



Terms and conditions for data reuse (incl. GDPR implications)

Status: final
Version: 1.0
Date: 07.01.2025

Legal disclaimer

The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. The European Commission is not responsible for any use that may be made of the information contained therein. All images are provided by the respective partners (unless otherwise noted) and are approved for reproduction in this publication.

Document information

Project acronym	NAPCORE
Full project title	National Access Point Coordination Organisation for Europe
Grant Agreement No.	MOVE/B4/SUB/2020-123/SI2.852232
Activity no. and title	Activity 7: “WG3 – NAP content and accessibility”
Author(s)	Maria Stavara, CERTH-HIT, GR; Chrysostomos Mylonas, CERTH-HIT, GR; Evangelos Mitsakis, CERTH-HIT, GR
Co-author(s)	Barry Koloway, KIOS CoE, CY; Rodolfo Da Silva, KIOS CoE, CY; Peter Lubrich, BAST, DE; Jasper Beernaerts, BE; Petr Bureš, TamTam Research, CZ; Frank Daems, Ertico, BE
Related to Milestone no.	M3.11
External Milestone	yes

Document history

Version	Date	created/ modified by	Comments
0.1	29.02.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Structure of the document
0.2	20.03.2024	Maria Stavara, CERTH-HIT, GR; Chrysostomos Mylonas, CERTH-HIT, GR Barry Koloway, KIOS CoE, CY Rodolfo Da Silva, KIOS CoE, CY	Chapter 1 and Subsections 2.1, 2.2, 2.3 Subsections 3.1, 3.2
0.3	27.09.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Subchapter 2.4, review the document, comments
0.4	17.10.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Subchapter 3.4, Subchapter 3.5, Subchapter 4.1, 4.2, 4.3
0.4	22.10.2024	Peter Lubrich, BAST, DE; Maria Stavara, CERTH-HIT, GR	Subchapter 4.4 (The German case) Subchapter 4.4 (The Belgian, Swiss, Norwegian, Swedish, Croatian and Slovenian case)
0.4	24.10.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Concluding remarks, abstract, finalizing the document
0.5	25.10.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Clean and send out the document to WG3 participants
0.6	30.10.2024	Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Final draft
0.7	19.11.2024	Jasper Beernaerts, BE; Petr Bureš, TamTam Research, CZ; Maria Stavara, Chrysostomos Mylonas, CERTH-HIT, GR	Review, resolve comments, final version
0.8	25.11.2024	Frank Daems, Ertico, BE	Review
1.0	07.01.2025	Hannah Walther, RC	Final version after SCOM approval

Document status:

☐	To be revised by partners involved in the preparation of the document
☐	For review/ approval by the Core Alignment Team and Peer Reviewers
☐	For approval by the NAPCORE Steering Committee
☒	Final
☐	Updated/revised final version (e.g., when a second version of Milestone is published)

Abstract

This document provides a thorough analysis of key aspects surrounding (a) terms and conditions for data reuse, (b) fair data exchange principles, and (c) GDPR compliance within the context of NAPs. The main objective of the current report is to offer a clear framework and practical guidance for handling the terms and conditions of data re-use across the ecosystem of European NAPs, hence promoting transparency and consistency in licensing practices, fair data exchange, and guaranteeing alignment with GDPR regulations to protect personal data. It covers a wide range of important issues, such as the varied licensing models adopted by NAPs, and strategies to foster reasonable data exchange between public and private stakeholders. Furthermore, a European inventory of licenses and terms and conditions revealed significant discrepancies in data reuse practices, underscoring the need for standardized and transparent approaches across NAPs. The report also includes an analysis of fair data exchange through a tailored survey, exploring the approaches of public data providers and the willingness-to-pay preferences of data consumers. Finally, it provides recommendations for ensuring GDPR compliance aiming at enhancing data governance across NAPs based on best practices that has been observed and recorded from various NAPs across Europe.

Abbreviations

Abbreviation	Meaning
CC	Creative Commons
DR	Delegated Regulations
DPIA	Data Protection Impact Assessment
DSG	Swiss Data Protection Act
EC	European Commission
EUPL	European Union Public License
FDPIC	Federal Data Protection and Information Commissioner
FRAND	Fair, Reasonable, and Non-Discriminatory
GDPR	General Data Protection Regulation
ITS	Intelligent Transport Systems
MSs	Member States
NAP	National Access Point
NAPCORE	National Access Point Coordination Organisation for Europe
NLOD	Norwegian License for Open Government Data
ODC	Open Data Commons
OGI	Open Government License
WG	Working Group
WG	Working Group
PTOs	Public Transport Operators
SSTP	Safe and Secure Truck Parking
SSTPA	Safe and Secure Truck Parking Areas



Table of contents

1. Introduction.....	7
2. Analysis and guidelines of terms and conditions for NAP data re-use.....	8
2.1. Introduction.....	8
2.2. European inventory	8
2.2.1. Utilized licenses	9
2.2.2. Specific survey questions and answers	10
2.3. Description of terms and conditions for data re-use	15
2.3.1. Permissions	15
2.3.2. Obligations	19
2.3.3. Prohibitions	22
2.4. Main types of common licenses	24
2.4.1. Creative Commons licenses	24
2.4.2. Open Data Commons licenses.....	25
2.4.3. Proprietary licenses.....	26
2.4.4. Other existing licensing framework	26
2.5. Summary and guidelines	27
3. Analysis of fair data exchange principles.....	29
3.1. Introduction.....	29
3.2. Review data pricing models	31
3.3. Survey design.....	35
3.4. Survey results (public data providers).....	36
3.4.1. Descriptive survey results	36
3.4.2. Validity of prespecified cost categories	37
3.4.3. Magnitude of costs.....	38
3.5. Survey results (data consumers)	41
3.6. Discussion	43
4. GDPR in the NAP context.....	44
4.1. Introduction.....	44
4.2. Basic principles of GDPR.....	44
4.2.1. Lawfulness	44
4.2.2. Fairness.....	45
4.2.3. Transparency	45
4.2.4. Data Minimization	45
4.2.5. Accountability.....	45
4.3. GDPR in relation to NAPs.....	45

4.4.	Existing approaches and best practices.....	47
4.4.1.	The case of the German NAP	47
4.4.2.	The case of Belgian NAP	48
4.4.3.	The case of Swiss NAP	50
4.4.4.	The case of Norwegian NAP	51
4.4.5.	The case of Swedish NAP	52
4.4.6.	The case of Croatian & Slovenian NAP	52
4.5.	Recommendations for NAP operators	53
5.	Concluding remarks	55

List of tables

Table 1: Questions posed in NAP operators related to the ambiguities observed in the specified licenses; answers in an aggregated manner	10
Table 2: Summary of the main types of Creative Commons licenses	24
Table 3: Open Data Commons licenses.	25
Table 4: Summary of terms & conditions with compatible licenses.	27
Table 5: Summary of license categories and available licensing options.....	28
Table 6: Recommendations to NAP operators for ensuring compliance with GDPR.....	53

List of figures

Figure 1: Utilized licenses across European NAPs.	9
Figure 2: Viscusi and Batini (2017) Proposed model for digital information asset evaluation	33
Figure 3: Fleckenstein et al (2023) Data Valuation Dimension	34
Figure 4: Number of provided datasets	36
Figure 5: Delegated Regulations in relation to the provided datasets	37
Figure 6: Cost categories are valid in the case of public data providers.....	38
Figure 7: Data collection and processing costs	39
Figure 8: Data exchange infrastructure costs.....	39
Figure 9: Data management and quality assurance costs.....	39
Figure 10: Security and privacy compliance costs.....	39
Figure 11: Licensing and intellectual property rights costs.....	39
Figure 12: Promotion and outreach costs.....	39
Figure 13: Technical support and maintenance costs.....	39
Figure 14: Preference on permissions granted to data consumers	40
Figure 15: Preference on obligations enforced to data consumers.....	41
Figure 16: Responses of the two data consumers	41
Figure 17: Preferences of data consumers in terms of permissions	43
Figure 18: Preferences of data consumers in terms of obligations	43
Figure 19: Data Privacy Statement and Terms & Conditions at Mobilithek	47
Figure 20: Terms & Conditions rule of the Mobilithek.....	47
Figure 21: Data provider's declaration in terms of GDPR	48
Figure 22: User rights in accordance with Article 7.3 and Article 12 to 22 inclusive of Regulation (EU) 2016/679	49
Figure 23: Measures applied by the Belgian NAP to safeguard the personal data.....	50



Figure 24: Users' rights at the Swiss NAP	51
Figure 25: Privacy policy of the Slovenian & Croatian NAP.....	53



1. Introduction

The activities of WG3 “NAP content and accessibility” of the NAPCORE project are focused on harmonizing the accessible content of European National Access Points (NAPs). This harmonization effort considers not only the current and upcoming European legislative framework for the Intelligent Transport Systems (ITS), but also the recorded and foreseen progress within the entire ITS domain. The activities of WG3 extend beyond mere harmonization. They aim to facilitate fair, trusted, and enhanced accessibility to ITS-related data across Europe. This objective is addressed through an investigation of several aspects, among others, the data availability, data quality, data use and reuse, fair data exchange and data visualization. By exploring all those dimensions, WG3 aims to establish a solid ecosystem that fosters both data exchange and utilization mechanisms. The objectives and goals of WG3 can be summarized as follows:

1. Support Member States (MS) towards a common understanding on the current and future accessible content of NAPs considering existing, planned, and foreseen European legislative and technological developments.
2. Monitor and assess the availability of ITS-related data at both national and Pan-European level in order to identify gaps and areas for improvement.
3. Establish a robust framework for evaluating data quality hosted on NAP platforms.
4. Investigate commonly accepted frameworks and technical options to achieve fair, trusted, and enhanced accessibility to ITS-related data through NAPs of Europe.
5. Create added value visualization tools to be used by NAP operators, data providers, and data consumers.
6. Support the enhanced use of NAPs in key application areas of priority and added value for EU MS.
7. Align the achievements on the NAP content and accessibility level with the remaining activities and needs of the project, including training.

The scope of the current report is aligned with and contributes to the achievement of the fourth objective of WG3. Specifically, this milestone is dedicated to creating guidelines that facilitate data exchange, by describing clear terms and conditions of data sharing and re-use through NAPs, including usage rights, responsibilities, and prohibitions. In addition to that, the milestone aims at analysing fair and reasonable data exchange structures and strategies, considering the sides of both data providers and consumers. Finally, it targets at creating recommendations to ensure that data exchange comply with the requirements of the General Data Protection Regulation (GDPR). The specific objectives of the current report can be summarized as follows:

- Provide guidance on the selection of appropriate license frameworks to strengthen the clarity of sharing and reusing ITS-related data through NAPs.
- Provide an analysis for fair data exchange in order to assist NAP operators and data providers in establishing fair structures for the provision ITS-related data.
- Develop a relevant recommendation framework to ensure that the NAP operation and ITS-related data exchange aligns with the requirements of the GDPR.

The structure of the document can be summarized as follows. The current chapter introduces this document and presents the objectives of WG3 in general and this document in particular.

Chapter 2, “Analysis and guidelines of terms and conditions for NAP data re-use” corresponds to the first objective of the current deliverable. In this respect, it

a) provides an overview of the European licenses currently utilized by the NAPs,

b) describes in greater detail the building blocks of the terms and conditions for data re-use based on the existing literature, and

c) offers a specific table that associates the various terms and conditions, described in the previous subsection, with specific licensing frameworks that could be adopted by NAP data providers.

Chapter 3, “Analysis of fair data exchange principles” highlights the importance of harmonized data pricing across Europe. Subsequently, by conducting a literature review of existing models and approaches, it identifies key influencing factors. On that basis, a tailored-made survey has been designed targeting to gather insights from data providers (both public and private) and data consumers concerning, respectively, their data pricing strategies and willingness-to-pay. Results are then presented and discussed in the last subsection of this chapter.

Chapter 4, “GDPR in the NAP context” primarily reviews the EU policy and legal framework on the protection of personal data. By that means, it provides an overview of the most important principles that NAPs need to consider and implement in order to ensure compliance with the GDPR regulations. Finally, it provides recommendations to NAP operators considering the approaches adopted by various NAPs across Europe and recorded best practices.

The last chapter sums up the main findings and the key points of the document.

2. Analysis and guidelines of terms and conditions for NAP data re-use

2.1. Introduction

In this section, the focus is on highlighting the importance of providing clear terms and conditions for all datasets hosted on NAPs. Such terms and conditions can provide a clear framework ensuring that all stakeholders understand their permissions, obligations, and prohibitions, while simultaneously making the data “as open as possible and as closed as necessary (when and if that is required)”. When data are shared under clear terms and conditions, the probability of being re-used and connected to operational ITS ecosystems and end-user services increases substantially. (Re)usability stands out as one of the key concepts of the ecosystem of NAPs, since the primary role of this digital node/infrastructure is to support the exchange, access, and (re-)use of data that are collected and digitized by various actors involved in transport system operations. Therefore, it is important that datasets are documented well enough, thus enabling potential data consumers to easily comprehend how to leverage and use them.

In essence, terms and conditions are strongly connected with licenses. Licenses establish the legal permissions and restrictions associated with accessing and utilizing datasets, outlining the rights and obligations of both data providers and data consumers. That is to say, terms and conditions are built upon the licenses providing specific guidelines that further elaborate on how the licensed data can be used, shared, and redistributed.

The following subsections describe the prevailing landscape of European NAPs as regards the licenses that are utilized by them and their data providers as well as delve into their associated terms and conditions for data reuse, considering both centralized and decentralized NAP approaches. Finally, practical guidelines are presented in a tabular format to facilitate the alignment of existing licenses with specific requirements and needs in order to assist data providers to select the appropriate license based upon their necessities and preferences.

2.2. European inventory



In the context of WG3, extensive desktop research has taken place targeting to record the licenses utilized across European NAPs. Amongst the aims of this endeavor was to understand and assess the level of harmonization of European NAPs and their data providers on this topic. In particular, this endeavor started in early 2023 to document all datasets hosted in several NAPs accompanied with their respective license framework. This was conducted by utilizing a highly representative sample of NAPs, i.e., operated by 21 European countries, with no restrictions as regards the typology of data (e.g., in relation to the data categories enlisted in the DRs supplementing the ITS Directive).

2.2.1. Utilized licenses

Figure 1 depicts the findings of the desktop research revealing the distribution of licenses utilized within the NAPs of the explored MSs. As can be observed therein, the research has indicated that 223 datasets hosted on European NAPs employ the “No license - no contract” approach. In addition, frameworks related to Creative Commons¹ attributions (more details and information on CC attributions are enlisted in **Table 3** in subsection 2.3.4), particularly “CC Zero” and “CC BY 4.0”, emerge as prominent choices, appearing in 146 and 135 datasets, respectively. On the other hand, only few datasets specify the “free” and “CC BY 3.0” licenses (1 in each case). However, certain datasets demonstrate ambiguity in their licensing models, as indicated in **Figure 1** by the specified license (or license category): a) “Special terms of use”, b) “Other”, c) “No license - no agreement”, d) “Similar license with CC”, and e) “Not specified”. These instances underscore the need for a more harmonized and transparent licensing framework across the ecosystem of European NAPs.

It is herein noted that while specific (metadata) values have been recorded in their current form, as published in the list of investigated NAPs, their validity is very limited. For instance, values such as “Not specified” do not provide any interpretable information about the rights to use a particular dataset. Likewise, while values such as “No license – No contract” has been recognized by the Coordinated Metadata Catalogue (Lubrich et al., 2019) as an option for the element “Contract or License”, they mainly serve as a default option to be utilized by NAP operators, which can then be specified by data publishers to reflect the applicable rights of data usage. Therefore, despite being recorded as existing values, their use is not endorsed by this document.

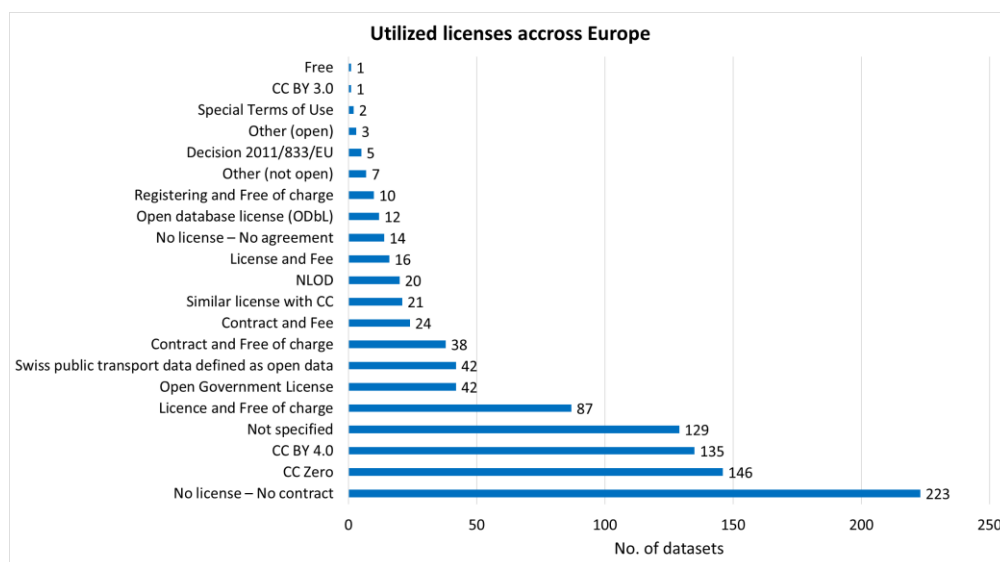


Figure 1: Utilized licenses across European NAPs.

¹ Creative Commons (CC) is a global nonprofit organization that provides free, legally sound copyright licenses, which help creators retain control over their work while also allowing for flexible sharing and reuse by others. <https://creativecommons.org/about/>

In addition, the current survey has revealed some issues regarding the harmonious publication of information about data licensing. Particularly, the values recorded in **Figure 1** span two distinct dimensions. The first dimension, rooted in the CMC ecosystem, reflects whether the data holder/publisher has a policy in place, while the other represents the specific type of policy. For instance, the “license and free of charge” value can correspond to multiple values on an orthogonal axis, such as CC BY 4.0, CC Zero, CC BY 3.0, and so on. This issue has been addressed by mobilityDCAT-AP, specifically by the controlled vocabulary associated with the property dct:license, and for this reason is not further discussed in the current document.

2.2.2. Specific survey questions and answers

In a second stage, a targeted survey was conducted, tailored to address specific questions formulated based on observed issues related to data licensing. These questions were tailored to the operators of each of the explored NAPs. Therefore, they have been requested to provide responses to these questions, aiming to gain further insights and clarify to the extent possible any ambiguities observed (see above). The first column of the **Table 1** summarizes the questions posed to the NAP operators, while the next column presents the corresponding responses in an aggregated manner to improve readability.

Table 1: Questions posed in NAP operators related to the ambiguities observed in the specified licenses; answers in an aggregated manner

	Questions	Answers
1	Which terms and conditions apply in the “No license – No contract” cases? Is the re-use of the corresponding datasets unrestricted?	a) The data are freely available with no restrictions on their use. For instance, there is an online publication that can be accessed and utilized at no cost. The re-use of the corresponding datasets is unrestricted. b) This means that the dataset is made available as open data and that the data owner has not specified any restrictions and/or limitations to the (re)use of the data/service (e.g., acknowledgements). c) While the use of datasets is unrestricted, all users are required to register before accessing selected datasets from the NAP.
Interpretation: In “No license – No contract” cases, the reuse of datasets is generally unrestricted, with varying nuances: (1) The data may be entirely free and openly accessible without any limitations, allowing unrestricted use. (2) The data may be available as open data without specified restrictions or limitations from the data owner, though practices like acknowledgments might still or might not apply (unspecified). (3) While the use of datasets is unrestricted, access to certain datasets may require user registration.		
2	How can a data consumer retrieve more information about applicable contracts and licenses (in case they are not fully specified)?	a) At the NAP, there is the option to provide a sample contract. If a sample contract is not available, the data publisher must be contacted directly. b) Contracts are available to download at the NAP along with description of the subscription process and contact to the data owner. c) This can be accomplished by contacting the data owner via email or by following the link provided under additional information. In many cases, datasets include a hyperlink directing users to a webpage where the data owner provides detailed explanations about the terms of use for the data.
Interpretation: Data consumers can retrieve more information about applicable contracts and licenses in the following ways: (1) The NAP may provide a sample contract; if not, contacting the data publisher directly is necessary. (2) Contracts can be downloaded from the NAP, which also		

provides details about the subscription process and the data owner's contact information. (3) Additional information can be obtained by emailing the data owner or using a hyperlink included with the dataset, often directing users to a webpage with detailed terms of use.		
3	Do specific licensing models (e.g., Creative Commons ones) apply in the "License and Free of charge" case? If no, why? If yes, why are they not explicitly mentioned?	Yes, Creative Commons licenses fall under the category of "license and free of charge". The license categories are structured based on the coordinated metadata catalogue. The concept behind this categorization is to encompass various similar licenses such as CC under a unified term. Additionally, there are contract forms available that may not be CC licenses but offer the same terms of free use.
Interpretation: The licensing categories are often structured using a coordinated metadata catalogue to unify similar licenses, such as Creative Commons, under a single term.		
4	How "Contract and Free of Charge" differs from "License and Free of Charge"? Which is the adopted distinction between a license and a contract?	Contracts for data use impose specific limitations and requirements, such as restrictions on usage for only specific pages or limitations on offline use, without any additional charges. CC licenses typically only require users to attribute the source and not changing the data.
Interpretation: The distinction between "Contract and Free of Charge" and "License and Free of Charge" lies in the level of specificity and restrictions: (1) Contracts are addressed by NAP operators as a means of imposing specific conditions, such as limiting usage to certain purposes or formats (e.g., online only), while still being free of charge. (2) Licenses are addressed as encompassing broader terms without imposing detailed usage restrictions.		
5	There is an SSTPA dataset published in the data.europa.eu portal. This dataset is made available to data consumers under a license model governed by the EC's Decision 2011/833/EU? How is this decision interpreted by the provider of this dataset?	a) The motorway operator has no additional license model for SSTPA dataset. The data was provided to the SSTPA portal according to the EC requirements. b) The dataset for SSTP is considered open data, indicating that it includes all public information accessible in the NAP for SSTP, as available to users of the NAP.
Interpretation: Datasets published on the data.europa.eu portal under the EC's Decision 2011/833/EU may not be associated with additional terms and conditions. They are addressed as being in compliance with EC's requirements. These datasets are mostly treated as open data.		
6	Are there any issues or difficulties that you need to overcome and can be further analyzed in the context of NAPCORE?	a) To achieve harmonization and interoperability within NAPCORE, it is essential to standardize license terms similar to the coordinated metadata catalogue. b) A legal analysis is required to evaluate the legal implications of "existing licenses" such as CC0, CC BY 4.0, CC BY SA 4.0, OGL 3.0, and ODbL 1.0 compared to a traditional "license contract". The aim is to determine if these existing licenses can effectively replace license contracts without causing concerns for data providers. c) NAPCORE might provide some guidance or best-practices in terms of licensing but should not prescribe any. d) We would like to have general recommendations and guidance from NAPCORE for licensing.

Interpretation: Several issues and challenges within the context of NAPCORE include: a) achieving harmonization and interoperability by standardizing license terms, similar to the approach used for the coordinated metadata catalog, b) conducting a legal analysis to compare the implications of existing licenses (e.g., CC0, CC BY 4.0, OGL 3.0) with traditional license contracts, ensuring that these licenses can replace contracts without raising concerns for data providers, c) providing guidance or best practices for licensing while avoiding prescriptive measures, and d) offering general recommendations to assist stakeholders in navigating licensing complexities.		
7	Which is the adopted distinction between a license and a contract?	Contracts require the signature of the data consumer, although their content closely resembles that of CC BY 4.0.
Interpretation: The distinction between a license and a contract lies in the formal agreement process: a contract requires the signature of the data consumer, while a license does not. Despite this procedural difference, the content of these contracts often closely aligns with that of standardized licenses, such as CC BY 4.0.		
8	What does “Not specified” mean?	a) The data provider does not provide license information. b) It means that the provider of the dataset or service did not specify in the metadata which license applies to the dataset or service.
Interpretation: “Not specified” case implies that a) the data provider has not included license information or b) while a license may exist, the provider has not documented it in the metadata.		
9	Does “None” mean that the (re-)use of a dataset is unrestricted?	It indicates that no specific license has been mentioned or provided.
Interpretation: “None” does not necessarily mean unrestricted reuse. It simply indicates that no specific license has been mentioned or provided, leaving the terms of use unclear.		
10	Do specific licensing models apply in the “Bilateral contract” case? If no, why?	“Bilateral contracts” regulate the re-usage of data in accordance with the data provider’s internal rules, i.e., independent of standard licensing models. Such a contract needs to be signed bilaterally. However, this is a very seldom case, as shown in the diagram.
Interpretation: No specific licensing models apply in the “Bilateral contract” case because these contracts are tailored to the data provider’s internal rules and operate independently of standardized licensing models. Each contract is negotiated and signed bilaterally, making it a customized agreement. However, this is a rare occurrence.		
11	Could you please provide some information about the licensing framework of the datasets for which no relevant information is provided?	Each data provider can OPTIONALLY describe the licensing model as part of the dataset’s metadata. In case there is no such metadata information, we assume there is either no conditions at all, or the data user needs to arrange something individually with the data provider.
Interpretation: For datasets with no relevant licensing information provided, the licensing framework can optionally be described by the data provider in the dataset’s metadata. If such metadata is absent, it is generally assumed that either no conditions apply to the dataset, or the data user must negotiate terms directly with the data provider.		
12	What is the reason that you prefer “Proprietary License” instead of a standardized license framework (e.g., a Creative Commons one)?	It is a very seldom case, as shown in the diagram. We assume there are some special rules for the affected data sets.

Interpretation: The preference for a “Proprietary License” over a standardized framework like Creative Commons is rare. It is likely chosen for specific datasets that require special rules or conditions not covered by standardized licenses.		
13	In the “License under Creative Commons or similar” case, there are links which provide information about the license framework (termed as “example contract”). What additional information is provided via these documents that is not provided by a standardized license framework (e.g., Creative Commons one)?	Through the links for the example contracts, dataset owners can include information about the terms of use for their datasets. This option is available for all datasets except those categorized as “No license - no agreement”. The information provided can cover various aspects such as terms of use, fees for data usage, and any other details pertaining to licensing and agreements.
Interpretation: In the “License under Creative Commons or similar” case, the linked example contracts allow dataset owners to specify additional details about the terms of use for their datasets. Unlike a standardized license framework, these documents can include information on usage terms, applicable fees, and other licensing or agreement-related specifics. This flexibility is available for all datasets except those classified as “No license - no agreement.”		
14	Which is/are the license model(s) behind “License and Fee” case?	a) These contracts and licenses, which are not Creative Commons and do not follow a standardized format, can encompass various types and terms. b) Publications utilizing this type of license typically belong to private companies, and their terms of use are linked within the NAP.
Interpretation: The “License and Fee” case involves non-standardized contracts and licenses that are not part of the Creative Commons framework. These licenses may vary in type and terms and are typically associated with publications from private companies., which specific terms of use are provided through links within the NAP.		
15	Does “No License – No Agreement” mean that the (re-)use of a dataset is unrestricted?	Yes, the data is entirely open for use without any restrictions.
Interpretation: The “No License – No Agreement” indicates that the dataset is completely open and unrestricted, allowing free reuse without any conditions or limitations.		
16	Why a national license model of the government is preferred compared to universal ones (e.g., Creative Commons ones)?	The data providers decide themselves which license they use for their datasets. It is not the government who sets a preference. I assume that the possible options are simply listed alphabetically.
Interpretation: A national license model is not necessarily preferred over universal ones like Creative Commons; instead, data providers independently choose the licenses for their datasets. The government does not establish a preference.		
17	What terms and conditions apply in the “Registering and free of charge” case?	Data for SRTI, SSTP, and RTTI is accessible to registered users, and once registered, the data is freely available for use. In contrast, MMTIS data is accessible without the need for registration.

Interpretation: In the “Registering and free of charge” case, users shall register to access data for SRTI, SSTP, and RTTI, but once registered, the data is freely available for use. On the other hand, MMTIS data does not require registration and is freely accessible without any such conditions.		
18	Does “Free” mean that the (re-)use of a dataset is unrestricted?	The “free” data refers to public transport data, which is fully accessible to everyone without any restrictions.
Interpretation: In this context, “free” means that the public transport data is completely open and accessible to everyone without any usage restrictions.		
19	Why the “Norwegian License for Open Government Data (NLOD)” is preferred compared to a universal licensing model (e.g., a Creative Commons one)? Which is the most matching universal licensing model with the NLOD?	The NLOD is compatible with CC BY 4.0. However, it was formulated before the release of CC 4.0. As CC 3.0 was deemed unsuitable for sharing public datasets the Norwegian Digitalization Agency developed and endorsed NLOD for use in Norway.
Interpretation: The “NLOD” is preferred over a universal licensing model like Creative Commons because it was specifically tailored to meet the needs of sharing public datasets in Norway, addressing limitations in earlier versions of CC, such as CC 3.0. NLOD aligns well with CC BY 4.0, which was released later, but its development by the Norwegian Digitalization Agency reflects a proactive approach to ensuring compatibility with local requirements and facilitating open data sharing.		

As it was initially planned, the survey aimed to address specific concerns regarding the utilized data licensing. Key questions focused on understanding the terms and conditions of various licensing models and their implications for data re-use. The responses from NAP operators (15 in total) revealed a diverse landscape of data licensing models, with some datasets being freely available at no cost, while others require registration first or adhere to specific licensing models such as Creative Commons. All responses were collected in 2023. In addition, several NAP operators indicate that the use of bilateral contracts allow data providers to apply their rules and conditions for data (re)use, giving them a degree of flexibility in such arrangements. This flexibility enables data providers to tailor licensing terms according to their specific needs and preferences and in certain cases accommodate limitations/requirements that may not be addressed by the existing licensing models. Lastly, from the collected responses of NAP operators, it is evident that NAPs currently use different licensing frameworks, which highlights the need for standardization and harmonization in data licensing across NAPs in Europe.

2.3. Description of terms and conditions for data (re)use

This section provides an analysis of the basic terms and conditions of data (re)-use, including permissions, obligations, and prohibitions, derived from the guidelines outlined in the EU's Licensing Assistant. Permissions, obligations, and prohibitions constitute the three main pillars under which several terms and conditions exist. The scope of this section is to provide clear and straightforward definitions of each term, particularly within the NAP context, in order to facilitate a comprehensive understanding of the rights and responsibilities associated with the (re)-use of ITS data.

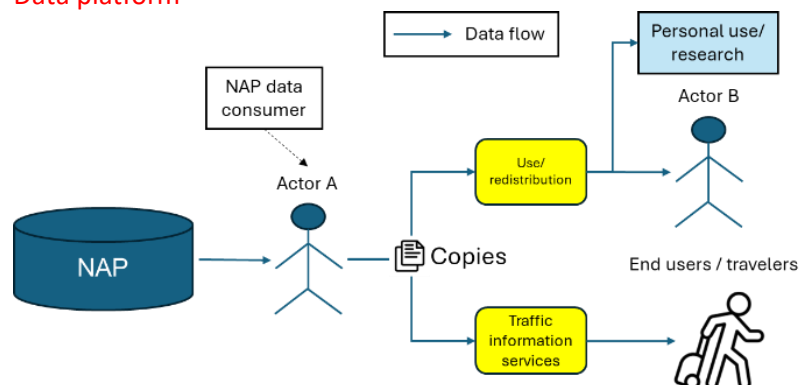
Each term is accompanied by a specific diagram illustrating how NAP platforms, data consumers, and data resources are connected. Considering the outputs of NAPCORE WG2 (Task 2.3), it is important to recognize that implemented NAPs may adopt either a centralized (data platform) or decentralized (metadata directory) operational approach. This architectural distinction impacts the associations depicted in the diagrams, as the terms and conditions for data re-use can vary between databases and metadata directories. Therefore, depending on the NAP implementations, the associations depicted in the following diagrams are adapted accordingly.

2.3.1. Permissions

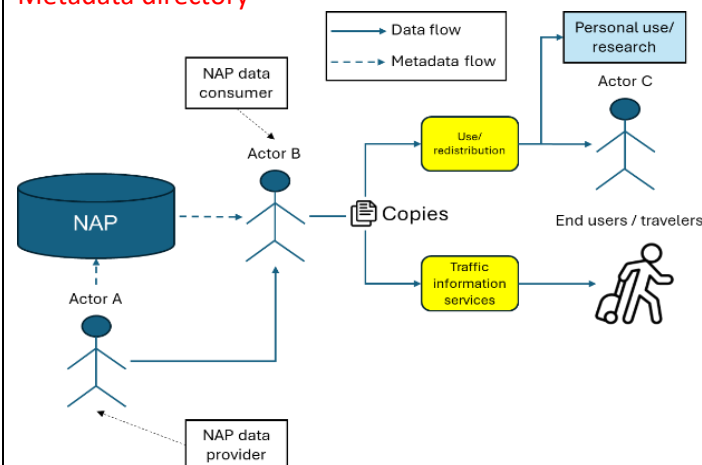
Permissions refer to the specific rights granted by the data provider to data users regarding the use of the data. In essence, permissions describe what users are allowed to do with the data under the conditions described by “obligations” and “prohibitions”. They encompass the following rights:

- Reproduction: This pertains to the right to *make copies* of the original data. Users may be granted permission to reproduce the data for various purposes such as personal use, research, or redistribution. In addition, they might reproduce the data in different formats, ensuring accessibility and usability across different platforms or systems. However, it is crucial to adhere to any restrictions or conditions specified by the data provider, such as acknowledging the source and maintaining data integrity during reproduction.

Data platform

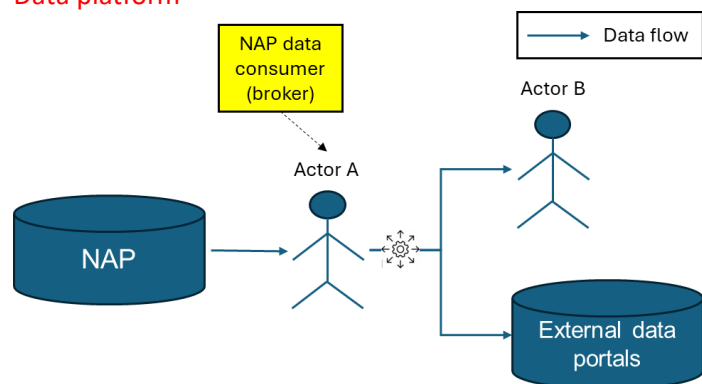


Metadata directory

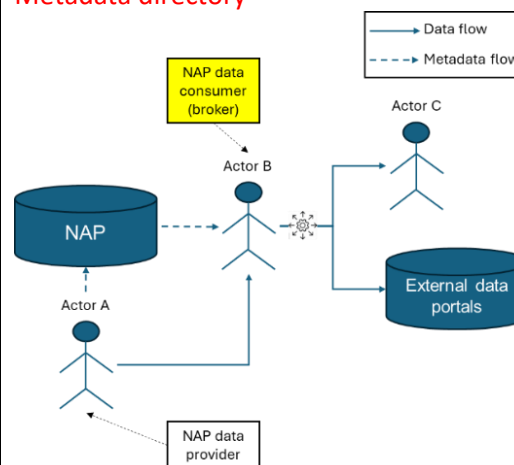


- Distribution: This refers to the right of *sharing or disseminating* the data to others (within an organization or publicly). Distribution involves sharing the data through various channels such as online portals, data repositories, or direct exchanges. It is important for users to comply with any distribution guidelines outlined by the data provider, including restrictions on commercial use, attribution requirements, or even limitations on the extent of distribution.

Data platform

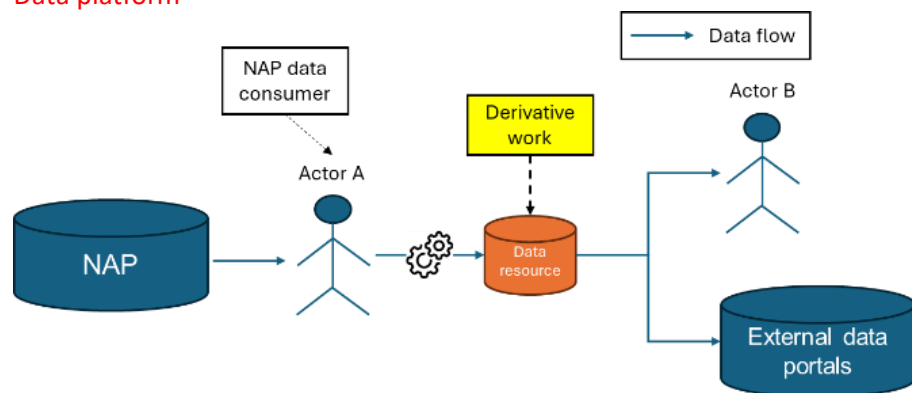


Metadata directory

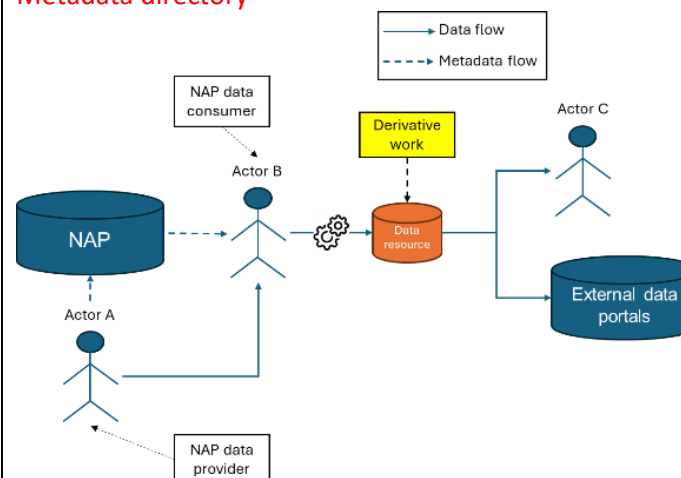


- Derivative work: Derivative work rights allow users to create new works based on the original dataset. This includes making modifications, adaptations, or enhancements to the data. However, users must respect any restrictions or conditions set forth by the data provider regarding the creation and distribution of derivative works, such as maintaining compatibility with the original data format or obtaining permission for commercial use.

Data platform

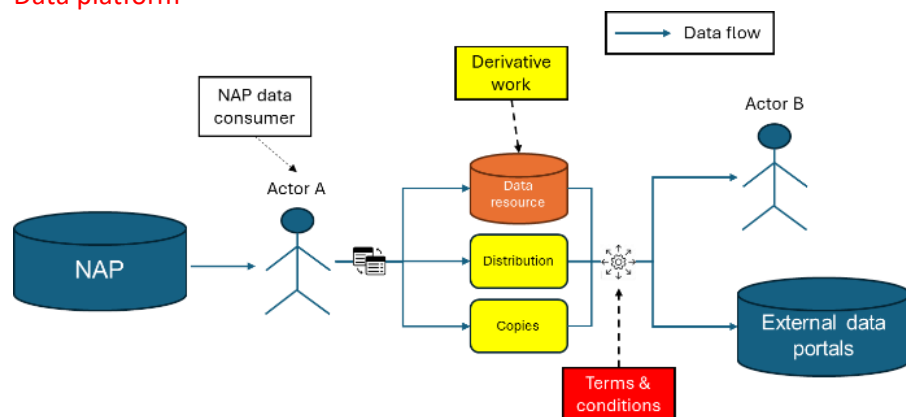


Metadata directory

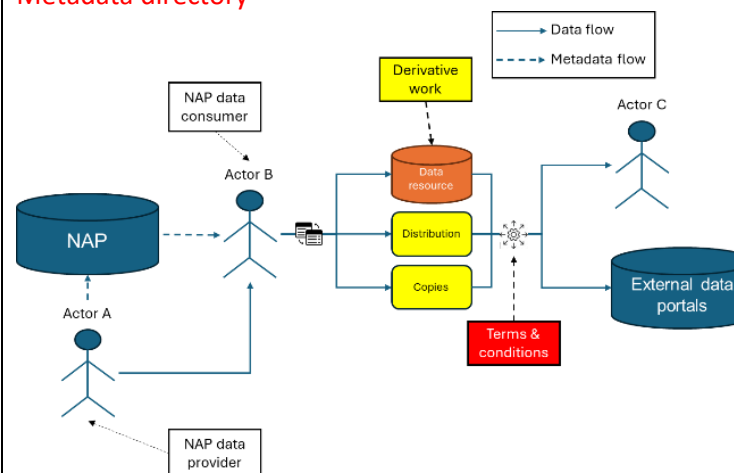


- Sub-licensing: Users with sub-licensing rights can *extend the usage rights* of the data to others, allowing them to reproduce, distribute, or create derivative works based on the original dataset. Sub-licensing enables broader access and utilization of the data within the user community or across different organizations. However, users must ensure that any sub-license agreements comply with the terms established by the data provider and do not violate any legal or contractual obligation.

Data platform

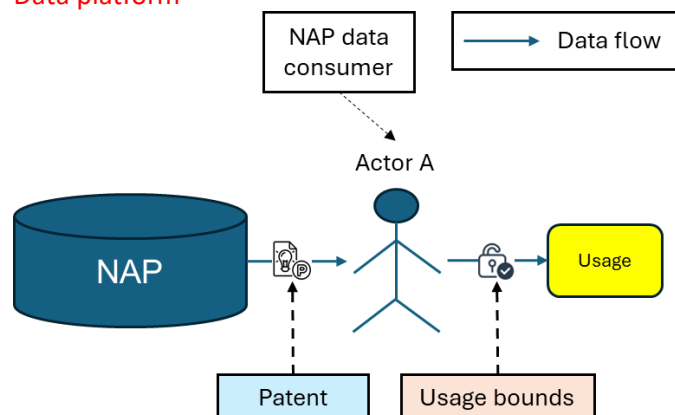


Metadata directory

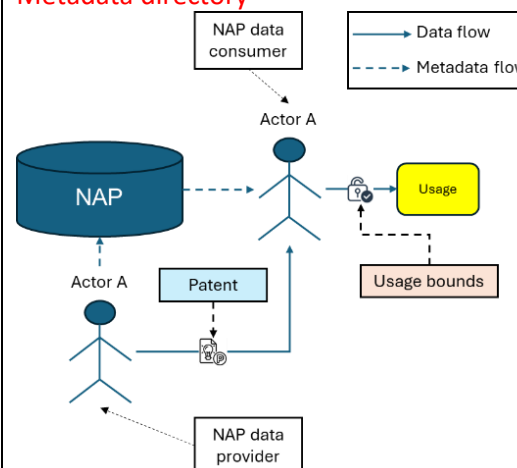


- Use Patent Claims: In cases where the data contains *patented technology* (algorithms, methods, or inventions for research, development, or commercial applications), users may be granted permission to utilize such data within the bounds of the provided license agreements. It is important to note that, under patent law, the visibility or access to the content of patented technology is a fundamental obligation, ensuring transparency of the patented data.

Data platform



Metadata directory

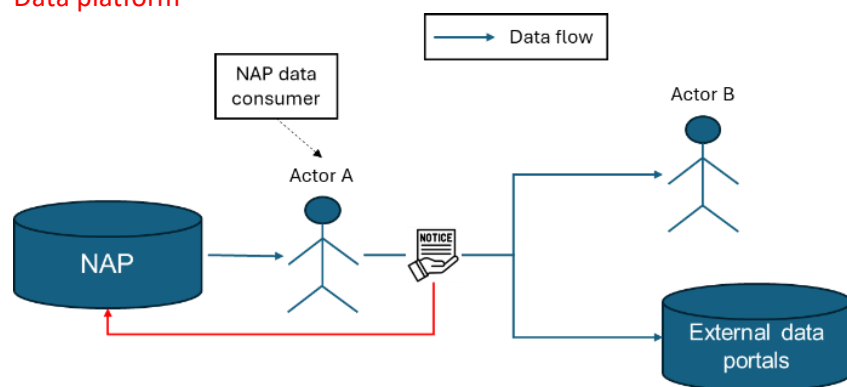


2.3.2. Obligations

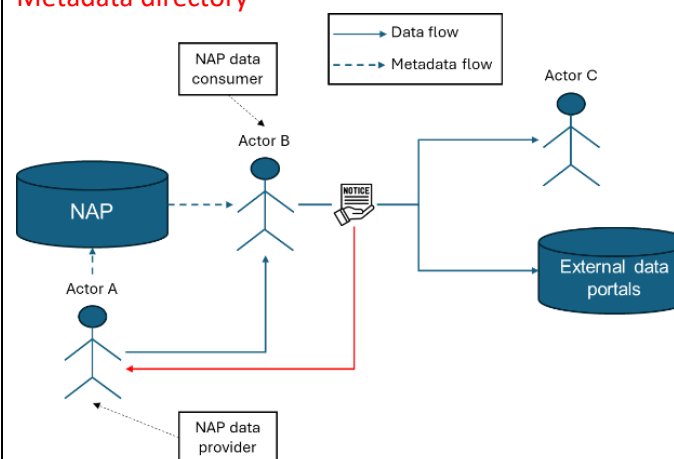
Obligation refers to the responsibilities and conditions set forth by the data provider, that users must fulfil when using and managing the data. Obligations encompass the following conditions:

- Notice: This obligation requires users to provide *a clear notification* whenever they distribute or redistribute the data. This notification must convey the pertinent details of the licensing terms concerning the usage of the data, including the type of license, any restrictions or permissions, and instructions for accessing the complete license agreement.

Data platform

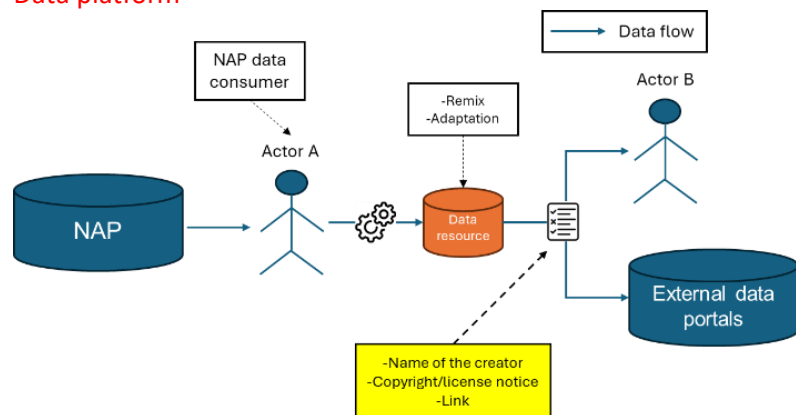


Metadata directory

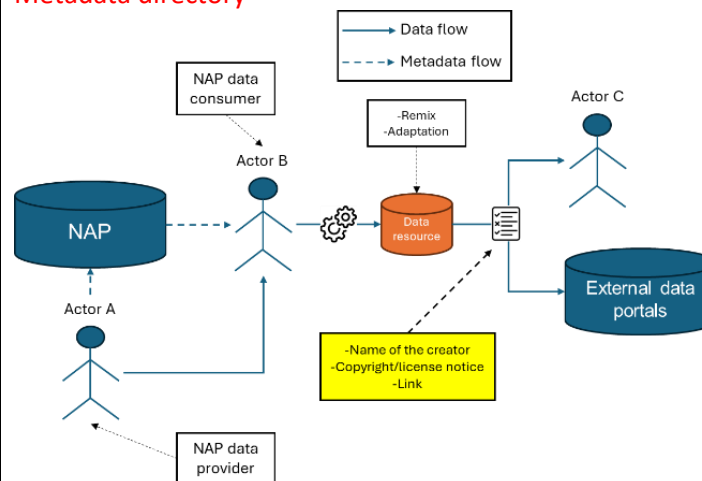


- Attribution: It is often referred to as “BY” in Creative Commons licenses, mandates that users give appropriate *credit* to the original provider of the datasets, when they redistribute, remix, adapt, or build upon the original datasets. Users must provide the name of the creator and attribution parties, a copyright notice, a license notice, a disclaimer notice, and a link to the material.

Data platform

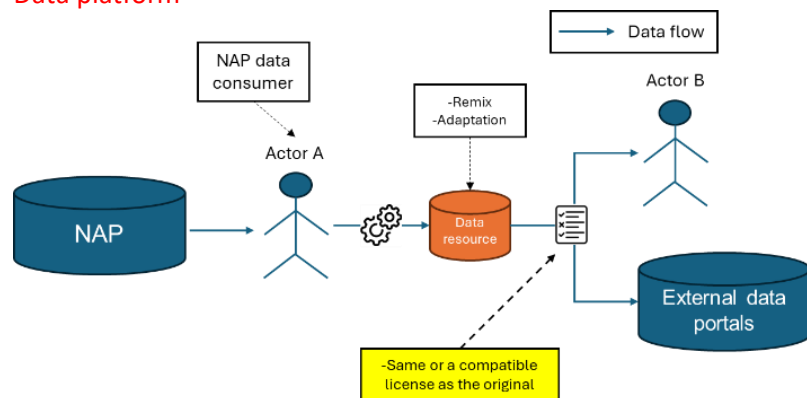


Metadata directory

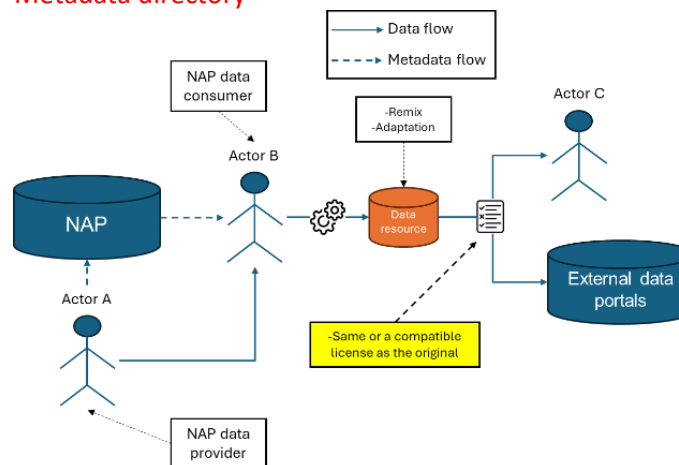


- Share-alike: denoted as “SA” in Creative Commons licenses, requires users to distribute any derivative works they create based on the original dataset under a compatible license as the original.

Data platform

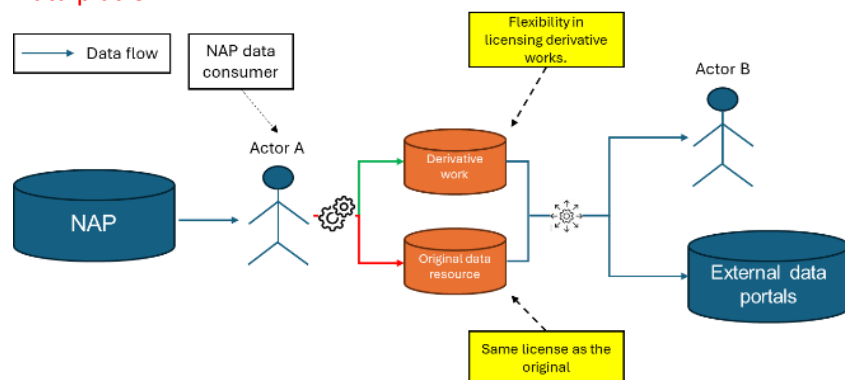


Metadata directory

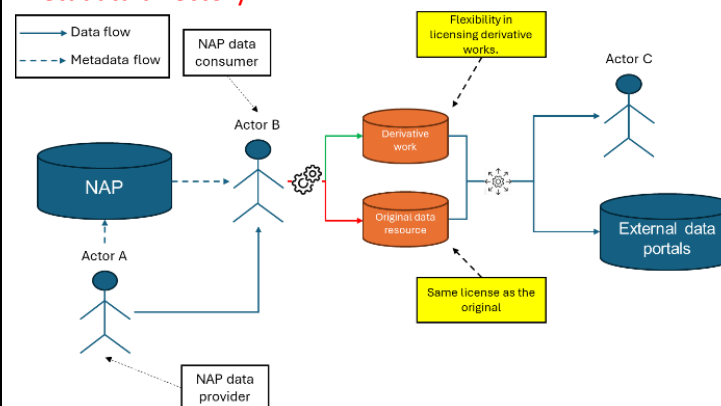


- Lesser copyleft: Under a lesser copyleft license, users are typically required to share their modifications on the datasets under the same license, but they have more flexibility in how they license their derivative works. That means that *combined works can be shared under different terms*.

Data platform

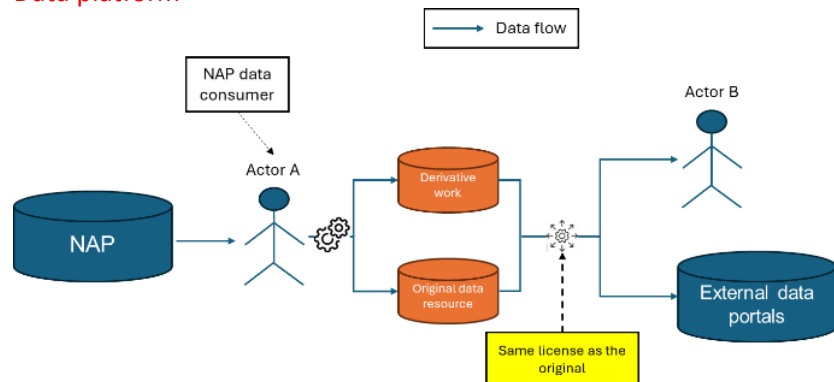


Metadata directory

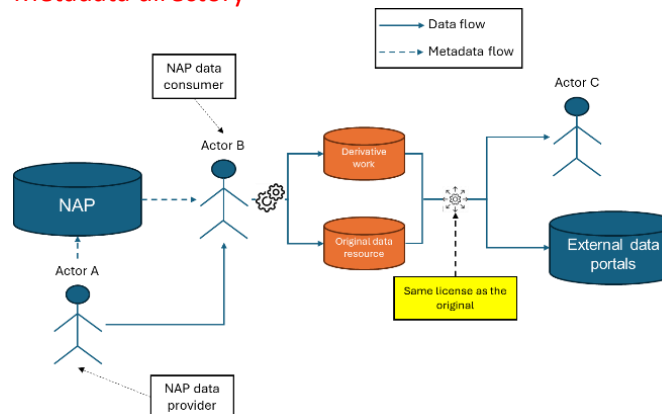


- Copyleft: This obligation ensures that derivative works or modifications made, based on the original datasets *remain open and freely available to others*. It is noted that copyleft is pretty similar to share-alike obligation (see above). The difference is that copyleft is (a) often more rigid (e.g., in the context of licenses such as GPL) that may require the use of the same (not compatible) license for any kind of derivative work and (b) focused on software-related products (SA is focused on content).

Data platform

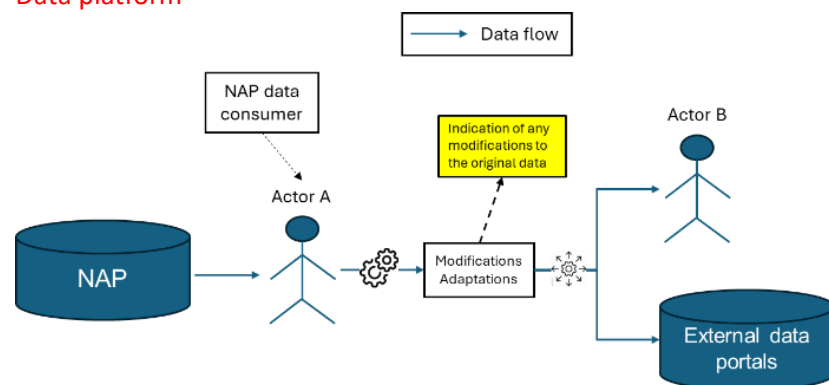


Metadata directory

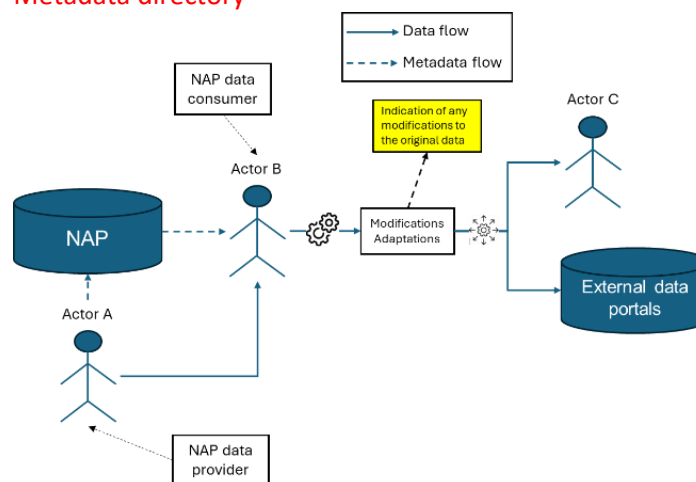


- State changes: This obligation refers to the requirements to *indicate* any modifications or adaptations made to the original data when redistributing or sharing it with others.

Data platform



Metadata directory

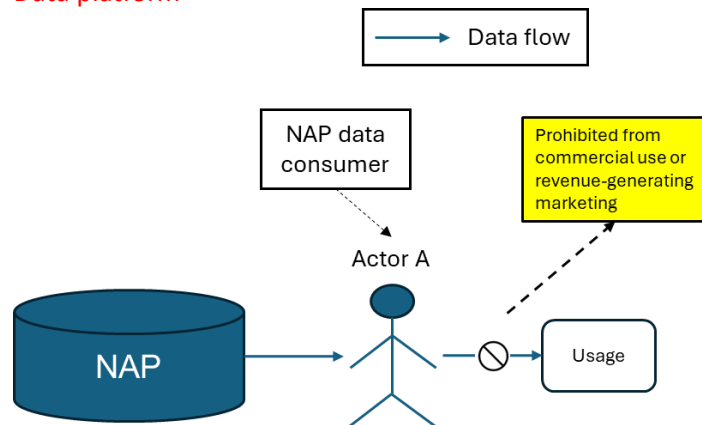


2.3.3. Prohibitions

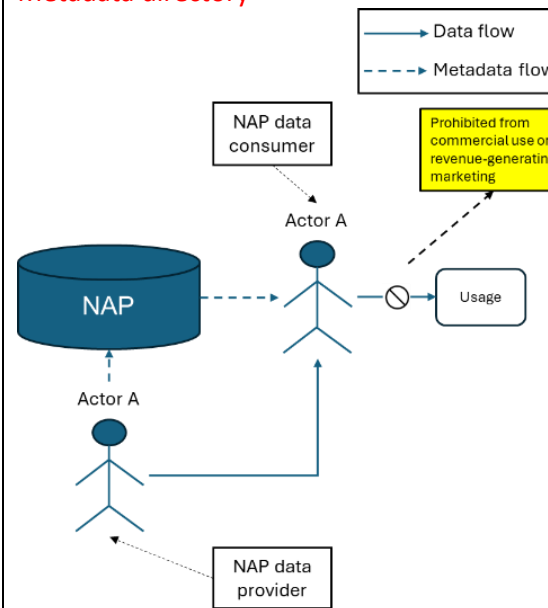
Prohibition refers to a restriction set forth by the data provider that forbids certain actions or uses of the dataset.

- Commercial use: This term refers to the prohibition of datasets from being used for commercial purposes. Users are restricted from employing it for purposes such as selling products or services, conducting business operations, or engaging in advertising or marketing initiatives with the intention of making money.

Data platform



Metadata directory



2.4. Main types of common licenses

This chapter explores the main types of common licenses used for sharing data and content, focusing on their frameworks and key characteristics. It covers Creative Commons licenses, which provide flexible options for creators to define how their work can be reused, modified, and attributed, while balancing openness with protection. The chapter also covers a comprehensive overview of the Open Data Commons licenses, specifically designed for open data and databases, addressing unique concerns such as database rights and encouraging data accessibility while safeguarding contributors' rights. Additionally, it examines proprietary licenses, which are often tailored to specific datasets or agreements, reflecting customized terms rather than standardized models. Finally, other notable licensing frameworks are also covered, showcasing the diversity in approaches.

2.4.1. Creative Commons licenses

This subchapter provides an analysis of the Creative Commons licensing framework. Creative Commons licenses serve as a standardized yet flexible mechanism, enabling rights holders to specify conditions for attribution, modification, and commercial use of their content. Widely recognized for its role in promoting transparency and interoperability, this framework strikes a balance between fostering openness and protecting intellectual property rights. By offering a range of licenses, **Table 2** outlines the six main types of Creative Commons licenses, detailing their permissions, obligations, and restrictions. Their correspondence with the terms and conditions introduced in Section 2.3 is provided next.

Table 2: Summary of the main types of Creative Commons licenses

1. CC BY (Attribution)	
This license allows users to share, copy, and redistribute the work in any medium or format, and to adapt, remix, transform, and build upon the work for any purpose, even commercially, as long as they give appropriate credit to the creator.	
2. CC BY-SA (Attribution – ShareAlike)	
This license allows users to share, copy, and redistribute the work in any medium or format, and to adapt, remix, transform, and build upon the work for any purpose, even commercially, as long as they give appropriate credit to the creator and share their modified material under the same license.	
3. CC BY-NC (Attribution – NonCommercial)	
This license allows users to share, copy, and redistribute the work in any medium or format for non-commercial purposes only, and to adapt, remix, transform, and build upon the work as long as they give appropriate credit to the creator.	
4. CC BY-ND (Attribution – NoDerivs)	
This license allows users to share, copy, and redistribute the work in any medium or format for any purpose, even commercially, as long as they give appropriate credit to the creator and do not make any modifications or derivatives of the work.	
5. CC BY-NC-SA (Attribution – NonCommercial – ShareAlike)	

This license allows users to share, copy, and redistribute the work in any medium or format for non-commercial purposes only, and to adapt, remix, transform, and build upon the work as long as they give appropriate credit to the creator and share their modified material under the same license.	
6. CC BY-NC-ND (Attribution – NonCommercial – NoDerivs)	
This license allows users to share, copy, and redistribute the work in any medium or format for non-commercial purposes only, as long as they give appropriate credit to the creator and do not make any modifications or derivatives of the work.	
7. CC Zero	
This license is a public dedication tool, which enables creators to give up their copyright and put their works into the worldwide public domain. CC0 enables re-users to distribute, remix, adapt, and build upon the material in any medium or format, with no conditions.	

2.4.2. Open Data Commons licenses

Open Data Commons constitutes a different initiative than Creative Commons, while sharing similar goals and values. The Open Data Commons licenses are compatible with the Creative Commons licenses, which means that creators can choose to apply both types of licenses to their works, if desired. Open Data Commons offers four different types of licenses, each of which is designed to meet different needs and use cases for open data. These four types are listed in **Table 3** below.

Table 3: Open Data Commons licenses.

1. Open Database License (ODbL)	This license is designed for databases that are made available to the public for use, sharing, and redistribution. The ODbL requires that any adaptations or modifications of the database be shared under the same license, and that any public use of the database includes attribution to the original creator. Source here .
2. Database Contents License (DbCL)	This license is designed for individual data sets or collections of data that are made available to the public. The DbCL requires that any adaptations or modifications of the data be shared under the same license, and that any public use of the data includes attribution to the original creator. Source here .
3. Community Data License Agreement (CDLA)	This license is designed for community-developed data that is made available to the public. The CDLA offers two different versions: a Sharing version, which requires that any adaptations or modifications of the data be shared under the same license, and a Permissive version, which allows for more flexibility in how the data can be used and reused. Source here .
4. Public Domain Dedication and License (PDDL)	The PDDL is designed to enable the public to freely use, modify, and distribute data that is in the public domain. It is used for data that is not subject to copyright or any other legal restrictions, and that the creator has intentionally placed in the public domain. Under the PDDL, the creator of the data dedicates their work to the public domain, and grants permission for others to use, modify, and distribute the data without any restrictions or requirements for attribution. This means that the data is

	completely free for use by anyone, for any purpose, without any legal or copyright limitations. Source here .
--	---

2.4.3. *Proprietary licenses*

Proprietary licenses, unlike open licenses, are restrictive and generally aim to maintain control over data usage. These licenses are typically used for software or other intellectual property that is owned by a company or individual, and they may include restrictions on how the software or intellectual property can be used, copied, modified, or distributed. Some examples of proprietary licenses include:

- **End-User License Agreement (EULA):** This type of license sets the terms between the software provider and the user, defining acceptable use, modifications, and any limitations. It typically restricts redistribution and can cover both paid and free software. EULAs are standard in commercial software, requiring user acceptance before installation or usage begins. They enforce terms that protect the provider's intellectual property rights while specifying user rights. This is particularly helpful for public sector data hubs that must enforce strict rules around data privacy and security.
- **Subscription License:** With a subscription license, users gain temporary access to the software, typically with recurring payments (monthly, annually, etc.). Subscription models often include regular updates and customer support, which makes them popular for software-as-a-service (SaaS) solutions. This approach provides flexible access, aligning with evolving technology while keeping users updated with the latest features. NAPs may use subscription-based models for organizations that require continuous access to up-to-date datasets. Subscription licensing allows NAPs to offer tiered access (e.g., different data access levels or types of datasets) while also generating revenue for maintenance and updates.
- **Network and Feature-Based Licenses:** Network licenses permit multiple users within an organization to access software under a single license but may restrict simultaneous use. Feature-based licenses allow organizations to purchase specific features or functions, often reducing costs by excluding unneeded components. This flexibility is beneficial for organizations needing customizable or scalable access.

2.4.4. *Other existing licensing framework*

In addition to Creative Commons and Open Data Commons, there are several other licensing frameworks specifically designed to meet the needs of public sector data, open-source software, and documentation. These frameworks provide unique combinations of permissions, obligations, and restrictions to encourage data sharing, maintain transparency, and ensure legal compatibility across various jurisdictions. Below are descriptions of some commonly used licenses, each serving specific purposes in the context of open data, software, and government publications.

Open Government License (OGL): The Open Government License (OGL) is a licensing framework primarily used by government organizations to openly share public sector data with the public. Developed originally by the UK government, the OGL aims to facilitate transparent data sharing by allowing anyone to freely use, modify, and redistribute government-published data, provided that proper attribution is given to the source. The license allows for both commercial and non-commercial reuse, encouraging a wide range of applications, from research and academic projects to commercial products and services.

European Union Public License (EUPL): The EUPL is an open-source license developed by the European Commission to provide a legally compatible framework across EU member states. It has a copyleft clause, meaning that any derivative works must remain open and be distributed under the EUPL or a compatible open-source license. The EUPL is notable for its legal adaptability within the EU, as it is



available in all official EU languages, making it suitable for software and datasets produced by public institutions in Europe.

Norwegian Licence for Open Government Data (NLOD): The NLOD is an open license developed specifically for Norway's public sector data, allowing anyone to use, modify, and share data provided by Norwegian government entities. It is compatible with open data principles, requiring attribution and sometimes additional terms of use but generally permitting broad reuse. The NLOD encourages transparency and accessibility of government data within Norway, while also aligning with broader open data initiatives in Europe.

2.5. Summary and guidelines

This section serves as a comprehensive guide for data providers (owners) who publish their datasets through NAPs, in selecting appropriate licensing frameworks for their published (referred) datasets. By categorizing a range of open data licenses, it highlights specific permissions, obligations, and prohibitions that each framework imposes and supports. This enables data providers to make licensing selections that align not only with their operational objectives and preferences but also with specific legal and regulatory standards. The licenses included in this section encompass Creative Commons (CC), Open Data Commons (ODC), the Open Government License (OGL), the European Union Public License (EUPL), and the Norwegian Licence for Open Government Data (NLOD). In this respect, the recommendation provided to NAP operators or data providers/publishers (depending on the type of implemented NAP architecture) is to indicate a specific license as applicable for their provided content (by matching their interests and preferences with the analysed permissions, obligations, and prohibitions) and avoid the sole use of simplified classifications, such as "license – free of charge". This will enable clarity of data (re-)use rights.

Table 4 showcases these terms and conditions by aligning them with the most compatible licensing frameworks previously discussed, while **Table 5** provides an overview of the broader license categories, summarizing their core characteristics and then listing specific licensing options per category.

Table 4: Summary of terms & conditions with compatible licenses.

License Category	Term	Short description	Compatible licenses
Permissions	Reproduction	The right to make copies of the original dataset.	CC BY 3.0, CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, CC-PDM 1.0, CC0 1.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL, ODC-PDDL, OGL 3.0, OGL-NC
	Distribution	The authorization to share the dataset with others.	CC BY 3.0, CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, CC-PDM 1.0, CC0 1.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL, ODC-PDDL, OGL 3.0, OGL-NC
	Derivative Works	The ability to create new works based on the original dataset, including modifications, adaptations, or enhancements.	CC BY 3.0, CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, CC-PDM 1.0, CC0 1.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL, ODC-PDDL, OGL 3.0, OGL-NC

	Sub-licensing	Granting permissions to third parties to use the dataset under specified terms and conditions.	CC0 1.0, EUPL-1.1, ODC-PDDL, OGL 3.0, OGL-NC
	Use Patent Claims	Permission to utilize any patented technology or intellectual property that includes the dataset.	EUPL-1.1
Obligations	Notice	Requirement to provide clear notification when distributing or redistributing the dataset, including licensing terms and instructions for accessing the complete license agreement.	CC BY 3.0, CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL, OGL 3.0, OGL-NC
	Attribution	Mandate to give appropriate credit to the original provider of the dataset when redistributing, remixing, adapting, or building upon it.	CC BY 3.0, CC-BY 4.0, CC-BY 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL, OGL 3.0, OGL-NC
	Share-alike	Requirement to distribute derivative works under the same or compatible license as the original dataset.	CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL
	Lesser Copyleft	Users must share modifications under the same license but have more flexibility in licensing derivative works.	CC-BY-SA 3.0
	Copyleft	Ensures derivative works or modifications remain open and freely available to others.	CC-BY-NC-SA 4.0, CC-BY-SA 4.0, EUPL-1.1, GFDL-1.3, NLOD, ODC-BY, ODC-ODbL
	State Changes	Obligation to indicate any modifications or adaptations made to the original dataset when redistributing or sharing it with others.	CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, GFDL-1.3
Prohibitions	Commercial Use	Restriction on using the dataset for activities aimed at generating profit, revenue, or financial gain.	CC-BY 4.0, CC-BY-NC-SA 4.0, OGL-NC

Table 5: Summary of license categories and available licensing options.

License Category	Characteristics	Available options
Creative Commons Licenses	Offers a range of permissions for reuse, modification, and distribution, with variations in the extent of restrictions.	CC BY 3.0, CC-BY 4.0, CC-BY-NC 4.0, CC-BY-NC-SA 4.0, CC-BY-SA 4.0, CC-BY-SA 3.0, CC-PDM 1.0, CC0 1.0
Open Data Commons Licenses	Provides open licenses tailored for data, allowing for broad reuse, modification, and redistribution while addressing specific needs of datasets.	ODC-BY, ODC-ODbL, ODC-PDDL

GNU General Public License	Ensures that derivative works remain open and freely available to others, often used for software but applicable to datasets as well.	GFDL-1.3
European Union Public License	Offers permissions for reuse and modification with requirements for sharing derivative works under the same license, designed for EU-funded software but applicable to datasets.	EUPL-1.1
Open Government License	Grants permissions for reuse and redistribution with various versions tailored to different jurisdictions and restrictions on commercial use.	OGL 3.0, OGL-NC
National License for Open Data	Specific licenses implemented at the national level by individual countries to govern the use and reuse of government or publicly funded datasets.	NLOD, HR-OD, FR-LO, DL-DE-BY-NC 1.0, DL-DE-BY 2.0, IODL v2.0

A list of helpful tools and material for helping NAP operators and data providers picking up a right license is provided below:

- <https://choosealicense.com/>
- <https://chooser-beta.creativecommons.org/>
- <https://ufal.github.io/public-license-selector/>
- <https://theodi.org/insights/guides/publishers-guide-to-open-data-licensing/>
- <https://user-guide.opendatasoft.com/en/articles/2045378>

3. Analysis of fair data exchange principles

3.1. Introduction

The rapid development of Intelligent Transport Systems (ITS) across Europe in recent decades has significantly enhanced transport efficiency, safety, and sustainability within EU Member States. As ITS technologies continue to advance, they underscore the necessity for seamless data exchange related to transport across Member States, ensuring that travel and traffic ITS services remain efficient, safe, and interoperable on an EU-wide scale. To facilitate this, the EU introduced the ITS Directive 2010/40 and the amendment 2023/2661, which provides a framework for the coordinated deployment of Intelligent Transport Systems across Member States. Under the ITS Directive, Member States have established National Access Points (NAPs), which act as centralized platforms through which national transport data can be accessed and reused across the EU. These NAPs enable stakeholders—ranging from transport operators to public authorities and private entities—to access standardized, high-quality transport data that supports the effective integration of cross-border ITS services. In this context, NAPs play a crucial role in enabling coordinated transport data exchange, enhancing mobility services, and supporting the broader objectives of a connected and sustainable European transport network.

To ensure that data exchange is effective and supports the continuity of ITS services, interoperability is a fundamental principle. This means that ITS systems, applications, services, and the associated business processes should be designed to exchange data and share information in standardized formats, enabling consistent and effective ITS service delivery across MSs. Interoperability in this context implies not only technical compatibility but also alignment in data formats, protocols, and

data-sharing processes, ensuring that ITS services are accessible and functional regardless of national boundaries. Achieving seamless cross-border data exchange across the EU is thus critical for the success of ITS and the broader goal of an integrated European transport network. For data exchange to be truly effective, it must account for and standardize key elements such as the technologies used, data formats, data interoperability, and reuse policies across stakeholders in different MSs. Harmonization of these factors reduces fragmentation and facilitates smooth data sharing, which is essential for enabling continuous and reliable ITS services.

As per the Public Sector Information Directive (PSI Directive 2013/37/EU), public sector bodies apply charges to cover the expenses associated with the collection, production, reproduction, and dissemination of data. However, it stipulates that these charges should be reasonable, ensuring that public data remains accessible while allowing public entities to recuperate a substantial portion of their costs. The ITS Directive also acknowledges the costs, human resources, and administrative burden associated with the need to minimize the risk of interfering with personal data and providing a sufficient level of data quality. It also considers the importance of these factors when it comes to data exchange, especially by private operators. Specifically, the Real-time Traffic Information Delegated Regulation (RTTI DR 2022/670), does not mandate that private entities share their data at no cost. Instead, the (re)-use of such data can be governed by license agreements.

Another ordinance regarding the cost that may be incurred due to the provisioning and disseminating of travel and traffic data is specified in Article 8 of the Multi-modal Travel Information Services Delegated Regulation (MMTIS DR 2017/1926). This DR mentions that the terms and conditions for using such data can be determined through a license agreement and such conditions should not limit reuse or competition. The license agreement should have minimal restrictions on reuse and any fees should be reasonable and proportionate to the actual cost for providing the data. Furthermore, the Delegated Regulation on Road Safety-related Minimum Universal Traffic Information (DR 886/2013) emphasizes the need to provide universal road safety-related traffic information to users free of charge, wherever feasible. However, the DR acknowledges that some costs may still be incurred, specifically in situations where additional measures are necessary to facilitate the reception of this information. This approach balances the objective of universal access to critical safety information with the practical costs of delivering it, allowing for minimal charges only when absolutely necessary.

It is acknowledged that a harmonized approach to data pricing is important to avoid disparities that could hinder the interoperability and seamless use of intelligent transport systems. By harmonizing data pricing, it should ensure that all providers and consumers of traffic information can participate on parity and have consistent and equitable access to valuable data resources, promoting the availability of quality transportation data across Europe.

Harmonizing data pricing across Europe is an essential step towards safeguarding FRAND (Fair, Reasonable, and Non-Discriminatory) conditions in data exchange, which aim to ensure that license terms are negotiated in good faith and that access to services or data are provided in exchange for a fair reward, with a same or similar condition as those provided to other users. These principles aim to create a balanced market environment where access to data is equitable, fostering innovation and competition. Practical implementation of FRAND involves transparent negotiation processes and the establishment of oversight mechanisms to prevent discriminatory practices. Furthermore, oversight mechanisms are crucial for monitoring compliance with FRAND principles. Regulatory bodies may be involved in setting guidelines and resolving disputes related to data access and pricing. Implementing FRAND principles in data exchange agreements helps to build trust among stakeholders, encouraging more entities to share their data. This leads to richer data pools, which can enhance the quality and scope of ITS services. By ensuring that data pricing and access terms are fair, reasonable, and non-

discriminatory, FRAND principles support the creation of a more integrated and efficient transport ecosystem across Europe.

Finally, the harmonization of data pricing has demonstrated clear benefits. By aligning data costs across regions, it has enhanced data interoperability and facilitated seamless data exchange among different providers. Standardized pricing frameworks allow for fair and transparent access to data, reducing administrative complexity and enabling easier integration of datasets from multiple sources. This consistency in pricing not only promotes broader data usage but also fosters collaboration between public and private entities by establishing a predictable and equitable cost structure.

3.2. Review data pricing models

This section summarizes the main data pricing principles based on a review of previous studies that formulated methodologies and frameworks for determining the valuation of data. Overall, despite the absence of established standards for measuring data value and the lack of a standardized pricing model (Fleckenstein et al, 2023; Yu & Zhang, 2017), numerous studies propose a range of approaches and models for data valuation.

According to Muschalle et al. (2013) and Yu and Zhang (2017), the following pricing models are commonly used in data markets:

1. **Free:** Data can be obtained by the public for free, for example, free statistical data from statistical authorities.
2. **Freemium:** Consumers are provided with a certain amount of data at no cost. However, should they require additional services beyond this limit, they must incur an extra expense.
3. **Usage-based pricing or pay-per-use:** Consumers are charged for data services based on the extent of their usage.
4. **Package pricing:** Consumers have the option to purchase a specified amount of data for a predetermined fixed fee.
5. **Flat-fee pricing:** Consumers pay a flat fee on a monthly or yearly basis, regardless of the amount of data they utilize.
6. **Two-part tariff pricing:** Consumers pay a fixed basic fee up to a certain usage limit, and any usage beyond this limit incurs an additional fee per unit consumed.

Zhang et al. (2023) mention some additional pricing models. **Tiered pricing** is characterized by a reduction in unit price as the quantity purchased by the consumer increases, thereby providing discounts for a larger volume of purchases. This approach serves as a strategic component of marketing and sales by incentivizing large purchases through lower unit costs. **Versioning** involves setting different prices based on different versions of the product, which may differ in terms of functionality, convenience, and operational speed. This model aims to meet diverse consumer needs by offering various product variants at different prices.

Koutris et al. (2015) introduce **query-based pricing**, enabling consumers to make a purchase based on their specific queries. In this model, sellers set prices for only the views requested by the consumers, thereby avoiding the need to establish prices for an extensive catalog of all possible queries.

Huang et al. (2015) propose a **hybrid model** that combines fixed-price reserved services, where the price remains constant, with spot-price on-demand services, where the price might change according to the demand.

However, the existing pricing models have several drawbacks as Yu and Zhang (2017) point out:

1. Lack of a standardized pricing model,



2. Neglect of data quality issues - there are limited data pricing models that consider data quality as an important element,
3. Opaqueness - pricing strategies are mostly provider-driven, with the cost of data processing not being made visible to the consumers.

The first point raises a question on how to define a data pricing method that properly accommodates all the different perspectives as described below. Zhang et al. (2023) propose a new taxonomy of data pricing methods based on the market structure. The classification is divided into three categories:

1. Sell-side Market: In this market, data prices are determined based on the utilization of the information derived from the data. The value is assessed using metrics such as quality, volume, and accuracy of the generated information. In the case of data services, the sell side market is further categorized based on the query type, e.g., null queries, one-off queries, and general queries.

- Null queries: Requests that yield no data or return an empty result. While they do not provide useful information, they can still incur minor processing costs due to resource allocation. Pricing for null queries may be minimal or absent, reflecting their limited utility, as these queries do not add informational value but might be tracked for service monitoring or system efficiency.
- One-off queries: Requests that retrieve data for immediate, specific needs without recurring access. In the sell-side market, pricing for one-off queries typically reflects the immediate value of the information provided, with costs based on the data's quality, volume, or accuracy.
- General queries: They provide access to broader datasets and may be used on an ongoing basis for continuous data needs. In the sell-side market, general queries are often priced higher, given the sustained and comprehensive access they provide.

2. Buy-side Market: In this market, the value of data is determined by the potential monetary loss that could occur due to privacy breaches. Data brokers set the prices according to the data owner's privacy preferences and the privacy loss incurred. The buy side market is classified according to the concept of privacy, which defines how individuals or groups control access to their personal data. Different privacy notions include:

- Differential Privacy: A mathematical mechanism to limit individual information disclosure from aggregate data, thereby protecting individual privacy.
- Ad Hoc Notions: Privacy notions used in specific scenarios, such as anonymization, are tailored to the requirements of the context in which they are applicable.

3. Two-sided Market: In this market, the value of data is determined by both the usage of the information and the privacy loss. The data brokers sell data for its intrinsic informational value while compensating data owners for their privacy loss. Therefore, they must balance the cost of acquiring data with the profit from selling it. The two-sided market is further categorized into, Null Queries and Ad Hoc Privacy Notion, One off Queries and Differential Privacy, and General Queries and Differential Privacy.

- Null queries and Ad Hoc privacy notion: In a two-sided market refer to data requests that yield no actual data (null queries), with privacy managed through flexible, context-specific rules (ad hoc privacy). In this market, data brokers still provide and price null queries, which have limited informational value but may involve privacy considerations, especially when the mere act of querying has implications for privacy. The ad hoc privacy notion

allows brokers to handle privacy flexibly, reducing unnecessary protections where they are not needed while still managing privacy risks.

- One off queries and differential privacy: This refers to single-use data requests in a two-sided market, where a data broker provides a one-time answer to a specific query from a consumer, with privacy protected through differential privacy. Differential privacy adds noise to the query result, masking individual data points to prevent re-identification and safeguard privacy. This approach reduces accuracy slightly, creating a trade-off between protecting data owners and maintaining data utility for consumers. The broker must balance this trade-off by adjusting prices: data owners with higher privacy requirements are compensated less, while consumers desiring higher accuracy pay more.
- General queries and differential privacy: In a two-sided market involve ongoing data access, where a data broker sells broader, repeated data queries to consumers while using differential privacy to protect data owners. Here, differential privacy ensures individual data points remain anonymous by adding noise to results, balancing privacy protection with data utility. This model faces a complex trade-off: the broker must compensate data owners for privacy loss while setting consumer prices that reflect the continuous informational value of general queries.

Zhang et al. (2023) study introduces a new taxonomy of data pricing, emphasizing the core value of data. Since the data hold value on both sides of a marketplace, and thus, they base their taxonomy on the market structure. The data value is assessed differently depending on query types and privacy notions; hence the query type was utilized to evaluate the data value on the sell side and privacy notions on the buy side.

Regarding the issue of neglecting data quality when designing a data pricing model, several studies attempt to identify characteristics and dimensions to evaluate data as an asset. One of them was performed by Viscusi and Batini (2017), who compiled prior studies classifying data characteristics and dimensions to propose a model for digital information asset valuation (**Figure 2**). Their study defines factors such as information quality (**accuracy, completeness, accessibility, relevance, timeliness**), information structure, information diffusion, and information infrastructure as complex characteristics of information capacity. Information diffusion (scarcity, sharing) influences information utility as the information flow and exchanges occur through selected business processes using specific queries. Together with the information utility, which determines the data's financial value and transaction cost, the information capacity is identified as the core component of information value.

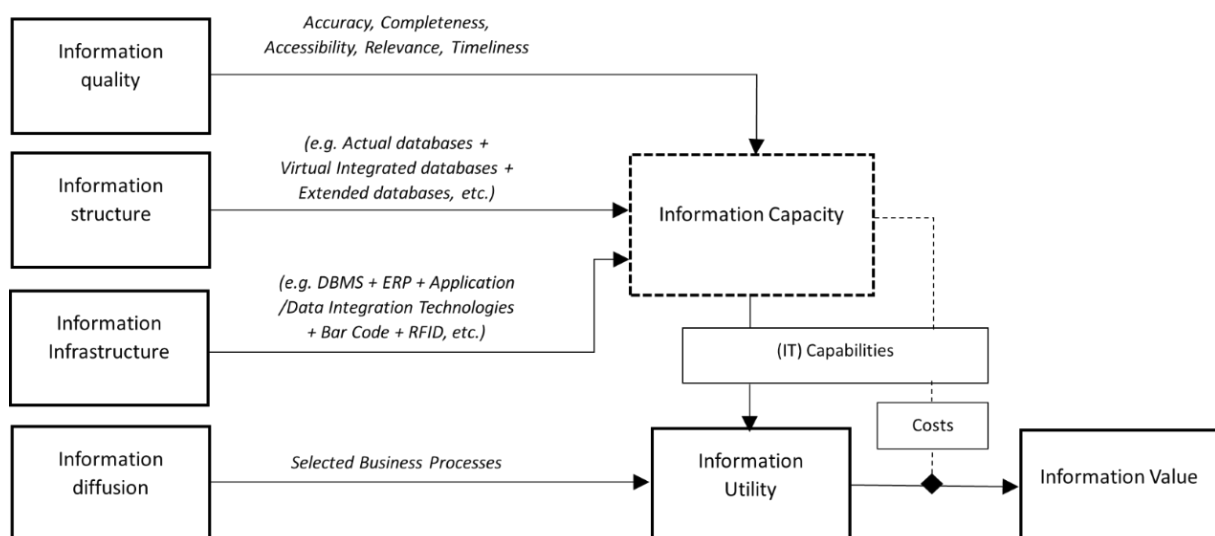


Figure 2: Viscusi and Batini (2017) Proposed model for digital information asset evaluation

Fleckenstein et al. (2023) recommend a framework that groups prior studies of data valuation approaches into three models: **market-based valuation**, **economic models**, and **dimensional data valuation**. Their dimensional data valuation approach assesses specific data by considering intrinsic factors such as data quality (**completeness, accuracy, timeliness, consistency**), and contextual factors such as **usage** and **ownership**. The final set of Fleckenstein et al. data dimensions can be seen in **Figure 3**.

Dimension	Description
Ownership	Addresses outright data set ownership plus licensing restrictions and service agreements
Cost	Addresses the cost of data set acquisition, maintenance, and replacement
Usage	Addresses dataset mission criticality, ability to integrate, usage scope, usage frequency, metadata, additional resources, expected increase in demand, and diminishing value
Age	Addresses refresh rate and available history
Privacy	Addresses whether the dataset contains sensitive data such as Personally Identifiable Information (PII) and Protected Health Information, and meets privacy standards
Data quality	Addresses completeness, accuracy, currency, consistency, duplication, trustworthiness, and timeliness
Volume and variety	Addresses the number of records, scope of information for each record, and ability to answer needed questions

Figure 3: Fleckenstein et al (2023) Data Valuation Dimension

They conducted a survey with questions on different data dimensions (**ownership, cost, utility, age, privacy, data quality, volume, and variety**) and then examined it with different stakeholders to understand how they might score different questions accordingly based on their own perspectives. Their scoring system shows the relative value of data sets, highlighting both clear and indistinct differences. They concluded that their model served well as a basic reference for assessing data set value through scores, but the weighting of these scores can change depending on the context and perspective of the stakeholder.

Heckman et al. (2015) in their study touch on the topics of data quality neglect in data pricing models and the opaqueness of pricing strategies. According to Heckman et al. (2015), when transparency is not present, there is room for the parties involved in the transactions to be misled. This condition creates the “market for lemons” condition, a term originated by economist George Akerlof. In this situation, sellers know more about their products than the buyers do, allowing them to demand higher prices for low-quality data. Consequently, consumers become cautious and reluctant to make purchases, fearing they might overpay for substandard data. This could drive away sellers of high-quality data, leaving inferior products in the market. To address this issue, they emphasize the importance of data valuation to develop a clear and fair pricing model.

Heckman et al. (2015) mention that the data characteristics that can give an impact to the value of data can be divided into three parameters:

- a. **Value-based parameters** (value data to the consumers)
 - Time, effort, or money savings
 - Return on investment (ROI) for the consumer
 - Risk exposure (data cleansed of personally identifiable information and privacy violations could be priced higher)
 - Data exclusivity (whether data is provided on an exclusive or non-exclusive basis, or a combination of the two would influence price)
 - Level of ownership (buying, leasing, or licensing)
- b. **Qualitative parameters** (attributes or meta-attributes of the dataset)
 - Age of data
 - Credibility

- Scarcity
 - Accuracy of the data elements
 - Volume of data
 - Quality (e.g., missing fields, incorrect types, data precision, etc.)
 - Format and level of structure (plain text, streaming data, tabular datasets, etc.)
- c. **Fixed and Marginal cost parameters** (directly measurable cost).
- Cost of collecting data
 - Storage, bandwidth, and other operational costs
 - Cost of data-as-a-service offerings (e.g., processing, computing resources, analytic reports, or aggregation of the data)
 - Delivery cadence (one time, batch, or continuous basis)

Based on the above parameters, a survey measured the qualitative parameters. Their preliminary survey identified how participants valued the importance of different data characteristics by calculating the Mean Importance Rating (MIR) from survey responses. Heckman et al. (2015) also suggest a more thorough qualitative research, including interviews and larger, more focused surveys, for a more comprehensive understanding.

According to Heckman et al. (2015) to develop the model, it is important to investigate factors affecting data value. A sufficient number of sample datasets with their prices and attributes are also essential to be collected, ideally diverse in size and originate from various industries and utilization. A general linear model they propose can be expressed as below, even though it should be stated that building out a model is not a straightforward task, and it could have many variations:

*Estimated value of data = fixed cost + β_1 * age of data + β_2 * Periodicity of data + β_3 * Volume of data + β_4 * Accuracy of data+...*

Selecting the appropriate model depends on the specific context. Each model is most effective under certain circumstances and no single model is universally applicable (Fleckenstein et al., 2023). Depending on the context, a combination of different models might be suitable.

Considering the above literature review, a survey has been designed to obtain insights from data providers (both public and private) and data consumers regarding their data pricing strategies preferences within the transport data sector.

3.3. Survey design

Building on the principles and models of fair data exchange discussed in previous subsection, our approach within this task was to gain a deeper understanding of the preferences and priorities of both data providers and consumers. The complexities surrounding data exchange topic, the diversity of existing pricing models, and the specific needs of public and private entities, all underscore the necessity for an approach that captures real-world perspectives and practices on the conditions for fair and reasonable data exchange. Recognizing this need, we designed and circulated a tailored survey targeting three main stakeholder groups: (a) data consumers, (b) private data providers, and (c) public data providers. The survey was specifically structured to address the specific perspectives of each group. For data consumers, the questions aimed to gain insights into their “Willingness-to-Pay” approach, exploring the value they place on the factors influencing their purchase decisions. For private data providers, the survey focused on identifying key elements that shape their pricing strategies, preferences, and any other competitive considerations. Finally, for public data providers, the emphasis was on understanding the various costs associated with making their datasets available on NAPs considering the provisions of the PSI Directive 2013/37/EU (see Section 3.4).

3.4. Survey results (public data providers)

This section presents the survey findings based on responses from various stakeholders across the transport data domain. The survey was distributed to Advisory Board members and task-involved members of NAPCORE, who were encouraged to circulate it further within their networks. A total of 17 responses were received from different MSs (BE, HU, LV, NL, NO, DK), including 10 fully completed and 7 partially completed surveys. The majority of responses came from public data providers (15), while data consumers provided 2 responses. Unfortunately, no responses were received from private data providers. In this analysis, we present the results for questions that received a sufficient number of responses to ensure representativeness. Questions with no responses or very few responses were excluded in order to not influence the representativeness of the results.

3.4.1. Descriptive survey results

Starting with the questions posed to public data providers, the initial one focused on the number of datasets they currently make available on NAPs (datasets that are provided through the NAP platform). As shown in **Figure 4**, the results indicate that 10 public data providers offer more than five datasets through the NAPs, while 2 providers offer between one and two datasets, and only 1 provider offers between two and five datasets.

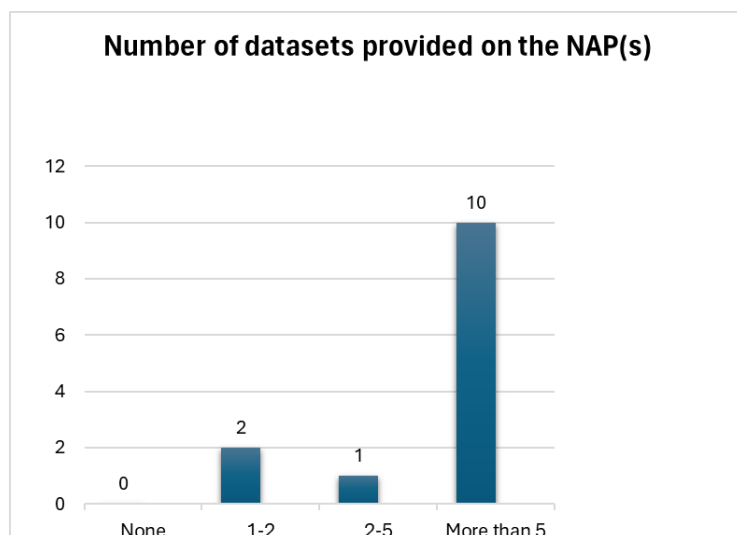


Figure 4: Number of provided datasets

Consequently, next question was related to the Delegated Regulations supplementing the ITS Directive. Public data providers were asked to declare the DR that is relevant to the datasets that they provide on NAPs. **Figure 5** indicates that 7 public data providers offer datasets relevant to the SSTP DR, while 9 providers include datasets that pertain to both the SRTI and RTTI DRs. Additionally, 7 providers make available datasets corresponding to MMTIS.

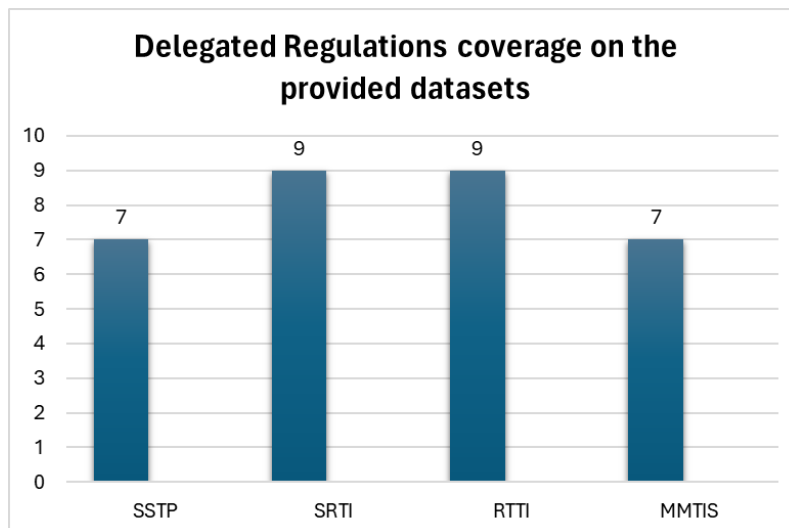


Figure 5: Delegated Regulations in relation to the provided datasets

In addition, public data providers have reported that the datasets they provide on NAPs cover a wide range of both static and dynamic data types. This includes static road attributes, road network details, locations and usage of parking places, road events, routing instructions, speed limits, common standard fares, open data API and national dataset for public transport information. Additionally, one responder mentioned that beyond the mandatory datasets associated with the SSTP, SRTI, RTTI, and MMTIS DRs, they provide also data with CO2 emissions as well as voluntary mobility datasets which hold public value.

The next question sought to identify the specific cost categories that public data providers incur when making their datasets available on NAPs, in alignment with the cost considerations acknowledged in the PSI Directive (2013/37/EU). Based on existing literature, the costs associated with providing mobility data on platforms like NAPs were divided into several categories:

- **Data collection and processing costs:** Expenses for gathering, formatting, and processing data to make it suitable for publication, often involving equipment installation.
- **Data exchange infrastructure costs:** Investments in IT infrastructure, including servers and storage systems, to facilitate data hosting and dissemination.
- **Data management and quality assurance costs:** Expenses related to on-going monitoring and quality assurance processes. This may involve employing data specialists or implementing automated systems to detect and correct errors in the data.
- **Security and privacy compliance costs:** Costs related to adhering to security and privacy regulations, including encryption, access controls, and regular compliance audits.
- **Licensing and intellectual property costs:** Fees for obtaining rights to proprietary data or intellectual property, where applicable, which may involve third-party agreements.
- **Promotion and outreach costs:** Investments in raising awareness of available datasets, which may include marketing and training to encourage data use and innovation.
- **Technical support and maintenance costs:** Resources dedicated to supporting data users, addressing technical issues, and updating data interfaces to meet evolving standards.

Therefore, public data providers were asked to indicate which of these cost categories were relevant to their operations, providing also insight into the magnitude of costs associated with those cost categories.

3.4.2. Validity of prespecified cost categories



Figure 6 illustrates that the majority of respondents identify “Technical support and maintenance costs” (7 responses), “Data exchange infrastructure costs” (7 responses), and “Data collection and processing costs” (7 responses) as relevant cost categories. Additionally, “Data management and quality assurance costs” and “Security and privacy compliance costs” are also recognized by 6 respondents. Promotion and outreach costs were acknowledged by 4 respondents, indicating that a smaller subset of providers invests in raising awareness and encouraging the use of their datasets. Licensing and intellectual property rights costs were identified by only 3 respondents, suggesting that these costs are less commonly incurred among public providers. Finally, one respondent indicated that none of the listed cost categories were applicable to their operations.

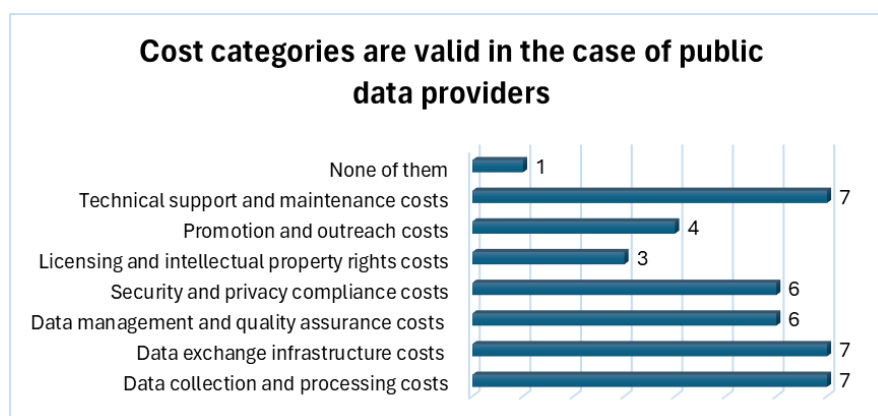


Figure 6: Cost categories are valid in the case of public data providers

3.4.3. Magnitude of costs

Figure 7 to **Figure 13** provide an overview of the cost magnitudes associated with the various categories for public data providers in making datasets available on NAPs.

Data collection and processing costs (**Figure 7**) are reported as moderate by 3 providers, while 2 providers noted high and very high costs. Finally, one provider reported low costs.

Figure 8 related to data exchange infrastructure costs indicates that the majority of respondents (4 providers), mentioned low costs for data exchange infrastructure, while 2 reported moderate costs. High and very high costs were each reported by 1 provider.

For the next category, data management and quality assurance costs, (**Figure 9**) 3 providers each reported moderate and high costs, while 1 provider noted very high costs and 1 indicated very low costs.

In security and privacy compliance costs category, (**Figure 10**) most providers, 6 in total, identified security and privacy compliance as a moderate-cost category, while 2 providers reported low costs. No responses indicated high or very high costs, suggesting that compliance is typically a moderate expense.

For the subsequent category, licensing and intellectual property rights costs, (**Figure 11**) most providers (4), have selected the moderate option, while 2 providers indicated very low costs and 1 reported low costs.

For the promotion and outreach cost category, (**Figure 12**) 3 providers have reported moderate costs, 2 have indicated very low costs, 1 has reported low costs, and 2 selected “not applicable”.

In the final category, technical support and maintenance costs, (**Figure 13**) 5 providers reported moderate costs, while 2 providers noted low costs and 1 indicated very low costs.

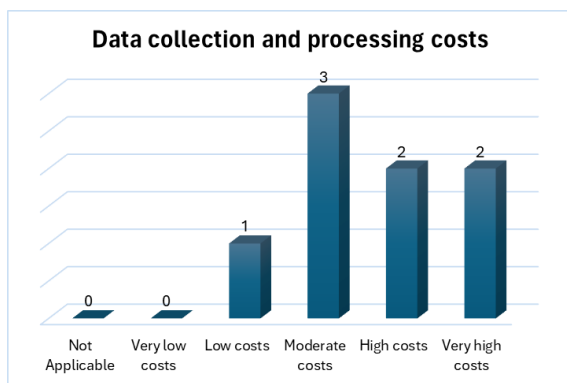


Figure 7: Data collection and processing costs

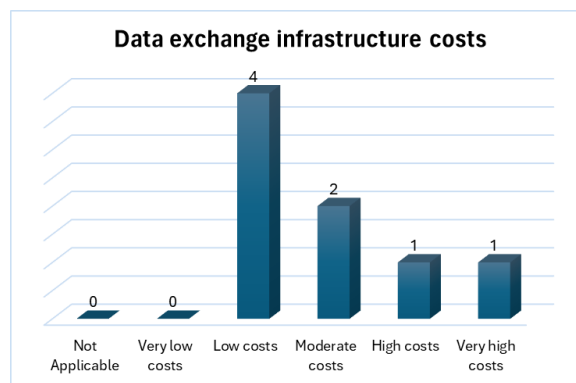


Figure 8: Data exchange infrastructure costs

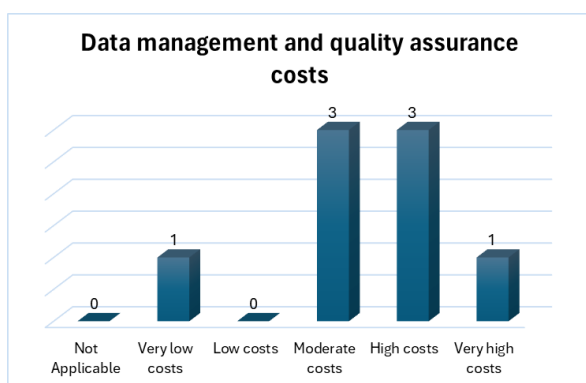


Figure 9: Data management and quality assurance costs

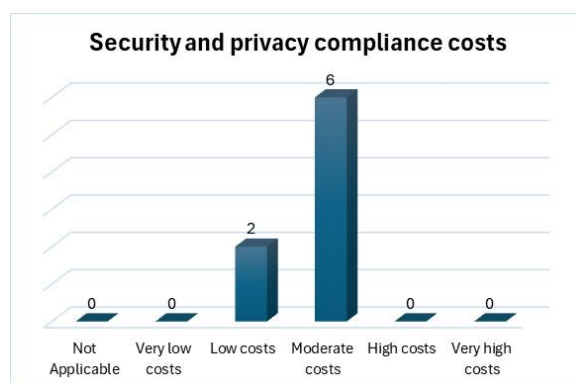


Figure 10: Security and privacy compliance costs

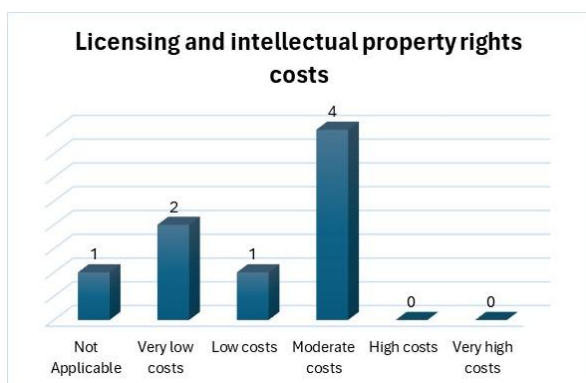


Figure 11: Licensing and intellectual property rights costs

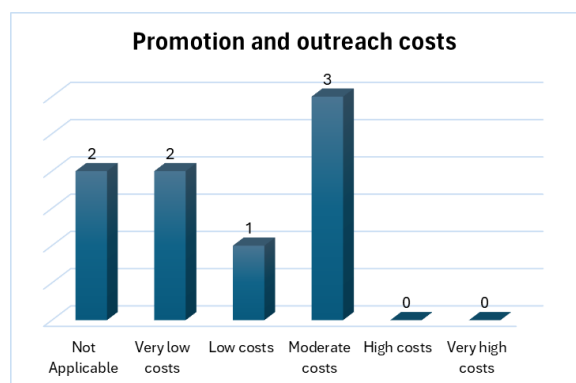


Figure 12: Promotion and outreach costs

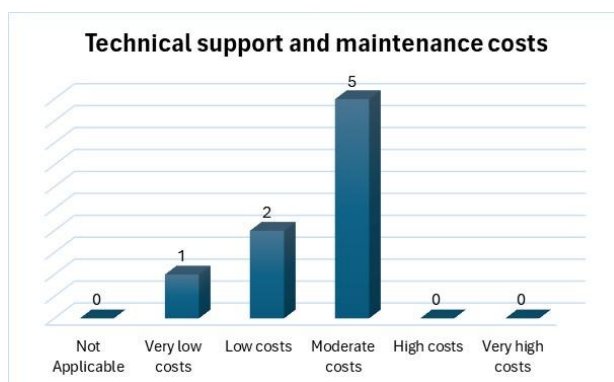


Figure 13: Technical support and maintenance costs

Another question posed to public data providers was to describe the main challenges they face in relation to the identified cost categories. The responses highlighted several recurring issues. One significant challenge is the coordination between public transport operators (PTOs) and authorities through bi-lateral meetings, which is essential for correctly interpreting and implementing delegated

acts at both national and European levels. Another key challenge lies in knowledge management around data standards, as providers should stay up to date with evolving standards and ensure compliance. Additionally, data providers pointed out the gap between the legal language in regulations and the specific technical requirements needed for implementation. This requires extra resources to interpret the legal texts and adapt them into actionable technical specifications. Other notable challenge includes the recurrent costs of technical support and maintenance, which are often underestimated but necessary to maintain the infrastructure over time. Finally, data management and quality assurance were highlighted as one of the most demanding aspects, requiring both significant resources and attention to detail to maintain high data quality and reliability.

The next question that was asked to public data providers is whether they had observed any differences in costs associated with different types of provided data, such as real-time, static, or historical datasets. Some responders reported that they do observe cost variations among these data types. Specifically, real-time data was frequently noted as more costly due to the need for continuous collection, processing, and immediate distribution, which requires robust infrastructure and higher maintenance efforts. In contrast, static and historical datasets generally incur lower costs, as they are often collected periodically rather than in real-time and do not demand the same level of continuous technical support.

With the following question we tried to explore how public data providers currently determine the cost for their datasets, specifically asking about the factors and criteria considered when setting prices. All respondents reported that for the time being, they provide all datasets free of charge.

The final two questions aimed to understand the preferences of public data providers regarding the permissions they grant to data consumers and the obligations they enforce. **Figure 14** illustrates the preferred permissions granted to data consumers. Distribution was the most frequently selected option (4 public data providers). Reproduction was chosen by 3 data providers, while derivative works was selected by 2 data providers. Notably, no data providers chose Sub-licensing or Use of patent claims, suggesting limited willingness to allow data consumers to extend permissions to others or utilize any patented technology associated with the datasets (or the lack of patented technologies in the provided data services).

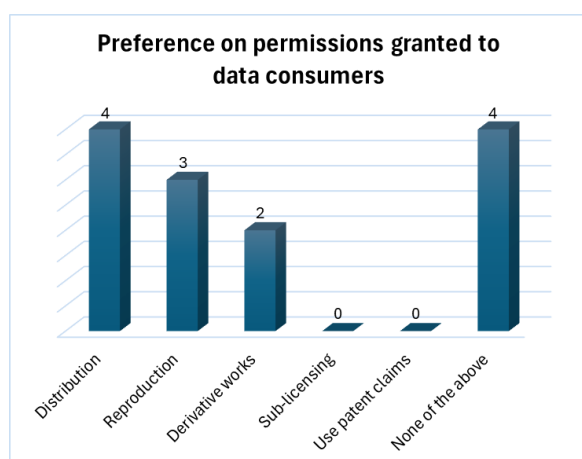


Figure 14: Preference on permissions granted to data consumers

Figure 15 represents the preferred obligations enforced on data consumers. Attribution was the most common choice, with 4 data providers indicating a preference to require consumers to credit the original data source. Notice was selected by 2 data providers, requiring data consumers to notify them once they give rights for usage to others. Share-alike was chosen by 1 data provider, enforcing that derivative works be shared under similar terms. Obligations such as Lesser copyleft, Copyleft, and State

changes were not selected by any providers. Finally, 3 data providers indicated that none of the above licenses is preferable to enforce conditions to data consumers.

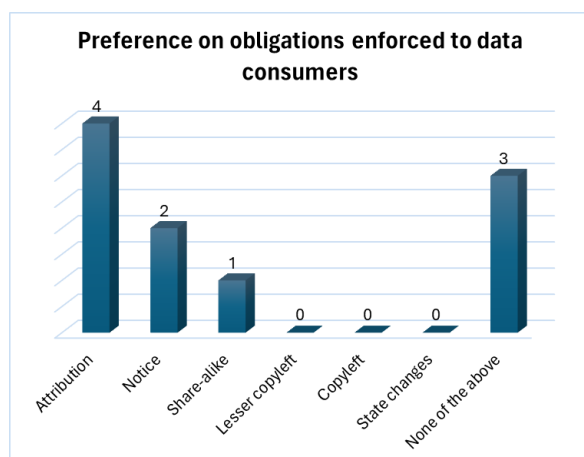


Figure 15: Preference on obligations enforced to data consumers

The final question sought to understand whether public data providers generally prefer to restrict certain actions or uses of their datasets by data consumers. Some respondents indicated a preference for prohibiting commercial use of their datasets, while others did not indicate any special preference.

3.5. Survey results (data consumers)

The subsequent questions involve the part of the WG3 survey targeting data consumers, asking them to select options that best matched their preferences. Two data consumers answered this survey. Each question was structured around two options as shown in the **Figure 16**.

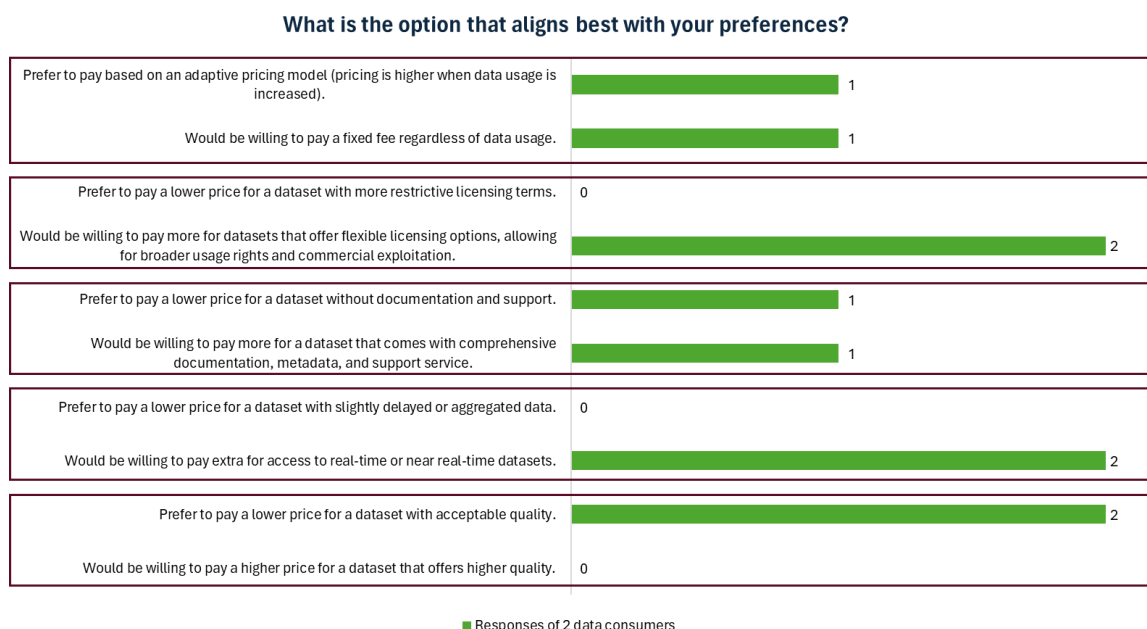


Figure 16: Responses of the two data consumers

Hence, **Figure 16** illustrates the preferences of the two data consumers regarding various options for data pricing and usage conditions, organized into five building blocks.

Starting from bottom to top, the answers to the first question group shows that both consumers prefer to pay a lower price for datasets with acceptable quality rather than a higher price for datasets offering

higher quality. Additionally, the first data consumer emphasized that part of private service provider's role is to enhance and enrich the data they acquire to create valuable outputs for their users. This data consumer indicated that they do not necessarily require high-quality data at the source because their services add value to the data through processing and integration. The second data consumer highlighted that the term "acceptable quality" might have different interpretations across countries, suggesting that what is considered "acceptable" in the one MS could differ from the standards of other EU MSs.

The answers to the second question group reveals that both data consumers are willing to pay extra for access to real-time or near real-time datasets, indicating a strong preference for timely data delivery, over slightly delayed or aggregated data. However, their specific comments highlight different perspectives on when real-time data is necessary. The first data consumer explained that the importance of real-time data depends on the data type and its application. For example, real-time data is crucial for dynamic speed limits, where immediate updates are necessary for effective traffic management. Conversely, in cases such as long-term roadworks, some delay in data updates may be acceptable. The second consumer noted that they already have access to near real-time public datasets through a "data for data" scheme, with no associated payments. In case that there were additional costs for using public data in their services, these expenses would be passed on to their clients.

The answers to the third question group addresses preferences related to documentation and support. Here, one data consumer was willing to pay more for datasets that included comprehensive documentation and support, emphasizing that this would save time and resources otherwise spent on self-directed knowledge gathering, testing, or re-engineering. In contrast, the other data consumer preferred to pay a lower price for datasets without documentation and support, as long as the data adhered to established standards, such as DATEX II. It was also noted that when the data complies with widely accepted formats additional documentation is not needed, as existing standards provide sufficient guidance themselves.

The answers to the fourth question group pertains to licensing flexibility, with both data consumers expressed a preference for paying more for datasets that offer flexible licensing options, allowing for broader usage rights and the possibility of commercial exploitation. Furthermore, one of the data consumers clarified that although they would pay extra for flexible licensing, those additional costs associated with using public data for their services would be transferred to their clients.

Finally, the answers to the fifth question group shows a split preference for pricing models, with one data consumer preferring a fixed fee regardless of data usage while the other expressed his/her desire for an adaptive pricing model where costs increase with data usage. In one of the data consumers' comments, it was explained that typically, pay-per-use pricing model is more cost-efficient for their data service needs, because it allows them to pay only for the amount of data they actually use.

Subsequently, in the next set of questions, data consumers were asked about their preferences regarding the permissions they would like to have when consuming datasets and obligations they would prefer to avoid. In **Figure 17**, the two data consumers provide insights into the permissions they prefer. Both respondents expressed a preference for the right to distribute, create derivative works, and sub-licensing, highlighting their need for flexibility in sharing and modifying datasets within their own services. One data consumer noted also the importance of reproduction, which allows them to manage access to the data in their own backend systems, improving data handling and usability internally. Use patent claims was not selected, indicating that this option is less relevant to their requirements. In **Figure 18**, the focus shifted to the obligations that data consumers would prefer to avoid. Share-alike and copyleft were marked as the least desirable obligations by both respondents,

reflecting a preference to avoid restrictions that would require them to share modifications or derivatives under the same or open licenses. Additionally, notice, attribution, lesser copyleft, and state changes were selected by one respondent each.

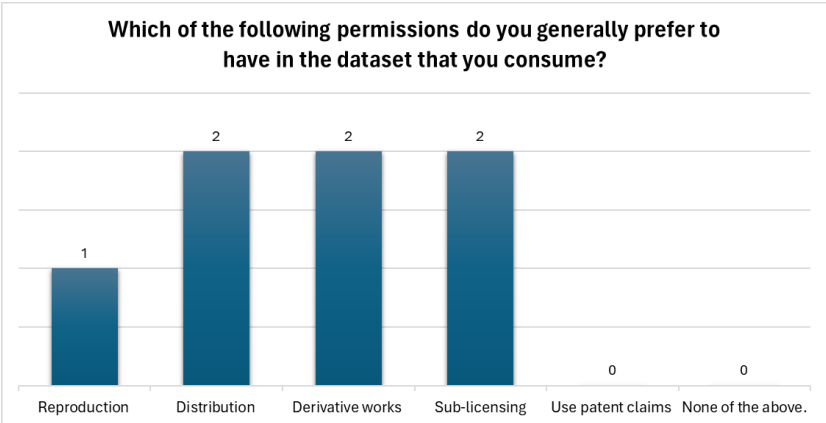


Figure 17: Preferences of data consumers in terms of permissions

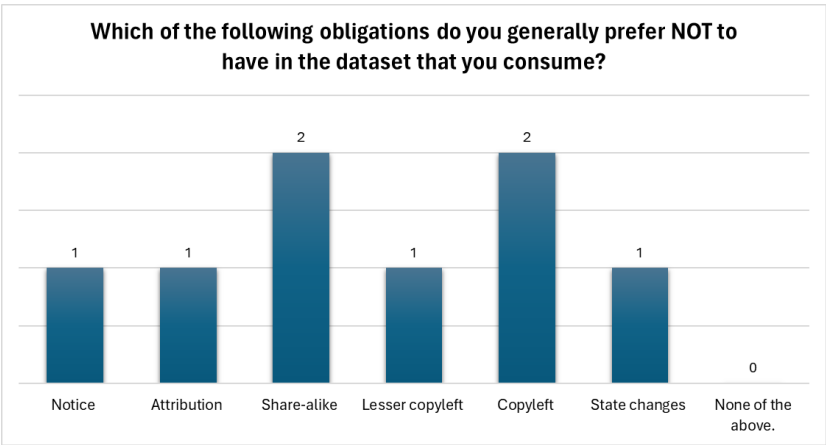


Figure 18: Preferences of data consumers in terms of obligations

3.6. Discussion

This section seeks to analyse the results of the previous subsections and highlight the key implications. One of the most significant takeaways that survey revealed from the perspective of public data providers is that technical support and maintenance emerged as one of the most pressing cost categories. Maintaining the infrastructure necessary to support data exchange via NAPs requires continuous investment. This includes not only ensuring that the systems remain operational and secure but also managing updates to comply with evolving technical standards, regulations, and legislative requirements. Therefore, the need to comply with evolving regulations adds another layer of complexity and cost to public data providers. In addition, technical support is essential to resolve any issues that users encounter when accessing or using datasets. These costs are ongoing, driven by the requirement to keep NAPs functional, secure, and interoperable across MSs. Moreover, the costs associated with data collection and processing emerged as another major concern, particularly given the extensive resources required to gather, standardize, and format data for public access. Hence, public data providers should be supported in investing in the necessary infrastructure as well as in staff and resources for processing the raw data into standardized formats that meet the technical and regulatory requirements. The importance of these processes is clear: ensuring that the data is accurate, timely, and of high quality. Similarly, to these upfront investments, data exchange infrastructure costs emerged as another area of significant expenditure. This includes the necessary



investments in the IT systems that allow for the storage, distribution, and secure data handling through NAPs. The importance of a robust infrastructure cannot be overstated, especially as the demand for real-time datasets increases. The infrastructure must be scalable to handle increasing data volumes, particularly as more dynamic data streams. The challenge for public data providers lies in maintaining the technical and security standards required to keep this data flowing smoothly, while also ensuring that the platforms remain accessible and reliable for users.

From the perspective of data consumers, the survey results indicate a preference for flexibility in both data charging and licensing. However, with participation from only two data consumers, the findings cannot be considered a comprehensive representation of the broader data consumer community. Therefore, while these responses provide valuable insights into perspectives of some data consumers, they do not offer a sufficient sample size to draw definitive conclusions about the preferences and behaviors of data consumers across the EU. Hence, in this section, we focus only on the insights gathered from the two available responses. Data consumers indicated a strong desire for flexible licensing terms that allow for reproduction, distribution, and the creation of derivative works. This reflects a broader trend where data consumers require the ability to adapt and build upon the data they use. This flexibility is particularly valuable for service providers who need to adapt the data for several applications and services. However, despite the willingness to pay more for flexible usage rights, data consumers still prioritize affordability. This is particularly evident in their preference for paying less for datasets with acceptable quality, rather than paying more for datasets that offer higher quality. This finding highlights that data consumers may be willing to strike a balance between cost and quality, where “acceptable” quality still meets their needs in many cases. This is especially true given that the definition of “acceptable quality” may vary between countries. This underscores the practical approach of data consumers, who are focused on obtaining data that is both functional and cost-effective, while maintaining the flexibility to tailor it to their specific needs and operational contexts.

4. GDPR in the NAP context

4.1. Introduction

The General Data Protection Regulation (GDPR) is a comprehensive legal framework enacted by the European Union (EU) to standardize data protection and privacy across its MSs and the European Economic Area (EEA). Effective as of May 25, 2018, GDPR imposes strict requirements on organizations regarding the processing of personal data, with its jurisdiction extending globally to any entity handling the personal data of EU residents. The regulation mandates precise adherence to several core principles, including lawfulness, fairness, transparency, data minimization, and accountability, which govern the collection, storage, and usage of personal data.

GDPR aims to enhance data subject rights, ensuring people have greater control over their personal data while compelling organizations to implement robust data protection measures such as the ones mentioned above. Non-compliance can result in substantial penalties; as a result, GDPR has established itself as a critical standard for data governance, requiring a technical and legal alignment to ensure full compliance with its provisions across all facets of data processing.

4.2. Basic principles of GDPR

4.2.1. Lawfulness

The principle of lawfulness requires that all personal data processing must have a legitimate legal basis. Organizations must ensure that data processing is grounded in one of the six legal bases: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public



interest, or legitimate interest. The selection of an appropriate legal basis must be explicit, and organizations must be able to justify the legality of their processing activities in accordance with the selected basis. If consent is used, it must be informed, freely given, and withdrawable at any time, necessitating robust consent management systems. Organizations must assess and document the legal justification for each processing activity to ensure compliance.

4.2.2. Fairness

The principle of fairness ensures that personal data is processed in a manner that is not misleading, deceptive, or harmful to the data subject. Processing activities must be conducted with the interests of the data subjects in mind, ensuring they are not exploited or disadvantaged by the use of their personal information. Organizations are required to process data in ways that are consistent with the expectations of the data subject, respecting their rights and freedoms. Fairness also necessitates that data controllers assess the potential negative impacts of data processing and implement safeguards to mitigate risks to the individuals involved.

4.2.3. Transparency

The transparency principle mandates that data subjects are provided with clear, accessible, and understandable information about the processing of their personal data. This includes informing individuals about the identity of the data controller, the purposes of the processing, the legal basis for processing, recipients of the data, and the data subject's rights. Transparency is critical to maintaining the trust of data subjects, as it ensures they are fully aware of how their personal data will be used, stored, and shared. Organizations must provide privacy notices that adhere to the GDPR's transparency requirements and ensure that communication with data subjects is consistent, timely, and unambiguous.

4.2.4. Data Minimization

The principle of data minimization limits the collection and processing of personal data to what is strictly necessary for the specified purposes. Organizations are required to assess the relevance and necessity of each piece of data they collect and to ensure that only data that directly supports the intended purpose is processed. This principle helps reduce the risks associated with excessive data collection, such as unauthorized access or misuse. Data controllers must establish strict internal policies to ensure continuous adherence to this principle, including regular reviews to eliminate unnecessary data from their systems and processes. By limiting the data footprint, organizations can also reduce compliance costs and mitigate the risk of data breaches.

4.2.5. Accountability

The principle of accountability holds organizations responsible for both their compliance with GDPR and their ability to demonstrate this compliance. Organizations must implement and document data protection measures, including technical and organizational safeguards, to ensure that GDPR obligations are met. This includes maintaining records of processing activities, conducting Data Protection Impact Assessments (DPIAs) where appropriate, and having mechanisms in place to monitor compliance on an ongoing basis. The appointment of a Data Protection Officer (DPO) may be necessary in certain contexts, ensuring dedicated oversight of GDPR adherence. Accountability requires that organizations not only comply with the law but are able to provide evidence of their compliance at any time, ensuring a proactive and structured approach to data protection.

4.3. GDPR in relation to NAPs



Given that NAPs operate at the core of data-driven transport services, the relevance of GDPR lies in the handling of personal data throughout various stages, including user registration, data provision, and data consumption. For instance, when a user registers on a NAP platform (when a NAP operates as a database architecture and not metadata directory), their personal information (e.g., name, contact details, and potentially location data) is collected and stored. Similarly, in some cases, accreditation processes for becoming a data provider or consumer may involve processing identifying information, which falls under the scope of GDPR.

Moreover, any interaction between users and the platform, such as accessing data, logging activities, or participating in the data exchange process, may involve tracking or storing user-specific information, further stressing the platform's responsibility to safeguard personal data integrity. Operational activities, such as user authentication and platform access control also necessitate adherence to GDPR, particularly in ensuring data subjects' rights are preserved during these processes. The technical infrastructure and workflows of NAPs must therefore align with GDPR principles, ensuring that personal data is processed lawfully and securely at all stages of platform interaction. Given that NAP is not responsible for the data holders' content, the compliance to GDPR might be sought through a claim of the data holders that exchanged content is "GDPR compliant".

Additionally, data must be relevant and limited to what is necessary for the purposes for which it is processed, accurate, and up to date, with mechanisms in place for rectifying any inaccuracies. For instance, it does not make much sense to request information during the registration process or as a part of publisher metadata that is not useful for communication reasons. Data should only be kept for as long as necessary and must be protected against unauthorized access or accidental loss, through appropriate technical and organizational measures, such as encryption and pseudonymization techniques. Controllers and processors of data are required to implement and maintain robust technical and organizational measures to ensure GDPR compliance. They must maintain detailed records of processing activities and are responsible for ensuring that any third-party data processors they engage follow GDPR standards. Controllers and processors are also responsible to conduct regular audits and assessments to ensure the security of the processing.

A Data Protection Impact Assessment (DPIA) is necessary when processing operations pose a high risk to individuals' rights and freedoms. This assessment involves evaluating the risks and necessary measures to mitigate them. Additionally, the controller and the processor must appoint a Data Protection Officer (DPO) when their core activities involve regular and systematic monitoring of data subjects on a large scale or involve large-scale processing of special categories of data, or when the processing is carried out by a public authority. The DPO's responsibilities include advising on compliance, monitoring adherence to GDPR, and acting as a liaison with supervisory authorities.

Transfers of personal data to third countries or international organizations are permitted only if the destination ensures adequate data protection, as determined by the EU Commission.

Responsible authorities in each MS, including nominated National Bodies, shall monitor GDPR compliance, acting with complete independence and cooperating with each other and, where relevant, with the Commission. Their tasks include investigative, corrective, authorisation and advisory activities.

Finally, GDPR allows for some flexibility in processing data for archiving research or statistical purposes, while maintaining safeguards to protect individuals' rights and ensuring respect for the principle of data minimization.

4.4. Existing approaches and best practices

This section will explore the existing approaches and best practices for ensuring compliance with the GDPR within the context of NAPs across Europe. This analysis mostly focuses on user data used by NAPs (e.g., information provided during the registration process) instead of data that are not strictly under the responsibility of NAP operators. As NAPs facilitate the exchange of transport related data between various stakeholders, including public authorities, private entities, and the general public, they should implement effective measures to protect personal data in line with GDPR principles. Best practices from selected NAPs provide valuable insights into how these platforms can manage personal data while maintaining the security, fairness, lawfulness, data minimization, transparency, and accountability required under GDPR. The examples presented below will serve as a foundation for improving data governance and ensuring that NAPs remain compliant with GDPR in the evolving transport landscape.

4.4.1. The case of the German NAP

The German NAP “Mobilithek” has established various measures to handle GDPR rules in its platform. These measures are implemented at several key stages of user interaction and data provision. For the interaction between a user and the platform, specific rules are noted in the Mobilithek Data Privacy Statement² as well as the Terms & Conditions³. Every user has to agree to these two regulations when registering to the platform. This ensures that users are fully aware of how their personal data will be processed and stored in compliance with GDPR. **Figure 19** indicates the Data Privacy Statement and the Terms & Conditions during registration phase.

Agreements

☒ I approve that my personal data is stored and processed according to the purposes indicated in the [Data Privacy Statement](#).

☒ I confirm that I have read and will adhere to the [Terms & Conditions](#).

Figure 19: Data Privacy Statement and Terms & Conditions at Mobilithek

The Data Privacy Statement includes, among others, details on which personal data (about the user) are saved and exchanged for which platform functions, as well as on how data subject rights (according to GDPR) are fulfilled by Mobilithek.

The Terms & Conditions include, among others, a GDPR rule as follows in **Figure 20**.

(2) The user is obliged to use the functionalities of the Mobilithek only in accordance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. The data provider is the controller under data protection law for the processing of the personal data it provides. The operator ensures that no personal data within the meaning of Article 4 (1) of the GDPR is offered, unless the data protection requirements for processing the data are met.

Figure 20: Terms & Conditions rule of the Mobilithek

This ensures that both the platform operator and data providers are aligned with GDPR requirements, maintaining accountability and transparency for any personal data handling within the platform.

² <https://mobilithek.info/privacy-policy>

³ <https://mobilithek.info/docs/terms-and-conditions>

In the end, the responsibility for GDPR compliance regarding data that is exchanged via Mobilithek is in the hands of the data provider. Before publishing any data on the platform, data providers shall submit a declaration confirming that the data/metadata they upload complies with GDPR, either because it is free of personal information or because they have obtained the necessary consents (**Figure 21**).

Declarations

I hereby confirm that the data provided are free of any personal

☒ information and third party rights or that I have the corresponding consents that allow a publication.

Figure 21: Data provider's declaration in terms of GDPR

Altogether, the usage of personal data (thus. GDPR-relevant data) within provided content data is allowed, as long as the data provider has the “corresponding consents”, and “the data protection requirements for processing the data are met”.

With these rules, the German NAP effectively integrates GDPR compliance into its operations by establishing a comprehensive framework that covers user consent, platform data interactions, and the responsibilities of data providers, thereby ensuring that personal data is processed in a lawful and transparent manner.

4.4.2. The case of Belgian NAP

The Belgian NAP is designed mainly as a metadata directory and therefore mostly stores metadata and not the datasets themselves. Only in a limited number of cases, e.g., when a data provider does not have its own means to place a dataset online (on its own website), the Belgian NAP can store the actual data. As such, GDPR arrangements regarding the data content are organised directly between data providers and data consumers, where the NAP facilitates this process by displaying the contact means of the data provider for each of the registered datasets in the metadata. GDPR policies on the Belgian NAP therefore mainly address the usage, storage and protection of the contact details of data providers and other stakeholders (potentially data consumers) by the NAP operator and Control Body. That being said, the Belgian NAP integrates robust data protection practices⁴, ensuring compliance with GDPR principles and standards, as outlined on their platform. Belgian NAP aligns with European regulations, specifically the GDPR (Regulation (EU) 2016/679). The platform's privacy declaration outlines the steps taken to maintain the security and confidentiality of personal data, emphasizing the importance of adhering to these rules in order to build trust with users and stakeholders. The specific rules regarding GDPR are noted in the “Terms of Use” and “Privacy declaration” in the about-section of the Belgian NAP. Every user automatically agrees to these two regulations when using the platform.

The platform acknowledges its responsibility to handle personal data with care, adhering to GDPR requirements. By doing so, it aims to safeguard individuals' privacy while maintaining the integrity of the data shared between stakeholders in the transport and mobility sectors. As part of its operations, the Belgian NAP collects specific personal data from stakeholders in the mobility sector. This typically includes names, addresses, phone numbers, and email addresses, which serve as contact details for those responsible for managing and providing datasets on the platform. This collection is based on legal requirements and is designed to ensure clear communication between users and the platform, as well as for managing client requests, processing orders, and delivering services.

⁴ <https://www.transportdata.be/en/pages/privacy-declaration>

Users of the Belgian NAP are entitled to several rights under the GDPR. These include the right to withdraw consent for data processing, request access or a copy of their data, correct or complete inaccurate information, request data deletion, restrict processing, or transfer their data to another entity. Additionally, users can also object to specific types of processing, such as direct marketing, and are encouraged to lodge complaints if they believe their data rights are not being respected and processed appropriately (**Figure 22**).

Rights:

In accordance with Article 7.3 and Article 12 to 22 inclusive of Regulation (EU) 2016/679 above, you have the right, after written request as mentioned below, to:

- withdraw your data processing authorisation at any time. However, the withdrawal of your authorisation shall not affect the legitimacy of the treatment on the basis of your authorisation before it is withdrawn;
- consult or receive a copy of your personal data;
- have your wrong personal data corrected or completed your incomplete personal data by giving us a correction and/or addition of your personal data with your request;
- have your personal data [1]deleted;
- obtain the restriction of the processing of your personal [2]data;
- obtain the transferability of your personal data, so that your personal data are transferred to you or to an organisation you have [3]designated;
- lodge a complaint against the processing of your personal data, for example for direct marketing, by sending us with your request the reasons relating to your specific [4]situation;

Figure 22: User rights in accordance with Article 7.3 and Article 12 to 22 inclusive of Regulation (EU) 2016/679

To exercise these rights, users shall submit a written request to the Belgian NAP or IGN (the National Geographic Institute, who acts as the NAP operator in Belgium), providing proof of identity to ensure the request is legitimate. The NAP commits to responding to these requests within one month, though this period may be extended in complex cases. Importantly, the exercise of these rights is free of charge, although the NAP reserves the right to charge administrative fees for excessive requests.

As indicated in **Figure 23**, the Belgian NAP, has implemented several technical and organizational measures to ensure the appropriate protection of personal data in line with the requirements of GDPR. These include, among others, encryption, anonymization of sensitive data where possible, and strict access controls to ensure that only authorized personnel can access personal information. Additionally, they have robust procedures in place for dealing with data breaches or unauthorized access, as mandated by GDPR requirements.

Measures applied by the IGN

The IGN shall take appropriate technical and organisational measures to protect your personal data and to ensure a level of protection appropriate to the risk.

Thus, the following measures are taken, inter alia, in this context:

- collaboration with an official designated by the IGN for data protection, who can be contacted in case of questions or problems via e-mail to [the address DPO-ign.be](mailto:DPO-ign.be);
- the limitation of access to certain personal data received from you and to data persons who need personal data in the performance of their function within the IGN. Submission of such persons to confidentiality undertakings;
- the maintenance of a register of processing activities;
- the testing, evaluation and regular correction of the effectiveness of our safety measures;
- the imposition of safeguards concerning the application of adequate technical and organisational protection measures, in the case of subcontracting processing personal data on the order of the IGN;
- the performance of an assessment of the effects of data protection prior to the processing of personal data in which new technologies are used, which creates a high risk to the rights and freedoms of the interested(s);
- notification of an infringement and other important information to the supervisory authority and, where appropriate, to the interested party, in the case of an infringement in relation to personal data generating a high risk to the rights and freedoms of the interested party(s);
- cooperation on request with supervisory authorities and consultation of supervisory authorities in the performance of our tasks.

Figure 23: Measures applied by the Belgian NAP to safeguard the personal data

Moreover, personal data collected by the NAP is retained only for as long as is necessary to fulfil its intended purpose. For instance, contact details related to a specific service agreement are stored for up to 15 years, while data related to a complaint may be stored for up to 10 years.

Finally, the Belgian NAP uses cookies to enhance the functionality and usability of its website. These cookies fall into several categories: essential cookies, which ensure the website operates correctly; functional cookies, which remember user preferences such as language settings; analytical cookies, which track user behaviour to improve website performance; and advertising cookies, which help deliver personalized ads based on browsing behaviour. The platform ensures that no cookie data is transmitted to third parties without the user's consent, and users are given the option to manage their cookie preferences.

4.4.3. The case of Swiss NAP

The Swiss NAP follows strict guidelines⁵ for personal data protection. The platform, operating within the framework of the Swiss Data Protection Act (DSG) and the EU GDPR, ensures that personal data is processed only when necessary and in compliance with legal requirements. The data processing operations occur due to various reasons such as technical necessity, contractual obligations, legal requirements, and legitimate interests, or as a result of user consent. The primary purposes include managing customer relationships, offering services, responding to user inquiries, and providing technical support.

When users interact with the platform, whether by visiting the website or using API interfaces, specific technical data is collected and stored. For instance, IP addresses, browser types, operating systems, and search queries are logged to ensure system security and performance, detect errors, and optimize

⁵ <https://opentransportdata.swiss/en/data-privacy-statement-2/>



the platform for better functionality. This data is primarily processed for system security, stability, performance analysis, and internal statistical purposes. Additionally, it helps optimize the website and customize it for specific target audiences. The platform uses cookies and similar tools to enhance user experience. When using API interfaces on the platform, users must register and obtain an API key. The platform records personal data associated with this registration, such as username, email address, and API key access logs. This data is stored to manage user access and may also be used for newsletters or other communications. Personal data associated with API keys can be deleted upon request, with deletion typically occurring within 14 days. Additionally, when users utilize the platform's contact form, personal data like name, email address, and message content are collected to allow for personalized responses to inquiries. The platform only stores data for as long as needed to provide services, comply with legal obligations, or for internal analysis and improvements. Marketing-related data processing on the Swiss NAP is limited. Occasionally, the platform may send users newsletters or information about relevant news and events, primarily targeting those who have registered for API access or submitted support inquiries. Beyond this, no additional marketing activities are carried out, ensuring minimal usage of personal data for advertising purposes.

Users of the Swiss NAP are entitled to several rights (**Figure 24**) concerning their personal data. These rights include accessing and rectifying their data, requesting deletion or blocking of their data, and objecting to the use of data for marketing purposes. Users can also request that their data be transferred or withdraw their consent for future processing. To exercise these rights, users can contact the platform through its designated communication channels. Additionally, they can report concerns to the Federal Data Protection and Information Commissioner (FDPIC).

You have the following rights with regard to your data. You can exercise them at any time.

- Obtaining information about your personal data stored by us
- Rectification, supplementation, blocking or erasure of your personal data (if due to legal storage obligations we can only erase your data at a later date, they will be blocked in the meantime)
- Have your customer account deleted.
- Object to the use of your data for marketing purposes
- Withdraw your consent for future data processing
- Transmission of your data

You can send us your request for information and deletion via the [contact form](#) or by email to opendata@sbb.ch.

You also have the right to submit your concerns or questions to the [Federal Data Protection and Information Commissioner \(FDPIC\)](#) at any time.

Figure 24: Users' rights at the Swiss NAP

Personal data is not sold or shared without necessity. Data is only passed on to third parties, such as IT support providers or platform operators, to the extent needed to fulfil the services offered on the platform. Some service providers, particularly those providing hosting services, may be located abroad.

Finally, the NAP employs comprehensive technical and organizational security measures to safeguard personal data against unauthorized access, manipulation, or loss. Security protocols are regularly updated and refined to match advancements in technology. Employees and third-party service providers involved in the operation of the platform are bound by strict confidentiality agreements, ensuring compliance with data protection standards. Despite these precautions, the platform acknowledges the inherent risks associated with transmitting data over the internet.

4.4.4. The case of Norwegian NAP

The Norwegian NAP⁶ follows GDPR regulations that guide how personal data should be processed to ensure lawful and fair treatment of data subjects.

⁶ <https://gdpr-info.eu/>

Furthermore, personal data must be processed securely, ensuring its protection against unauthorized access, loss, or damage through appropriate technical and organizational measures. The data controller, typically the entity that determines the purpose and means of data processing, is responsible for ensuring and demonstrating compliance with these principles. Lawfulness of data processing is guaranteed if one of several conditions is met, such as obtaining consent from the data subject, fulfilling a contract, or complying with legal obligations. Processing can also be lawful if it protects vital interests, serves public interest, or is necessary for legitimate interests that do not override the rights and freedoms of the data subject.

Finally, for international data transfers, stringent conditions are applied to ensure that the level of data protection is not compromised when data is transferred outside the EU. These transfers are only permitted if they comply with GDPR regulations and provide adequate safeguards for the rights of data subjects.

4.4.5. The case of Swedish NAP

The Swedish NAP, managed by Trafikverket⁷, complies with the General Data Protection Regulation (GDPR) to safeguard personal data. Trafikverket, responsible for the processing of personal data on its website, collects data when individuals use services such as newsletters, text messaging, and various case or webshop services. Personal data collected includes identifiers like name, personal ID number, email address, IP address, vehicle registration number, and other details necessary for legal or contractual obligations. Trafikverket commits to using personal data solely for the specified purposes and ensures that all data is retained and processed securely for the duration needed to fulfill the defined purposes.

The Swedish NAP has detailed protocols on who can access the collected data, limiting it to Swedish Transport Administration employees and vendors, who require it for rights management, project handling, or communication purposes. Additionally, no personal data is transferred outside of the EU/EEA, and no profiling or automated decision-making processes are employed. The authority emphasizes the secure management of data through stringent security rules and regulatory compliance.

Data retention is regulated by Swedish laws such as the Public Access to Official Documents and Secrecy Act, meaning that personal data in public documents may be retained indefinitely unless a specific regulation mandates its deletion. Users have several rights under the GDPR, including the ability to request data deletion, corrections, or restrict processing, as well as filing complaints.

4.4.6. The case of Croatian & Slovenian NAP

The Croatian and Slovenian NAPs share a common privacy policy that focuses on the collection and management of user data. According to this policy, the platform collects information such as email addresses, language preferences, the devices used, user rights, user location, and various administrative details, including timestamps, counters, IP addresses, users, tokens, and encrypted passwords. Importantly, only authorized personnel from the service provider have access to this data, with the user also having visibility over specific aspects such as their content and language preferences.

The policy, as indicated in **Figure 25**, emphasizes the use of best practices for storing and transmitting sensitive data, ensuring that user information is handled securely. Additionally, the platform reserves the right to use anonymized data in summary formats for statistical purposes. Additionally, users are

⁷ <https://bransch.trafikverket.se/en/startpage/about-us/Trafikverket/About-the-website/Legal-information/this-is-how-trafikverket-works-with-the-general-data-protection-ordinance-gdpr/>



informed that the privacy policy may change, with any modifications communicated in advance through the website. By using the services on the platform, users agree to this privacy policy.

Finally, the platform employs necessary cookies, such as ASP.NET_SessionId, which is essential for maintaining user sessions and expires once the user closes their browser.

Privacy policy

Website collects the following user data:

- email,
- language,
- devices they use,
- user rights,
- user location,
- administration information (timestamps, counters, IPs, users, tokens, irreversibly encrypted passwords).

Only authorized persons of the service provider can see all the information. Where the content makes sense, this information is also seen by the user himself (my content, content, language, ...). We reserve the right to use the data in an anonymised summary format for statistical surveys. We use recommended practices for storing and transmitting sensitive data. We reserve the right to change our privacy policy, to which users will be informed in advance on the website. By using the services of www.nap.si, the user agrees to this privacy policy.

The cookies used on this site are absolutely necessary for the operation.

cookie name	source	used where?	used for?	expires
ASP.NET_SessionId	this website	throughout the site	contains the user session ID	when the user closes the browser

Figure 25: Privacy policy of the Slovenian & Croatian NAP

4.5. Recommendations for NAP operators

In the context of ensuring compliance with the GDPR, NAPs play a pivotal role in managing and processing transport-related data across EU MSs. To maintain trust and ensure that personal data is handled with the respective care, NAP operators shall adopt strict policies and procedures aligned with GDPR's principles. The overarching aim is to guarantee that personal data is processed lawfully, fairly, and transparently, with a focus on minimizing data collection, ensuring accuracy, and upholding data subjects' rights. This section provides a set of actionable recommendations that NAP operators could implement to ensure compliance with GDPR. These recommendations highlight, among others, the importance of data security, user consent, third-party processing agreements, and the need for ongoing training and awareness. **Table 6** indicates recommendations and critical considerations for NAP operators.

Table 6: Recommendations to NAP operators for ensuring compliance with GDPR

Recommendation	Description	Actions to implement
1. Appoint a Data Protection Officer (DPO)	NAP operators may designate a DPO to oversee data protection activities and ensure compliance with GDPR regulations.	• Identify whether a DPO is needed. • Appoint a qualified DPO. • Ensure the DPO provides guidance on data protection issues and acts as a liaison with authorities.
2. Conduct Data Protection Impact Assessments (DPIA)	Assess high-risk processing activities, especially involving sensitive or large-scale data, to identify risks and recommend mitigation.	• Conduct DPIA before processing high-risk data. • Review new technologies that may impact data privacy. • Take necessary steps to mitigate identified risks.
3. Provide transparency and privacy notices	Ensure clear and accessible privacy notices to inform users about the purposes and conditions of processing personal data.	• Develop concise privacy notices. • Include identity of the person who is responsible for managing the data, the legal purposes for processing the data, the duration that data will be kept, and users' rights.

		• Regularly review notices for updates.
4. Minimize data collection	Only collect data that is strictly necessary for specific, legitimate purposes to minimize risk and ensure compliance with the data minimization principle.	• Limit data collection to essential information. • Implement data relevance checks (process of reviewing and verifying that the data being collected is directly applicable and necessary for the intended purpose) during collection.
5. Ensure lawful data processing	Processing activities shall have a valid legal basis, such as consent, legitimate interest, or legal obligation. Ensure proper documentation and justification for each processing activity.	• Identify legal bases for processing. • Obtain clear consent where required. • Provide users with options to withdraw consent easily.
6. Implement technical and organizational measures	Establish strong technical measures like encryption, pseudonymization, and access controls to protect data from breaches, unauthorized access, and loss.	• Use encryption and other security measures. • Limit access to authorized personnel only. • Conduct regular security audits and updates.
7. Define data retention policy	Set clear retention periods for personal data based on legal requirements. Ensure data is securely deleted when no longer needed.	• Define retention periods for each data type. • Securely delete data after the retention period. • Monitor data storage regularly.
8. Define users' data rights	Ensure users can easily exercise their rights to access, rectify, delete, restrict, and transfer their personal data. Establish efficient and transparent processes for responding to requests.	• Set up systems for responding to access and deletion requests. • Process data subject requests within the legal timeframes. • Train staff on GDPR-compliant handling.
9. Secure international data transfers	For transfers of personal data outside the EU, ensure appropriate safeguards.	• Review cross-border data transfers. • Use standard contractual clauses or binding corporate rules. • Monitor compliance with international data transfer laws.
10. Train employees on GDPR compliance	Regularly train staff on data protection regulations, handling personal data securely, and identifying potential data breaches.	• Develop GDPR training programs for staff. • Ensure all employees handling personal data are trained. • Update training regularly to reflect new guidelines.
11. Engage with data protection authorities	Communicate with Data Protection Authorities (DPA) to ensure ongoing	• Build relationships with DPA for guidance.

	compliance and address any concerns related to data processing.	• Engage proactively on emerging data protection issues. • Consult DPA when deploying new data processing policies
12. Monitor evolving GDPR Guidelines and national laws	Stay updated on changes to GDPR regulations and relevant national laws, as well as emerging best practices for data protection. Ensure the NAP platform evolves to comply with new requirements.	• Assign team members to monitor national data protection laws. • Adjust policies and practices as needed to comply with new regulations.

5. Concluding remarks

This section provides a comprehensive overview of the key findings, observations and recommendations of the critical aspects related to terms and conditions for data reuse, fair data exchange strategies, and GDPR compliance within the context of NAPs.

As regards the terms and conditions, there has been an endeavor to record the licenses used by NAPs with the aim of providing a comprehensive understanding of the terms and conditions governing data reuse across different MSs. The European inventory revealed diverse approaches to terms and conditions applied by NAPs. More specifically, while most NAPs adopt open data licenses such as Creative Commons (CC), Open Data Commons (ODC), and the Open Government License (OGL), the license types (e.g., CC-BY, CC-BY-SA, CC0) can vary significantly. These variations in licensing frameworks reflect the differing legal, operational, and technical environments in which NAPs operate. In addition, specific questions were posed to NAP operators, as part of this effort, to address ambiguities related to the application of licenses. Questions addressed issues like the distinction between “license and contract” and the interpretation of open license terms such as “commercial use” and “derivative works,” which varied across the responses received from different NAPs. The survey also brought attention to the lack of clarity around license categories such as “No license – No agreement”, where NAP providers struggled to answer regarding data reuse permissions. Hence, it became evident the need for more harmonized, standardized terms across the European NAP landscape that could greatly enhance cross-border data exchange as well.

In terms of fair data exchange, this milestone focused on the understanding of critical aspects of the literature concerning the fair principles, exploring several data exchange strategies, and understanding the perspectives of key stakeholders such as public data providers and data consumers. The review undertaken revealed that existing literature entails several important pricing models, including free, freemium, usage-based, flat-fee, and tiered. These models offer different pathways for managing data exchange, balancing public benefit, and supporting the sustainability of data provision. However, what emerged clearly from the review is that strategies often need to be tailored to the specific needs of both data providers and consumers, with consideration for the legal and operational context of the NAPs. To delve deeper into these issues, a tailored survey was circulated targeting three different stakeholders: (a) data consumers, (b) public data providers, and (c) private data providers. The survey was designed to gather insights into their fair data exchange preferences, the factors shaping their decisions, and their general willingness to engage in data exchange chain at various levels cost. The survey results offered several important insights. Through the survey responses, it was evident that public data providers currently offer most datasets free of charge, while emphasizing the costs of technical support, infrastructure, and data management. Data consumers, on the other hand,

indicated a preference for flexible licensing options while balancing affordability with acceptable data quality. These findings underscore the need for NAP operators to develop sustainable, equitable models for data exchange that accommodate the diverse needs of stakeholders.

In conclusion, with respect to GDPR compliance, an analysis of NAP practices across different MS has been executed, providing insights into how NAP operators handle privacy policies, user consent, data security, and the users' rights. The objective was to assess whether NAPs are aligned with the requirements of the GDPR and to identify common practices that ensure compliance. The findings highlight various approaches taken by NAP operators and existing best practices. One of the key aspects observed is that most NAPs have taken significant steps to ensure that privacy policies are accessible and clearly state how personal data is processed, including the scope, purposes, and legal bases for data processing. Moreover, the analyzed NAPs have implemented various technical and organizational measures to protect personal data against unauthorized access, loss, or breach. In conclusion, the last part of the milestone outlines recommendations for NAP operators that serve as a roadmap to enhance the governance of their platforms, considering the identified best practices.

Finally, by taking into consideration the outlined recommendations to all topics discussed in the document earlier, NAP operators could foster a more transparent, clear, and secure data exchange ecosystem across MSs, ensuring that the needs of both data providers and consumers are effectively balanced.

References:

COMMISSION DELEGATED REGULATION (EU) 2017/1926 (2017). Provision of EU-wide multimodal travel information services. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1926>

COMMISSION DELEGATED REGULATION (EU) 2022/670 (2022). Provision of EU-wide real-time traffic information services. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0670>

COMMISSION DELEGATED REGULATION (EU) 886/2013 (2013). Road safety-related minimum universal traffic information free of charge to users. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R0886>

DIRECTIVE (EU) 2019/1024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2019). Open data and the re-use of public sector information. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L1024>

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, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>

Fleckenstein, M., Obaidi, A., Tryfona, N. (2023). A Review of Data Valuation Approaches and Building and Scoring a Data Valuation Model, *Harvard Data Science Review*. Issue 5.1.

Heckman, J.R., Boehmer, E.L., Peters, E.H., Davaloo, M., Kurup, N.G. (2015). A Pricing Model for Data Markets. in *iConference 2015 Proceedings*.

Huang, J., Kauffman, R.J., Ma, D., (2015). Pricing Strategy for cloud computing: A damaged services perspective. in *Decision Support Systems*, Volume 78, Pages 80-92.

Koutris, P., Upadhyaya, P., Balazinska, M., Howe, B., & Suci, D. (2015). Query-based data pricing. *Journal of the ACM (JACM)*, 62(5), 43.

Lubrich, P., Ansorge, J., Böhm, M., ..., & Vlemmings, T. (2019). EU EIP SA46 Coordinated Metadata Catalogue: Monitoring and Harmonisation of National Access Points in Europe. Retrieved from: https://www.its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/NAP/EU%20EIP_Coord.%20Metadata%20Catalogue_v2.0_191115.pdf

Maxar Technologies (2024). Evaluation License – END USER LICENSE TERMS. Retrieved from: <https://www.maxar.com/legal/evaluation-license>

Muschalle, A., Stahl, F., Loser, A., Vossen, G. (2012). Pricing approaches for data markets. *Proc. Int. Workshop Bus. Intell. Real-Time Enterprise*, Springer, pp.129-144.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2016). Protection of natural persons with regard to the processing of personal data and on the free movement of such data. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

Thalesgroup (2024). Software License Models. Retrieved from: <https://cpl.thalesgroup.com/software-monetization/software-license-models>

Viscusi, G., & Batini, C. (2017). Digital information asset evaluation: characteristics and dimensions (Working Paper). EPFL and University of Milano-Bicocca.



Yu, H., & Zhang, M (2017). Data pricing strategy based on data quality. Computers & Industrial Engineering 112, 1-10.

Zhang, M., Beltran, F., Liu, J. (2023). A Survey of Data Pricing for Data Marketplaces. In IEEE Transactions on Big Data, VOL. 9, No. 4.