- Improve the robustness, scalability, reliability, and resilience of NAP digital infrastructures;
- Align the implementation and versioning of data standards with NAPCORE recommendations and the DRs supplementing Directive 2010/40/EU – the Intelligent Transport Systems (ITS) Directive;
- Support compliance with further applicable legal and regulatory requirements, including those related to data provision, quality, monitoring, and reporting;
- Strengthen cybersecurity and operational security measures across the NAP data chain, taking into account European requirements and best practices;
- Enable harmonised, yet nationally adaptable, technical upgrades across Member States.

The scope of task T4.3 covers both technical and organisational aspects of NAP operations insofar as they directly affect the digital transport infrastructure. This includes, but is not limited to:

- Upgrades to NAP back-office architectures and tooling, including user and data management functionalities;
- Integration of relevant toolboxes;
- Implementation and upgrade of data formats and exchange mechanisms to newer or more appropriate standard versions, where required to meet regulatory or interoperability needs;
- Introduction or enhancement of automated quality checks, monitoring, and reporting functions for published data and metadata;
- Cybersecurity improvements addressing risk management, access control, secure data exchange, and operational monitoring.

Although upgrades related to the mobilityDCAT-AP – which specifies a harmonised metadata structure and definitions – and metadata at large are being taken up by task T4.3, and upgrades to user interfaces (UIs) and user experience (UX) fall within the purview of task T4.4 – "User experience enhancement" –, they are important pieces of the upgrade plan, and are thus considered in task T4.3.

Task T4.3 is explicitly implementation-oriented, focusing on how required or recommended capabilities can be realised in practice, rather than redefining harmonisation principles, which remain under the remit of NAPCORE. At the same time, the task recognises the diversity of existing NAP architectures and maturity levels across Member States; therefore, it promotes harmonised outcomes rather than uniform technical solutions.

Task T4.3 is divided into two complementary subtasks:

- T4.3.1 – Implementation, covering the deployment and reporting of concrete upgrades and enhancements to NAP infrastructures;
- T4.3.2 – Implementation support, facilitating coordination, information exchange, and alignment with related activities in tasks T4.1 and T4.5 – “Description of best IT practices, sample architecture, future improvements needs”.

1.2 Purpose of deliverable D4.4

Deliverable D4.4 – “Digital Transport Infrastructure Upgrade Plan” – is the short-term output of task T4.3 and is intended to provide a structured, implementation-oriented

upgrade plan for the digital transport infrastructure supporting NAPs. Its purpose is to consolidate, in a common and practical way, the main technical needs, legal and compliance aspects, standards-related improvements, and cybersecurity and resilience considerations identified across the participating partners, so as to support future NAP upgrade actions and provide a shared reference point for the task. In this sense, D4.4 serves as the bridge between the broad objectives of T4.3 and the later, more complete recommendations to be presented in D4.5 – "Final Report and Recommendations on NAP Upgrades with Cybersecurity Improvements".

More specifically, D4.4 is intended to support the planning of upgrades to NAP back-office architectures, tooling, data management, and exchange mechanisms, as well as the introduction or improvement of validation, monitoring, and reporting functions where needed. It also aims to capture the main upgrade priorities linked to compliance with DRs, evolving standards, and operational security requirements, while recognising that NAPs across Member States have different levels of maturity and different implementation contexts. Accordingly, the deliverable promotes harmonised directions and common priorities, rather than prescribing a single uniform technical solution for all NAPs.

At the same time, D4.4 is not intended to be a full technical implementation document, a detailed architecture design for each NAP, or a replacement for work already covered by related tasks such as T4.1, T4.2, or T4.5. D4.4 is also not an audit, certification exercise, or deep partner-by-partner technical assessment. Instead, its role is to establish a practical and sufficiently concrete framework that helps partners identify priority upgrade domains, align their short and medium-term actions, and prepare the ground for the more comprehensive final report and recommendations on NAP upgrades with cybersecurity improvements.

1.3 Legal background

The upgrade of NAPs is shaped by a multi-layered European regulatory framework. The following legal acts are of particular relevance for T4.3:

- The ITS Directive, as substantially revised by Directive (EU) 2023/2661, and its supplementary DRs, define what transport data must be made available and in which technical form;
- Directive (EU) 2022/2555 – the NIS 2 Directive – governs cybersecurity risk management;
- Regulation (EU) 2016/679 – the General Data Protection Regulation (GDPR) – constrains the handling of personal data;

- Directive (EU) 2019/1024 – the Open Data Directive – shapes the reuse conditions for public sector datasets.

These regulatory drivers are outlined below.

1.3.1 Data availability and data exchange standards

The revised ITS Directive is the primary legal basis for NAPs. The original 2010 framework was largely enabling, supporting voluntary and coordinated ITS deployment; the 2023 revision transforms it into a framework of mandatory obligations. Member States must now ensure that specified data types are available through their NAPs by defined deadlines, and that certain ITS services are deployed according to a concrete timetable. The revision also introduces a cooperation obligation requiring Member States to work together on NAP architecture interoperability, common metadata, quality requirements, and secure access – which is precisely what NAPCORE and TISGRADE aim to facilitate.

The revised ITS Directive's priority actions are operationalised through four DRs, each requiring a NAP for a specific data domain, offering discovery services for available datasets and ensuring data accessibility in machine-readable formats:

- Delegated Regulation (EU) 2022/670 – the Real-time Traffic Information (RTTI) DR – is the most directly relevant to TISGRADE. It covers RTTI across three broad categories – static road data, dynamic road status data, and real-time traffic data – with its primary data exchange standards being DATEX II and TN-ITS. The DR entered into application in January 2025, with full network coverage expected by the end of 2027;
- Delegated Regulation (EU) 2017/1926 – the Multimodal Travel Information Services (MMTIS) DR –, as amended by Delegated Regulation (EU) 2024/490, covers the exchange of multimodal travel information, primarily using NeTEx, SIRI, and Transmodel;
- Delegated Regulation (EU) 886/2013 – the Safety-related Traffic Information (SRTI) DR – specifies the use of DATEX II or other interoperable standards;
- Delegated Regulation (EU) 885/2013 – the Safe and Secure Truck Parking (SSTP) DR – defines DATEX II as the principal standard for SSTP-related data exchange.

Many Member States operate a single NAP serving several or all of these regulations, while some maintain separate platforms. In either case, simultaneous compliance with multiple DRs – each with its own data types, standards, timelines, and quality requirements – is a key operational challenge to be addressed by the NAP upgrades

within T4.3 through back-office modernisation, validation tooling, and alignment of data standards across domains.

The Open Data Directive reinforces and extends these data availability requirements for NAPs operated by public bodies. It requires that public sector data, including transport data, be made available in open, machine-readable formats and, for dynamic data and high-value datasets, via application programming interfaces (APIs). Mobility is one of the high-value dataset categories designated under Commission Implementing Regulation (EU) 2023/138, meaning that the relevant transport datasets must be provided free of charge and under open licences. This directly complements the ITS DRs and reinforces the value of API modernisation and open data integration.

1.3.2 Cybersecurity

The NIS 2 Directive is the principal cybersecurity act relevant to NAP operations and is explicitly referenced in the TISGRADE grant agreement. It identifies transport as a sector of high criticality and expressly covers operators of ITS as defined by the ITS Directive, creating a direct legal link to NAP operations. NAP operators may fall within the NIS 2 Directive's scope where they qualify as ITS operators or as public administration entities under national transposition, subject to the directive's entity size thresholds or its size independent inclusion criteria.

The NIS 2 Directive requires covered entities to implement proportionate cybersecurity risk management measures – including risk analysis policies, incident handling procedures, business continuity planning, supply chain security, vulnerability management, encryption, access control, and multi-factor authentication. Additionally, when a significant cybersecurity incident occurs, an early warning is required, within 24 hours of its detection, followed by a complete incident notification within 72 hours, and the submission of a final report within one month. The directive also introduces governance accountability: management bodies must approve and oversee cybersecurity measures and undergo dedicated training.

The revised ITS Directive complements the NIS 2 Directive by providing for emergency implementing acts to address cybersecurity or availability incidents affecting ITS services. Together, the two instruments establish the regulatory baseline for the cybersecurity component of T4.3.

1.3.3 Data protection and privacy

Although NAPs primarily handle transport metadata, they also process personal data - user accounts, API credentials, contact details of data publishers, and usage logs. The GDPR therefore applies and requires, among other things, that:

- Privacy be embedded into platform architecture from the design stage;
- Processing by third-party information technology (IT) service providers be governed by appropriate contracts;
- Adequate security measures be in place;
- Personal data breaches be notified to the supervisory authority within 72 hours.

Where NAP upgrades introduce new large-scale processing features, a Data Protection Impact Assessment may also be required. Where personal data are transferred to recipients outside the European Economic Area – for example, to third-country cloud providers – the GDPR's transfer safeguards apply.

The ITS Directive reinforces these obligations within the transport domain by limiting personal data processing to what is strictly necessary for ITS applications and establishing an anonymisation-first hierarchy. The GDPR's breach notification requirement runs alongside the NIS 2 Directive's incident reporting obligations, and both may need to be coordinated.

1.3.4 Adjacent regulatory context

Regulation (EU) 2023/1804 – the Alternative Fuels Infrastructure Regulation (AFIR) –, as amended by Delegated Regulations (EU) 2025/656 and (EU) 2025/671, creates obligations regarding the provision of alternative fuels data: Member States must make static and dynamic data on recharging and refuelling infrastructure accessible through NAPs, in open formats and via APIs, with a Common European Access Point for cross-border access. While the AFIR operates under a separate legal basis, some Member States are pursuing a single-NAP architecture covering both ITS and AFIR-related data. Implementing Regulation (EU) 2025/655 further specifies DATEX II as the required format, with stringent update frequencies and quality requirements.

Two further acts provide relevant context without imposing direct obligations on NAP operators. Regulation (EU) 2022/868 – the Data Governance Act – excludes NAPs from its data intermediation regime, but its interoperability principles and the broader European Mobility Data Space (EMDS) ecosystem remain relevant for NAP development. Regulation (EU) No 910/2014 – the eIDAS Regulation – does not create

obligations for NAPs either, but offers a framework for electronic identification and authentication that may support NAP user verification in cross-border contexts.

1.4 Relation with other work

T4.3 is related to work that has been done and is ongoing in other WPs and tasks within TISGRADE, as well as other European initiatives. These relationships are broadly described in this section.

Deliverable D4.1 explores these connections in greater detail, as well as those not specific to T4.3, but relevant to WP4 at large.

1.4.1 TISGRADE: other WPs and tasks

The TISGRADE work packages most directly linked to T4.3 cover complementary parts of the RTTI data value chain. WP2 – "Data collection and digitalization tooling" – addresses data collection and digitisation, WP3 – "Quality validation of static and dynamic data" – addresses data quality validation and compliance checks, WP4 addresses NAP upgrades, and WP5 – "Feedback Loop" – addresses the public-private feedback loop on data quality. The upgrade planning developed in T4.3 therefore both depends on and supports activities elsewhere in the project.

WP2 focuses on the collection, digitisation, and standardisation of RTTI data, particularly traffic circulation plans and traffic management measures, with the aim of making standardised RTTI data available through NAPs. This creates a direct link with T4.3, because NAP back-office systems must be able to handle the datasets and formats deployed through WP2. In practice, WP2 informs upgrade needs related to data pipelines, format support, storage architecture, and the operational management of published data.

WP3 concerns the quality validation of static and dynamic RTTI datasets, as well as best practices for data compliance checks, and it explicitly takes into account the output of the public-private feedback loop being developed in WP5. This is relevant for T4.3 because NAP upgrades may need to support stronger validation, monitoring, reporting, and quality-management capabilities so that datasets can be checked, maintained, and improved in a more systematic way. In this sense, WP3 and WP5 together help indicate where NAP-side technical improvements may be needed to support data quality processes.

WP5 conceptualises, demonstrates, and implements the public-private feedback loop on data quality. The grant agreement notes that the role of NAPs in this loop is to be

defined; depending on the adopted approach, this may require T4.3-related upgrades to support the technical interfaces, data flows, or system capabilities through which NAPs may participate in the feedback loop. As the relevant WP5 outputs are not yet available at the time of writing, D4.4 treats this mainly as a forward-looking dependency for later refinement.

Within WP4 itself, T4.3 is coordinated with the other tasks of the work package. T4.1's main goal is to coordinate the NAP upgrades across the WP4 tasks, other WPs, and other projects, ensuring the implementations are done in a harmonised manner. T4.2 addresses the implementation of the mobilityDCAT-AP and is therefore closely related wherever metadata improvements form part of broader NAP upgrades. T4.4 covers UX enhancements, complementing the back-office and infrastructure focus of T4.3. Finally, T4.5 will consolidate best practices and lessons learned from the other WP4 tasks and identify future improvement needs.

1.4.2 NAPCORE

NAPCORE has a strong connection to task T4.3 and deliverable D4.4. Upgrade plans for the NAPs should take into consideration NAPCORE's reference documents and guidelines – more specifically, the NAP LoS Key Performance Indicator (KPI) Framework (NLKF) and the NAP Reference Architecture (NRA). These are crucial inputs for developing the upgrade plan. On the other hand, the rollout of this plan, i.e., the developments and their respective results, should be used to provide feedback to NAPCORE's partners to further enhance and adapt this documentation and the guidelines.

The NLKF is a methodology developed to estimate and harmonise the LoS and interoperability of NAPs across Europe. It utilises a structured set of KPIs to provide NAP operators with a self-assessment tool, helping them identify the current state of their platforms and the technical gaps to be addressed in their roadmaps. Beyond individual assessment, the NLKF supports supervising bodies and helps establish a European benchmark reference for NAP performance. This framework allows operators to define exactly which features are missing or underperforming in their current setup and prioritise them within their individual upgrade plans. Consequently, the NLKF assists in selecting specific technical upgrades to implement, ensuring that short-term actions align with long-term European interoperability goals. Section 2.2.1 explores the NLKF in greater detail.

The NRA complements the NLKF by providing a technology-agnostic blueprint for developing and upgrading NAPs. The NRA consists of several layers and views that define a harmonised set of functionalities and technical interfaces. While the NLKF is

used to identify the necessary features (the “what”), the NRA provides the detailed specifications and structural levels (the “how”) essential for actual software development. The NRA is described more thoroughly in section 2.2.2.

During the TISGRADE planning stage, the primary focus remains on the NLKF to identify priority features, with the NRA serving as the overarching reference for the technical implementation phases.

1.4.3 UVAR Box

Urban Vehicle Access Regulations (UVARs) encompass a wide range of schemes through which cities and regions manage vehicle access, including low emission zones, congestion charging schemes, limited traffic zones, and pedestrian zones. As they proliferate across Europe, making UVAR-related information digitally accessible and machine-readable has become increasingly important for cities and regions, service providers, and end users.

The UVAR Box project was a European Commission (EC) preparatory action that addressed this need by developing the UVAR Box tool: an open-source web application for the creation, management, and publication of UVAR data. The project concluded in 2022, and the tool has not undergone further development since then.

The TISGRADE grant agreement explicitly references the integration of the UVAR toolbox as one of the possible digital infrastructure improvements for NAPs within task T4.3. This reference recognises that NAPs have an increasingly important role not only in providing real-time traffic information, but also in making access regulation data available to service providers and end users. The UVAR Box tool’s relevance to the NAP upgrade planning is multifaceted, as is described below.

The tool produces outputs in the format of the DATEX II UVAR profile, which can be exported and made accessible through NAPs. This facilitates data standardisation and extends the scope of data type available to users, and contributes to compliance with the revised ITS Directive, which now covers access restrictions within its expanded data requirements.

One of the challenges identified in the scope of T4.3 is the integration of relevant toolboxes into NAP back-office operations. The UVAR Box tool is an example of a relevant toolbox, with features such as map-based geometry editing, template management, validation against the DATEX II schema, and import/export capabilities – including REST API endpoints. The tool’s functionality thus aligns with the broader T4.3 objective of improving the robustness and functionality of the digital infrastructure supporting NAPs.

Adoption of the tool is facilitated by its open-source availability, as it is licensed under the European Union Public Licence (EUPL). It also uses common technologies – such as Java, Vue.js, PostgreSQL and PostGIS, and Docker – making integration into existing NAP architectures simpler. The tool will also potentially be hosted under the napcore.eu domain, which would further improve accessibility for stakeholders. This is because NAPCORE's task T5.2 – "Tools" – foresees further developments to the tool, such as an upgrade to DATEX II version 3.6 or higher, including an expansion of the supported traffic regulation and restriction data types. This ongoing development is also relevant for TISGRADE's T4.3, as NAP operators considering UVAR data integration can expect a modernised, actively maintained toolbox aligned with the latest data standards.

It should be noted that the direct integration of the UVAR Box tool into NAP operations is not a universal requirement under T4.3. The tool represents one possible approach to addressing UVAR data provision – relevant primarily to those NAP operators whose planned upgrades include the integration of UVAR data or the expansion of their data catalogues to cover access restrictions. For the broader scope of T4.3, the UVAR Box serves as a practical example of how purpose-built and standards-aligned tooling can support NAP digitalisation objectives.

1.4.4 C-Roads

C-Roads is a major European initiative coordinating the deployment, harmonisation, and cross-border interoperability of Cooperative Intelligent Transport Systems (C-ITS). Its work covers technical specifications, security frameworks, public key infrastructure governance, and large-scale pilot deployments across Member States. Although C-Roads does not operate NAPs, its outputs directly influence the DTI that NAPs rely on. C-ITS services generate dynamic, safety-critical information – such as hazard warnings, road works notifications, and traffic management messages – using standardised message sets – such as Decentralised Environmental Notification Messages (DENMs) and Cooperative Awareness Messages (CAMs) – and secure communication channels. As Member States scale up C-ITS deployments, NAPs increasingly need to interface with these data flows, either by publishing C-ITS-derived information, aligning metadata and data models, or ensuring that back-office systems can ingest, validate, and expose relevant C-ITS content in line with the ITS Directive and the RTTI DR.

For task T4.3, C-Roads represents both a dependency and an enabler. Its harmonised specifications and security requirements inform several upgrade domains addressed in D4.4: alignment of data standards and profiles, secure data exchange mechanisms,

certificate and trust management, and operational monitoring of safety-related information. C-Roads' work on the C-ITS Security Credential Management System (SCMS) and its governance model is particularly relevant for the cybersecurity dimension of T4.3, as NAP operators may need to ensure compatibility with C-ITS trust frameworks when handling or redistributing C-ITS-derived data. Moreover, as C-Roads pilots increasingly integrate DATEX II interfaces for back-end exchange, their outputs support the convergence of C-ITS and NAP ecosystems. In this sense, C-Roads provides practical technical foundations that T4.3 can build upon, ensuring that NAP upgrades remain interoperable with emerging cooperative services and future large-scale C-ITS deployments.

2 State of practice

2.1 Task T4.3 questionnaire to assess the current challenges

To inform the development of the DTI upgrade plan, a questionnaire was distributed to all TISGRADE partners active in T4.3. The questionnaire was designed to capture a baseline picture of each partner's NAP in terms of:

- Its current setup and known challenges;
- Infrastructure, architecture, and data exchange practices;
- Main pain points related to standards, regulatory compliance, and cybersecurity;
- Ongoing or planned improvement initiatives.

Respondents were also asked to identify their priority actions and express what they would like D4.4 to address.

Fourteen responses were received:

- Austria – NAP operator;
- Cyprus – NAP operator;
- Czechia – NAP operator;
- Croatia – NAP operator;
- Finland – NAP operator;
- Germany – NAP operator;
- Hungary – NAP operator;
- Italy – potential NAP data provider (Port Authority of La Spezia);
- Latvia – NAP operator;
- Lithuania – NAP operator;

- Netherlands – NAP operator;
- Slovenia – NAP operator;
- Spain – NAP operator;
- Sweden – NAP operator.

Although the limited sample may not be fully representative of the overall European landscape, it serves to showcase the variety in the maturity of NAPs and identifies some common issues and needs.

While the respondents who are not NAP operators contributed expectations towards NAP evolution and the relevance of D4.4 for non-NAP stakeholders, this section's analysis focuses primarily on the NAP operator responses unless otherwise noted.

2.1.1 NAP maturity landscape and common challenges

The responses confirm that the NAPs which were analysed in T4.3 span a wide range of maturity levels. At one end, some NAPs already offer validation services, monitoring dashboards, automated reporting, and broad adoption of European data standards. At the other end, one NAP was only launched in early 2025 and is still in a foundational stage, with limited back-office capabilities, no active service providers consuming its data, and significant upgrade needs across the board. Between these extremes, several NAPs have established metadata management and API-based exchange but face persistent constraints in automation, back-office tooling, and available resources.

Despite these differences, most of the responding NAPs function primarily as a repository of links and metadata, although some also serve as data platforms or data brokers in certain domains. Three of the NAP operators reported a fragmented landscape with separate platforms for different data categories or partial solutions. Validation or quality-checking capabilities are present in nearly half of the responding NAPs, and roughly a third possess monitoring, reporting, and dashboard functionalities. Only one NAP has fully automated or semi-automated reporting in place.

The most widely reported challenge is gaps in data availability, flagged by most respondents. Resource and budget constraints are also widespread, reported by the majority of the NAP operators. Other common current constraints are limited automation, largely manual reporting processes, and limited integration with other national systems. A significant minority described having limited interoperability with European initiatives. The following difficulties were also signalled:

- Limited back-office capabilities;

- Operational complexity arising from coordination across multiple systems and data providers;
- Difficulty of engaging stakeholders and ensuring data quality at the source;
- Fragmented operational responsibilities, with NAP related tasks distributed across multiple departments or organisations;
- Difficulty estimating maturity, coverage, or readiness;
- Lack of visibility and accessibility for data owners and providers, which can be improved by modernising the NAP infrastructure;
- Institutional and legal barriers, including incomplete transposition of the ITS Directive and unclear official appointments of NAP operators for all data domains.

2.1.2 Data standards and exchange practices

Regarding the use of standards and data exchange practices, DATEX II and API-based data exchange form a universal baseline across all responding NAPs. Both NeTEx/SIRI (or other public transport standards) and GTFS/GTFS-RT are represented in most of the analysed NAPs. TN-ITS is also present in nearly half of the responding NAPs, as is simple file-based exchange.

As for metadata, the mobilityDCAT-AP is currently in use by over half of the respondents, while others have explicitly identified its adoption as a short-term priority within TISGRADE.

Beyond this common foundation, data exchange practices vary. Some NAPs operate predominantly via metadata APIs, with data providers responsible for maintaining quality at the source. Others rely on a combination of API-based and file-based exchange, with validation and update frequency depending on the data type and the capabilities of individual providers. One NAP also offers MQTT-based data streaming, and another uses harvesting from external, decentralised platforms – including regional mobility data platforms and domain-specific public transport portals – to consolidate metadata visibility. One NAP currently has no public API at all, relying on web-only access with manual metadata updates; its comprehensive redesign is planned.

Manual uploads and manual publication processes remain prevalent, with nearly all responding NAPs still using them alongside more automated channels. A few NAPs have scheduled file or data imports.

One respondent noted that the development of a national DATEX II profile is ongoing, with publication expected in 2027.

2.1.3 Architecture and technical infrastructure

Architecture-wise, the responding NAPs are distributed across all major models, with no single dominant pattern: roughly a third follow a centralised platform model, roughly a quarter report a distributed architecture, and another quarter describe a hybrid approach; one NAP follows a federated model. This diversity reflects the fact that each NAP has evolved according to national needs, existing institutional structures, and available resources rather than from a common architectural blueprint.

Hosting is split almost evenly between cloud-based and on-premise deployments, with one respondent reporting a hybrid model. Cloud-based hosting is not correlated with higher maturity, as both cloud and on-premise NAPs span the full range of capability levels represented in the sample.

Regarding data provider connectivity, most NAPs support manual or direct upload as at least one mechanism, and about half offer API-based integration for data providers. Automated ingestion pipelines, allowing data to flow into the NAP without manual action, are rare, reported by only two respondents. This suggests that, for most NAPs, the process of connecting a new data provider still requires significant manual effort.

Where respondents provided detail on API implementations, REST is the dominant protocol, often alongside SOAP for legacy integrations or specific domains.

Authentication mechanisms for API or system access are largely minimal: half of the responding NAPs use no authentication at all, while the remainder employ API keys, Open Authorization (OAuth) or token-based mechanisms, or Hypertext Transfer Protocol (HTTP) basic authentication. This indicates an area for attention in the context of cybersecurity upgrades.

2.1.4 Data discovery and dataset availability

Most of the responding NAPs offer dataset search and filtering functionality, but one NAP reports only limited discovery capabilities and another has none at all. This indicates that data discoverability is generally addressed but not universally mature.

Dataset counts reported by the respondents vary considerably across data domains. For RTTI, the number of datasets ranges from 1 to approximately 150. MMTIS dataset counts range from 1 to 250, reflecting the diversity of multimodal data landscapes. The SRTI, SSTP, and AFIR domains generally have fewer datasets – often in the single digits – though some NAPs report significantly higher numbers.

2.1.5 Notifications

Notification mechanisms for informing users when datasets or APIs are updated are underdeveloped across the sample: half of the responding NAPs have no notification system at all and, among those that do provide notifications, manual approaches (such as direct communication from operators) are more common than automated mechanisms. Only two NAPs report fully automated notifications. Where notification channels exist, e-mail is the most common mechanism, followed by portal notifications; no respondent reported having RSS feeds or API-based notifications.

This gap in notification capabilities is relevant for the upgrade plan, as it directly affects how efficiently data consumers can react to changes in available data, particularly in the context of near real-time information services.

2.1.6 Pain points

Pain points flagged by the questionnaire respondents are presented below, divided by subject: standards, compliance, and cybersecurity.

The concerns related to standards and data are broadly distributed. The most commonly reported pain points, each flagged by over half of the responding NAPs, are low or inconsistent coverage of required data types, insufficient quality in provider-side data, difficulty capturing and publishing urban data, and challenges related to versioning and migration when standards evolve. Close behind, about half of the respondents signalled inconsistent metadata quality and lack of adequate tooling to validate standards compliance.

Still regarding the use of data standards, uneven implementation of required data standards across providers and domains was also reported by a significant minority. Some NAPs report difficulties mapping national data formats to EU-level formats. One of the responses highlights that, for some data categories requested by the EC, no international profiles are available; the same response also signals a practical barrier to compliance in the fact that the data standards mentioned by the EC are not publicly available and their specifications must be purchased.

Compliance concerns are less uniformly distributed, but still significant. The majority of the respondents described reporting obligations as burdensome or unclear, making it the most widely shared compliance concern, and over half identified a general difficulty in demonstrating compliance. Some NAP operators identified difficulty in demonstrating compliance or different interpretations of the legal and regulatory scope, and others yet pointed to insufficient traceability or audit evidence. A few respondents raised issues with fragmented roles and responsibilities, national legal

constraints affecting implementation choices, and weak alignment between legal and technical requirements. One respondent highlighted the complexity and inflexibility of public procurement procedures as a barrier to responding quickly to emerging needs or technological changes. Another respondent flagged the incomplete transposition of the ITS Directive and the absence of a clear legal appointment for the NAP operator as a fundamental constraint. Overall, the responses suggest that, while the regulatory framework is broadly understood, the practical tools, processes, and evidence trails needed to demonstrate compliance remain underdeveloped.

The cybersecurity landscape is polarised: while a few respondents explicitly indicated that they have no major cybersecurity pain points at present, over half reported that the cybersecurity scope for the NAP is not yet clearly defined – the most commonly flagged issue in this category. Access control and identity management was identified as needing improvement by a nearly half of the NAPs. Some NAP operators reported limited operational logging and monitoring. Other pain points that were signalled in some of the NAPs are:

- Third-party or supplier dependencies being a risk factor;
- Concerns about secure data exchange;
- Concerns about backup, recovery and resilience measures;
- Unclear security governance and responsibilities.

The responses suggest that, for some partners, cybersecurity is either adequately addressed for the moment or is simply not yet a priority compared to more pressing operational and standards-related issues. While cybersecurity is a recognised concern, for a lot of NAPs the more immediate priorities lie in operational maturity, standards alignment and validation capabilities. One respondent emphasised that clear requirements for NAP cybersecurity should be prioritised, noting that it is currently unclear what specific activities should be implemented, and another respondent explicitly referenced NIS 2 compliance as a key concern.

2.1.7 Planned improvements and funding

Most of the NAPs stated plans to improve interoperability with national or European systems; the majority also intend to strengthen back-office capabilities and operational tooling – including improvements to the management of users and data, and enhancements to monitoring and reporting mechanisms – and upgrade standards, formats and exchange mechanisms. A large majority plan to introduce or improve validation and quality support, align with the NLKF and common guidance developed through NAPCORE, and strengthen cybersecurity, resilience and secure

digital operations. Over half plan to align with the NRA. Other upgrade initiatives include:

- Full NAP platform redesigns to improve usability and align with NB tasks;
- Consolidation of multiple existing NAPs into a single platform following the NRA;
- Upgrades related to the mobilityDCAT-AP and metadata harvesting and exposure;
- Comprehensive NAP redesigns;
- Replacement of legacy platform components with modern technology stacks;
- Extending metadata registers with use-case-based access and multilingual functionality;
- Dataset discovery assisted by artificial intelligence (AI);
- AI-powered compliance reporting;
- UI modernisation.

In line with the analysis of the reported pain points, respondents generally described phased approaches, addressing data quality in the short term, followed by cybersecurity improvements, focused on resilience and secure digital operations.

Some respondents reported that their planned improvements are fully funded and approved, but the initiatives of two-thirds of the NAPs are still only partly funded or under preparation. More than one NAP operator cautioned that the implementation may take longer than expected due to budget and resource limitations. This manifestly affects the upgrade timelines in the plan.

2.1.8 Expectations towards T4.3 and D4.4

Respondents would like T4.3 to provide valuable input in different areas:

- Practical architectural guidance:
  - Adoption of the NRA;
  - Definition of roles and interactions with national domain systems;
  - Data onboarding, validation, monitoring, and reporting workflows;
  - Federated NAP set-ups with centralised metadata management but keeping data distributed at the source;
  - Multi-level data governance (e.g., national, provincial, and municipal);
  - Data lifecycle management;
- Standards evolution and adoption:
  - Knowledge and experience sharing on upgrading the versions of data standards;

    - Knowledge and experience sharing for the mobilityDCAT-AP: versioning, currently used metadata interfaces, and extensions;
    - Implementation guidelines and recommended data standard profiles for shared data;
- Visibility and stakeholder integration:
    - Support on making NAPs more visible and accessible, both nationally and at the European level;
    - Alignment of the data digitalisation efforts with NAP evolution;
    - Support on making local-level data digitalisation compliant with and publishable to the NAPs;
    - An overview of available data collection tools and methods for urban data providers;
- Compliance and reporting support:
    - Common approaches to compliance reporting and demonstration;
    - Practical guidelines for compliance mapping per DR;
    - Clarity on how evolving standards and regulatory requirements should be reflected in NAP operations;
    - Best practices for NAP operation;
- Guidance on cybersecurity and operational resilience, including clarity on what specific activities NAPs should implement;
- Alignment with NAPCORE specifications and outcomes;
- Peer learning and experience sharing in general.

Regarding D4.4 content, the following proposals were put forward:

- Analysis and justification of the application (or lack thereof) of NAPCORE outcomes;
- Definition of a reference approach for mobilityDCAT-AP implementation including national profiles;
- Definition of recommended measures for:
    - Access control;
    - Monitoring;
    - Secure data exchange;
    - Reliable and interoperable NAP operations overall.

2.2 NAPCORE

2.2.1 NAP LoS KPI Framework

The NLKF, broadly described in section 1.4.2, was created to allow for the assessment of the LoS and interoperability of NAPs across Europe, which in turn facilitates the evolution of NAPs in an aligned manner.

The framework organises NAP features into seven distinct categories to ensure a comprehensive evaluation of the platform: Access, Communication, Data Discovery, Maintenance and Update, Dataset Information, Interoperability, and Data Exchange and Operational Policy.

The Access category evaluates the public availability of the NAP over the web, its compliance with web design standards, and the implementation of security and authentication mechanisms for data exchange. Communication focuses on the available means to support users, monitoring related services, and establishing official promotional channels. Data Discovery assesses functionalities such as free-text search, filtering options, map-based discovery, and machine-readable metadata. Maintenance and Update examines the continuity of IT services and the procedures established for checking links and maintaining the accuracy of metadata and data content. Dataset Information revolves around the documentation and description of datasets, their classification according to standard vocabularies, and the availability of data and metadata visualisation. Interoperability ensures the adoption of common metadata specifications – such as the mobilityDCAT-AP – and the support for harvesting across different portals. Data Exchange and Operational Policy deals with the transparency of terms and conditions for reuse, the clarity of operational procedures, and indicators for compliance assessment.

To support this evaluation, the NLKF includes 47 individual KPIs across the seven categories, each defined by a specific question in a self-assessment questionnaire. All KPIs share a common description in tables that identify the KPI numbering, a definition by question, the possible KPI values that answer the question, and several KPI limits that define the minimum acceptable threshold for interoperability. These thresholds, including Required (REQ) and Acceptable (ACC) limits, ensure that all assessed features are measured against a common European baseline. Finally, the evaluation considers differences between NAP types: data platforms, which provide metadata alongside real data or data services, and metadata directories, which exclusively provide metadata for the identification and discovery of data resources. The 47 KPIs are presented in Table 1; more information on each KPI can be found in NAPCORE's milestone M2.1's deliverable – "NAP LoS KPI Framework".

The results of the assessment are processed into a quantitative Grade of Achievement (GA) for each feature category, ranging from 0 to 100. These grades are then interpreted qualitatively as Maturity Levels: Beginner, Basic, Intermediate, Advanced, or Expert. Additionally, a Total GA is calculated as a weighted mean of all category scores, providing a single high-level indicator of the entire NAP platform's overall maturity.

The features identified via the NLKF, translated into measurable KPIs, serve as a practical baseline for the NAP operators involved in the TISGRADE project.

Feature category	KPI index	KPI name
Access	1.1	Online availability
	1.2	Compatibility with web browsers
	1.3	Web performance – homepage load time
	1.4	Responsiveness
	1.5	Web performance – simplicity / usability
	1.7	Web performance – consistency and navigability
	1.8	Support of commonly used languages
	1.9	Security – technical
	1.10	Security – providers verification
	1.11	Personal data protection
	1.12	Procedure for input of metadata or data to the NAP
	1.13	Metadata access restrictions
	1.14	Authentication and security mechanisms for data upload
	1.15	Authentication and security mechanisms for data download
	1.16	Indication of provided data modification
	1.17	Data transfer optimization
	1.18	API usage for data transfer
	1.19	Web performance – (meta)data load time

Feature category	KPI index	KPI name
	1.21	Metadata about data modification
Communication	2.1	Support to users to register or add data/metadata
	2.2	Related services monitoring process
	2.4	NAP promotion channels
	2.6	Contact details
	2.7	Mass notifications – data providers
	2.8	Mass notifications – data consumers
	2.9	Monitoring and evaluation
Data discovery	3.1	Free-Text Search
	3.2	Filtering options
	3.3	Provision of machine-readable metadata
	3.4	Map-based search
Update and maintenance	4.1	IT services
	4.2	Link checking frequency
	4.4	Metadata maintenance frequency
	4.5	Data (content) maintenance
Dataset information	5.1	Documentation & description of datasets
	5.2	Classification of datasets
	5.3	Quality indicators for datasets
	5.4	Data visualization
	5.5	Metadata visualization
Interoperability	6.1	Metadata specification
	6.2	Harvesting functionalities
Data exchange and operational policy	7.1	Terms and conditions for reuse of metadata and NAP website content
	7.2	Terms and conditions for data reuse from data providers

Feature category	KPI index	KPI name
	7.3	Operational procedure information
	7.4	Dataset indicators
	7.5	Compliance assessment
	7.6	Association of published datasets with Delegated Regulations

Table 1: NLKF KPIs

2.2.1.1 Latest results

Section 4.2 of the latest NLKF document describes the current state of practice of NAP LoS across European countries, based on the already processed EU-aggregated results. Since 2023, NAPCORE has been organising yearly NAP LoS self-assessment workshops, where NAP operators are requested to complete the NLKF questionnaire and then gather in a physical or hybrid setting to discuss results and plan further developments and enhancements. Highlights from the latest workshop – in March of 2025, at the time of writing – are presented below.

Regarding the types of NAPs currently operational in Europe, the 2025 assessment included 24 NAPs from 23 different Member States. Roughly two-thirds of these NAPs function as data platforms, providing both metadata and real data services, while the remaining third is comprised of metadata directories.

The results produced by this framework serve two distinct goals: European benchmarking through EU-aggregated results, which are explicitly integrated into NAPCORE's public reports, and individual results for each Member State, which are sent directly to NAP operators and are not made public. This section will only explore the public results in a more summarised manner – specifically the EU-aggregated outputs. Further information can be found in NAPCORE's report.

The distribution of achievement grades across the different feature categories is visualised through box plots, which illustrate the variance and average performance levels EU-wide. These plots show the maturity range from Beginner to Expert for each category, with background colours indicating the maturity level.

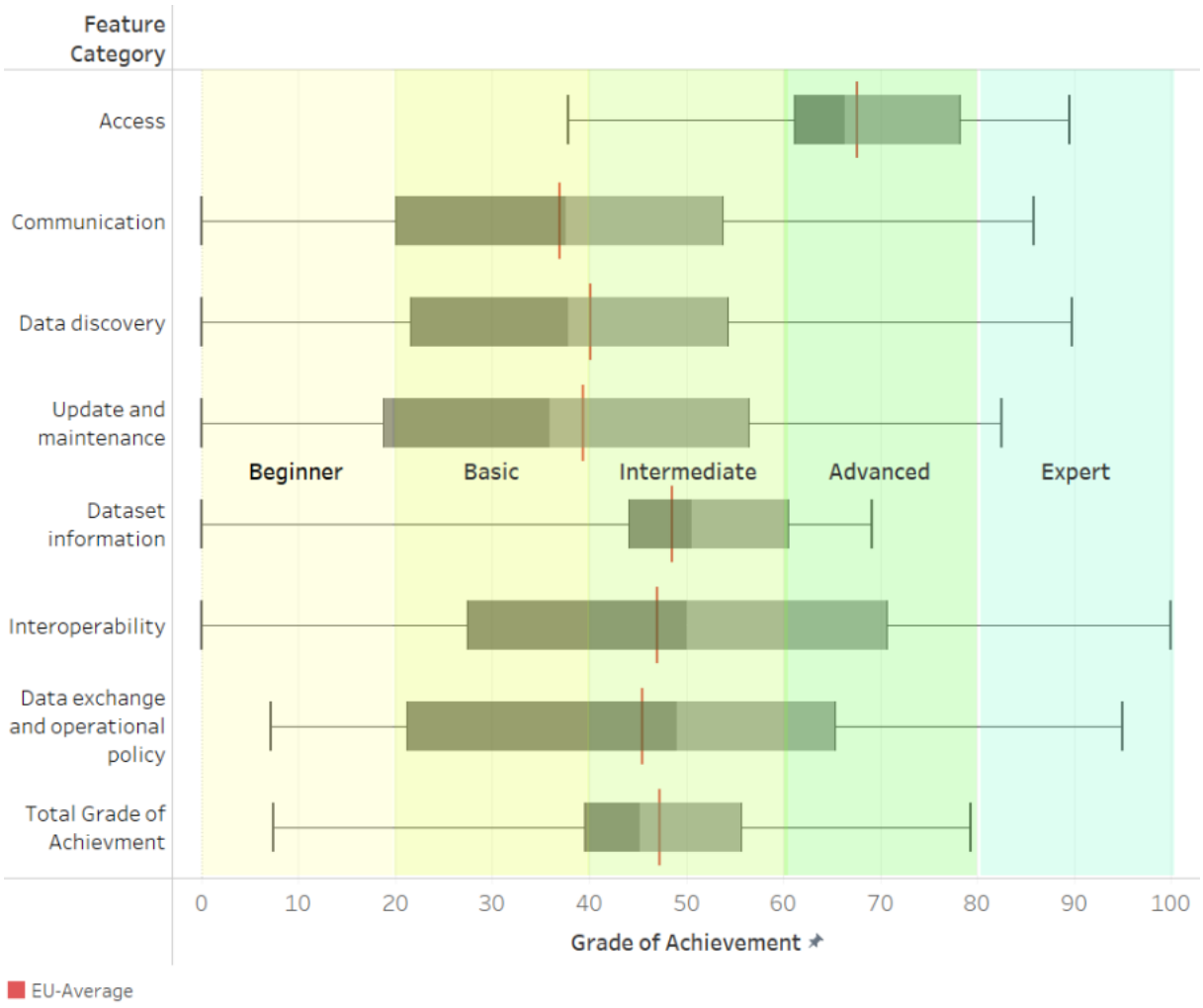

Figure 1: Distribution of NAP GAs per feature category

The highlights from this analysis show that most feature categories currently show an Intermediate maturity level. The Access category consistently achieves the highest grades with the least variance among Member States, whereas several other categories still show minimum values of zero, emphasising a continued need for harmonisation efforts. On average, the Total GA across the EU aligns with the Intermediate level.

To better understand the depth of implementation, the assessment also tracks the number of NAPs reaching each maturity level within each category. This provides a clearer view of how many Member States have reached Advanced or Expert status, versus those still at the Beginner stage.

Figure 2: Number of NAPs in each level of maturity per category

The data reveals that, while a majority of NAPs have reached Advanced or Expert levels in Access, there is significant variation across categories such as Communication, Data Discovery, Update and Maintenance, and Interoperability, with many NAPs still at Beginner or Basic maturity levels. Notably, the Dataset Information category has seen an increase in the number of features, leading to most NAPs remaining at the Intermediate level. Overall, the majority of NAPs fall into the Intermediate levels for their Total GA, as already observed in the previous visual.

A comparison between the 2024 and 2025 results highlights the evolution of the European NAP landscape over the past year. This year-over-year analysis tracks the average GA to see where the ecosystem is progressing and where new challenges are being faced.

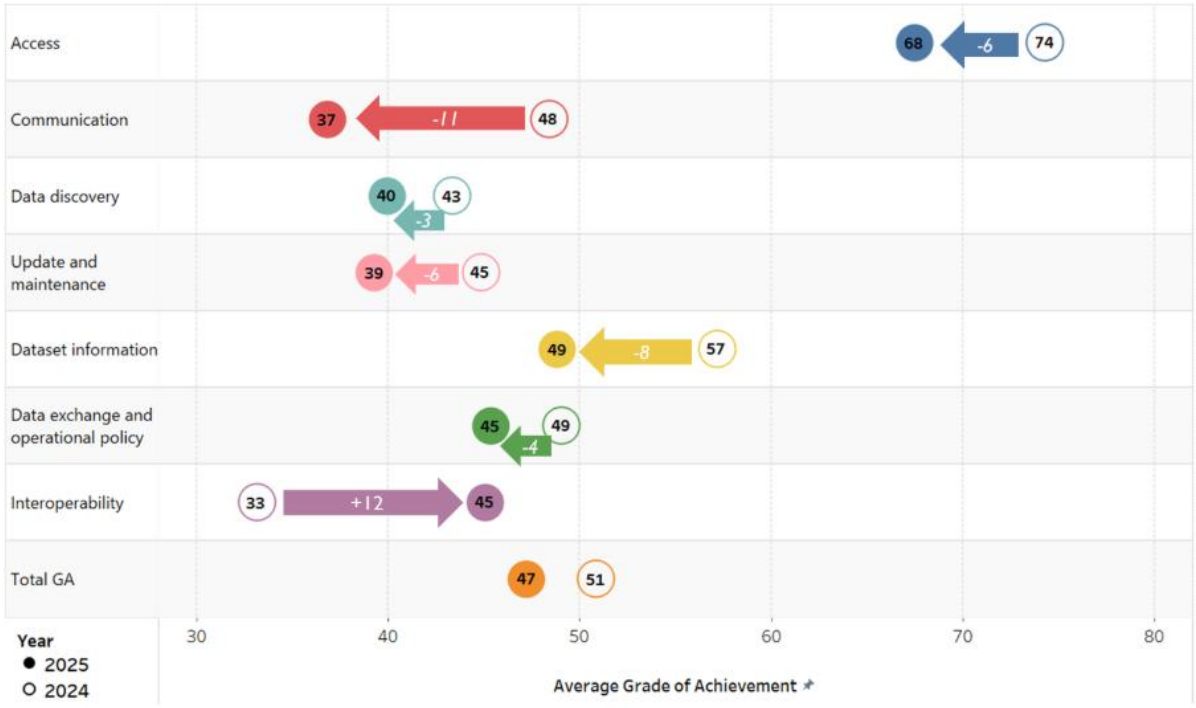

Figure 3: Comparison between 2024 and 2025 NAP GA results

The 2025 analysis shows lower average grades in most categories compared to 2024. This does not indicate a downgrade in NAP quality; instead, it reflects the increased rigour of the 2025 framework, which introduced new KPIs and higher minimum requirements. A significant positive outlier is the Interoperability category, which saw a notable improvement (+12 points) as Member States made progress in adopting common standards.

It is worth noting that the framework is updated annually, which can make it harder to compare results across years. Nevertheless, the framework is becoming increasingly stable, which is why future assessments will be able to show more consistently whether the implementations, such as those planned for the TISGRADE project, are indeed improving the EU-wide LoS results.

The most significant gaps across the EU were identified by combining the frequency of insufficient KPI levels – i.e., the ones below the acceptable limit – with the relative importance, or weight, of those features. The top gaps, as suggested by the table below, include online availability (specifically automated checking), provision of machine-readable metadata, and quality indicators for datasets. The analysis shows that security mechanisms for data upload and download also remain a primary challenge for many data platforms. This result highlights that, while basic access is stable, the more technical and automated aspects of data sharing require further attention.

#	KPI index	KPI name	Weighted % of NAPs	% of NAPs
1	1.1	Online availability	44	50
2	3.3	Provision of machine-readable metadata	40	75
3	5.3	Quality indicators for datasets	37	92
4	4.4	Metadata maintenance frequency	37	75
5	6.1	Metadata specification	35	58
6	7.2	Terms and conditions for data reuse from data providers	35	83
7	1.14	Authentication and security mechanisms for data upload	30	44
8	1.15	Authentication and security mechanisms for data download	30	56
9	2.6	Contact details	28	54
10	2.9	Monitoring and evaluation	27	83

Table 2: NLKF KPIs with the most significant gaps

Understanding this current status is relevant to developing the TISGRADE Digital Transport Infrastructure Upgrade Plan. The upgrades planned under the TISGRADE project are designed to directly bridge these identified gaps, improving the LoS of NAPs across the EU. By focusing on these specific weaknesses, the project aims to improve overall data availability and ensure greater interoperability across the European digital transport network.

2.2.2 NAP Reference Architecture

The NRA defines the minimum required functionalities, processes, and interfaces needed to enable a harmonised exchange of metadata and data across Europe. It provides a common architectural foundation for NAPs and establishes the basis for the EMDS. The architecture follows the FRAME methodology and consists of several complementary views:

- The motivational layer, explaining why the system exists;

- The functional view, describing bounded system functions and their information exchanges;
- The physical view, outlining how these functions can be implemented in subsystems and identifying critical interfaces;
- The communications view, describing interactions and data exchange between components;
- The organisational view, defining roles, responsibilities, and relationships between actors.

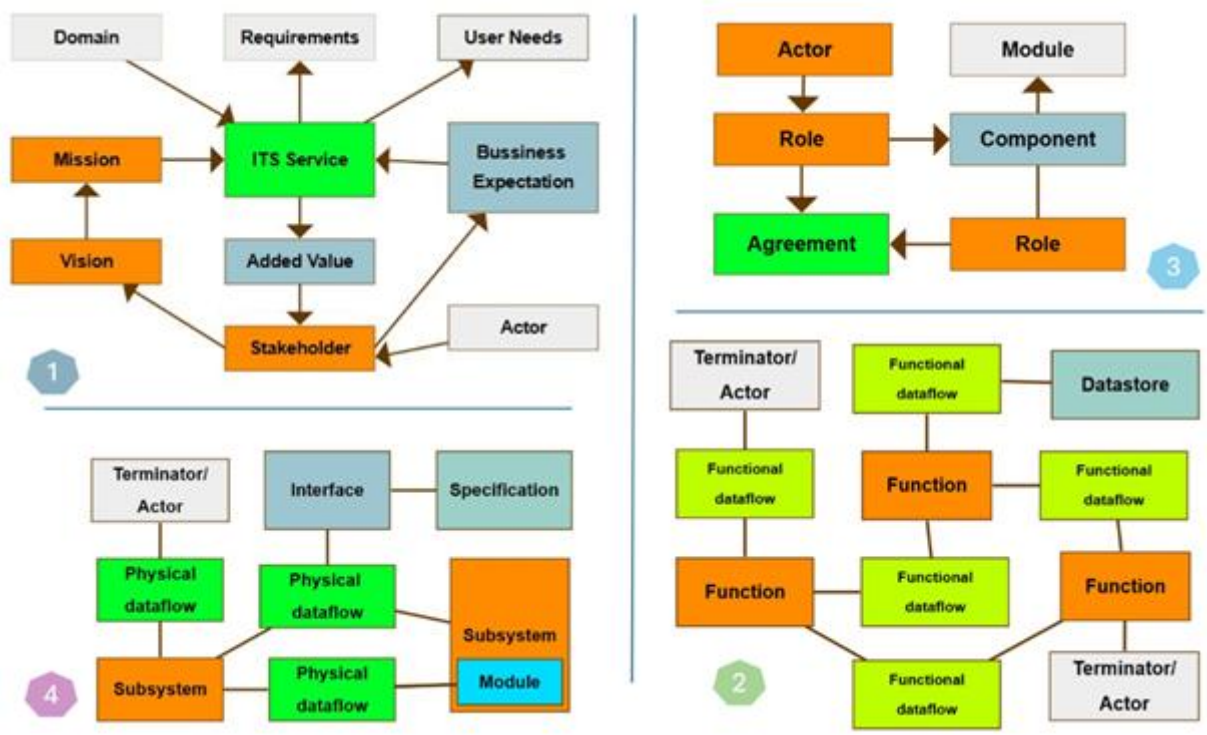

Figure 4: Components of FRAME views, Motivational (1), Functional (2), Organisational (3), Physical (4), and Communications (4) views [NAPCORE, 2025]

The DTI represents the target state of Europe's mobility data ecosystem: a coherent, interoperable, secure, and standards-aligned digital environment enabling the publication, discovery, exchange, and reuse of transport data across borders.

The NRA provides the formal architectural expression of this target state for NAPs. It translates the abstract principles of a DTI into concrete, implementable architectural elements – functions, interfaces, subsystems, and organisational responsibilities that can be upgraded, monitored, and maintained.

A DTI is defined by several core principles, each of which is operationalised in the NRA:

- Interoperability – standardised interfaces, protocol choices, and specification catalogues (e.g., DATEX II, NeTEx, SIRI, and the mobilityDCAT-AP);
- Discoverability – metadata management functions and catalogue subsystems (metadata ingestion, validation, and indexing);
- Reliability and resilience – modular physical subsystems and decoupled data flows supporting robust and scalable back-office architectures;
- Regulatory compliance – requirements and agreements linked to DRs, expressed through roles, responsibilities, and compliance artefacts;
- Secure data exchange – trust boundaries, authentication flows, secure endpoints, access control, and operational monitoring.

Through these mappings, the NRA becomes the reference model that expresses what a DTI requires in a form that NAP operators can implement. A fully realised DTI, as described by the NRA, would exhibit several architectural characteristics:

- Harmonised and predictable data exchange, with all NAPs exposing data and metadata through consistent and standards-aligned interfaces enabling seamless cross-border harvesting and integration;
- High-quality, validated, and monitored metadata, harmonised according to the mobilityDCAT-AP, automatically validated, and continuously monitored for freshness and correctness;
- Robust, modular, and scalable back-office systems, with clear separation of ingestion, validation, storage, publication, monitoring, and reporting;
- Automated compliance with DRs, including enforcement of required metadata fields, update frequencies, data quality indicators, and reporting obligations;
- Secure and trustworthy data exchange, with authenticated access, secure APIs, audit trails, operational monitoring, and incident response processes embedded at architectural level;
- Consistent governance and operational roles, clearly defined and traceable across the data chain.

Within Task T4.3, the NRA provides the reference model that translates the DTI goals into concrete upgrade actions. It supports implementation in several ways:

- Identifying required back-office capabilities, with the functional and physical views defining which subsystems must exist, how they interact, and what minimum capabilities they must provide – directly informing upgrades to ingestion pipelines, metadata processing, monitoring, and reporting;
- Aligning data standards and exchange mechanisms, with the NRA's catalogue of 38 specifications linked to specific interfaces and functions, enabling

partners to identify outdated implementations, plan migrations to newer versions, and ensure DR-aligned data exchange;
- Embedding cybersecurity into architectural design, with trust boundaries, authentication points, secure communication channels, and operational responsibilities clearly identified in the communications and organisational views;
- Supporting harmonised but adaptable national upgrades, by defining a common European structure while allowing variation in deployment models, technology stacks, and internal workflows.

In this way, the NRA acts as the translation layer between the high-level concept of a DTI and the practical upgrade actions required under T4.3. It defines what a fully interoperable, resilient, secure, and standards-aligned DTI looks like and expresses this target state in implementable architectural terms. For T4.3, the NRA provides the blueprint that guides back-office improvements, standards alignment, DR compliance, and cybersecurity enhancements across Member States.

3 Upgrade plan

The upgrades planned for each NAP are explored below, as is the envisioned upgrade calendar. The individual upgrades are described per NAP in section 3.1. Section 3.2 maps these upgrades – grouped by NLKF KPI – to the year and quarter in which implementation is expected to be finalised.

3.1 Plans for the future

The individual upgrades planned for each NAP are described below. These plans are self-reported by each partner, except when stated otherwise. This allows for finer detail than included in the grant agreement, resulting in a more concrete vision of the planned upgrades.

The efforts to reach these goals will be documented in deliverable D4.5 – “Final Report and Recommendations on NAP Upgrades with Cybersecurity Improvements”, thus providing a basis for future improvements in other NAPs.

3.1.1 Austria

The Austrian NAP currently operates as a metadata directory with metadata validation checks and API-based metadata provision using mobilityDCAT-AP version

1.0. The usability and design have not been changed since the NAP's implementation in 2018. In TISGRADE, a broader redesign of the platform is aimed at improving usability and aligning it more closely with NB tasks, including the planned introduction of eID (European Digital Identity) / EUID (European Unique Identifier) and the migration to mobilityDCAT-AP version 3.0. The main issues highlighted were the fact that reporting is still manual, limited interoperability and integration, stakeholder engagement, incomplete or weak dataset descriptions, and the lack of publicly available international profiles for some EC-requested data categories.

In summary, the following upgrades are planned for the Austrian NAP:

- Redesign of the platform;
- Enhance usability and procedures;
- Integration of surveillance mechanisms for UVARs and other data provision;
- Integration of NB needs as self-declaration and reporting;
- Alignment with the EMDS and Austrian Mobility Data Space;
- Automated ITS Directive reporting;
- Implementation of TISGRADE results from WP2, WP3, and WP4;
- Any other new NAP requirements from TISGRADE, NAPCORE-X, or the ITS Directive and ITS revised DRs.

3.1.2 Croatia

The Croatian NAP is a centralised national platform for the exchange of traffic and mobility data, combining the functions of a metadata catalogue, a data distribution platform, and an operational hub for real-time data exchange. The platform started operating at the end of 2020, in line with the technical and organisational capabilities available at the time. Unlike NAPs that operate only as metadata directories, the Croatian NAP also provides direct access to datasets through registered services and APIs. It integrates data from multiple providers, including Croatian Roads, Croatian Motorways, the Croatian Automobile Club, motorway concessionaires, and public transport operators, and distributes static and dynamic data through standardised formats such as DATEX II, GTFS, and NeTEx. Considering the results of the latest NLKF assessment from 2025, future improvements will focus on usability, metadata management, data quality, interoperability, monitoring, automated reporting, user support, and the integration of multimodal and AFIR-related data.

In short, the following upgrades are planned for the Croatian NAP:

- Improve the usability, accessibility and navigation of the Croatian NAP through a better UI and updated metadata workflows;

- Use AI to automate ITS Directive reporting and improve data quality, compliance and interoperability;
- Develop support services for users, end users, and data providers, based on AI;
- Develop a national stop point registry for the Croatian NAP to support harmonised public transport data exchange in line with MMTIS requirements;
- Develop a national system for collecting, validating and publishing alternative fuels infrastructure data for the Croatian NAP in line with the AFIR and ITS requirements.

3.1.3 Cyprus

The information on the Cypriot NAP and its upgrade plan, below, was not directly self-reported and was instead compiled based on the grant agreement, the response to the questionnaire explored in section 2.1, and a spreadsheet with the self-reported upgrade plan which is transposed in Table 3.

The Cypriot NAP was launched in January of 2025 by the Department of Public Works in collaboration with KIOS Research and Innovation Centre of Excellence (KIOS CoE). It is currently a metadata repository integrated with the national geographic information system (GIS) platform and a smart mobility management solution for road works and live events. The NAP currently uses a distributed architecture hosted in the cloud, with API-based provider connections and API key authentication.

The NAP's level of maturity is still low: back-office operations are largely manual, no service providers are yet retrieving data from it, and several foundational upgrades are needed. The top identified pain points are related to data standards: uneven implementation, difficulty mapping national data to EU formats, and lack of tooling for standards compliance validation. Data discovery is also limited and no notification system is currently in place.

The following upgrades have been identified:

- Alignment of metadata elements and vocabulary from national non-conformant or proprietary system with the mobilityDCAT-AP and conversion of metadata entries to better suit national needs;
- Ensuring the correct categorisation and handling of mandatory, recommended, and optional metadata elements;
- Facilitation of compliant metadata entry through the implementation of a mobilityDCAT-AP Resource Description Framework (RDF) model, with features for the import/export of machine-readable metadata and compliance validation – likely by using Shapes Constraint Language (SHACL);

- Introduction of validation and quality-checking capabilities;
- Introduction of monitoring, reporting, and dashboard functionalities to support operational oversight;
- Strengthening of cybersecurity, including addressing current gaps in access control, identity management, operational logging, and backup and recovery measures;
- Alignment with the NLKF and NAPCORE guidance, improving interoperability with EU-level NAP infrastructure.

3.1.4 Czechia

The Czech Republic currently operates a metadata directory type NAP. A comprehensive feasibility study for the NAP 2.0 has been completed, and the team is now preparing the technical specifications and tender documentation required for the next implementation phase. The planned upgrades can be expressed through the NLKF feature categories as follows:

- Access:
  - Strengthening user and data provider management, including improved verification via the state registry;
  - Enhancing secure upload and download mechanisms and overall cybersecurity of the back-office infrastructure;
  - Improving platform resilience and reliability;
- Communication:
  - Establishing a user forum to support two-way communication and feedback;
  - Introducing dissemination and promotion activities for new datasets and projects;
  - Improving support processes for users entering or updating information;
- Data discovery:
  - Implementing visualisation of metadata validation results to help users understand dataset status and quality;
  - Enhancing catalogue entries with user and validation feedback to improve dataset discoverability;
- Update and maintenance:
  - Introducing on-the-fly and scheduled validation of user-entered information;

    - Strengthening monitoring processes, including link checking, metadata freshness, and system performance;
- Dataset information:
    - Improving metadata quality through validation feedback loops and clearer presentation of dataset status;
    - Enhancing dataset descriptions and metadata completeness through automated checks;
- Interoperability:
    - Improving organisational and technical integration with the Czech national open data portal;
    - Ensuring consistent metadata structures and validation aligned with EU specifications;
- Data exchange and operational policy:
    - Implementing tracking of data usage to support operational monitoring and reporting;
    - Enhancing the clarity of operational procedures and interactions with external systems (e.g., the state registry and open data portal).

3.1.5 Denmark

The description of the Danish NAP upgrade plan, below, was not self-reported within T4.3 and was instead extracted from the grant agreement.

The following upgrades have been identified:

- Update of the mobilityDCAT-AP metadata profile with newer versions;
- UX testing and implementation of improvements based on findings, to increase usability;
- Upgrade of the NAP with the Interchange functionality, via either a Basic Interface (BI) or an Improved Interface (II), as described in NAPCORE's milestone M2.6's deliverable – "Interoperable NAP demonstrator with real world use of the NAP information".

3.1.6 Finland

The information on the Finnish NAP and its upgrade plan, below, was not directly self-reported and was instead compiled based on the grant agreement, the response to the questionnaire explored in section 2.1, and a spreadsheet with the self-reported upgrade plan which is transposed in Table 3.

Finland currently operates two NAPs: one for MMTIS data and another for SRTI, RTTI, and AFIR-related data. The main planned upgrade is the Single NAP project, which aims to merge these two platforms into one unified architecture aligned with the NRA and the NLKF. This project is fully funded and already underway.

The following upgrades have been identified:

- Single-NAP IT architecture for RTTI, SRTI, MMTIS, and AFIR-related data based on NAPCORE's NLKF and NRA;
- Update of the mobilityDCAT-AP's usage and implementation of catalogue harvesting functionalities;
- Implementation of secure user management for data providers and consumers, including provider verification and authentication mechanisms for uploads and downloads;
- Enhancement of metadata and data input workflows and tools;
- Integration of data validation capabilities, including quality indicators for datasets;
- Provision of machine-readable metadata;
- Establishment of procedures to ensure the continuity of NAP IT services.

3.1.7 Germany

The upgrades to the German NAP will be focused on:

- Automated quality checks for metadata published on NAPs;
- AI chatbot to discover data sets on NAP metadata registry, and to acquire help about NAP usage.

3.1.8 Greece

No description or timing of the upgrades to the Greek NAP were self-reported within T4.3. The grant agreement mentions minor IT developments on the NAP according to the recommendations of NAPCORE.

3.1.9 Hungary

The Hungarian NAP provides access to many transport-related datasets. It is a mixed model: in the case of multimodal data the system functions as a repository of metadata, while, in most cases, NAP functions as a data platform.

In the TISGRADE project, based on the NAPCORE NLKF assessment results and recommendations, the following improvements are in preparation to improve the

interoperability and functionality of the system, ensure operational security, and address newly emerging challenges:

- Renew queries and reports functionality for business monitoring of NAP operations;
- Ensure interoperability and automatic collection of metadata.

3.1.10 Latvia

The NAP is based on a microservices architecture built on open-source technologies and requires further development to address evolving functional, performance, and interoperability requirements. It currently supports core functionality for data providers, including dataset registration, metadata management using mobilityDCAT-AP version 1.0.0, and data upload via API. Submitted datasets are validated against defined XML schemas prior to publication, ensuring a baseline level of data quality and consistency.

Improvements to individual data management microservices are already ongoing within this architecture, forming a basis for continued platform evolution, including potential future extension within the TISGRADE framework.

Within the scope of NAP development, improvements are planned to enhance platform performance, interoperability, and compliance with the minimum LoS defined by NAPCORE. These include the following:

- Enhancements to security monitoring, cybersecurity, and overall safety and risk management capabilities;
- Improvements to platform performance and scalability, including optimisation of data distribution and processing mechanisms;
- Development and evolution of data standards and interoperability specifications, including implementation of a newer mobilityDCAT-AP version;
- Strengthening of data exchange and integration capabilities between the NAP and external platforms, including open data ecosystems;
- Improvements to core back-end systems, data management components, and underlying platform architecture;
- Continuous quality assurance activities, including testing, audits, and usability evaluations to support reliable and user-oriented development;
- Additional improvements aimed at increasing automation, efficiency, and usability for platform operators and users;

- Additional enhancements contributing to the continuous improvement, automation, and usability of NAP operations and UX, as measured against defined KPIs and operational performance indicators.

The need for clearer and more concrete definition of cybersecurity requirements for NAPs is also identified, as this area is currently not sufficiently specified in this deliverable and will be explored in T4.3 in the upcoming months.

3.1.11 Lithuania

The information on the Lithuanian NAP and its upgrade plan, below, was not directly self-reported and was instead compiled based on the grant agreement and the response to the questionnaire explored in section 2.1.

The Lithuanian NAP is a GIS-based platform that provides access to transport and mobility data through web maps and standardised interfaces such as DATEX II, Open Charge Point Interface (OCPI), and APIs. Lithuania uses a hybrid architecture with hybrid hosting, API-based provider connections, and API key authentication. Automated notifications are already in place, via e-mail. While static data and metadata are managed within the NAP, operational data is maintained in supporting systems and accessed through the platform, with some processes still partly manual.

The current challenges are mainly related to operational complexity, partial automation, and coordination across multiple systems and data providers, rather than interoperability or data standardisation.

The following upgrades have been identified:

- Strengthening of back-office processes, including the reduction of manual steps and the improvement of validation, monitoring, and reporting capabilities;
- Enhancement of data provider and dataset management, including clearer publication and maintenance workflows;
- Updates to data standards' support and interoperability;
- Alignment with the NRA;
- Other minor IT developments in line with NAPCORE recommendations.

3.1.12 Netherlands

The Dutch NAP, maintained by Nationaal Dataportaal Wegverkeer (NDW) / Nationaal Toegangspunt Mobiliteitsdata (NTM), operates as a metadata repository. Due to the

way the NAP is structured and governed, changes can be implemented swiftly in the technical environment, resulting in an advanced position with regard to the technical implementation of the NAP.

The primary objective for the Netherlands within WP4 is to ensure that other member states and their NAPs are able to align with and benefit from the experience of the frontrunner countries.

In addition, a number of upgrades will be carried out within the Dutch NAP, in line with broader European developments. These include the upgrade to mobilityDCAT-AP version 3.0.x, the implementation of an AI-powered chatbot to assist users in discovering and interpreting data sources, and the establishment of automated linkages with other national registers to enhance the findability and usability of data sources.

3.1.13 Slovenia

The information on the Slovenian NAP and its upgrade plan, below, was not directly self-reported and was instead compiled based on the grant agreement and the response to the questionnaire explored in section 2.1.

The Slovenian NAP was established in compliance with the ITS Directive and its DRs, and the AFIR. It includes static and dynamic information on road conditions, safety-related information, multimodal data, alternative fuels infrastructure, traffic flow, and transport infrastructure. Information is provided in real-time via standardised formats (DATEX II and NeTEx) through business-to-business (B2B), REST, and SOAP interfaces. The data is collected and processed by the National Traffic Management Centre (NTMC), which acts as the central data warehouse for Slovenia's transport network.

The following upgrades have been identified:

- Implementation of a TN-ITS data validation procedure to ensure good quality data for service providers;
- Introduction of validation capabilities, monitoring tools, and compliance assessment support;
- Improvement of the UI and alignment with Directive (EU) 2016/2102 – the Web Accessibility Directive;
- Implementation of metadata according to the mobilityDCAT-AP and alignment of the digital procedure for data compliance assessment with the catalogue;
- Improvement of the searchability of data;
- Alignment of the NAP architecture with NAPCORE recommendations;

- Strengthening of back-office capabilities, including improvements to user and data management.

3.1.14 Spain

The Spanish NAP, managed by Dirección General de Tráfico (DGT), acts as the central platform for the discovery and access to traffic and mobility datasets in line with the ITS Directive and its DRs. It already combines a metadata catalogue approach with back-office functions, validation mechanisms, and interfaces to external services, but still relies partly on semi-manual processes.

The current plan is to develop a new version of the NAP, funded from its own budget, incorporating the NAPCORE recommendations, the results obtained from TISGRADE, and the insights gained from the analysis and evaluation of best practices identified in the NAPs of other partners.

The planned improvements include:

- Implementation of tools for the collection and publication of static data in standard formats, while also incorporating feedback from users and service providers;
- Improving latencies and consumption patterns according to the typology of publication and adapting this for the NAP's own publications;
- Updating metadata and strengthening quality control of both own and third-party data;
- Incorporating recommendations and functional requirements defined by NAPCORE, TISGRADE, and other European working groups to ensure compliance with service levels;
- Development, implementation, and ongoing adaptation of the NAP and DATEX II;
- With regard to DATEX II, improvements need to be made to usability for service providers and end-user applications in order to facilitate the dissemination of traffic data.

The main pain points are as follows, relating to the role of DGT as NAP operator:

- Obtaining data from other road authorities with responsibility for traffic management, particularly urban data;
- Obtaining data from the relevant road authorities in accordance with the TN-ITS standard;
- Variability in the quality of third-party data, for which the providers themselves are responsible.

3.1.15 Sweden

The information on the Swedish NAP and its upgrade plan, below, was not directly self-reported and was instead compiled based on the grant agreement, the questionnaire explored in section 2.1, and a spreadsheet with the self-reported upgrade plan which is transposed in Table 3.

The Swedish NAP is a single platform that functions as a metadata repository, aligned with EU standards (DATEX II) and national open data standards. However, the current data environment and underlying architecture require modernisation, and the NAP should become more visible and accessible to data owners and providers.

The following upgrades have been identified:

- Upgrade of the mobilityDCAT-AP's usage;
- Replacement of the current platform, which is based on Comprehensive Knowledge Archive Network (CKAN), with a solution based on Angular and .NET, constituting a major architectural overhaul that is expected to affect multiple KPI areas;
- Strengthening of cybersecurity and secure digital operations;
- Other minor IT developments according to NAPCORE recommendations.

Budget and resource constraints may cause implementation to deviate from the Swedish NAP's upgrade plan, which is presented in Table 3.

3.2 Common Digital Transport Infrastructure Upgrade Plan

This section presents a consolidated view of the planned upgrades across the participating NAPs.

Not all partners were able to provide specific quarterly timelines at the time of writing. As a result, only those NAPs for which specific upgrade timelines could be identified are included in the consolidated upgrade plan. The absence of a NAP from this section does not imply that no upgrades are planned for said NAP; rather, the timeline for implementation has not yet been specified at the quarterly level, or the required information has not yet been provided.

Table 3 presents the planned quarter for the upgrades in each NAP, grouped by the KPIs defined by the NLKF. To conserve space, only the KPIs' indexes are provided in this table; Table 1 identifies all KPIs and provides their descriptions.

Figure 5 offers a different, aggregated view of the same data, showing how many NAPs plan to finalise the implementation of upgrades related to each KPI in each quarter.

KPI	Austria	Croatia	Cyprus	Czechia	Finland	Germany	Hungary	Latvia	Spain	Sweden
1.1										
1.2										
1.3										
1.4								2028 Q2		
1.5		2028 Q2					2028 Q2	2028 Q2	2028 Q2	
1.7		2028 Q2					2028 Q2			
1.8										
1.9	2028 Q2			2028 Q2	2026 Q1			2028 Q2	2028 Q2	
1.10				2028 Q2	2026 Q3					
1.11										
1.12	2028 Q2			2028 Q2	2026 Q4	2027 Q2		2028 Q2		
1.13										
1.14					2026 Q3					
1.15	2028 Q2				2027 Q1					
1.16										
1.17								2028 Q2		
1.18				2028 Q2				2028 Q2		

KPI	Austria	Croatia	Cyprus	Czechia	Finland	Germany	Hungary	Latvia	Spain	Sweden
1.19								2028 Q2		
1.21	2028 Q2									
2.1				2028 Q3		2027 Q2		2028 Q2		
2.2										
2.4				2028 Q3						
2.6										
2.7	2028 Q2						2028 Q2			
2.8	2028 Q2						2028 Q2			
2.9	2028 Q2	2028 Q2		2028 Q3			2028 Q2	2028 Q2		2028 Q2
3.1				2028 Q3						
3.2									2028 Q2	2027 Q1
3.3				2028 Q3	2026 Q4	2027 Q2	2028 Q2	2028 Q2	2028 Q2	2027 Q1
3.4	2028 Q2									
4.1	2028 Q2	2028 Q2		2028 Q3	2026 Q3		2028 Q2	2028 Q2	2028 Q2	2027 Q2
4.2										2027 Q1
4.4										2027 Q4
4.5										
5.1		2028 Q2							2028 Q2	2027 Q4
5.2									2028 Q2	2027 Q4
5.3					2026 Q4	2027 Q2				2027 Q4

KPI	Austria	Croatia	Cyprus	Czechia	Finland	Germany	Hungary	Latvia	Spain	Sweden
5.4				2028 Q3			2028 Q2	2028 Q1	2028 Q2	
5.5				2028 Q3						2027 Q4
6.1	2027 Q1		2028 Q1	2028 Q3	2026 Q3		2028 Q2	2028 Q1	2028 Q2	2027 Q2
6.2			2028 Q2	2028 Q3	2027 Q1		2028 Q2	2028 Q2	2028 Q2	2027 Q2
7.1	2027 Q1									
7.2										
7.3										
7.4				2028 Q3						
7.5	2027 Q1			2028 Q3						
7.6	2027 Q1									

Table 3: Planned quarters for upgrades to each NLKF KPI, per NAP

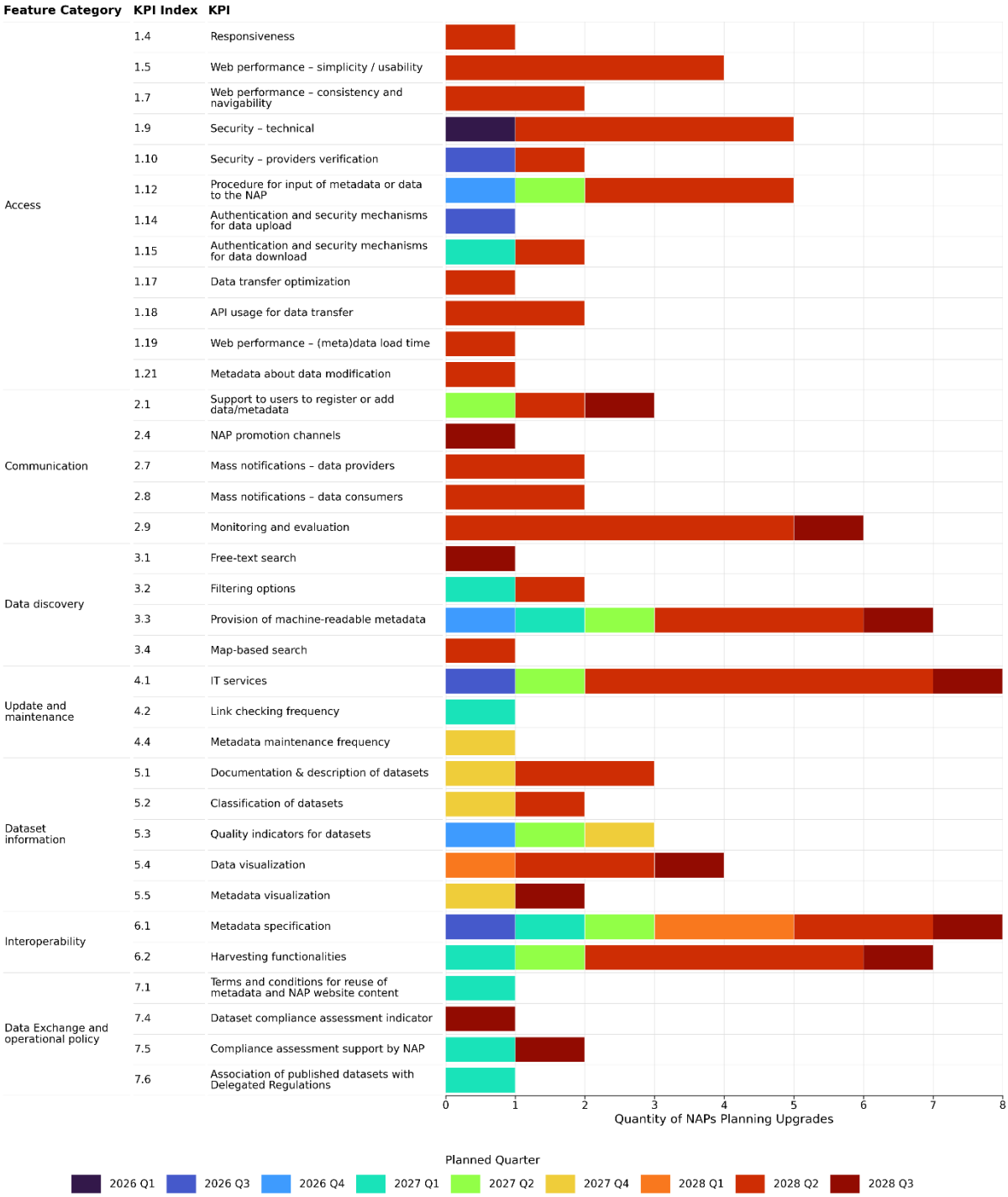

Figure 5: Quantity of NAPs with planned upgrades to each NLKF KPI, per quarter

The bulk of implementation activity is concentrated between the first quarter of 2027 and the second quarter of 2028, with the planned upgrades increasing over time. This reflects the fact that many NAPs are still in the planning, procurement, or early

implementation phases, with most upgrades expected to materialise in the second half of the TISGRADE project period.

The aggregated upgrade plan reveals a strong focus on improving interoperability, especially concerning the improvement of metadata provision, which often is a prerequisite for interoperable data discovery; machine-readable metadata in particular is of utmost importance to enable automated data discovery and exchange. Assuring the continuity of the NAPs' IT services is another prevalent concern, which is reflected by the corresponding KPI – 4.1 – being tied for the single most widely planned upgrade. Security-related upgrades are also commonly planned, reflecting the increasing importance given to user authentication and access management, and cybersecurity at large.

Upgrades related to operational policy and DR compliance assessment, by contrast, are planned by a small number of NAPs. This likely reflects both the regulatory complexity of these areas and the fact that many NAPs consider them secondary to the more immediate technical and interoperability improvements. Nonetheless, as described in section 2.1.6, compliance demonstration is a common pain point; as foundational upgrades are completed and as the topics of compliance mapping per DR, reporting, and demonstration are explored within T4.3, the Data Exchange and Operational Policy feature category may gain priority for NAP operators.

Finally, it is worth noting that a significant share of planned upgrades is concentrated in 2028. While this reflects the genuine scheduling at the time of writing, some timelines may shift as implementation progresses and potential deviations occur. The upgrade plan presented here is exactly that: a plan, which is subject to change due to unforeseen circumstances.

4 Conclusion

4.1 Expected outcomes

This deliverable establishes a structured, implementation-oriented upgrade plan for the DTI supporting the NAPs participating in TISGRADE task T4.3. It consolidates the technical needs, standards-related improvements, compliance considerations, and cybersecurity concerns identified through a dedicated questionnaire, maps them against the NAPCORE NLKF, and translates them into a common – yet nationally adaptable – upgrade calendar.

Over the remaining TISGRADE project period, the planned upgrades are expected to raise the participating NAPs' NLKF GAs across multiple feature categories. In practical terms, the implementations aim to make NAPs more robust, versatile, reliable, and secure. More concretely:

- Interoperability and data discovery will improve as NAPs adopt the mobilityDCAT-AP, implement machine-readable metadata, and introduce harvesting functionalities. These are preconditions for cross-border data discovery and the Interchange functionality envisaged by NAPCORE, and represent the most broadly planned upgrade area across the T4.3 partners;
- Operational maturity will increase through back-office modernisation, the introduction of IT service continuity procedures, and the strengthening of validation, monitoring, and reporting capabilities – addressing the widespread manual and fragmented processes documented in section 2.1;
- Security and trust will be strengthened across multiple dimensions: implementation or upgrade of user authentication and access management, provider verification mechanisms, secure upload and download procedures, platform resilience and reliability improvements, operational logging, security monitoring, and backup and recovery measures. Several NAPs are planning their first authentication mechanisms, while others are hardening existing back-office infrastructure and extending cybersecurity to cover the full data chain;
- Standards compliance will advance as NAPs upgrade data exchange formats (e.g., DATEX II version migrations), integrate new data domains (e.g., alternative fuels and UVARs), and improve compliance demonstration and reporting tools.

Beyond the individual NAP improvements, the harmonised approach promoted by T4.3 is designed to produce outcomes that extend beyond the participating partners. By implementing upgrades in a coordinated manner – informed by common reference documents (the NLKF and NRA), shared pain points, and peer exchange – practical implementation experience is generated, which can serve as a reference for future NAP upgrades elsewhere in Europe. This includes both the technical solutions deployed and the organisational approaches to planning, prioritising, and sequencing upgrades across diverse national contexts.

In this sense, D4.4 fulfils its role as described in the introduction: it provides the bridge between the broad objectives of T4.3 and the later, more comprehensive recommendations to be presented in D4.5. It is intended not as a final assessment, but as a practical planning instrument that supports aligned action across Member

States and prepares the ground for the documentation of best practices, lessons learned, and future improvement needs.

4.2 Next steps

The upgrade plan presented in this deliverable represents the state of planning at an early stage of the TISGRADE project. As implementations progress, several activities will follow:

- Implementation and reporting (T4.3.1) – The NAPs will deploy the upgrades described in section 3.1, document their progress, and report on deviations from the planned timelines. This implementation work constitutes the core of T4.3 for the remaining project period;
- Coordination and harmonisation (T4.3.2 and T4.1) – Ongoing coordination will ensure that implementations across partners remain aligned, that common challenges are addressed collectively, and that the upgrade experiences feed into the broader WP4 harmonisation effort;
- Exploration of compliance and cybersecurity topics – Compliance demonstration and cybersecurity remain areas where practical guidance is still being developed within T4.3. These topics will be explored in greater depth in the coming months, potentially leading to updated or expanded upgrade priorities;
- Integration with other WPs – The upgrade implementations will take into account evolving outputs from WP2, WP3, and WP5, as these become available and mature. Conversely, T4.3's implementation experiences may inform the feedback loop design and the validation approaches being developed in those work packages;
- Deliverable D4.5 – D4.5 will consolidate the outcomes of T4.3 at the end of the project period. It will document the upgrades that were actually implemented, assess their impact on NLKF GAs, capture best practices and lessons learned, and identify remaining or newly identified improvement needs;
- Feedback to NAPCORE – The implementation experiences and results generated through T4.3 – including challenges encountered, workarounds adopted, and suggestions for framework refinement – will be provided as input to NAPCORE, supporting the continuous improvement of the NLKF and NRA.

5 References

5.1 Figures and tables

Figures

Tables

5.2 References

1. C-Roads Platform. (n.d.). C-Roads – The Platform of Harmonised C-ITS Deployment in Europe. C-Roads. https://www.c-roads.eu
2. European Commission. (2013). Commission Delegated Regulation (EU) No 885/2013 of 15 May 2013 supplementing ITS Directive 2010/40/EU with regard to the provision of information services for safe and secure parking places for trucks and commercial vehicles. *Official Journal of the European Union*, L 247. https://eur-lex.europa.eu/eli/reg_del/2013/885/oj
3. European Commission. (2013). Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users. *Official Journal of the European Union*, L 247. https://eur-lex.europa.eu/eli/reg_del/2013/886/oj
4. European Commission. (2017). Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU with regard to the provision of EU-wide multimodal travel information services. *Official Journal of the European Union*, L 272. https://eur-lex.europa.eu/eli/reg_del/2017/1926/oj
5. European Commission. (2022). Commission Delegated Regulation (EU) 2022/670 of 2 February 2022 supplementing Directive 2010/40/EU with regard to the provision of EU-wide real-time traffic information services. *Official Journal of the European Union*, L 122. https://eur-lex.europa.eu/eli/reg_del/2022/670/oj
6. European Commission. (2023). Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use. *Official Journal of the European Union*, L 19. https://eur-lex.europa.eu/eli/reg_impl/2023/138/oj
7. European Commission. (2024). Commission Delegated Regulation (EU) 2024/490 of 29 November 2023 amending Delegated Regulation (EU) 2017/1926 as regards the provision of EU-wide multimodal travel information services. *Official Journal of the European Union*, L 2024/490. https://eur-lex.europa.eu/eli/reg_del/2024/490/oj
8. European Commission. (2025). Commission Delegated Regulation (EU) 2025/656 of 11 December 2024 supplementing Regulation (EU) 2023/1804 as regards technical specifications for data types concerning the alternative fuels infrastructure. *Official Journal of the European Union*, L 2025/656. https://eur-lex.europa.eu/eli/reg_del/2025/656/oj
9. European Commission. (2025). Commission Delegated Regulation (EU) 2025/671 of 11 December 2024 supplementing Regulation (EU) 2023/1804 as regards common technical specifications. *Official Journal of the European Union*, L 2025/671. https://eur-lex.europa.eu/eli/reg_del/2025/671/oj
10. European Commission. (2025). Commission Implementing Regulation (EU) 2025/655 of 11 December 2024 specifying data formats and other technical details for the deployment of alternative fuels infrastructure. *Official Journal of the European Union*, L 2025/655. https://eur-lex.europa.eu/eli/reg_impl/2025/655/oj

11. European Parliament and Council of the European Union. (2010). Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. *Official Journal of the European Union*, L 207. https://eur-lex.europa.eu/eli/dir/2010/40/oj
12. European Parliament and Council of the European Union. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). *Official Journal of the European Union*, L 257. https://eur-lex.europa.eu/eli/reg/2014/910/oj
13. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119. https://eur-lex.europa.eu/eli/reg/2016/679/oj
14. European Parliament and Council of the European Union. (2016). Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. *Official Journal of the European Union*, L 327. https://eur-lex.europa.eu/eli/dir/2016/2102/oj
15. European Parliament and Council of the European Union. (2019). Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. *Official Journal of the European Union*, L 172. https://eur-lex.europa.eu/eli/dir/2019/1024/oj
16. European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, L 333. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
17. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). *Official Journal of the European Union*, L 152. https://eur-lex.europa.eu/eli/reg/2022/868/oj
18. European Parliament and Council of the European Union. (2023). Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. *Official Journal of the European Union*, L 2023/2661. https://eur-lex.europa.eu/eli/dir/2023/2661/oj
19. European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1804 of the European Parliament and of the Council of 13 September 2023 on the deployment of alternative fuels infrastructure (AFIR). *Official Journal of the European Union*, L 234. https://eur-lex.europa.eu/eli/reg/2023/1804/oj
20. NAPCORE. (2024). mobilityDCAT-AP – Version 1.0.1. NAPCORE. https://mobilitydcat-ap.github.io/mobilityDCAT-AP/releases/index.html
21. NAPCORE. (2025). NAP LoS KPI Framework (Milestone M2.1). NAPCORE. https://www.napcore.eu/documents/M2.1%20NAP%20LoS%20KPI%20Framework.pdf
22. NAPCORE. (2025). NAP Reference Architecture. NAPCORE. https://napcore.eu/reference-architecture
23. NAPCORE. (2025). Interoperable NAP demonstrator with real world use of the NAP information (Milestone M2.6). NAPCORE.
24. UVAR Box. (2022). UVAR Box – Urban Vehicle Access Regulations data tool. European Commission. https://uvarbox.eu

Co-funded by
the European Union

Authors

André Rehberg

João Montenegro

Lígia Conceição

Petr Bureš

Sara Linhas