MECON

Ethics report and personal data management strategy

Document Summary Information

Project ID	C2022/2-3
Deliverable Number	D1.4
Deliverable Title	Ethics Report and Personal Data Management Strategy
Deliverable Lead	PMO (Beyond Vision)
Version	1.0
Editor	PMO (Beyond Vision)
Authors (organisations)	BEV, IT
Reviewers	PDMFC
Dissemination Level	Public (PU)
Contractual Due Date	M15
Submission Date	M20

CELTIC-NEXT
Σeureka Cluster

Document Revision History

Version	Date	Description of Change
0.0	28/11/2025	ToC
0.1	19/01/2026	First draft by PMO
0.2	19/01/2026	PDMFC review
0.3	26/01/2026	Second draft by PMO
0.4	27/01/2026	PDMFC review
1.0	27/01/2026	Final version

Disclaimer

This document contains material which is the copyright of certain PARTICIPANTS and may not be reproduced or copied without permission.

All PARTICIPANTS have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the PARTICIPANTS nor CELTIC-NEXT warrant that the information contained in the report is capable of use, or that use of the information is free from risk and accept no liability for loss or damage suffered by any person using this information.

Copyright Notice

Table of Contents

Contents

Executive Summary

The Ethics Report and Personal Data Management Strategy (DMS) is an essential part of the MECON project. The main purpose of the DMS is to demonstrate the consortium's commitment to managing the entire lifecycle of data involved. Thus, we are committed to identifying, designing and implementing the best practices according to the FAIR (Findability, Accessibility, Interoperability, Re-use) principles.

The proposed strategy ensures full compliance with the General Data Protection Regulation (GDPR), national data protection laws, and CELTIC-NEXT ethical requirements. It adopts privacy-by-design and data minimisation principles, defines clear roles and responsibilities, and establishes secure procedures for data collection, storage, retention, and deletion.

The document concludes that MECON poses low ethical risk and that appropriate safeguards are in place to ensure responsible and compliant project execution. This document provides for how the consortium plans to manage data related to our use-cases and intended demonstrations within the context of a longer management strategy.

List of Figures and/or List of Tables

List of Tables

Abbreviations

Abbreviation	Extended text
DMP	Data Management Plan
DMC	Data Management Council
PCA	Project Co-operation Agreement
PMO	Project Management Officer
TMO	Technical Manager Officer
IPR	Intellectual Property Right
NTN	Non-terrestrial networks
TN	Terrestrial networks

1 Introduction

The Ethics Report and Personal Data Management Strategy is an essential part of the project, in particular Work Package 1, to ensure a commitment to implement the best practices in data management.

The DMS provides a general overview of the measures that the project will follow to curate, store, process, disseminate and secure the data collected or generated within the lifetime of the project and beyond. Overall, this document describes a long-term data management strategy within the context of the project.

The DMS evolves as the project develops and will be reviewed for a fine-tuning in accordance with the data collected or generated to reflect important changes that may occur, such as new consortium policies or external factors.

This document is structured as follows: In Section 1, an overview of the project and Data Governance are outlined. Section 2 provides an overall summary of the ethical considerations we take into account in connection to the objectives of MECON. Section 3 provides an overview of the DMS, including defining the scope of information and the role of processors. Section 4 expands further on what best practices have been identified and incorporated, while Section 5 emphasises our intended alignment with GDPR principles. Section 6 states the intra-consortium measures to ensure continuous compliance and Section 7 concludes the document.

1.1 Project Description

Project Acronym	MECON
Project Title	Multi-Access Edge Computing (MEC) over NTN for beyond 5G & 6G
Project Coordinator	Peretz Shekalim
Funding Agency	CELTIC-NEXT
Consortium Members	• PenteNetworks (Coordinator) • Instituto de Telecomunicações • ISRD • Nexat • Koala Tech • Beyond Vision • PDMFC Pending funding approval: • ADVTEC Ltd • University of Exeter
Start-End Month/Year	June 2024 – May 2027
Project Description	The primary objective of the MECON project is to research and develop the technologies needed to seamlessly integrate satellite networks into future TN & NTN Unified Networks. This integration aims to ensure global connectivity that is universally accessible, available everywhere and at any time, and affordable for all. The main project innovations and outcomes are as follows: • Unification of NTN and TN encompasses concepts like native integration of air and space to enhance cost- efficiency and user experience. • Enhancing MEC operation efficiency involves aspects of power processing, steerable beams, Radio Resource Management (RRM), and dynamic allocation of network functions, to enable

	near-real time configuration and provisioning of 5G/6G RAN and Core functions dynamically over Cloud native MEC platforms of NTN platforms. • Self-Organizing Network (SON) and ISAC concepts for NTN-TN automation facilitate efficient Network Slicing, smart beam and traffic steering, and bandwidth management. • E2E delay reduction enables real-time services over NTN and URLLC services over non-static TN channels. • Multi-tenant O&M for resource sharing and neutral host networking for creation of new market opportunities. • A distributed orchestrator manages NTN-TN services and infrastructures, supporting autonomous operations across multiple clouds and domains.
Work Packages and Leaders	01. Project and Technical Management (M1-M36), led by PMO. 02. MECON Requirements, challenges and System Architecture (M1-M30), led by PenteNetworks. 03. NTN on Systems Beyond 5G (M7-M26), led by Koala Tech. 04. 5G Enabler and Operations over NTN (M7-M33), led (temporarily) by PenteNetworks. 05. Use Cases, Interoperability, Unification and Testing (M24-M36), led by Nexat. 06. Communication, Dissemination, Exploitation and Engagement (M1-M36), led by Instituto de Telecomunicações.

1.2 Ethics and Data Management Governance

To ensure rigorous and consistent handling of data throughout the project lifecycle, MECON has established a Data Management Council (DMC). The DMC oversees all data-related activities, ensuring alignment with the FAIR principles (Findable, Accessible, Interoperable, Reusable), and supporting compliance with data protection regulations such as the General Data Protection Regulation (GDPR).

The DMC is composed of representatives from key consortium partners involved in data collection, generation, analysis, and sharing. It brings together expertise from both technical and ethical/legal perspectives. Its primary responsibilities include:

- Monitoring implementation of the Data Management Plan (DMP), including necessary updates.
- Ensuring compliance with ethical, legal, and security obligations related to data protection.
- Supporting classification of data and validation of storage, access, and sharing policies.
- Advising on the necessity and implementation of Data Protection Impact Assessments (DPIAs).
- Providing guidance on metadata standards, data formats, and data interoperability.
- Overseeing the application of FAIR principles and preparation of datasets for long-term use and open access.
- Advising on data preservation, reuse, and deletion policies.

The DMC collaborates closely with the Project Coordinator, and Work Package Leaders to ensure that data governance is integrated across all project activities.

The members of the DMC are:

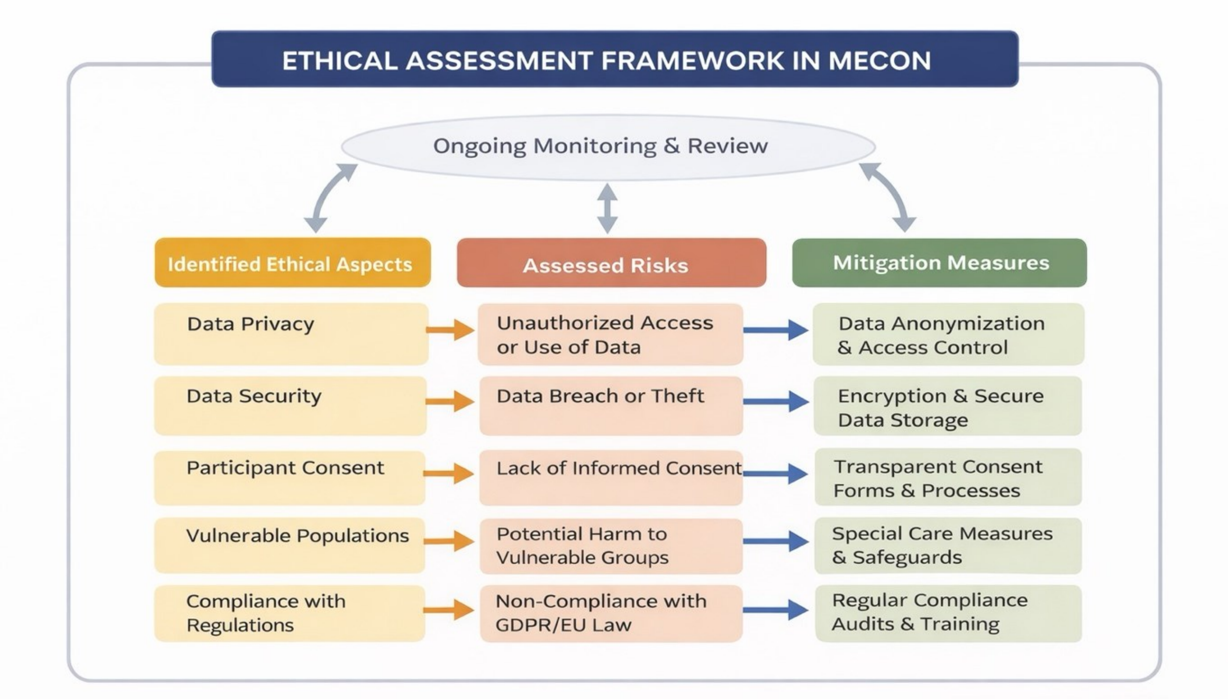
Partner	Member Name
Instituto de Telecomunicações (Chair)	Joaquim Bastos
Beyond Vision (Current PMO)	Natalia Tsolaki
PDMFC	Paolo Calciati

2 Ethical Summary

This section examines the ethical dimensions of the MECON project in a holistic and proportionate manner. Rather than treating ethics as a narrow compliance exercise, the analysis considers the broader societal, environmental, and governance implications of developing advanced telecommunications solutions and associated Proof-of-Concept (PoC) activities. Given MECON's technical focus, non-intrusive methodologies, and absence of direct human experimentation, ethical risks are limited in scope and intensity. Where potential concerns do arise, they are identifiable at an early stage and can be effectively addressed through established ethical principles, regulatory frameworks, and project-level safeguards.

Figure 1 presents the ethical assessment framework applied within MECON, illustrating how relevant ethical aspects are identified, how potential risks are assessed, and how proportionate mitigation measures are integrated into project activities through ongoing monitoring and review.

Figure 1. Ethical Assessment Framework


ETHICAL ASSESSMENT FRAMEWORK IN MECON
Ongoing Monitoring & Review
Identified Ethical Aspects
Assessed Risks
Mitigation Measures
Data Privacy
Unauthorized Access or Use of Data
Data Anonymization & Access Control
Data Security
Data Breach or Theft
Encryption & Secure Data Storage
Participant Consent
Lack of Informed Consent
Transparent Consent Forms & Processes
Vulnerable Populations
Potential Harm to Vulnerable Groups
Special Care Measures & Safeguards
Compliance with Regulations
Non-Compliance with GDPR/EU Law
Regular Compliance Audits & Training

Overview of Potential Ethical Concerns

The ethical assessment of MECON begins with a screening of ethical domains typically relevant to research and innovation projects, with particular attention to those that may arise in large-scale telecommunications and infrastructure-oriented initiatives.

MECON does not involve medical or clinical research, interventions on human subjects, behavioural experiments, or the intentional collection of sensitive personal data. The project does not target children or vulnerable populations, nor does it seek to influence individual decision-making, behaviour, or rights. As such, many high-risk ethical categories commonly associated with social, biomedical, or surveillance-oriented research are not applicable.

Ethical considerations relevant to MECON instead arise primarily from its role in developing and validating advanced digital and communication technologies that may ultimately support critical infrastructure and future deployment scenarios. These considerations include:

- the responsible design and testing of technologies with potential downstream societal impact;
- proportionality and necessity in the use of experimental platforms and PoCs;
- transparency and accountability in research activities;

- environmental and contextual sensitivity during technical demonstrations.

In this context, MECON may include limited PoC activities, such as demonstrations involving unmanned aerial systems or radio infrastructure components, conducted strictly for technical validation. While these activities are not designed to interact with individuals, there is a residual ethical consideration related to the surrounding environment in which demonstrations take place, including the possibility of incidental interaction with public or private spaces. These concerns are addressed through careful site selection, operational planning, and adherence to applicable regulatory and ethical standards.

Overall, the ethical profile of MECON is characterised by low intrinsic risk, with ethical relevance emerging primarily at the level of responsible innovation and contextual awareness rather than direct impact on individuals.

Table 1. Overview of potential ethical concerns in the MECON project

Ethical Area	Description	Applicability to MECON	Risk Level	Remarks
Personal Data Protection	Processing of personal data such as names, professional contact details, and affiliations	Applicable (limited scope)	Low	**Data limited to project coordination and dissemination activities**
Sensitive Personal Data	Processing of special categories of data (Article 9 GDPR)	Not applicable	None	**No health, biometric, political, or other sensitive data processed**
Vulnerable Groups	Involvement of children or other vulnerable populations	Not applicable	None	**No interaction with vulnerable individuals or groups**
Human Subjects Research	Research involving direct participation of individuals	Not applicable	None	**No experiments, interviews, or behavioural studies conducted**
Surveillance or Monitoring	Systematic observation or monitoring of individuals	Not applicable	None	**MECON does not deploy monitoring or tracking technologies**
Data Security	Risk of unauthorized access, data loss, or breaches	Applicable (limited)	Low	**Mitigated through access control and secure storage**
Regulatory Compliance	Compliance with GDPR and national data protection laws	Applicable	Low	**GDPR-compliant procedures implemented by all partners**
Ethical Governance	Oversight mechanisms for ethical and data protection issues	Applicable	Low	**Responsibilities clearly assigned within consortium**
Drone-based Proofs of Concept	Use of drones for technical validation may incidentally capture personal data via sensors	Applicable (limited scope)	Low	**Flights are controlled; no intentional personal data collection; mitigation measures applied**

2.1 Analysis of Ethical Risks Related to Project Activities

Building on the identification of relevant ethical domains, MECON's ethical risks are assessed in qualitative terms, focusing on the likelihood and potential impact of harm to individuals, society, or the environment.

From a societal perspective, the project's research activities are oriented toward improving the resilience, efficiency, and interoperability of telecommunications systems. Ethical risk therefore does not stem from the research objectives themselves, but from the need to ensure that experimental activities remain proportionate, transparent, and aligned with public interest. This includes avoiding unnecessary intrusion into public spaces and ensuring that demonstrations are clearly bounded in scope and duration.

From an environmental standpoint, MECON recognises that even small-scale technical demonstrations may have localized effects, such as temporary noise, energy consumption, or physical presence of equipment. While these effects are minimal and short-lived, they are nevertheless considered as part of the ethical assessment. PoC activities are designed to minimise environmental footprint, comply with applicable regulations, and avoid sensitive locations wherever possible.

At the governance level, ethical risk is linked to the management of responsibilities within the consortium. Clear allocation of roles, documented procedures, and internal oversight mechanisms ensure that ethical considerations are not treated as ad hoc concerns but are embedded into project planning and execution.

Taken together, the identified ethical risks are assessed as low and manageable, arising mainly from contextual and operational factors rather than from the nature of the research itself. Importantly, these risks do not accumulate or compound across work packages, further supporting the conclusion that MECON does not raise systemic ethical concerns.

2.2 Overall Ethical Impact and Proportionality

The final step of the ethical assessment considers the overall ethical impact of MECON in light of its objectives, methods, and safeguards. The project's limited engagement with individuals, absence of invasive techniques, and focus on technical validation support a finding of low ethical impact.

Crucially, MECON adheres to the principle of proportionality: ethical safeguards are commensurate with the scale and nature of the activities undertaken. Rather than imposing heavy approval or oversight mechanisms that would be disproportionate to the risks involved, the project integrates ethical awareness into standard project governance, risk management, and compliance processes.

The ethical framework applied ensures that:

- potential ethical issues are identified early;
- mitigation measures are preventive rather than reactive;
- ethical considerations evolve alongside technical development through continuous monitoring.

On this basis, MECON does not require additional ethical authorisation procedures beyond those already embedded in its governance structure and applicable regulatory obligations. The project demonstrates responsible research and innovation practices, ensuring that technological advancement is pursued in a manner that is socially acceptable, environmentally conscious, and ethically sound.

3 Personal Data Summary

This section explains how personal data are defined, identified and governed in the MECON project. It clarifies what personal data may be processed, who the relevant data subjects are, and how responsibilities are shared across the consortium.

In MECON, personal data may arise both from day-to-day project management activities (such as coordination, meetings, reporting and collaboration) and from communication, dissemination and exploitation actions involving external stakeholders.

This section provides the basis for the procedures described in Section 4 by defining the scope of processing and the roles applied across the consortium.

3.1 Definition and Scope of Personal Data

For MECON, “personal data” refers to any information relating to an identified or identifiable natural person, in line with GDPR. In practice, MECON mainly processes basic professional identification and contact details needed to run the project and to engage with external stakeholders when relevant. This includes, for example, names and professional contact details of partner representatives and staff involved in project governance and daily execution.

In MECON, personal data typically fall into two areas. The first relates to project management and governance, such as contact lists, meeting invitations, attendance records and minutes, as well as documents stored and shared through project repositories (including the electronic library of major project documents and deliverables). The second relates to communication, dissemination and exploitation activities, for example through the project website and online channels, the organisation of workshops and events, and internal tracking of dissemination actions and related materials. Exploitation activities may also involve maintaining professional stakeholder contact details for outreach and follow-up, where this is necessary and proportionate.

MECON does not require the processing of special categories of personal data, and personal data are not part of the project’s technical objectives. Where personal data appear in project documentation or engagement records, they are limited to what is needed for coordination, reporting, dissemination and exploitation planning, and are handled in line with the data minimisation and purpose limitation principles described in this strategy.

3.2 Identification of Data Subjects

In MECON, the main data subjects are individuals whose personal data may be processed as part of routine project management and the project’s communication, dissemination, exploitation and engagement activities. This includes consortium personnel involved in execution and governance, such as staff contributing to project management, technical coordination, quality assurance and reporting.

MECON also engages external actors through dissemination and exploitation activities, including stakeholder engagement, communication of results through appropriate channels, and the organisation of workshops. As a result, data subjects may also include external stakeholders who interact with MECON through these activities, such as workshop registrants and attendees, participants at conferences and industrial events, and contacts involved in exploitation-related exchanges. The project also plans a public website and internal tracking of dissemination actions and related materials; where these activities involve collecting professional contact details for invitations, registration, follow-up communication, or evidence of dissemination, the individuals concerned fall within the scope of this strategy.

3.3 Roles: Data Controllers, Processors, and Recipients

Personal data processing in MECON is organised according to the three roles defined by GDPR: Data Controller, Data Processor and Recipient. This applies both to project management data (such as contact lists, meeting attendance records and minutes) and to personal data associated with dissemination and exploitation activities (such as stakeholder contact databases). Given MECON's consortium set-up, it is important to clarify how these roles apply in practice.

A **Data Controller** is the organisation that determines the purposes and essential means of processing personal data. In MECON, each partner acts as Data Controller for the personal data it collects and processes within its own responsibilities, such as managing contact details for coordination, handling meeting-related records, or managing stakeholder contact details connected to dissemination and exploitation activities.

A **Data Processor** processes personal data on behalf of a Data Controller and only under the Controller's instructions. In MECON, this role may apply where a partner or an external service provider operates tools or platforms used for project administration, such as shared repositories or managed collaboration infrastructure, on behalf of another partner.

A **Recipient** is any entity to whom personal data are disclosed. In MECON, recipients may include other consortium partners where sharing is necessary for project execution (for example, circulating meeting minutes or participant lists) and programme-level bodies where disclosure is required for reporting, review or audit activities. Disclosures are limited to what is necessary and follow access-control and need-to-know principles.

This allocation of roles supports accountability and consistent data protection across the project, while keeping sharing and access limited to what is needed for MECON objectives.

4 Procedures for Fair Data Management

This section outlines the concrete procedures applied by the MECON consortium for handling personal data throughout their lifecycle. In line with best practices observed in Horizon Europe deliverables, it addresses data collection, storage, protection, retention, and destruction, demonstrating how GDPR principles are translated into operational measures.

4.1 Data Collection: Methods and Justification

Data collection within MECON is driven by clearly defined project needs and adheres to the principles of necessity and proportionality. Only data that are required to support project implementation, coordination, dissemination, and technical validation activities are collected.

- Personal data collection is limited to contexts such as:
- project coordination and internal communication;
- organisation and reporting of meetings, workshops, and dissemination events;
- fulfilment of contractual, administrative, and funding obligations.

Data minimisation is applied systematically, ensuring that no superfluous or excessive information is gathered. Data collection activities related to stakeholder engagement, dissemination, and market-oriented interactions are further detailed in Deliverable D6.2 (Intermediate Exploitation Plan). These activities follow the same data governance principles described in this report and do not introduce additional ethical or legal risks.

Where Proof-of-Concept activities involve technical demonstrations using drones or other sensing-enabled platforms, data collection is strictly confined to what is necessary for technical validation. Any incidental capture of personal data is neither intentional nor required for project objectives and is avoided through appropriate sensor configuration, controlled environments, and limited operational duration.

4.2 Data Storage: Platforms and Security Measures

MECON adopts a structured storage strategy to ensure the integrity, confidentiality, and availability of data. Data are stored on secure platforms operated by consortium partners, including institutional servers and protected cloud-based services.

Access to stored data is governed by role-based permissions and is restricted to authorised personnel only. Security measures include:

- role-based access control;
- strong authentication mechanisms;
- regular system updates and security monitoring;
- routine backups to prevent data loss.

Storage solutions are selected to balance accessibility for legitimate project use with appropriate safeguards against unauthorised access, loss, or misuse.

4.3 Data Protection: GDPR Compliance and Technical Safeguards

All data handling activities in MECON comply with the principles set out in the General Data Protection Regulation (GDPR), including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality.

Consortium partners implement appropriate technical and organisational measures to ensure that data are protected throughout their lifecycle. Responsibilities for data handling are clearly allocated within the consortium, ensuring accountability and traceability.

For drone-based Proofs of Concept, **privacy-by-design** principles are applied as a precautionary measure. These include minimising sensor activation, avoiding populated or sensitive areas, and applying post-processing measures such as deletion or anonymisation of non-relevant data. A case-by-case assessment is performed to determine whether additional safeguards are required, taking into account the specific operational context of each demonstration.

4.4 Data Retention: Policies and Timeframes

Data retention within MECON is governed by clearly defined criteria linked to project objectives and applicable legal requirements. Personal data are retained only for as long as necessary to fulfil their intended purpose.

Upon completion of the project, data will be deleted or anonymised unless continued retention is required by law or justified for audit, reporting, or accountability purposes.

Data generated during Proof-of-Concept activities, including drone-based demonstrations, are retained only for the period necessary to assess technical performance and validate results. Once this purpose has been fulfilled, such data are securely deleted or anonymised.

4.5 Data Destruction: Procedures and Verification

At the end of their lifecycle, data are securely destroyed in accordance with institutional policies and recognised best practices. Secure deletion methods are applied to ensure that data cannot be recovered once destruction has taken place.

Responsibility for data destruction lies with the respective Data Controller within each consortium partner organisation. Where required, verification procedures are applied to confirm that deletion has been completed in line with applicable standards.

5 Compliance with GDPR and CELTIC-NEXT Requirements

This section demonstrates MECON's compliance with applicable data protection regulations and programme-level ethical requirements. It describes how GDPR principles are operationalised within the project, how the need for Data Protection Impact Assessments (DPIAs) is assessed and how compliance is documented and monitored throughout the project lifecycle.

The measures described reflect the limited and low-risk nature of personal data processing within MECON, while ensuring that appropriate safeguards and escalation mechanisms are in place should project activities evolve.

5.1 GDPR Implementation in MECON

MECON ensures compliance with the General Data Protection Regulation (GDPR) across all activities involving the collection and processing of personal data. Personal data are processed primarily in the context of project coordination, stakeholder engagement, dissemination activities, and fulfilment of contractual and funding obligations.

Such processing may include personal data of consortium members and external stakeholders (e.g. names, professional affiliations, contact details), as well as limited data collected through voluntary participation in meetings, workshops, or dissemination events. All processing activities are conducted in accordance with GDPR principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, and integrity and confidentiality.

MECON does not intentionally collect personal data through technical experimentation. However, limited Proof-of-Concept activities may involve platforms equipped with sensing or recording capabilities (e.g. drones used for technical validation). While the primary focus of these activities is on technical and operational parameters, there is a possibility of incidental capture of personal data (e.g. individuals or private property within the operational environment). In such cases, GDPR principles are strictly applied, including minimisation of data collection, anonymisation or deletion of non-relevant data, and secure storage and access control.

MECON ensures that data subjects are able to exercise their rights under the GDPR, including the right of access, rectification, erasure, and restriction of processing. Personal data are relevant and limited to project purposes, and retention periods are clearly defined in line with the data minimisation principle.

5.2 Assessment of DPIA Requirement

Article 35 of the GDPR requires a Data Protection Impact Assessment (DPIA) where data processing is likely to result in a high risk to the rights and freedoms of natural persons. A DPIA serves to describe the processing, assess its necessity and proportionality, and identify mitigation measures for potential risks.

5.1.2. General Data Processing Activities in MECON

Based on the data processing activities foreseen within MECON at the time of writing, a project-wide DPIA is not required under Article 35 GDPR. In particular:

- MECON does not involve systematic or extensive evaluation of individuals, profiling, or automated decision-making that would significantly affect data subjects;
- No large-scale processing of special categories of personal data is performed;
- MECON does not engage in systematic monitoring of publicly accessible areas;
- Personal data processed for project management, dissemination, and voluntary stakeholder engagement are limited in scope and adhere to the principles of data minimisation and purpose limitation.

In line with the European Data Protection Board (EDPB) Guidelines on DPIAs (WP248), a DPIA is typically required only where multiple high-risk criteria are met simultaneously. MECON's general data processing activities do not meet these thresholds.

Accordingly, no formal DPIA is required for general project data processing at this stage. Data protection risks are nevertheless monitored on an ongoing basis, and the need for a DPIA will be reassessed should new or substantially modified processing activities arise.

5.2.2. Proof-of-Concept Activities and Mission-Level DPIA Assessment

MECON acknowledges that certain Proof-of-Concept activities, particularly those involving drones or other mobile platforms, may introduce context-specific privacy considerations due to the possibility of incidental personal data capture. To address this, MECON applies a **mission-level DPIA assessment approach**, proportionate to the scale and nature of the activity.

Responsibility for assessing DPIA requirements lies with the consortium partner conducting the PoC activity. The assessment considers factors such as:

- the presence of individuals in the operational area;
- the sensitivity of the environment (e.g. private property or restricted spaces);
- the visibility of the activity and public awareness measures.

Where relevant, the following safeguards are applied:

- **Pre-activity assessment** to determine whether a DPIA is required for the specific mission;
- **Data minimisation in practice**, including planning activities to avoid populated areas and limiting sensor activation to what is technically necessary;
- **Privacy-by-design measures**, such as short recording windows and deletion or anonymisation of non-relevant data during post-processing;
- **Transparency measures**, where appropriate, including information notices or contact points enabling the exercise of data subject rights;
- **Secure data management** throughout the data lifecycle, with access restricted to authorised personnel.

This mission-level approach ensures that any personal data processing associated with PoC activities remains proportionate, transparent, and compliant with GDPR requirements, while avoiding unnecessary procedural burdens where risks are demonstrably low.

5.3 Monitoring and Auditing Procedures

Data protection compliance within MECON is supported through structured documentation, monitoring, and internal review mechanisms coordinated by the **Data Management Council (DMC)**. The DMC oversees data processing activities across the consortium, ensuring consistency with GDPR requirements, CELTIC-NEXT ethical standards, and the procedures defined in this deliverable.

Data processing activities are documented by consortium partners in accordance with their institutional procedures and applicable legal requirements and are subject to review by the DMC. Any personal data incidents or breaches, should they occur, are managed in line with GDPR Articles 33 and 34, including notification to supervisory authorities and affected data subjects where required. The DMC supports coordination, documentation, and follow-up actions related to such incidents.

Compliance with GDPR and CELTIC-NEXT ethical requirements is monitored on an ongoing basis by the DMC and reviewed periodically during consortium meetings. The Project Coordinator is informed of relevant findings and supports the implementation of corrective actions where necessary. Documentation and procedures are updated as the project evolves or where changes in processing activities or regulatory guidance require adjustment.Measures to Ensure Ethics Standards

This section presents the organisational and procedural measures adopted within MECON to ensure that ethical standards are consistently upheld throughout project lifecycle. The measures outlined reflect the project's low-risk ethical profile while ensuring that appropriate oversight, awareness and response mechanisms are in place in line with European best practices.

5.4 Ethical Review Processes

Ethical considerations in MECON are reviewed as part of routine project planning, implementation, and review activities. The ethical implications of project tasks are assessed at the design stage and revisited where project activities evolve or new use cases are introduced.

The Data Management Council (DMC) plays a central role in supporting ethical oversight related to data processing activities, including the identification of potential risks and the review of mitigation measures. Where activities involve new or modified data processing operations—such as additional Proof-of-Concept demonstrations—these are assessed prior to implementation to confirm that existing safeguards remain appropriate.

Where necessary, ethical issues or uncertainties are escalated to the Project Coordinator for coordination and resolution at consortium level. This ensures that ethical considerations are addressed in a timely and proportionate manner.

5.5 Training and Awareness for Consortium Members

MECON promotes awareness of ethical and data protection responsibilities among consortium members through internal coordination, guidance, and information-sharing activities. Consortium partners are informed of relevant GDPR obligations, ethical principles, and project-specific procedures through project documentation and regular communication.

Targeted guidance is provided to partners involved in activities with higher contextual relevance—such as stakeholder engagement or Proof-of-Concept demonstrations—to ensure that ethical considerations are understood and applied in practice. This includes awareness of data minimisation, transparency, and privacy-by-design principles.

Rather than formal training programmes, MECON adopts a proportionate approach focused on ensuring that relevant personnel have adequate understanding of their responsibilities in relation to the specific tasks they perform.

5.6 Incident Response and Breach Notification

Although the likelihood of ethical incidents or personal data breaches in MECON is low, the project has established clear procedures to respond effectively should such events occur.

In the event of a personal data incident, the consortium partner responsible for the affected data will activate its internal incident response procedures in line with GDPR requirements. This includes prompt assessment of the incident, containment measures, and documentation.

The DMC supports coordination and oversight of incident handling, ensuring that reporting obligations under GDPR Articles 33 and 34 are met where applicable. The Project Coordinator is informed of any significant incidents and supports communication and corrective actions at consortium level.

Lessons learned from incidents, where relevant, are used to refine procedures and strengthen preventive measures for the remainder of the project.

6 Conclusions and Recommendations

This deliverable has outlined a structured and proportionate approach to ethics and personal data management within the MECON project. The ethical assessment demonstrates that MECON presents a low-risk profile, with no involvement of vulnerable populations, no intrusive research activities, and only limited processing of basic personal data required for project coordination, dissemination, and stakeholder engagement. Ethical considerations are integrated into the project's governance framework and addressed through preventive, context-appropriate measures rather than ad hoc controls.

Data management within MECON follows the FAIR principles and is supported by clearly defined procedures covering the full data lifecycle, as well as compliance with GDPR and CELTIC-NEXT ethics requirements. Oversight by the DMC, combined with ongoing monitoring and review, ensures that ethical and data protection safeguards remain effective as the project evolves. This approach supports transparency, accountability, and responsible innovation throughout the project duration, while allowing flexibility to adapt procedures in response to future developments or regulatory changes.