ePower Move

Project deliverable D7.4

Data Management Plan

Funded by
the European Union

DELIVERABLE ADMINISTRATIVE INFORMATION

Deliverable Administration					
Grant Agreement	101192753	Project name	ePowerMove		
Deliverable no.	D7.4	Deliverable Name	Data Management Plan		
Status	Final	Due	M6	Date	30/06/2025
Editor/Lead author	Johannes Hasibar (AustriaTech)				
Co-authors	Dominik Schallauer (AustriaTech), Magdalena Lindner (AustriaTech)				
Peer reviewers	Aki Lumiaho (VTT) Haibo Chen (UNIVLEEDS)				
Dissemination level	SEN - Sensitive				
Quality Control					
Document history	Version	Date	Submitted	Comments	
	V0.1	15/05/2025	Johannes Hasibar	First draft	
	V0.2	27/05/2025	Johannes Hasibar	Final draft for review	
	V0.3	03/06/2025	Aki Lumiaho	Internal peer review	
	V0.4	10/06/2025	Haibo Chen	Internal peer review	
	V0.5	30/06/2025	Johannes Hasibar	Pre-final document treating peer review comments	
	V1.0	30/06/2025	Andrew Winder	Final submission	

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor CINEA can be held responsible for them.

TABLE OF CONTENTS

List of tables

EXECUTIVE SUMMARY

This document serves as the Data Management Plan (DMP) for the project ePowerMove. It outlines a comprehensive framework for handling project-related data, including the types of data that will be collected or generated, procedures for data management, and the tools used to access and utilize these data for research purposes throughout the project lifecycle and beyond.

Within the scope of ePowerMove, a variety of data will be generated and handled. They fall into three main categories: internal administrative data, technical data and data on user needs and preferences. Each category serves distinct objectives and requires specific management practices.

Internal administrative data, such as meeting minutes, internal reports, and legal or contractual documents, are used for project coordination and compliance. These data are considered internal working materials and will not be shared outside the project consortium. Technical data - collected and reused for the development and integration of EV charging infrastructure into power grids - along with selected project outcomes, will be made available as openly as possible. This will always be done in compliance with applicable laws, the protection of Intellectual Property Rights (IPRs), and legitimate commercial interests. User-related data, including information on user needs, charging behavior, and preferences, will be processed and shared only in anonymised or aggregated form, in full accordance with the General Data Protection Regulation (GDPR).

The project is committed to following the FAIR principles - ensuring that data is Findable, Accessible, Interoperable, and Reusable. The degree to which these principles apply may vary across data categories, and these variations are addressed in detail throughout this document. Where possible, datasets will be published in machine-readable formats such as CSV or JSON, accompanied by clear metadata and documentation. Open and non-sensitive data will be made available through trusted open-access repositories, with **Zenodo** proposed as the primary platform. To maintain consistency, the consortium will develop internal guidelines on how to upload and describe datasets on Zenodo. Sensitive or proprietary data will be handled with appropriate restrictions, ensuring legal and ethical compliance.

This DMP was developed under Work Package 7 (Project Coordination and Management), specifically Task 7.4 – Data Management Plan, and fulfills the requirements of Deliverable 7.4. It is primarily intended as an internal reference and guidance document for all project beneficiaries. All partners are expected to handle data in accordance with the standards and practices outlined.

The structure of this deliverable is as follows:

- Chapter 1 – Introduction – introduces the project and the purpose of the deliverable.
- Chapter 2 – Data summary – provides a description of the types of data to be generated by the project and specifies information about the data types.
- Chapter 3 – FAIR data – describes how data will be made findable, accessible, interoperable and re-useable.
- Chapter 4 – Other research outputs – describes management of other research outputs.
- Chapter 5 – Allocation of resources – describes how allocation of required resources for data management is implemented.
- Chapter 6 – Data security – describes the approach towards guaranteeing data security.
- Chapter 7 – Ethics –describes the consideration of ethical aspects.
- Chapter 8 – Conclusions – concludes the deliverable.

This deliverable is the first version of the Data Management Plan, which presents the Data Management Plan for ePowerMove with the state of information at M6 of the project. The Data Management Plan will be updated in M18, M30 and in M42 respectively.

LIST OF ABBREVIATIONS AND ACRONYMS

Acronym	Meaning
2FA	Multi-Factor Authentication
API	Application Programming Interface
BESS	Battery Energy Storage Systems
CINEA	European Climate, Infrastructure and Environment Executive Agency
CSV	Comma-Separated Values
Dx.x	Deliverable x.x in ePowerMove
DAC	Data Access Committee
DCAT	Data Catalogue Vocabulary
DMP	Data Management Plan
DOI	Digital Object Identifier
DUA	Data Use Agreement
EU	European Union
EV	Electric Vehicle
FAIR	Findable, Accessible, Interoperable, and Reusable
GDPR	General Data Protection Regulation
IPR	Intellectual Property Right
JSON	JavaScript Object Notation
LEA	law enforcement agency
M	Month (in ePowerMove; M1 is January 2025)
NDA	Non-Disclosure Agreement
R&D	Research and Development
RES	Renewable Energy Source
SoC	State of Charge

Acronym	Meaning
V2G	Vehicle-to-Grid
XML	Extensible Markup Language
WP	Work Package

1 INTRODUCTION

As electric vehicle (EV) markets continue to grow rapidly, ensuring affordable, accessible, and efficient charging infrastructure is critical to supporting mass adoption. The ePowerMove project designs flexible, scalable, and interoperable bidirectional smart and slow-charging solutions that adapt to diverse regional power systems and evolve with technology and policy, reducing infrastructure costs while being less intrusive. The project optimises global energy usage by combining advanced charging technologies and intelligent grid energy control to enhance system efficiency and support the increasing share of renewable energy. Social innovation, affordability, and user acceptability drive the project's developments, ensuring solutions meet real-world needs across diverse socio-cultural and economic contexts.

The ePowerMove project demonstrates its innovative non-intrusive, efficient and slow-charging solutions across three key locations, each addressing a critical aspect of EV charging and integration. In Helsinki, Finland, the focus is on reducing infrastructure costs and enhancing user experience. Klagenfurt, Austria, explores new business models to drive sustainable e-mobility, while Nicosia, Cyprus, optimises grid compatibility and energy flow management. Together, these real-world demonstrations ensure that ePowerMove delivers scalable, cost-effective, and user-centric charging solutions that support the mass adoption of EVs across Europe.

ePowerMove works to ensure the seamless integration of slow, smart and bidirectional charging into the energy system, making EVs a valuable asset in sustainable energy management. The project also focuses on developing advanced user-centric applications, ensuring friendly and efficient access to charging infrastructure. Additionally, ePowerMove explores scalable planning and mass deployment models. The project builds on proven models from previous EU-funded projects, providing a scalable, flexible, and interoperable architecture that aligns with a variety of regional power systems and Vehicle-to-Grid (V2G) technologies. By exploring new business and usage models, the project aims to accelerate policy interventions and mass deployment strategies for widespread EV adoption. By creating a flexible, scalable, and interoperable architecture, the project will contribute to reducing greenhouse gas emissions and fostering sustainable urban e-mobility, supporting the EU's electrification and decarbonisation goals.

For more information on the project, see https://epowermove.eu

1.1 Overview of this deliverable

This Data Management Plan (DMP) provides a comprehensive set of guidelines, including a description of the data and the tools for managing, accessing, and using ePowerMove data for research purposes during and after the project.

Developed as part of Work Package 7 - Project Coordination & Management (WP7), this DMP defines procedures for handling personal data to protect citizens' fundamental rights and prevent any misuse of project results. It outlines how data will be securely stored and whether it will be deleted at the end of the project or archived for future use by the research community. In the case of data archiving, the DMP offers recommendations for long-term maintenance and controlled access for consortium partners and external stakeholders.

This plan ensures that data follows the FAIR principles - making it Findable, Accessible, Interoperable, and Reusable. Data privacy and security considerations are addressed in detail, specifying the relevant requirements and applicable standards. The overarching principle is to be as open as possible while ensuring compliance with legal regulations, commercial interests, and the intellectual property rights (IPRs) of project partners. The DMP adheres to European Union (EU) and international regulations on data management and aligns with the General Data Protection Regulation (GDPR).

This deliverable is the first version of the Data Management Plan. As a first version, it provides a high-level overview, while aiming to be as comprehensive as possible given the current knowledge. Updates of the Data Management Plan will be published in M18 and M30 of the project, and the final version of it will be published in M42 in form of D7.7.

1.2 Intended audience

This deliverable is an internal project document intended primarily for the ePowerMove consortium partners and the European Commission. It supports project coordination, ensures alignment with data management best practices, and provides a reference for handling data across work packages. While it is not intended for public dissemination in its current form, the principles and methodologies outlined herein may inform public project deliverables and contribute to transparent, responsible data governance in line with Horizon Europe requirements.

1.3 Structure of the deliverable and links with other work packages/deliverables

This deliverable begins by providing a detailed overview of the various types of data that are collected, generated, and processed within the scope of the ePowerMove project. It outlines the nature, structure, and intended use of these data types, offering insights into how they contribute to the project's overall objectives.

To gather comprehensive and consistent information, a structured questionnaire was developed and distributed to all project partners. Each partner was asked to provide specific details regarding the data they handle, including its source, format, frequency of collection, and relevance to the project goals. The responses to these questionnaires formed the basis of the analysis presented in this deliverable. For the next versions of the DMP, partners will be asked to update the information they have given via the questionnaire.

2 DATA SUMMARY

This chapter provides an overview of the data categories that are collected, processed, re-used and stored in the ePowerMove project. The following data categories were identified:

- **Internal administrative data**: data generated/shared internally for administrative and management purposes.
- **Technical data**: related to the technical development and operation of charging infrastructure at the pilot sites.
- **Data on User needs and preferences:** collected in workshops and in user questionnaires during the project.

2.1 Internal administrative data

Within the scope of the project, various categories of internal administrative data will be generated and managed. These include meeting minutes, voting records, financial reports from consortium partners, internal progress reports, communication logs (e.g., email correspondence relevant to project coordination), personnel records related to project time allocation, and legal or contractual documentation (e.g., amendments, subcontracts, and NDAs). These data types are essential for project coordination, compliance monitoring, and reporting to the funding body.

2.2 Technical Data

To develop and evaluate grid-level optimisation, control, and forecasting models, data on the power grid is generated and reused. This data includes Historical Load Profiles, Peak Demand Patterns, Renewable Energy Source (RES) Generation and Curtailment Data and Battery Energy Storage Systems (BESS) availability.

Charging point data is collected in the project and reused from previous projects or existing charging infrastructure. Specifically, in addition to static data on location, grid connection and technical specifications, dynamic data such as charging times (start and end time of the charging session, amount of electricity charged and discharged, charging and discharging power) are also used.

It is intended that existing operational and telematics data from the current car fleet will be reused. Especially data from the e-car sharing fleet. This data includes vehicle location, battery state of charge (SoC), charging behaviour, and trip information. By reusing this data, vehicle usage patterns and energy consumption will be benchmarked prior to the implementation of V2G, which will help in assessing the effectiveness of bi-directional charging strategies.

Table 1 - Technical Data Overview

Technical data subcategories	Description of data	Examples	Data provision format
Grid data	Data on the power grid to calculate and forecast future needs	Historical Load Profiles, Peak Demand Patterns, Renewable Energy Source (RES) Generation and Curtailment Data	.csv
Charging point data	Data from charging point developed and used during the project.	Energy consumption, charger info, model of the EV (future), Time stamps, amount of uploaded energy, number of charging and discharging sessions	.csv; JSON
Vehicle Data	Data from vehicle and on vehicle usage	Vehicle location, battery state of charge (SoC), charging behaviour, and trip data	JSON

2.3 Data on User needs and preferences

The involvement of users and potential users is a central element of the project. Online surveys, workshops at the pilot locations, online workshops and individual interviews are used to collect data on user preferences, user behaviour and preferences in relation to charging infrastructure. This data, together with existing data from previous projects, will be incorporated into the development of the charging infrastructure and the development of the sharing service.

The surveys will feature structured multiple- and single choice questions to facilitate straightforward processing and analysis. In certain instances, participants may be given the option to provide free-text responses for more detailed qualitative feedback. In order to identify different user groups, personal demographic data is also collected. However, it will be carefully evaluated whether these data, and in what format, can be made available in compliance with GDPR regulations.

Table 2 – Data on User needs and preferences overview

User data subcategories	Description of data	Examples	Data provision format
Usage Data	Data on the actual use of charging infrastructure and vehicles	Frequency of use, utilisation period	Not clear yet
User Preference data	Data on preferences for the design of charging infrastructure of potential infrastructure users	Preference of infrastructure surroundings, housing, usability	Not clear yet

3 FAIR DATA

This chapter explains how research data and outputs will be made Findable, Accessible, Interoperable, and Re-usable (FAIR). The adoption of the FAIR principles is essential to support data sharing and reuse—both during the project and beyond its lifetime—thus enhancing the overall impact of the research[1].

As outlined in Chapter 2, the different categories of data each have specific characteristics, which means that FAIR principles are applied in slightly different ways depending on the type of data. For this reason, the following sections describe the FAIR aspects separately for each data category.

3.1 Internal administrative data

Internal administrative data will be stored in a secure, access-controlled project management environment (e.g., SharePoint). Access will be granted strictly on a need-to-know basis and governed by user roles defined in the consortium agreement.

These data will not be shared publicly and are not subject to open data requirements. However, relevant metadata, such as document version history and authorship, will be maintained for internal auditing and transparency.

3.2 Technical data

Technical datasets, such as aggregated results and non-sensitive operational data, may be shared openly via trusted repositories like Zenodo, institutional data portals, or project websites. However, some datasets—especially those owned by infrastructure operators or third parties—are restricted due to legal, contractual, or proprietary constraints. Where openly shared, datasets will follow the FAIR principles and be accompanied by metadata licensed under a public domain dedication (e.g. CC0), if permitted by the data owner. The metadata will include access or request instructions when possible.

For long-term availability, openly shared technical datasets will be stored in repositories that ensure persistence (e.g. CERN's infrastructure behind Zenodo[2]), whereas restricted datasets will remain available internally as long as the institutions responsible and their IT systems operate. Persistent identifiers (e.g. DOIs) will be assigned where applicable, ensuring that datasets remain findable even if the data itself is eventually deprecated.

Standard documentation will accompany open datasets, and where data requires special processing tools or APIs, relevant software or scripts (e.g. in Python or JavaScript) will be provided via platforms like GitHub. However, proprietary software or internal platforms used for data generation or analysis will not be made public.

Technical datasets will primarily be made available in widely accepted, machine-readable formats such as CSV, JSON, and potentially XML, to ensure interoperability. Where applicable, community-endorsed

[1] https://www.openaire.eu/how-to-make-your-data-fair
[2] https://zenodo.org/

metadata standards like Dublin Core and DCAT, and domain-specific standards like OCPI, OCPP and ISO 15118 (related to V2G communication) will be followed.

If project-specific ontologies or non-standard terminologies are used, efforts will be made to map them to widely accepted standards. These mappings, along with documentation, will be shared to support reuse, where permitted by data owners.

Although formal linking to external datasets is not typically planned due to ownership and complexity of permissions, internal referencing (e.g. linking charging events to hardware IDs) will be used where relevant. In select cases, references to prior research or public benchmarks may be included, especially for contextualising energy or mobility performance data.

Openly shareable datasets will be published in standard, machine-readable formats and accompanied by comprehensive documentation, including README files, methodological notes, and data dictionaries. These datasets are expected to support research, innovation, and policy development in fields such as energy systems, smart mobility, and urban planning. For proprietary or sensitive technical data (e.g. involving commercial operations or detailed hardware specifications), reuse may be limited and subject to explicit approval from the respective data owners. Embargo periods or restrictions may apply on a case-by-case basis. In one case data of charging sessions cannot be made publicly accessible, because the data is not owned by an ePowerMove partner.

3.3 Data on User needs and preferences

Data related to user opinions and acceptance will be made openly available in aggregated and anonymised form. No personal user information will be shared. Raw user data (e.g., individual telemetry tied to user sessions) will remain under restricted access due to GDPR compliance and ethical standards. In rare cases, if sensitive user-related data must be accessed, access will be governed by signed Data Use Agreements (DUAs), and identity verification will be required through credentials or institutional affiliation. If necessary, a Data Access Committee (DAC) may be formed to evaluate requests involving sensitive user data, ensuring that data sharing aligns with privacy and ethical requirements.

The exact format in which the processed user data will be stored and provided is still to be determined. In principle, the data is intended to be stored in machine-readable and structured formats (e.g., CSV, JSON), but the final choice will depend on the structure of the data and the processing tools used. Clear and descriptive variable names, along with accompanying documentation, will be provided to facilitate future reuse.

Project- or domain-specific ontologies are not planned for user-related data. If internal categorisation is applied, it will be explained in the documentation; formal mapping to external vocabularies will only be pursued if relevant for reuse scenarios.

Reuse will only be permitted where data has been fully anonymised or aggregated to remove any identifiable elements. The final storage format of processed user data is not yet fully determined, which may impact its accessibility and reusability. Any potential reuse will require the explicit consent of data owners and may include restrictions regarding purpose, audience, and duration. Where reuse is granted, basic accompanying documentation may be provided. The primary reuse audience would be researchers analysing user behaviour, charging habits, or user acceptance of e-mobility solutions.

4 OTHER RESEARCH OUTPUT

This section describes how research outputs that are generated or re-used within ePowerMove will be managed, shared, and made available for re-use in line with the FAIR principles.

For this first version of the DMP, early-stage information on research outputs have been identified. These include software tools designed for grid-level optimisation, management, and analysis, as well as solutions at the prosumer and EV charging levels to support local energy resource management. Further software outputs include modules enabling vehicle-to-grid (V2G) communication within the project's app, backend APIs for bidirectional energy tracking, and data collection scripts. Additional outputs comprise simulation models and algorithms for forecasting energy demand and modelling user behaviour, potentially using machine learning techniques.

The project will also produce internal documentation such as technical diagrams, development-related workflows, and detailed process descriptions.

Upcoming iterations of the DMP will be adapted to reflect any new findings or developments, ensuring comprehensive and up-to-date coverage of all relevant research outputs in alignment with the evolving goals of the ePowerMove project.

5 ALLOCATION OF RESOURCES

Effective data management requires appropriate allocation of both human and financial resources. Each partner organisation will designate personnel responsible for data handling tasks, including data collection, documentation, storage, and sharing in accordance with FAIR principles. Technical infrastructure, such as secure servers, collaboration platforms, and repositories, will be provided either through institutional resources or existing infrastructures.

Most partners do not anticipate any additional costs associated with making project data FAIR (Findable, Accessible, Interoperable, and Reusable). Some partners indicated that any potential costs are either currently unknown, will be discussed internally if needed, or are covered under other funded projects.

One partner identified potential future costs, including long-term repository storage, data anonymisation and access control tools, and efforts for metadata documentation. However, these costs have not yet been fully allocated. Overall, no immediate or significant financial burden is foreseen for implementing FAIR data principles within the project.

Long-term preservation strategies vary across project partners and are in some cases still under development. Several institutions plan to use secure internal servers or systems already integrated within their IT infrastructure (e.g., M-Files with Office 365 integration), ensuring version control, standardised formats, encryption, and regular backups. When data is stored in trusted repositories such as Zenodo, DOIs to key datasets to support accessibility and citation will be assigned. The repository to be used for long-term storage is still under discussion and will be defined and implemented in the Data Management Plan at a later stage. Where plans are not yet finalised, discussions are ongoing to determine appropriate solutions. Metadata retention beyond the data lifecycle is considered an important measure to maintain context and facilitate future reuse. In general, preservation efforts will rely on institutional resources and infrastructure, not on project-specific funding.

6 DATA SECURITY

All partners have outlined their approaches to data security, risk management, and compliance with data protection regulations such as the GDPR.

At the time of writing, not all project partners have provided detailed information regarding their internal data security measures or confirmed the existence of an incident response plan. As a result, a comprehensive overview of data security practices across the consortium cannot yet be presented.

However, it is expected that all partners handle project-related data in accordance with GDPR and institutional best practices. The consortium acknowledges the critical importance of data security and will address this gap in the next version of the DMP as well as a more detailed look into data security practices of each partner.

The primary risks identified include unauthorised access, data leakage, cyberattacks, data loss, and the misuse of sensitive information. A major concern is the possibility of individuals without proper clearance gaining access to confidential reports, legal assessments, or user data. Accidental or intentional sharing of such information, along with human error or insufficient access control, could result in significant breaches. Additionally, threats such as hacking attempts, malware, and system failures pose further risk, particularly if backup and recovery procedures are inadequate.

To mitigate these risks, several partners have implemented certified systems in accordance with ISO 27001 and use CIS-compliant hardened infrastructures. Risk mitigation strategies include the implementation of strict access control measures, regular backups, version control, firewall protection, antivirus solutions, and security awareness training programs, including phishing simulations.

Data encryption practices vary among partners. While data in transit is typically encrypted using TLS 1.3, encryption at rest is less consistently applied. Where used, AES-256 is the standard for data in storage. Several partners also plan to implement role-based access controls and access logging to enhance security and accountability.

Additional data protection measures during project implementation include the use of multi-factor authentication (2FA), network segmentation, regular security audits, and penetration testing. Many partners have also instituted security procedures for their IT environments, including segmented networks, restricted syncing of work apps to company devices only, and managed antivirus and firewall solutions. Communication protocols are often in place to ensure stakeholders are informed in the event of a breach.

Data breach response procedures are generally defined and aligned with legal requirements, including GDPR. Most partners report having incident response plans in place, which include rapid threat identification, containment, analysis, and communication both internally and externally. In case of a breach, protocols include notifying the Data Protection Officer (DPO), informing affected individuals as required, and reporting to the relevant Data Protection Authority within 72 hours.

As for data retention, policies differ depending on the data type and purpose. Personal data is only stored for as long as the reason for processing it exists, while anonymised operational data and project outcome data may be stored for up to 10 years or longer. The long-term storage location varies: internal servers, institutional repositories, or certified third-party data centres are common choices. It is proposed that all data, including anonymised data, will be deposited in the public repository Zenodo.

To comply with GDPR requirements on data retention, deletion protocols are established. These include automated deletion schedules, manual verification for backups, and periodic reviews of stored data. Responsibilities for data deletion are often assigned to specific data managers, and audits may be conducted to ensure compliance.

Third-party involvement in data storage is generally limited and carefully regulated. Where third-party providers are used, such as cloud service providers or data centre operators, GDPR-compliant Data Processing Agreements (DPAs) are in place. Some partners store data on secure Microsoft cloud environments, while others rely on national providers such as Atea or Elmo ICT in Finland, responsible for server maintenance and backup integrity.

In summary, the partners in this project demonstrate a strong commitment to data security and GDPR compliance. Through the use of encryption, defined breach protocols, secure infrastructure, and careful access control, they aim to safeguard all data collected, processed, and stored throughout the project lifecycle.

7 ETHICS

At the current stage of the project, no major legal or ethical concerns regarding data sharing have been identified by all partners, who are processing personal data. All data handling procedures will comply with applicable laws, particularly the GDPR, and internal institutional policies.

All relevant partners confirmed that they will collect or process personal data, mainly limited to contact information, survey responses, or user identifiers from project applications. All participants of surveys will sign an informed consent form that explicitly states how their data will be used, stored, and (if applicable) shared in anonymised form. No data on criminal convictions or offences, no operational data for law enforcement agencies (LEAs), and no classified information on national or international grounds will be processed by the consortium. A few partners indicated the potential handling of sensitive information related to critical infrastructure protection, though access will be restricted to specific project partners when necessary. Similarly, some commercially confidential information (e.g., company-specific operational data) may be processed under Non-Disclosure Agreements (NDAs). These categories will be treated in full compliance with applicable data protection and confidentiality regulations.

Vulnerable groups, such as individuals with reduced mobility or partially disabled users, will be engaged in project activities like workshops or pilot studies. These activities will be designed to ensure ethical inclusion and uphold participants' rights. All involved individuals will be capable of providing informed consent, and ethical safeguards will be implemented. Most partners do not plan to share personal data within the consortium. If limited sharing becomes necessary - such as contact information or pseudonymised data for evaluation purposes - it will only occur with prior agreement from all involved parties and under strict GDPR-compliant conditions.

Some partners plan to implement pseudonymisation and/or anonymisation techniques where appropriate. These measures will help ensure that personal or sensitive data cannot be linked back to individuals. Methods include replacing identifiable information with unique user IDs (pseudonymisation), and removing or aggregating data to eliminate re-identification risks (anonymisation). Manual redaction and review processes will be applied where needed, especially before sharing documents externally. In specific cases—such as smart metering data or questionnaire results—data will be anonymised prior to any processing or analysis. For some partners, the need for these techniques is still under consideration and will be addressed as the project progresses.

Many project partners have developed their own research ethics policy. For example, the University of Leeds has a responsibility to ensure that all researchers and research organisations it supports have rigorously considered any ethics implications arising from the research design, methodology, conduct, dissemination, and the archiving, future use, sharing and linkage of the data produced. It has a thorough ethical review procedure[3], in line with the University's Research Ethics Policy[4], which all researchers should follow. Careful reflection and planning in relation to research ethics should not only benefit participants but should also enhance the overall quality of the research.

[3] https://secretariat.leeds.ac.uk/research-ethics/how-to-apply-for-research-ethics-approval/
[4] https://secretariat.leeds.ac.uk/wp-content/uploads/sites/109/2023/12/Research-ethics-policy.pdf

8 CONCLUSIONS

The Data Management Plan (DMP) of the ePowerMove project provides a structured and forward-looking framework for the responsible handling of data throughout the project's lifecycle. It ensures that all data - whether administrative, technical, or user-related - is managed in line with legal, ethical, and technical standards, while supporting openness, transparency, and reuse where feasible.

By categorising data into internal administrative data, technical data, and user needs and preferences, the DMP allows for a tailored application of the FAIR principles (Findable, Accessible, Interoperable, and Reusable) that reflects the specific characteristics. Internal data - such as meeting minutes, financial reports, and NDAs - will remain within the consortium for operational and legal purposes. Technical data including grid load profiles, charging station usage, and e-car sharing vehicle telematics (e.g., battery SoC, trip data), will be made available as openly as possible in interoperable formats like CSV and JSON. Some sensitive data from infrastructure operators will remain restricted and subject to legal agreements. User-related data gathered via surveys, workshops, and interviews, will be published only in an anonymised, aggregated form to protect privacy. This includes insights on mobility behaviour, charging preferences, and demographic trends from the project’s pilot sites in Finland, Austria, and Cyprus.

Future research outputs—such as V2G communication tools, optimisation algorithms, and forecasting models—will be managed in line with FAIR principles and made accessible where feasible.

This deliverable is the first version of the Data Management Plan, which presents the Data Management Plan for ePowerMove with the state of information at M6 of the project. It will be updated in M18, M30 and M42 respectively.