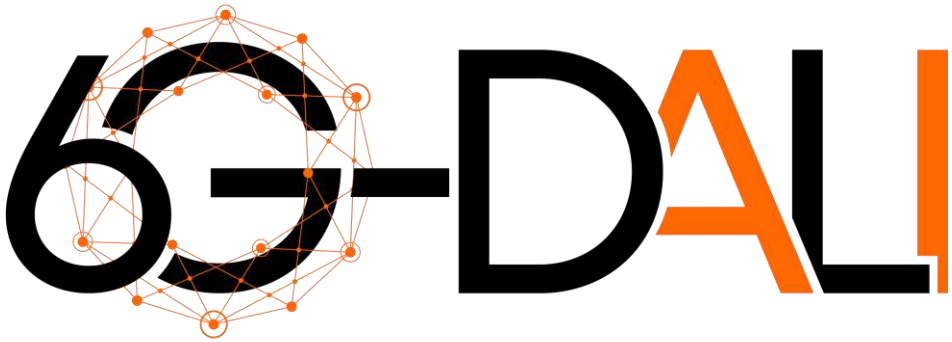
16th March, 2026



6G-DALI compliance with data legislation and ethical requirements - Initial

Deliverable 2.4, Work Package 2

Co-funded by the European Union

6GSNS

6G-DALI project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe Research and Innovation programme under Grant Agreement No 101192750. 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 SNS JU. Neither the European Union nor the SNS JU can be held responsible for them.

Project Identifier	HORIZON-JU-SNS-2024-STREAM-B-01-08, Project 101192750		
Project Name	6G DAta and ML operations automation via an end-to-end AI framework		
Acronym	6G-DALI		
Start Date	01 January 2025	End Date	31 December 2027
Project URL	www.6gdali.eu		
Deliverable	D2.4 "6G-DALI compliance with data legislation and ethical requirements-Initial"		
Work Package	WP2 - 6G-DALI Framework architecture and business model		
Contractual due date	28/02/2026	Actual submission date	16/03/2026
Type	R	Dissemination Level	Public
Lead Beneficiary	CEL		
Responsible Author	Francesca Morpurgo (CEL), Lucas Pereira Carwile (CEL), Valeria Cesaroni (CEL), Carmela Occhipinti (CEL), Luigi Briguglio (CEL), Antonio Fiorentino (CEL)		
Contributors	Michalis Rantopoulos (OTE)		
Peer reviewer(s)	Theodora Tsapikouni (ISI/ATH), Vasiliki Parousidou (ICOM)		
Version	**Authors**	**Comments**	
1.0	CEL	Final release submitted	

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial Intelligence
AI Act	Regulation EU 2024/1689 “Artificial Intelligence Act”
AIaaS	AI-as-a-Service
CEN	European Committee for Standardization (French: Comité Européen de Normalisation)
CENELEC	CENELEC stands for the European Committee for Electrotechnical Standardization (French: Comité Européen de Normalisation Électrotechnique)
DataOps	Data Operations
Data Act	Regulation EU 2023/2854
DGA	Regulation EU 2022/868 “Data Governance Act”
DPIA	Data Protection Impact Assessment
EL-HL-R	Ethics and Legal High-Level Requirement
EL-LL-R	Ethics and Legal Low-Level Requirement
EL-ML-R	Ethics and Legal Medium-Level Requirement
ETHAI	Ethics of Artificial Intelligence
ETSI	European Telecommunications Standards Institute
GDPR	Regulation EU 2016/679 “General Data Protection Regulation”
GPAI	General-Purpose Artificial Intelligence
HPO	Hyperparameter Optimization
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KV	Key Value
KVI	Key Value Indicator
MLOps	Machine Learning Operations
ODD	Operational Design Domain
OOD	Out-Of-Domain
PoC	Proof-of-Concept
QMS	Quality Management System
QoS	Quality of Service
RLOps	Reinforcement Learning Operations
SNS JU	Smart Networks and Services Joint Undertaking
SSH	Social Sciences and Humanities

STEM	Science, Technology, Engineering, and Mathematics
SQuaRE	System and Software Quality Requirements and Evaluation
ZSL	Zero-Shot Learning

Executive Summary

Deliverable D2.4, entitled "6G-DALI compliance with data legislation and ethical requirements – Initial" serves as the foundational report for establishing a robust governance framework within the 6G-DALI project. This document primarily addresses the ethical and regulatory dimensions of an AI-native 6G network architecture. It focuses specifically on the upstream activities of dataset retrieval, curation, and generation intended for machine-learning training as a core requirement for 6G development. By positioning these data-driven preparatory tasks within a normative framework, the deliverable ensures that societal values and legal obligations are integrated into the technology from its earliest design phases.

The purpose of this deliverable is to operationalise ethical principles and regulatory requirements into concrete, design-oriented constraints through an ethics-by-conception approach. It aims to safeguard fundamental rights (e.g., privacy, dignity, and non-discrimination) while embedding governance principles such as transparency, accountability, and human oversight directly into the architectural and functional design of the 6G ecosystem. By defining a structured, design-embedded methodology that integrates ethical principles and regulatory requirements from the earliest stages of system conception through to validation, the project provides a pathway for 6G researchers and industry stakeholders to share qualified, compliant datasets within a secure European 6G Data Space, thereby supporting the reliable and trustworthy development of next-generation networks.

The work carried out relied primarily on the Ethics of AI (ETHAI) model as the core methodological framework. ETHAI was applied as a lifecycle-oriented governance instrument, enabling the translation of high-level ethical values and binding regulatory obligations into traceable, assessable design requirements. Elements inspired by the Social Acceptance of Technology (SAT) approach informed selected parts of the analytical process, particularly in framing context-sensitive considerations and reflecting on previously identified societal expectations. In this respect, the consortium also built upon results and empirical insights generated in earlier projects (e.g., 6G4Society) where structured analyses of social perceptions and acceptance dynamics had already been conducted. These prior findings were used as contextual background knowledge rather than through a full re-application of the SAT methodology within 6G-DALI. The combined analytical effort enabled the consortium to perform a structured review of the European ethical and regulatory landscape, incorporating key binding instruments such as the GDPR, AI Act, Data Act, and Data Governance Act. This process led to the identification of 14 primary ethics and regulatory risks (e.g., “Validation Mismatch” and “Silent Policy Change”) associated with the AI-native characteristics of 6G systems. These risks provide a detailed elaboration of risks “Lack of compliance with trustworthy legal and ethical requirements” and “Difficult to understand and apply legal and ethical requirements” identified during the project proposal phase.

These risks were subsequently mapped to a three-level hierarchy of requirements consisting of 11 ethics and legal high-level requirements (EL-HLRs), linked to ethics and regulatory principles, and 37 medium-level requirements (EL-MLRs), derived from the EL-HLRs and contextualised with respect to use cases and architectural layers and components.

The third level builds on 70 technical functional and non-functional requirements previously defined in Deliverable D2.2. In this deliverable, these technical requirements were systematically mapped against the EL-MLRs to establish a preliminary set of low-level requirements (EL-LLRs). This mapping represents an initial alignment step rather than a finalised correspondence. Further work will be carried out in the coming months to refine and stabilise the relationship between the medium-level ethics and legal requirements and the technical functional and non-functional specifications, as architectural development progresses.

The project built upon the seven Key Value Indicators (KVIs) already defined during the proposal phase, treating them as stable reference points to be maintained throughout the development process. Rather than establishing new KVIs, the work analysed and operationalised them within the ETHAI framework, linking each KVI to concrete ethics and regulatory requirements in order to enable structured monitoring of their implementation.

In addition, five categories of evidence artefacts were defined as part of the ETHAI governance layer. These artefacts are structured verification instruments designed to document, substantiate, and trace

the implementation of ethics and legal requirements across the system lifecycle. They serve as formalised mechanisms to demonstrate alignment between normative commitments, technical specifications, and operational practices, thereby enabling traceability, accountability, and auditability within the 6G-DALI framework.

Although the activities addressed in 6G-DALI operate at a preparatory research stage, focusing on dataset retrieval and generation for AI training, and therefore do not systematically trigger all regulatory obligations applicable to deployed systems, the project has deliberately adopted an anticipatory governance approach. Regulatory principles and constraints were integrated from the outset, even where not strictly mandatory at this stage, to ensure normative coherence and to reduce potential downstream risks in safety-critical 6G contexts. This early integration strengthens the project's capacity to align emerging 6G technologies with European legal standards and value-based digital governance.

Overall, the governance architecture established in this deliverable creates a structured point of convergence between the Social Sciences and Humanities (SSH) and the Technology and Engineering (STEM) components of the consortium. Through this collaboration, ethics and regulatory risks were identified, prioritised, and translated into structured requirements aligned with technical development. The preliminary alignment between normative objectives and system specifications represents a significant step toward embedding iterative ethics-by-conception assessment within the ongoing evolution of 6G technology.

By integrating normative constraints into architectural choices at an early stage, 6G-DALI contributes to shaping a European approach to AI-native 6G that combines technological innovation with regulatory readiness and value-based design. The framework will be progressively refined and consolidated as the architecture matures, with a stabilised and integrated version foreseen by the end of 2026.

1 Introduction

This document, identified as Deliverable **D2.4** and entitled "**6G-DALI compliance with data legislation and ethical requirements – Initial**", is the first outcome of project task T2.4 "Societal acceptance, and compliance with data legislation and ethical requirements". This task builds on the Social Acceptance of Technology (SAT) methodology[1] , a main outcome[2] of the 6G4Society project[3] , extending and consolidating an outcome[4] of the 5G-SOLUTIONS project[5] . Within 6G-DALI, this methodological foundation is further developed to analyse the societal, ethical, and legal dimensions of the project in a way that enables emerging considerations to be embedded and assessed during technology design and development.

In this context, Deliverable D2.4 examines 6G-DALI's compliance with data legislation and ethical requirements. Compliance is understood here primarily as regulatory compliance, namely, adherence to applicable EU laws and regulations. However, it also encompasses ethical compliance, grounded in relevant domain-specific frameworks.

Drawing on these sources and on indicators (i.e., Key Value Indicators - KVIs), fixed at proposal stage in alignment with prior Smart Networks and Services Joint Undertaking (SNS JU)[6] work, a structured set of **requirements** is derived to translate **legal obligations and ethical principles** into operational and design-oriented constraints. These requirements are intended to be incorporated from the earliest stages of system design. Rooted in **core ethical and regulatory principles**, they represent central project commitments: their fulfilment, demonstrated through **evidence-based artefacts** during the assessment phase, substantiates both ethical and data regulatory compliance.

Ensuring compliance with **ethical and regulatory requirements** is essential to guarantee that 6G-DALI technological solutions and their applications **respect and protect fundamental rights** (such as privacy, data protection, dignity, and non-discrimination), uphold the constitutional values of the Union, and advance broader regulatory objectives and governance principles, including safety, well-being, transparency, and accountability. To this end, the project integrates Social Sciences and Humanities (SSH) perspectives and methodologies throughout its research activities. This interdisciplinary approach enables a comprehensive analysis of potential **risks** and impacts on ethical, social, and legal values, as well as on the rule of law.

To achieve this objective, the document sets out the project approach, structured around the following core elements:

- The **methodological framework,** which supports the development team from the identification of societal values through the definition of the ethics and regulatory requirements, and ultimately to the compliance assessment process;
- The **ethics and regulatory framework,** identifying the ethics and legal instruments, principles, and guidelines relevant for ensuring compliance;
- The identification and contextualisation of **societal concerns, values** and **related KVIs**;
- The analysis of potential **ethics and regulatory risks,** namely those risks that may undermine protected values or breach applicable rules, and which have therefore to be monitored, mitigated and assessed throughout system development. These risks provide a detailed elaboration of risks identified during the project proposal phase;
- The elicitation of **ethics and regulatory requirements,** defined to address the identified concerns and to operationalise compliance within the project lifecycle.

These elements are reflected in the structure of the present document, which mirrors the steps followed through the 6G-DALI methodology described herein. The methodological steps are implemented incrementally and iteratively, allowing for the progressive refinement and consolidation of requirements as the project evolves.

Accordingly, this document represents the initial release of the compliance assessment framework for 6G-DALI. An updated and consolidated version will be issued at the end of the project's second year, reflecting further methodological iterations and technical developments.

1.1 Mapping 6G-DALI outputs

The purpose of this section is to map 6G-DALI Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed (see Table 1).

Table 1. Adherence to 6G-DALI GA Deliverable & Tasks Descriptions

Deliverable description			
D2.4 '6G-DALI compliance with data legislation and ethical requirements- Initial' - Report on requirements for ethical data sets and AI algorithms, reflecting societal values - Initial version			
6G-DALI Task No. and Title	**6G-DALI GA Task Description**	**Respective document section(s)**	**Justification**
Task 2.4 Societal acceptance, and compliance with data legislation and ethical requirements	The task will define the requirements for ethical data sets and AI algorithms, reflecting societal values and addressing biases and risks associated with data collection and analysis. This includes implementing a model, called ETHAI, based on the seven key requirements of EU trustworthy AI guidelines (human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability) and the AI Act, as well as the relevant EU regulatory framework (e.g. Data Act, GDPR) to ensure their wide acceptance and usage for future initiatives.	2. Methodological framework toward 6G-DALI compliance	It describes the methodological framework to ensure compliance, including the ETHAI model and the process to perform the compliance assessment, from the identification of value-driven concerns and risks to the elicitation of requirements.
		3. 6G-DALI European ethics and regulatory background	It describes the relevant European ethics and regulatory principles and rule of laws that are applied in 6G-DALI during the development and the compliance assessment.
		4. 6G-DALI value-driven concerns	It recalls the concerns, the values and the KVIs already defined at project proposal time.
		5. 6G-DALI Ethics and regulatory risks	It performs the ethics and regulatory analysis and provides insights in terms of potential risks. The analysis is carried out on 6G-DALI Architecture (defined in D2.2 and D2.3), Proof-of-Concepts and Uses Cases (defined in D2.1) with respect to the principles identified in Section 2. These risks are mitigated and addressed by implementing safeguards defined in terms of requirements, defined in the next section.
		6. 6G-DALI Ethics and regulatory requirements	It provides the initial formal description of requirements to ensure 6G-DALI compliance with relevant ethics and regulatory principles. The section also provides KVIs, evidence artefacts and links to system requirements to assess compliance.

1.1 Deliverable overview and report structure

This document consists of the following sections which may be summarised as below:

- **Section 1**: Introductory part to the document with clear identification of the sections' contents.
- **Section 2**: This section describes the methodological framework to be used during the whole 6G-DALI project to perform the compliance assessment with respect to the ethics and regulatory aspects. This methodology shows how the compliance is ensured through the identification of potential risks, key value indicators (KVIs) and corresponding requirements to be fulfilled during the assessment. A special focus is devoted to ethics of Artificial Intelligence (AI).
- **Section 3**: This section describes the identified ethics and regulatory principles relevant to the 6G-DALI development, including the rationale of these principles to be followed.
- **Section 4**: This section reports the initial analysis with respect to ethics and regulatory aspects, performed according to the methodological framework. This part identifies potential concerns and challenges that may raise during technology development (i.e., data, models, architecture, implementation) and its instantiation (i.e., proof-of-concepts and use cases).
- **Section 5**: This section reports the analysis of relevant ethics and regulatory risks.
- **Section 6**: This section maps ethics and regulatory principles, values, risks and KVIs to the corresponding ethics and regulatory requirements to be embedded in the 6G-DALI development process to ensure compliance. For each requirement, this section identifies evidence artefacts that provide raw data and proof of system behaviour, making them essential for assessing requirement fulfilment.

The document provides a conclusion with summary of the relevant outcomes achieved in the context of the 6G-DALI task T2.4, and insights to perform the assessment.

Finally, the document includes three annexes. The first annex provides the questionnaire and aggregated answers from the consortium to assess and rank ethics and regulatory risks. The second annex provides examples from standards to guide the definition of evidence artefacts. The third annex provides the list of linked system requirements from D2.2.

2 Methodological framework toward 6G-DALI compliance

The ethical and regulatory framework adopted in 6G-DALI is a governance framework that operationalises ethical and regulatory principles throughout the system lifecycle. It is designed to identify, assess, and mitigate ethically salient risks related with data processing and AI models developed within the project. The framework is not conceived merely as a compliance mechanism applicable to systems once deployed. Rather, it embeds a structured, iterative methodology within the development process itself, ensuring that ethical and legal considerations inform system design, implementation, and evolution from the earliest stages.

To this end, the framework is structured around the following steps:

1. Definition of the relevant **ethics and regulatory background framework** to be considered throughout project development, with particular attention to AI ethics and data governance obligations;
2. Identification and contextualisation of relevant **ethics and regulatory concerns** that may affect protected **societal values,** together with associated **Key Value Indicators (KVIs)**. In the case of 6G-DALI, the underlying values and KVIs were already identified during the proposal stage, fine-tuning and extending the conclusions of previous projects, in particular 6G4Society and other SNS JU initiatives, to 6G-DALI specific context. Accordingly, although this step is conceptually embedded within the methodology, it is not developed anew in the present deliverable;
3. Identification of potential **risks or critical pain points** that may undermine those societal values and the rule of law, as grounded in the established principles and rules of the relevant ethics and regulatory background framework;
4. Establishment of **countermeasures and safeguards**, mapped to specific ethical and regulatory requirements to be implemented during system design and development in order to mitigate the identified concerns and risks;
5. Operationalisation of the **assessment procedure,** aimed at verifying the effective implementation and fulfilment of these requirements through structured compliance artefacts.

These **five steps** are applied **iteratively and incrementally** (see Figure 1), allowing for the progressive refinement and consolidation of requirements as the project evolves.

While Sections 3 to 6 of this document operationalise the first 4 steps of the methodological framework described above, applying them to the specific technical and organisational scope of 6G-DALI, step 5 (concerning the structured assessment and verification phase) will be further developed and implemented during the next phase of the project.

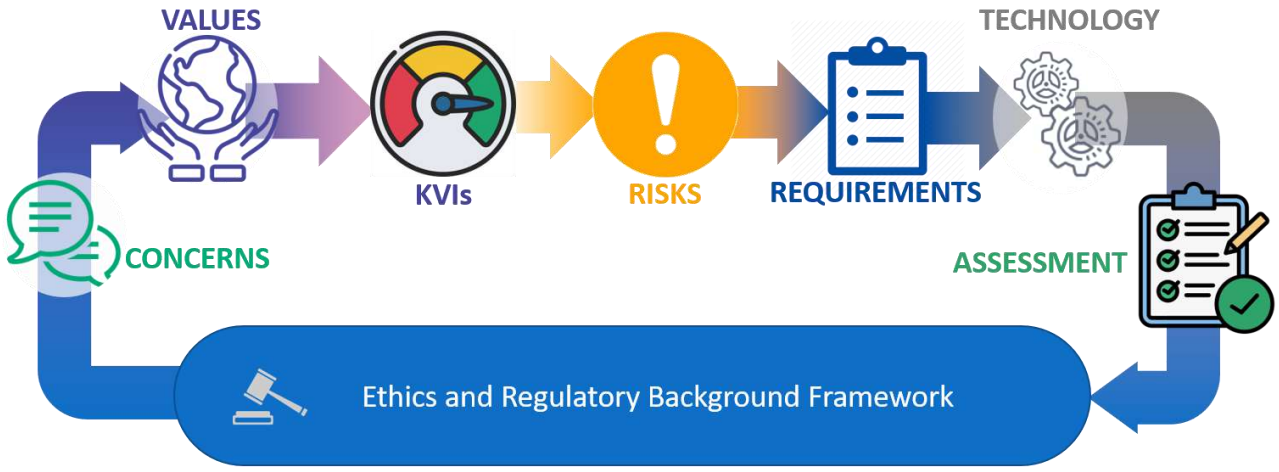


Figure 1. Compliance Assessment Process in 6G-DALI

2.1 Step 1: European ethics and regulatory background framework

The first step — the reconnaissance of the ethical and regulatory background framework — is based on the assumption that the transition towards sixth-generation (6G) communication systems is not merely

an incremental technological evolution, but a paradigmatic shift towards AI-native network architectures, in which AI systems are deeply embedded in decision-making, resource allocation, and optimisation processes across the network stack. As highlighted in the recent literature[2] [6] [7] this transformation raises a set of ethical and societal challenges that extend well beyond traditional concerns related to performance, efficiency, or security, and instead implicate broader questions of governance, legitimacy, and societal trust.

Against this background, the scope and positioning of the 6G-DALI project must be clearly understood. 6G-DALI creates a comprehensive end-to-end framework supporting Data Operations (DataOps) and Machine Learning Operations (MLOps) in 6G networks[8] . A special focus is devoted to the retrieval, curation, and generation of datasets intended to support the training and evaluation of machine-learning models for future 6G applications[9] . This upstream positioning is normatively significant, as the applicability of EU digital regulation is generally triggered by specific functions, risks, and deployment contexts, rather than by the mere use of AI-related techniques. Consequently, this positioning places 6G-DALI outside the immediate scope of many regulatory instruments triggered by operational use or direct impact on individuals. Simultaneously, the legal and normative frameworks relevant to 6G-DALI must be interpreted through the lens of proportionality, retaining ethical importance due to the potential downstream effects of data-related design choices.

2.1.1 Ethics of Artificial Intelligence

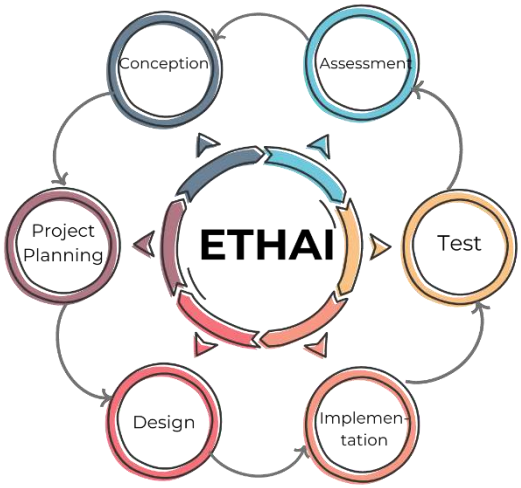


Figure 2. The ETHAI Model

For the elicitation of **specific requirements addressing ethical aspects of AI systems**, the 6G-DALI adopts and extends the **ETHAI (Ethics of AI)** methodology[10] in the context of the 6G development. ETHAI is a comprehensive "ethics-by-conception" methodology that integrates ethical considerations into the lifecycle of AI systems from their inception. Developed within projects targeting the challenges of decision supporting systems powered by AI/ML technology in the healthcare domain (i.e., MeSCobraD [11] , COMFORTage [12]), it has been adopted also in security domain projects dealing with AI systems and drones (i.e., PRESERVE [13]). This model relies on ethics and legal principles (i.e., [14] [15] [16] [17]) and bridges the gap between high-level ethics principles and low-level technical implementation details.

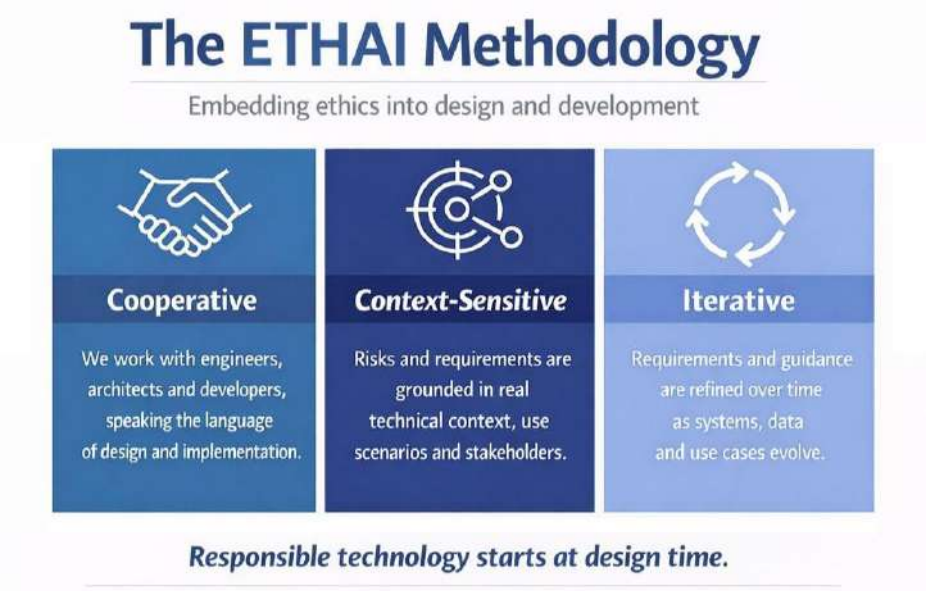


Figure 3. ETHAI Methodology foundations

The methodology is defined by four foundational principles that ensure the framework remains both robust and applicable:

- **Context-sensitivity**: Ethical requirements are tailored to specific domains and use cases;
- **Actionability**: The framework translates high-level theory into concrete, implementable requirements to guide engineers during development;
- **Interdisciplinarity**: It facilitates collaboration between ethics experts, technical developers, domain specialists, and end-users;
- **Iterativity**: It employs a cyclical process of definition, implementation, evaluation, and refinement to adapt as new challenges emerge.

This approach aligns with the value-sensitive methodology adopted in 6G-DALI for ethical and legal compliance. The **ETHAI framework** builds on established insights from AI ethics scholarship and policy analysis [18] [19] , which stress that responsible innovation in AI-native infrastructures requires the systematic translation of **high-level values** (e.g., accountability, robustness, transparency, and respect for fundamental rights) into concrete design and governance **requirements**, even at early stages of the technology lifecycle. Therefore, by structuring ethical concerns as identifiable risks, mapping these risks to context-specific requirements, and assessing their fulfilment through documented artefacts and indicators, ETHAI provides a proportionate and methodologically grounded response to the ethical challenges highlighted in the literature. In doing so, it aligns with the broader view, articulated in current scholarship [18] [20] , that ethical governance in 6G should function not merely as a constraint on innovation, but as an enabling condition for trustworthy, socially legitimate, and sustainable AI-enabled infrastructures.

2.2 Step 2: Identification of value-driven concerns

Concerns refer to identifiable thematic areas of interest or tension that signal the potential compromise of established ethical, legal, or societal values within a specific domain. In the context of 6G-DALI, concerns are identified at a level where meaningful governance, design, and assessment interventions remain possible, with a focus on system-level properties and practices rather than on downstream societal harms that may materialise only at deployment or operational stages. More generally, a concern delineates the conditions under which a value may be placed at risk, thereby helping to clarify which values are vulnerable in a given context and why they are normatively significant. This stage involves an assessment of existing response strategies and the prospective value of improved technological interventions.

Subsequently, the identified concerns are mapped against the set of **Key Values** [21] [22] previously established at proposal stage. This mapping exercise does not aim to redefine values, but rather to contextualise and operationalise them within the specific scope of 6G-DALI. In this sense, values function as normative reference points against which concerns are interpreted and prioritised. Here, values are interpreted as context-specific normative priorities that are collectively anchored in frameworks such as the UN Sustainable Development Goals (SDGs) [23] , the European Green Deal, the GDPR[24] , the AI Act[15] , the EU Ethics Guidelines for Trustworthy AI[14] , the UNESCO Recommendation on Ethics of AI[16] , the European Living guidelines on the responsible use of generative AI in research[17] and democratic principles of fairness, inclusion, and autonomy. A distinction is maintained between values as guiding criteria that orient technological development and values as outcomes that may emerge from technology use. This systematic approach that explicitly considers values throughout the entire process of technology innovation is referred in literature with the “Value-Sensitive” methodology [25] .

For the purposes of 6G-DALI project, respecting the widely agreed definition in the SNS JU ecosystem, Values are defined as:

Values – *In the context of Value-Sensitive methodology, the term refers to principles or qualities that individuals or groups deem important, desirable, or intrinsically good.*

The project does not aim to redefine values or KVIs, but to contextualise and operationalise them within its specific scope.

For monitoring progress with respect to performance, QoS and societal values, the 6G-DALI project defined both **Key Performance Indicators (KPIs) and KVIs** during the proposal phase. In line with the methodological approach promoted by the SNS JU Test, Measurement and KPIs Validation Working Group[6] and papers on 6G KVIs[26] [27] , both KPIs and KVIs were identified at proposal stage and formalised in the Description of Action, in order to ensure early alignment with project objectives, experimental scope, and cross-project evaluation criteria.

KVIs serve a complementary role to conventional KPIs, by capturing how technology facilitates broader societal goals rather than mere technical (performance) efficiency and effectiveness[2] . Their development requires triangulation of stakeholder insights, domain expertise, and scenario-based analysis to ensure contextual validity and traceability.

While the operationalisation and assessment phases are described in detail in the following sections, it is important to emphasise that Key Value Indicators (KVIs) and Key Performance Indicators (KPIs) are considered in parallel throughout the process. This ensures continuous alignment between normative objectives and technical performance.

Assessment results do not serve merely to verify compliance; rather, they feed back into the refinement of technical design choices and, where necessary, into the adjustment of ethics and regulatory requirements. In this iterative process, KPIs may evolve in response to technical developments, while KVIs remain stable normative reference points that anchor the project's ethical commitments throughout its lifecycle.

In doing so, the methodology presents a recursive value-technical alignment mechanism whereby KVIs inform design goals through requirements and assessment criteria, and KPIs indicate progress toward technical and performance objectives.

2.3 Step 3: Identification of risks

Building on the value-driven concerns identified in Step 2, the methodology introduces an intermediate risk-identification phase aimed at translating abstract value vulnerabilities into concrete and operationally relevant risk scenarios. While concerns delineate the conditions under which societal values may be placed at risk, this step specifies how such vulnerabilities may materialise within the technical architecture, data practices, and governance structures of 6G-DALI.

The identification and prioritisation of risks provide the analytical basis for the subsequent requirement elicitation phase. By clarifying how value-driven concerns may concretely materialise within the project's technical and governance architecture, this step enables the systematic translation of prioritised risks into structured ethical and legal requirements tailored to the specific scope of 6G-DALI.

2.4 Step 4: Elicitation of requirements

The elicitation of ethics and regulatory requirements constitutes a central component of the assessment framework. It requires structured collaboration among a multidisciplinary team (encompassing ethical, legal, technical, and social expertise) to reconcile different disciplinary perspectives and ensure coherent and consistent requirement definition. For this reason, a structured approach is considered in the context of the 6G-DALI project, enabling collaboration and ensuring interoperability between the social sciences and humanities (SSH) and the technology (STEM) experts.

Elicitation of ethics and legal requirements is iteratively carried out and utilizes a three-level hierarchy (Figure 4) to effectively bridge ethics and regulatory principles with technical implementation:

- **Ethics and Legal High-Level 'CORE' Requirements (EL-HLRs):** derived from the regulatory framework (*what* must be achieved). These requirements are primarily defined by ethicists, lawyers, and compliance experts and are understandable to them.
- **Ethics and Legal Mid-Level Requirements (EL-MLRs):** represent intermediate level of requirements, derived from EL-HLRs, and apply to the project's domain/context (*how* principles apply). This level acts as a communication bridge between legal/ethics and engineering/product teams.

- **Ethics and Legal Low-Level Requirements (EL-LLRs):** map EL-MLRs to detailed, implementable and verifiable technical actions (*where* and *when* actions occur in a specific part of the architecture or use case scenario). These requirements are linked with functional and non-functional requirements from the technical specifications.

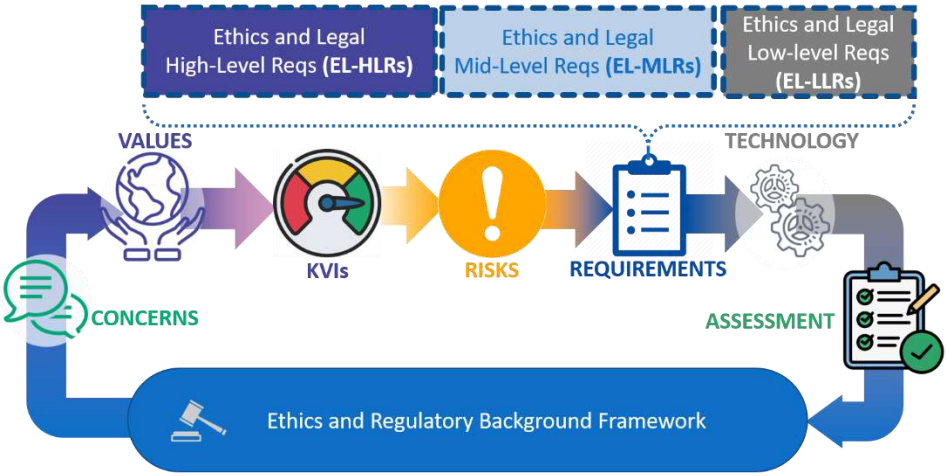


Figure 4. Three-levels Hierarchy approach for requirements elicitation

In this manner, ethics and legal requirements are developed in parallel with system requirement specifications, ensuring their continuous alignment throughout the design process. This parallel progression enables the project to adopt an "ethics-by-conception" approach, meaning that ethical considerations are embedded from the earliest stages of technological definition and design. By integrating compliance directly into development activities, the project reduces regulatory and societal risk while fostering the creation of socially responsible and trustworthy technologies.

In defining the ethical and legal requirements underpinning the ETHAI framework, the project has drawn on a broad pool of authoritative resources, including the Ethics Guidelines for Trustworthy AI[14] developed by the High-Level Expert Group on Artificial Intelligence (HLEG), alongside binding regulatory instruments [15] , institutional recommendations [16] [17] and established academic literature on AI ethics [19] .

However, **the resulting set of core requirements does not reflect, nor aim to reproduce, a one-to-one correspondence with the categories or principles articulated in [14] and [15]** . This is a deliberate methodological choice. First, the requirements elicitation process integrates multiple normative and ethical sources, each reflecting different levels of abstraction, legal force, and analytical focus. Second, and more importantly, requirements have been derived through a contextualised analysis of the specific scope, domain, and risk profile of the 6G-DALI project, which addresses preparatory activities such as data retrieval and dataset generation rather than the deployment or operation of AI-enabled 6G systems. As a result, **ethical principles are not transposed as abstract categories, but translated into context-specific requirements** that respond to concrete domain problems and foreseeable governance challenges within the project's remit.

Furthermore, risks within ETHAI are identified and structured at a level where meaningful governance and design interventions remain possible, focusing on system-level properties and practices (e.g., data quality, traceability, robustness, and accountability mechanisms) rather than on downstream societal manifestations of harm that may only materialise at deployment or operational stages. This **system-oriented and governance-focused perspective** serves as a foundation for compliance, iteratively bridging the gap toward full normative consistency as the technology development evolves. Instead, ETHAI should be understood as a synthesising and context-sensitive framework that integrates ethical principles, guidelines, and regulations as normative reference points. These sources inform the identification of risks and the definition of requirements, providing a solid yet **technically agile basis for assessment criteria as the system develops**.

2.5 Step 5: Assessment of the requirements fulfilment

During the assessment phase, the development team evaluates structured compliance artefacts in order to verify the fulfilment of ethical and regulatory requirements. These artefacts are not produced during the assessment itself; rather, they are defined ex ante within the framework and generated throughout system development, validation, and operation — including within testbeds and Proofs of Concept (PoCs).

Within the ETHAI methodology, such outputs are referred to as evidence artefacts and constitute the documentary and operational basis for compliance verification. Each requirement is explicitly linked to one or more corresponding evidence artefacts, which provide the material basis for determining whether the requirement has been satisfied or whether additional mitigation measures are necessary.

During each ETHAI cycle, the available evidence is systematically reviewed, and the level of compliance associated with each requirement is assessed. The results are then consolidated into an aggregate compliance index reflecting the overall status of requirement fulfilment. Where residual risks are identified, or where contextual developments call for a more granular adaptation of requirements, both the system design and the associated requirements are iteratively refined in subsequent assessment cycles.

2.5.1 Linking concerns, requirements and KVIs

In this context, KVIs operate as verifiable claims: if a specific design choice is implemented under a stated policy, then a given value should improve, as substantiated through a defined set of indicators. The 6G-DALI specification of business use cases [8] outlines, for each PoC and experiment, the corresponding KVIs, clarifying how they should be interpreted within the specific context of each experiment. For example, although Experiments 2.1 and 2.2 are associated with the same KVI ("Demonstrate accuracy, reliability, robustness, accountability, and transparency of AI/ML models through the ETHAI assessment report"), the constituent values of this KVI are interpreted differently in the two cases. In the former, the emphasis is placed on respect for the user's intent, whereas in the latter attention is also given to potential silent accuracy degradation resulting from model drift.

When assessing KVIs to determine whether they have been achieved, it is essential to first identify the specific PoC and experiment to which the KVI applies, and then map all relevant ethical and legal requirements to that context. The same KVI may therefore correspond to different sets of requirements depending on the PoC in which it is instantiated.

For instance, transparency may in one case be linked to requirements concerning user satisfaction and user intent, and in another to requirements related to robustness, reliability, or epistemic integrity. Thus, within each PoC, values such as accuracy, robustness, accountability, and transparency are operationalised differently and must be assessed through ETHAI using context-specific criteria.

To evaluate the ethical and legal compliance of each PoC - and, through the KVIs, their embedding of societal values - an ETHAI assessment cycle is conducted for each requirement associated with a given KVI. Each KVI is linked to a defined subset of risks and to the corresponding ethical and legal requirements derived from those risks. As described in the preceding sections, the fulfilment of each requirement is evaluated on the basis of the relevant artefacts defined in Section 6. The results of this evaluation are documented in an ETHAI assessment report.

At the KVI level, the outcomes of the associated requirement assessments are consolidated into an aggregate index. This index does not constitute a single quantitative score, but rather a structured, evidence-based synthesis of requirement-level findings. It reflects the extent to which the value represented by the KVI is effectively embedded within the specific PoC and experiment.

In this way, KVIs provide an interpretable indication of societal value integration and impact mitigation. Where the requirements linked to a KVI are satisfied, the corresponding value (e.g., transparency, accountability, robustness, or reliability) can be considered demonstrably incorporated into system design and operation. Conversely, unmet or partially satisfied requirements signal areas where value embedding remains incomplete and where corrective or adaptive measures may be required.

3 6G-DALI European ethics and regulatory background

This section outlines the ethics and regulatory framework adopted within 6G-DALI, establishing a foundational pathway toward the development of human-centric, AI-native infrastructures. It examines the applicable ethics principles alongside key binding regulatory instruments, including the General Data Protection Regulation, the Data Act, the Artificial Intelligence Act, the European Data Act and the Data Governance Act. Their relevance, implications, and compliance requirements are analysed in the specific context of the 6G-DALI architecture.

3.1 Ethics principles

The ethical approach adopted in 6G-DALI is rooted in a human-centric understanding of AI-native 6G infrastructures, where technological progress is continuously interpreted through the lens of fundamental rights, societal values, and long-term sustainability. Rather than being treated as an external constraint applied after technical development, ethics is integrated from the outset as a guiding design orientation ("ethics-by-design" and "ethics-by-conception"), in coherence with the Ethics of Artificial Intelligence (ETHAI) model used in the project (see Section 2) and with the European Ethics Guidelines for Trustworthy AI[14] . Taking these guidelines as a reference framework, 6G-DALI uses their key principles (such as human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and fairness, societal well-being, and accountability) not as a checklist, but as a conceptual basis for responding to the specific risks identified within the project and for shaping appropriate system-level safeguards.

This ethical orientation is further reinforced by the regulatory logic introduced by the AI Act, which promotes a risk-based approach and emphasises lifecycle governance, traceability, and meaningful human control over AI systems with infrastructural relevance. Within 6G-DALI, this perspective is reflected in the systematic documentation of design choices, the continuous monitoring of models and data practices (including drift, uncertainty, bias, and unintended effects), and the explicit attribution of responsibilities across the different phases of system configuration, deployment, and evolution. In this way, ethics becomes inseparable from system governance, extending beyond individual algorithmic outputs to the organisational and technical conditions under which AI-mediated behaviour emerges.

Within this broader ethical and regulatory framework, 6G-DALI complements European guidelines with concepts from academic research in data ethics and digital infrastructures[18] [19] , using them as interpretative tools to better understand emerging risks in AI-driven, data-intensive environments.

Alongside European ethical guidelines and binding regulatory frameworks, 6G-DALI also mobilises selected concepts from academic research[20] in order to better interpret structural dynamics typical of AI-native, data-intensive infrastructures. These perspectives do not introduce new obligations; rather, they function as analytical lenses that clarify why specific governance mechanisms, risks, and requirements become necessary within the project.

A first lens is offered by the notion of data extractivism[28] . In this context, the term does not refer to individual unlawful processing operations, but to the gradual evolution of data practices whereby reuse expands, informational value becomes concentrated, and long-term dependencies may emerge between actors and infrastructures. What makes this dynamic ethically relevant in 6G environments is its cumulative nature: each step may appear legitimate, while the overall trajectory can progressively reshape control, access, and benefit distribution. Within 6G-DALI, this perspective helps illuminate several of the risks identified in the project, including silent policy change, loss of governance in model drift, and expansion of secondary uses. Consequently, the theme resurfaces across multiple requirements, particularly those related to **Privacy** and **Data Governance**, **Accountability**, and **Fairness**, where emphasis is placed on documented purposes, traceability of changes, explicit governance review, and revisability of evolving data practices.

A second conceptual contribution concerns the interpretation of Digital Twins as epistemic infrastructures [29] [30] . Beyond their operational function of enabling experimentation and data generation, Digital Twins participate in defining what counts as valid knowledge about network behaviour. Assumptions embedded in modelling choices, abstractions, reward structures, and validation environments may stabilise partial representations of reality and thereby influence optimisation outcomes and governance decisions.

For this reason, reflection on Digital Twins directly informs requirements connected to Epistemic Integrity, Explainability, Reliability, Robustness and Resilience, and Bias, where the project stresses documentation of provenance, limits of validity, scenario diversity, and visibility of modelling constraints.

By incorporating these perspectives, 6G-DALI strengthens the continuity between theoretical reflection, risk identification, and the operational formulation of ethics and regulatory requirements, ensuring that governance mechanisms remain responsive to how AI-native infrastructures evolve over time.

3.2 Relevant Regulatory framework

While acknowledging that formal compliance obligations are not automatically triggered by the project's preparatory activities, 6G-DALI integrates key European regulatory frameworks as normative reference points within its development lifecycle.

As 6G is an AI-native technology, 6G-DALI recognises and addresses the need for high-quality data, which is currently scarce for a network that is still under development. This scarcity constitutes a structural ethical concern, as limitations in data availability, representativeness, and quality may directly affect robustness, fairness, traceability, and accountability. In response to these structural data-related concerns, 6G-DALI adopts a dedicated DataOps layer to clean, organise, and manage raw data for AI use. To overcome data scarcity, 6G-DALI also employs Digital Twins and experimental environments to generate "on-demand" data. In doing so, 6G-DALI lays the foundation for a 6G Data Space, facilitating the sharing of qualified and compliant datasets for 6G researchers and industry verticals. These design choices are ethically relevant, as they directly affect data quality, bias mitigation, traceability, and compliance with data governance requirements addressed within ETHAI.

In this context, the ethics and regulatory framework needs to consider the following relevant principles, including the General Data Protection Regulation (GDPR – EU 2016/679)[24] , the Artificial Intelligence Act (AI Act – EU 2024/1689)[15] , the Data Act (EU 2023/2854)[31] , and the Data Governance Act (DGA – EU 2022/868) [32] . Together, these instruments provide the regulatory backdrop against which risks, requirements, and assessment criteria are defined within ETHAI, supporting a systematic, human-centric governance approach without anticipating deployment-stage compliance obligations.

3.2.1 General Data Protection Regulation

GDPR serves as the cornerstone for protecting personal data and individual rights within the 6G-DALI framework. By design, the architecture adheres to the principles of **data minimisation** and **purpose limitation** (Art. 5), alongside **transparency** (Art. 12): all of which are vital when processing the expansive datasets required for 6G experimentation. Furthermore, 6G-DALI integrates continuous compliance monitoring and risk assessment throughout the project lifecycle to satisfy the accountability requirements of Article 24.

Indeed, dataset retrieval and generation activities may involve personal data, metadata, or data that could become personal when combined with other datasets, and GDPR principles such as lawfulness, purpose limitation, data minimisation and accuracy therefore constitute a baseline normative framework for 6G-DALI. Given the fact that 6G-DALI framework datasets are synthetic, anonymised, aggregated or used strictly in controlled research environments, a Data Protection Impact Assessment (DPIA) under Article 35 is not automatically triggered. Imposing such an obligation at this stage would result in a disproportionate regulatory burden without corresponding gains in risk mitigation.

Furthermore, the project's "ethics-by-conception" approach is conceptually aligned with the obligation of data protection by design and by default enshrined in Article 25 GDPR, which requires that appropriate technical and organisational measures be implemented both at the time of determination of the means for processing and at the time of processing itself. While the specific technical measures required under Article 25 will depend on the nature and scope of processing activities as they materialise in downstream deployment, 6G-DALI embeds data protection considerations into its framework architecture from the earliest design stages, thereby anticipating the substance of this obligation.

3.2.2 Artificial Intelligence Act

AI Act marks the first comprehensive framework for governing AI-based systems. It is adopted to mitigate potential risks in the development and operation of AI models, ensuring they remain **trustworthy**, **explainable**, and subject to **human oversight**.

The AI Act introduces a harmonised, risk-based governance model for AI systems, distinguishing between levels of regulatory obligation depending on the potential impact on fundamental rights, safety, and societal interests. Particularly relevant for 6G-DALI is the emphasis on lifecycle responsibility, whereby compliance is not limited to the moment of deployment but extends to design, development, validation, monitoring, and post-deployment management.

The Regulation clarifies the distribution of duties among different actors, including providers, deployers, and operators, and requires that AI-enabled functionalities remain subject to documented risk management procedures, human oversight arrangements, transparency obligations, and technical robustness measures.

For an AI-native infrastructure such as 6G-DALI, where automated optimisation, adaptive learning, and large-scale orchestration are intrinsic features, this perspective reinforces the need to embed governance mechanisms capable of maintaining visibility, traceability, and controllability as the system evolves. The AI Act therefore acts as a bridge between high-level ethical principles and the operational requirements later defined in this deliverable, supporting the translation of regulatory expectations into implementable safeguards and assessable evidence.

As analysed in the Future Network Services White Paper[33] on the relevance of the AI Act to 6G AI Act applies broadly to AI systems and general-purpose AI (GPAI) models placed on or put into service in the EU, and its definitions are sufficiently expansive to encompass advanced AI techniques envisioned for 6G environments. At the same time, the White Paper demonstrates that the AI Act's high-risk regime—particularly the provisions concerning AI systems used as safety components in radio equipment or critical digital infrastructure—is unlikely to apply systematically to 6G research and innovation activities, and even less so to upstream, preparatory activities such as dataset generation.

In this respect, 6G-DALI does not develop, place on the market, or put into service AI systems operating 6G networks, nor does it design or deploy network components that could qualify as safety components under Article 3(14) AI Act. The project's activities therefore fall outside the regulatory triggers for conformity assessments, post-market monitoring obligations, or high-risk AI system requirements under Articles 8–15 AI Act. Nevertheless, the AI Act remains normatively relevant for 6G-DALI as a horizon-setting framework, insofar as it articulates expectations regarding data quality, traceability, risk awareness and documentation that are likely to shape downstream compliance once AI systems trained on the datasets are deployed. These expectations are addressed within the project through internal governance and assessment mechanisms, rather than through formal AI Act compliance claims.

3.2.3 Data Act

The **Data Act** establishes cross-sector rules that define who may access, use, and share data generated within the EU (particularly data produced by connected devices and related digital services, such as smart appliances, vehicles, and industrial equipment). Its purpose is to eliminate obstacles to data reuse, thereby fostering innovation in areas such as artificial intelligence and industrial analytics, while ensuring the protection of personal data and trade secrets.

The Data Act serves as a vital regulatory pillar for 6G-DALI by rebalancing power in the digital economy and mandating that industrial data be made more accessible and usable. For the project's high-level requirements (see Section 6), Article 3 and Article 4 establish the foundational legal right for users to access and share data generated by connected devices (e.g., Digital Twins, 6G devices, antennas and network testbeds) fostering competition and cross-vendor innovation. By operationalising these rights, 6G-DALI facilitates the seamless movement of datasets between its internal architecture and broader European 6G Data Spaces, adhering to the essential **interoperability** requirements of Article 33.

Furthermore, Article 5 empowers users to mandate that data holders (i.e., entities having the right or obligation to make available certain data) share this information with third-party service providers, a critical mechanism for the fair, reasonable, and non-discriminatory exchange of data required to train

next-generation AI models. This alignment ensures that 6G research is not hindered by proprietary silos or vendor lock-in, as Articles 23–31 further mandate the removal of technical and contractual obstacles to data portability. Therefore, Data Act aims to ensure all processed data remains structured, machine-readable, and ready for collaborative innovation within the European data ecosystem.

3.2.4 Data Governance Act

The Data Governance Act (DGA) serves as a foundational regulatory pillar for 6G-DALI by establishing a framework to increase **trust in data sharing** through neutral intermediaries. It directly supports 6G-DALI's objective of creating a secure 6G Data Space, enabling the **altruistic** and **cross-sectoral reuse** of sensitive data for scientific research. Under Chapter III (Articles 10–12), the DGA regulates data intermediation services, ensuring that the platforms connecting 6G-DALI participants function as neutral, trustworthy brokers that cannot monetise the data for their own benefit. This structural separation is vital for multi-vendor 6G environments where competitive sensitivities otherwise hinder data pooling.

Furthermore, 6G-DALI leverages the DGA's Data Altruism framework (Articles 16–25), which allows for the voluntary sharing of telemetry and network data for "general interest" objectives, such as optimising energy efficiency in 6G infrastructure or enhancing public safety. By utilising Article 25's common European data altruism consent form, 6G-DALI ensures that data contributions from diverse stakeholders are legally streamlined and technically interoperable. Collectively, these measures (supported by the oversight of the European Data Innovation Board, Article 29) ensure that 6G-DALI operates within a "Single Market for Data" that prioritises **data sovereignty** and **secure**, research-driven innovation.

3.3 Harmonised Standards

The integration of the 6G-DALI methodology with the EU AI Act is supported by the emergence of harmonised standards[34] , which operationalise legal mandates into auditable technical requirements. Although many are currently work-in-progress documents, they provide the technical plumbing needed to bridge the gap between high-level ethics and regulatory principles and the implementation details to carry out the compliance.

A central pillar is CEN/CLC prEN 18286[35] , which focuses on establishing a Quality Management System (QMS) specifically tailored to the AI Act's requirements. Complementing this, ISO/IEC 42005[36] offers a guidance framework for AI system impact assessments, facilitating the identification of risks from the earliest design stages. To address the technical complexities of AI-native systems, ISO/IEC TS 6254:2025[37] provides methodologies for transparency and explainability, directly supporting the translation of high-level principles into interpretable model decisions.

Furthermore, ISO/IEC DIS 25059 [38] extends the SQuaRE (System and Software Quality Requirements and Evaluation) series to AI systems, providing a quality model that is essential for assessing technical robustness and reliability.

In the context of 6G environments, ETSI released in January 2026 the TS 104 008 [39] . This technical specification is critical, as it defines requirements for data provenance and integrity, ensuring that data-intensive layers remain robust against unauthorised exposure or inference.

Together, these and other evolving standards[40] provide a validated theoretical and practical foundation for the 6G-DALI project's ethics-by-conception approach, specifically supporting the translation of the high-level requirements into low-level and technical implementation details. Moreover, these standards provide formal descriptions of the evidences to be generated for assessing and validating the fulfilment of the compliance requirements.

3.4 Highlights from the Ethics and Regulatory analysis

The absence of formally triggered regulatory obligations does not imply the absence of ethically or legally relevant risks.

On the contrary, **6G-DALI explicitly recognises that upstream activities (particularly the retrieval, curation and generation of datasets for machine-learning training) may give rise to downstream risks if left unaddressed.**

These **risks are systematically identified and managed through the ETHAI framework**, which **translates high-level regulatory expectations into context-specific risks and requirements** appropriate to the project's preparatory scope.

For example, although 6G-DALI does not deploy AI systems on the market yet and therefore does not currently fall under the AI Act's high-risk regime, the project acknowledges that its MLOps and datasets generated or curated during its activities may later be used to train AI systems operating in safety- or mission-critical 6G contexts. This downstream relevance warrants anticipatory governance at the preparatory stage, integrating data logging and quality requirements directly into the development phase.

Within ETHAI, this potential downstream relevance is reflected in risks related to data quality, representativeness and robustness, such as the risk that training datasets may encode hidden biases, structural gaps or artefacts that could lead to degraded model performance or silent accuracy loss once deployed. Corresponding ETHAI requirements therefore address dataset documentation, traceability of data sources, justification of data generation methods (including synthetic data generation), and validation of dataset fitness for intended downstream use.

Similarly, while a formal DPIA is not required in the absence of high-risk personal data processing, ETHAI captures residual data protection and fundamental-rights concerns through requirements addressing re-identification risks, unintended inference and misuse of datasets beyond their original research purpose. In this way, ETHAI operates as a proportionate upstream governance mechanism: it does not anticipate or replace compliance obligations that may arise at deployment stage, but it ensures that ethically and legally salient risks associated with preparatory data practices are identified early and mitigated to the extent possible within the project's remit.

Overall, the legal and normative approach adopted in 6G-DALI reflects a deliberate commitment to regulatory alignment without regulatory overreach. By explicitly acknowledging the limits of formal regulatory applicability while embedding relevant regulatory values (e.g., accountability, robustness, transparency and fundamental-rights protection) into its internal risk and requirement framework through ETHAI, the project supports responsible innovation and enhances legal robustness, while preserving flexibility for downstream actors who will ultimately bear formal compliance obligations once 6G systems and AI applications are placed on the market or put into service.

4 6G-DALI value-driven concerns

Although 6G-DALI does not operate at the stage of deployment on the market, its upstream role in shaping datasets, model pipelines, and operational infrastructures carries normative significance. Ethical and regulatory concerns therefore emerge not from immediate use-contexts, but from the structural conditions that the project contributes to establishing. These concerns refer to identifiable risks or issues that indicate the potential compromise of key ethical, legal, or societal values within a specific domain. In the context of 6G-DALI, concerns are identified at a level where meaningful governance, design, and assessment interventions remain possible, with a focus on system-level properties and practices rather than on downstream societal harms that may materialise only at deployment or operational stages. More generally, a concern delineates the conditions under which a value may be placed at risk, thereby helping to clarify which values are vulnerable in a given context and why they are normatively significant. This stage involves an assessment of existing response strategies and the prospective value of improved technological interventions. The concerns identified in this section are subsequently operationalised as concrete risks in the next methodological step, ensuring continuity between value-driven concerns and risk specification.

In this context, the project recognises that the transition towards AI-native 6G environments has prompted the consolidation, in both academic literature and regulatory discourse, of a set of foundational ethical principles guiding the development and governance of AI systems. A central concern identified in the literature is the increasing autonomy of AI-driven decision-making in 6G environments, which amplifies risks related to transparency, accountability, fairness, and privacy[20] . These principles are consistently recognised as the core normative pillars of AI ethics and are particularly salient in telecommunications, where algorithmic decisions may affect access to essential services, quality of connectivity, and the distribution of network resources. The opacity of complex machine-learning models, especially when deployed at scale and in real time, challenges traditional accountability mechanisms and complicates the attribution of responsibility for harmful outcomes. At the same time, biases originating in training data or data collection practices risk reproducing or amplifying existing social inequalities in digital infrastructures that are increasingly foundational for social and economic participation.

Beyond these system-level concerns, the literature emphasises that ethical risks in 6G are not confined to the moment of deployment or operation, but can emerge upstream, during earlier phases of the AI lifecycle. In particular, data-related practices—including data collection, curation, generation, and reuse—are identified as critical points at which ethical and societal risks may be introduced and later propagated throughout the system. Issues such as dataset representativeness, hidden bias, data quality degradation, and unintended inference are widely acknowledged as structural sources of downstream harm, potentially leading to reduced robustness, discriminatory outcomes, or silent performance degradation in operational AI systems.

4.1.1 Mapping relevant values

6G-DALI considers four high-level thematic and conceptual groupings intended to structure and organise families of related KVIs relevant to the responsible development of technologies, PoCs, and use cases. These groupings are neither values nor KVIs in themselves, but function as an organising layer that supports the systematic articulation, interpretation, and operationalisation of a larger set of more granular KVIs, which are instantiated and assessed in relation to specific PoCs and experimental contexts. These are:

1. *Coherence between users' intent and outcomes* – focusing on the relevance of human in the loop and oversight principles, and specifically considering the alignment of system outcome with the users' expectations;
2. *Respect EU values and rules* – highlighting that the system as a whole has to not harm humans and society, in line with the European ethics and regulatory principles;
3. *Responsible Use of resources* – considering that system has to responsibly and sustainably use resources of the planet, ensuring long-term viability for the current and future generations;
4. *Ethical AI* – addressing an overall societal request for ethically designing, developing, deploying and using AI-based technology, according to EU ethics and regulatory principles.

These Key Values represent the set of values used to perform the assessment of the 6G-DALI outcomes with respect to ethics, social and regulatory perspectives.

Following the identification of risks and the mapping of values, the methodology operationalises these values through the use of KVIs defined at proposal stage, which serve as stable, high-level reference constructs for the project's ethical and societal assessment.

4.1.2 Defining Key Value Indicators

6G-DALI already defined its own KVIs in the DoA, as illustrated in[8] .

Table 2. 6G-DALI KVIs

KVI #	KVI Title and Description	KVI Target
KVI-1	**Intent adherence -** User satisfaction from intent-based data requests	> 90% (surveys)
KVI-2	**Ethical and legal compliance -** Compliance with relevant legal requirements (Task 2.4)	100%
KVI-3	**User satisfaction -** Alignment of experiment results with users' objectives/priorities	> 90% (surveys)
KVI-4	**Environmental trade-off -** Energy reduction through model compression and quantization with ≤5% loss of accuracy compared to the FP32 precision model	90%
KVI-5	**AI Ethics: Accuracy, Reliability and Robustness -** Demonstrate accuracy, reliability, robustness, accountability, transparency of AI/ML workload operations through the ETHAI assessment report	Success (ETHAI Report)
KVI-6	**AI Ethics: Transparency and Accountability -** Demonstrate transparency & accountability of AI/ML models through the ETHAI assessment report	Success (ETHAI Report)
KVI-7	**Absence of Bias -** Demonstrate absence of bias in the specific context where the AI/ML models are applied through the ETHAI assessment report	Success (ETHAI Report)

5 6G-DALI Ethics and regulatory risks

Following the incremental and iterative process defined in the methodological approach illustrated in Section 2, the project initiated a structured assessment aimed at bridging the gap between abstract ethical principles and technical implementation. This phase focuses on identifying and analysing the potential ethical and regulatory risks that may arise from the development and deployment of 6G-DALI technologies, including those stemming from their integration into complex data flows, system layers, and interactions between autonomous components and human oversight mechanisms.

Through the involvement of a diverse range of stakeholders within the 6G-DALI project, 14 risks were identified and prioritised. For the sake of clarity, these risks are a detailed elaboration of risks (i.e., 18 "Lack of compliance with trustworthy legal and ethical requirements" and 19 "Difficult to understand and apply legal and ethical requirements") identified during the project proposal phase. This collaborative process addresses the "operationalisation challenge" by focusing on risks that can be meaningfully mitigated through design adaptations and technical specifications. In doing so, it ensures that the identified risks are suitable for translation into concrete ethical and legal requirements in the subsequent requirement-elicitation and implementation phases.

5.1 Potential risks

The 14 risks identified for this project reflect the intrinsic characteristics of AI-native, data-intensive 6G systems, where large-scale datasets, autonomous optimization, and intent-based abstractions are tightly coupled across the data, model, and system layers.

A first group of risks relates to **autonomy and abstraction** (see Table 3). In AI-native 6G environments, decision-making and optimization processes are increasingly delegated to AI/ML components operating with limited or no human intervention. This creates the possibility of ***policy bypass*** through autonomous model behaviour, as well as ***silent policy changes*** arising from incremental system evolution or reconfiguration that is not explicitly surfaced or reviewed. Over time, these dynamics may be exacerbated by ***model drift***, where the absence of adequate monitoring data or procedures leads to a gradual ***loss of governance*** over model behaviour. When combined with ***limited explainability***, such conditions may prevent the reconstruction of the causes underlying degraded or anomalous behaviour, undermining effective oversight and corrective action.

Table 3. Autonomy and abstraction risks

Risk ID	Risk Title	Risk Description
EL-RSK-01	Silent policy change	Significant changes in data processing practices (e.g. retention, reuse, access, or sharing) may be introduced without notification, explicit review, or formal approval, resulting in data use that deviates from the originally defined policy constraints.
EL-RSK-02	Policy bypass through autonomous model behaviour	The autonomous operation of AI/ML models may unintentionally bypass or circumvent predefined usage, access, or governance policies, leading to data processing or system behaviours that fall outside the intended policy constraints.
EL-RSK-03	Loss of governance in model drift	The absence of adequate procedures or monitoring data may prevent the detection and assessment of model drift over time, leading to loss of control over model behaviour and performance.
EL-RSK-04	Explainability failure	Limited explainability may prevent the reconstruction of the causes underlying degraded, unexpected, or anomalous system or model behaviour.

A second cluster of risks concerns the **translation of intent into data and models** (see Table 4) which is a defining feature of emerging 6G paradigms. The project's focus on generating or extracting datasets based on high-level descriptions or user-expressed intent introduces the risk of ***bias or intent mismatch***, whereby the produced dataset does not fully or accurately reflect the original intent. Given the scale and complexity of the datasets involved, users typically rely on metadata as the primary means of inspection and validation. Where ***metadata is incomplete, inaccurate, or insufficiently expressive***, users may lack effective means to detect such mismatches, leading to unintended downstream effects during model training and deployment.

Table 4. Intent-based risks

Risk ID	Risk Title	Risk Description
EL-RSK-05	Bias/Intent Mismatch	Datasets generated or extracted from user-expressed intent (e.g. natural-language descriptions) may not accurately reflect that intent, while metadata describing the dataset may be insufficient to reveal such mismatches, leaving users without effective means to detect deviations between the requested and the actual dataset content.
EL-RSK-06	Lack of metadata	Insufficient or missing metadata may prevent users from effectively checking and validating datasets, models, decisions, or applied policies (e.g. provenance, integrity, or contextual information).

A third set of risks emerges from the **data-intensive and distributed nature of AI training and adaptation** (see Table 5) in 6G systems. ***Bias amplification*** may occur when reward structures or optimization loops disproportionately favour dominant patterns and suppress rare or edge conditions, reducing model reliability outside expected operating regimes. Similarly, ***misapplied transfer***, including transfer learning or zero-shot learning (ZSL) performed with insufficient or misleading contextual information, may result in inappropriate model adaptation in target domains. These risks are closely linked to ***validation mismatch***, where simulation or validation environments fail to adequately reflect real deployment conditions, creating false confidence in model performance, ***robustness***, or compliance properties.

Table 5. AI training and adaptation risks

Risk ID	Risk Title	Risk Description
EL-RSK-07	Bias amplification	Reward structures or optimisation loops may amplify dominant patterns or systematically suppress rare, edge, or under-represented conditions, leading to skewed model behaviour or degraded performance under atypical or low-frequency operating conditions.
EL-RSK-08	Misapplied transfer	Transfer learning and zero-shot learning (ZSL) are susceptible to misapplied transfer, which occurs when a model is forced to adapt to a target domain using incomplete or mismatched contextual data. This causes the model to draw incorrect domain assumptions, leading to inappropriate adaptation. In this state, the model erroneously optimises its internal parameters to align with 'noise' or irrelevant features rather than meaningful signals. The result is a loss of general reasoning and a significant degradation in performance within the new environment

EL-RSK-09	Validation mismatch	Validation and simulation environments may fail to adequately reflect real deployment conditions, creating false confidence in model performance, robustness, or policy compliance.
EL-RSK-10	Lack of robustness	Datasets, models, or system components may not achieve the required level of robustness, resulting in unstable or unreliable behaviour, including non-graceful failure modes, under varying or adverse operating conditions.

Additional risks relate to **data governance, security, and exposure** (see Table 6) across the data and model lifecycle. ***Data leakage*** may arise not only through direct exposure during data storage or exchange, but also indirectly through model training, updates, or adaptation processes, including federated or distributed learning paradigms. ***API security*** represents a further concern in highly modular 6G architectures, where APIs exposed or consumed by internal components, autonomous AI/ML systems, or unauthorised parties may compromise system behaviour or control if inadequately protected. Where datasets contain personal data, insufficient technical and organisational measures may result in ***unfair or inappropriate processing***, particularly in large-scale or automated contexts.

Table 6. Data governance and security risks

Risk ID	Risk Title	Risk Description
EL-RSK-11	Data Leakage	Unintentional or unauthorised exposure or inference of data by external or unauthorised parties may occur during data generation, processing, storage, exchange, or model training and adaptation.
EL-RSK-12	API Security	APIs exposed or consumed by internal components, autonomous AI/ML systems, or unauthorized third parties may be inadequately protected, potentially compromising system behaviour, integrity, or control.
EL-RSK-13	Unfair processing of personal data	Where datasets contain personal data, the applied technical and organisational measures may be insufficient to ensure fair and appropriate data processing and protection.

Finally, the **cumulative effects** (see Table 7) of large-scale data generation, processing, storage, and AI model training raise ***environmental sustainability*** risks, notably in terms of energy consumption and associated emissions, which may become significant if not adequately monitored and optimized over the project lifecycle.

Table 7. Cumulative risks

Risk ID	Risk Title	Risk Description
EL-RSK-14	Environmental sustainability	The cumulative environmental impact of data generation, storage, processing, and model training (e.g. energy consumption and CO_2 emissions) may be significant if not adequately monitored or optimized.

Taken together, these risks reflect systemic properties of AI-native 6G systems rather than isolated implementation flaws. They arise from the interaction of autonomy, scale, abstraction, and continuous adaptation, and therefore require careful consideration throughout the design, development, and validation of datasets and AI-based components, without presupposing specific architectural or operational solutions.

The assessment of these risks, through a questionnaire shared with the whole 6G-DALI consortium, allowed to rank them in term of relevance. The answers of the questionnaire are reported in the Annex

I: Risk Assessment Questionnaire and Answers. The questionnaire enabled responders to provide the relevance of each risk (i.e., High =5, Medium = 3, Low = 1) for each layer of the 6G-DALI architecture (i.e., MLOps, DataOps, Adaptation, DTT, Testbed). Answers were weighted based on the role of the responder in the architecture. Weighting answers based on the accountability of responders is a technically sound and common practice in risk management. This ensures that individuals with direct responsibility and deeper expertise have a more significant impact on the final ranking. Indeed, this approach effectively reduces the 'regression to the mean' observed in the initial ranking, where respondents tended to provide middle-ground answers. These weighted scores are reported in the Table 8, while Table 32 in Annex I provides details for answers, weights and scores. The risk EL-RSK-09 "Validation mismatch" is the most relevant risk, and it belongs to a high value range (i.e., greater than 3,8). All the other identified risks belong to a medium range (i.e., weighted score greater than 2,5), a part of the last two risks. It is important to remark that 35% of the responders answered that they will potentially use dataset containing personal data. This justifies that EL-RSK-13 "Unfair processing of personal data" has a weighted score of 2,9.

Table 8. Risk Assessment

#	Risk ID	Risk Title	Weighted Score
1	EL-RSK-09	Validation mismatch	4.3
2	EL-RSK-10	Lack of robustness	3.6
3	EL-RSK-04	Explainability failure	3.6
4	EL-RSK-06	Lack of metadata	3.5
5	EL-RSK-01	Silent policy change	3.4
6	EL-RSK-07	Bias amplification	3.4
7	EL-RSK-08	Misapplied transfer	3.3
8	EL-RSK-12	API Security	3.2
9	EL-RSK-14	Environmental sustainability	3.1
10	EL-RSK-03	Loss of governance in model drift	3.0
11	EL-RSK-13	Unfair processing of personal data	2.9
12	EL-RSK-05	Bias/Intent Mismatch	2.9
13	EL-RSK-11	Data Leakage	2.5
14	EL-RSK-02	Policy bypass through autonomous model behaviour	2.5

The results of this assessment demonstrate that the consortium is aware of these ethical and legal risks and the necessity of addressing them with appropriate countermeasures. The increasing complexity of autonomous, adaptive, and federated AI systems poses challenges that extend beyond organizational maturity. As autonomy and cross-domain data sharing grow, risks related to governance, policy compliance, explainability, and validation realism become increasingly prominent.

6 6G-DALI Ethics and regulatory requirements

Building on the ethical and regulatory framework described in Section 3 and informed by the risk analysis presented in Section 5, this section defines the ethics and regulatory requirements that operationalise compliance within the 6G-DALI governance framework.

These requirements specify the conditions under which the system's behaviour, configuration, and evolution (including data, models, orchestration mechanisms, and operational processes) remain aligned with applicable legal obligations and protected societal values throughout the system lifecycle.

Furthermore, the requirements are explicitly aligned with the Key Value Indicators (KVIs) established at the project's inception and recalled in Section 4. Together, the ethical and regulatory framework, the identified risks, and the KVIs form an integrated architecture that underpins the project's ethics-by-conception approach and its compliance assessment process:

- **Ethics and Legal High-Level Requirements (EL-HLRs)**, which capture governance objectives and expected properties of the system. This level of requirements is elicited from the ethics, social and legal experts and relies on the relevant ethics and legal principles identified in Section 2. Fulfilment of these requirements is assessed through KVIs, which aggregate the performance of underlying requirements into a measure of societal value;
- **Ethics and Legal Medium-Level Requirements (EL-MLRs)**, which contextualise and operationalise those objectives within the concrete architectural and procedural environment of 6G-DALI. This level of requirements is elicited from an interdisciplinary team composed of experts in social sciences and humanities (SSH) and engineering and technology (STEM). Fulfilment of these requirements is assessed through the collection of evidences, providing raw data and operational proof of system behaviour. Crucially, this assessment compares the gathered evidence against predefined thresholds (e.g., for accuracy or bias) or qualitative constraints (e.g., architectural guardrails), which serve as the triggers for automated governance actions or human review. Thresholds and qualitative constraints are intended to be agreed and refined as the technology development evolves;
- **Ethics and Legal Low-Level Requirements (EL-LLRs)**, which map down to functional and non-functional requirements, considering specific 6G-DALI components and use case conditions. In this initial elicitation of requirements, the EL-LL-Rs are linked directly to the system requirements defined in [8] and [9] (see Annex III: Linked system requirements from D2.2). Fulfilment of these requirement is assessed through technical validation and KPIs. At this stage, these linked requirements act as a feasibility check for ongoing technical development and its alignment with the ethics and regulatory aspects.

This three-level structure supports the progressive transformation of ethical and regulatory commitments into elements that can be implemented, monitored, and assessed within the technical framework.

Compliance with these requirements is supported through KVIs, KPIs, and the generation and maintenance of evidence artefacts, which document the observable and controllable aspects of the 6G-DALI framework. These artefacts provide the basis for supporting traceability, assessment, audit, and review activities, enabling governance bodies to verify whether the intended objectives and safeguards are achieved and effectively in place.

To document, trace, report, and assess the 6G-DALI framework, the project has identified five types of evidence artefacts, that describe occurring events and any system observable information:

- **A – System Information**: static documentation for a specific version of the system, required by the ethics and legal framework regarding key system details (e.g., purpose, data provenance, AI model identifiers, known limitations, and ethics and legal risks). This documentation states the assumptions and conditions to use the system and inform deployers and end-users.
- **B – System Control Record**: real-time documentation automatically generated during execution (including testing), primarily consisting of system logs by data practices (e.g., [timestamp][component]: positive feed from [userX] for [datarequestX1] [dataset Z] and [metadata Z1]).

- **C – System Control Report**: event-driven automatically generated documentation based on stored System Control Records, providing specific details configured by stakeholders for specific purposes (e.g., validator checking satisfaction rate after 100 data requests). This is used to verify thresholds or constraints satisfaction.
- **D – System Configuration**: documentation required during the revision of system settings and parameters.
- **E – Authorisation**: documentation about the governance bodies, the governance processes, the operational assumptions and effects, enabling governing bodies to authorise experiments and use cases within controlled environments.

The structure and content of these evidence artefacts depend on the specific operations carried out by the system, and during system implementation, collaboration with the development team will ensure the successful specification of data and their structures generated within each evidence artefacts and event types. Therefore, the EL-MLRs provide details regarding the minimum information required for assessment under specific conditions, laying the foundation for further improvement and refinement within next steps of development. For clarity, this document references templates for System Information and System Control Record from harmonised standards (see Annex II: A template for System Information).

This contributes to embedding ethics and legal requirements more effectively into the system.

Within the broader SAT framework adopted by the project, these same artefacts contribute to the measurement of Key Value Indicators (KVIs). KVIs enable the evaluation of whether the system's evolution remains aligned with the societal values identified for specific use cases and PoCs.

In this way, requirements, artefacts, and KVIs form a continuous chain linking ethical and legal reflections to technical implementation and operational validation.

The following subsections present the set of **11 High-Level Requirements (EL-HL-Rs)** and the **37 corresponding Medium-Level Requirements (EL-ML-Rs)** that constitute the foundation for ethics and regulatory compliance in 6G-DALI.

6.1 Privacy and Data Governance

Given the risks identified in relation to silent policy change, lack of metadata, unfair processing, and progressive expansion of data uses, privacy and data governance (see Table 9 and Table 10) in 6G-DALI are interpreted as a matter of explicit and revisable governance of data practices (i.e. encompassing both data pre-processing pipelines and model adaptations) defined as *"structured, goal-oriented tasks that combine multiple data processing operations to achieve a defined system function"* over time.

In AI-native environments characterised by continuous reuse, transformation, and inference, compliance cannot rely solely on the legitimacy of individual operations; it requires that purposes, access conditions, reuse logic, and value implications remain documented, traceable, and subject to structured review whenever the system evolves.

Table 9. High-level requirement "Privacy and Data Governance"

EL-HLR-PR "Privacy and Data Governance"
The 6G-DALI framework shall ensure that decisions concerning the collection, use, inference, sharing, reuse and monetization of data by AI-driven components are subject to explicit governance processes that articulate purpose, policies, necessity, and expected impact, respecting also ethics and legal constraints. Data extraction and inference practices shall not rely on implicit assumptions of legitimacy or proportionality, but shall be supported by documented justifications that are reviewable, contestable, and revisable over time. Data practices and processing shall not evolve into extractive, exclusionary, or opaque practices, by requiring that acceptable data scopes, secondary uses, value distribution, and access conditions—particularly for non-personal data—are defined ex ante, monitored over time, and subject to explicit governance review whenever expansion, concentration of value, or dependency emerges. Governance shall apply at the level of distinct data practices, rather than individual data processing events, and the framework shall support traceability

between the governance criteria applied, the resulting decisions, and the corresponding technical configurations.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-01 Silent policy change* • *EL-RSK-06 Lack of metadata* • *EL-RSK-13 Unfair processing of personal data*
KVIs	• KVI-2, KVI-3, KVI-6

Table 10. Medium-level requirements for Privacy and Data Governance

EL-MLR-PR.1 "Framework Information"	
The framework shall support explicit, structured information (including identifiers, purpose, provenance, integrity, rationale, and applicable machine-readable usage policies) for each governed data processing activity (e.g. collection, inference, reuse) and data practice (e.g. data generation through experimentation), specifying inter alia permitted and restricted access, processing, reuse, and sharing. The information shall ensure that any processing of (personal) data is strictly limited to purposes for which a valid legal basis exists under applicable data protection law, as defined and communicated at the time of data collection. The information shall provide assumptions under which datasets are treated as personal data, non-personal data, or anonymised, considering the context of processing and the means reasonably likely to be used for identification.	
System Requirements	*FR-DS 4, FR-DS 7, FR-DS 14, FR-MO-37*
Evidence Artefacts	• A – System Information
Trigger Mechanisms	• At system design/revision
EL-MLR-PR.2 "Assessment Records"	
The framework shall require assessment records documenting events and decisions. These records shall include information about applied policies (e.g. criteria and thresholds), data purposes, residual inference risks, and model constraints, together with the associated rationale for each data practice governance task. Records shall consider three levels of severity: info, warning, error.	
System Requirements	*FR-MLOPS-4, NFR-DS 7, FR-DATAOPS-8, NFR-MO-1, NFR-DATAOPS-2*
Evidence Artefacts	• B - System Control Record
Trigger Mechanisms	• Triggered by every data practice task
EL-MLR-PR.3 "Data Governance"	
Access to personal and non-personal data and related services within the 6G-DALI Data Space shall be governed by fair, transparent, and non-discriminatory conditions, preventing unjustified exclusivity, technical lock-in, or arbitrary access restrictions. Where datasets are mixed, appropriate safeguards shall be applied to ensure that personal data remain subject to applicable data protection law, including governance of secondary use and mediation roles.	

System Requirements	*FR-DS 10, FR-DS 12, FR-MLOPS-3, NFR-DS 3, FR-MO-15, NFR-MO-2*
Evidence Artefacts	• A – System Information
Trigger Mechanisms	• At system design/revision
EL-MLR-PR.4 "Data Governance Revision"	
The framework shall support revision of data practices and processing over time. Revision shall be triggered by specific events (e.g., user request, exception, policy violation) during monitoring of the system operation. The framework shall enable the data controller to review and update such qualification where the processing context, purposes, or reasonably foreseeable means of identification materially change, without implying a requirement for continuous or automated reassessment of identifiability.	
System Requirements	*FR-MO-22, FR-MO-39, FR-MO-29*
Evidence Artefacts	• D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by specific event

6.2 Accountability

Considering risks such as policy bypass through autonomous model behaviour and loss of governance in model drift, accountability (see Table 11 and Table 12) in 6G-DALI is framed at the level of lifecycle governance rather than single decisions. The objective is to ensure that system evolution, policy enforcement, and optimisation dynamics remain attributable to identifiable actors, roles, or procedures, preventing autonomy from dissolving responsibility.

Table 11. High-level requirement "Accountability"

EL-HLR-AC "Accountability"	
The 6G-DALI framework shall ensure accountability for autonomous AI-mediated behaviour through system-level governance mechanisms, rather than through oversight of individual decision instances. Accountability shall be established through explicit governance of system lifecycle (i.e., design, configuration, deployment, and evolution) and through traceability of governance-significant actions, such that responsibility for AI-mediated behaviour remains attributable to identifiable organisational actors and roles over time.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-02 Policy bypass through autonomous model behaviour* • *EL-RSK-03 Loss of governance in model drift*
KVIs	• KVI-2, KVI-6

Table 12. Medium-level requirement for Accountability

EL-MLR-AC.1 "Accountability Mechanism"
The framework shall design accountability mechanisms at system/operation level. Accountability mechanisms shall be triggered according to specific events (e.g., user request, exception, ex-post review)

System Requirements	*FR-MLOPS-4, NFR-DS 15*
Evidence Artefacts	• A - System Information • D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by specific event
EL-MLR- AC.2 "Attribution and Responsibility"	
The framework shall ensure that actions, decisions, objective and system behaviours can be attributed to accountable actors, roles, or processes, and that autonomous operation shall not be used to obscure responsibility. Attribution and responsibility shall be documented and traced through assessment records.	
System Requirements	*NFR-DS 7, FR-DS 10, NFR-MLOPS-1*
Evidence Artefacts	• B - System Control Record • D - System Configuration
Trigger Mechanisms	• Triggered by every data practice task
EL-MLR-AC.3 "Policy Enforcement Traceability"	
The framework shall support traceability of policy enforcement actions (grant/deny/constrain) to enable accountability and audit.	
System Requirements	*FR-DS 15, NFR-DS 7, FR-MO-15, NFR-MO-2*
Evidence Artefacts	• A - System Information • B - System Control Record • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task • Triggered by specific event
EL-MLR-AC.4 "Accountability Reports"	
The framework shall support generation of reports for specific and relevant events, as defined in the system information. Reports shall contain at minimum the following information: the responsible actor or system component; the nature of the action performed; the time and operational context; the declared purpose or intent; the active policy or governance constraint applied; the associated confidence or uncertainty; and the observed outcome or effect. The framework shall treat the following categories of actions as significant by default for accountability purposes, irrespective of context or frequency: (a) governance and policy changes; (b) changes to data scope, inference, or reuse; (c) model lifecycle and learning-related actions; (d) changes to autonomy scope or control boundaries; (e) system-wide operational regime changes.	
System Requirements	*FR-MO-35, NFR-MO-6, NFR-EH-1*

Evidence Artefacts	• C - System Control Report
Trigger Mechanisms	• Triggered by specific event

6.3 Reliability, Robustness and Resilience

In view of risks related to lack of robustness and loss of governance in model drift, reliability and robustness (see Table 13 and Table 14) are understood as the system's capacity to operate within governance-defined limits while keeping failure visible and manageable. Resilience therefore supports not only performance continuity but also oversight, auditability, and informed intervention.

Table 13. High-level requirement "Reliability, Robustness and Resilience"

EL-HLR-RR "Reliability, Robustness and Resilience"	
The 6G-DALI framework shall ensure that AI system behaviour remains reliable and within governance-defined performance and behaviour limits when operating under specified and comparable conditions, as assessed against reliability metrics and baselines appropriate to the relevant operational context. AI systems shall behave in a controlled and predictable manner under uncertainty, abnormal but plausible conditions, and adversarial influences, and that they degrade gracefully when optimal performance cannot be maintained, so as to avoid disproportionate harm due to cascading or uncontrolled failures. Robustness and resilience mechanisms shall not be designed or optimized to conceal failures or mask degradation; failure, degradation, and recovery events shall remain observable and traceable for governance, audit, and accountability purposes.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-03 Loss of governance in model drift* • *EL-RSK-10 Lack of robustness*
KVIs	• KVI-1, KVI-5

Table 14. Medium-level requirements for "Reliability, Robustness and Resilience"

EL-MLR-RR.1 "Identification of Failure Modes and Adversarial Conditions"	
The framework shall identify failure modes (e.g., internal/environmental stress) and adversarial conditions (e.g., external/malicious attacks), as well as corresponding mitigation plans. Failure modes and adversarial conditions include inter-alia: detection of behavioural drift, instability, uncertainty or reduced trustworthiness, uncontrolled degradation over time.	
System Requirements	*FR-MO-16, FR-TAI-5, FR-ELT-7*
Evidence Artefacts	• A - System Information • D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by specific event
EL-MLR-RR.2 "Monitor and Prevent"	
The framework shall support continuous monitoring to identify degradations and preventing failures, based on contextualised assumptions and operating conditions. Monitoring indicators associated with robustness risks shall feed into accountability reports, enabling governance review of preparedness, degradation behaviour, and recovery effectiveness without implying automated	

assessment of harm or ethical acceptability. The framework shall support signalling of uncertainty, degraded behaviour or failures to relevant stakeholders when reliability cannot be ensured with mitigation plans.	
System Requirements	*FR-TAI-6, NFR-MO-7, FR-MO-28*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-RR.3 "Mitigation and Recovery Mechanisms"	
The framework shall support mitigation and recovery mechanisms to enact mitigation plans and restore acceptable behaviour after disruption.	
System Requirements	*FR-MO-22, FR-MO-23, FR-MO-18, NFR-DS 4*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task • Triggered by specific event

6.4 Transparency

Given the risk that AI mediation may shape outcomes while remaining difficult to perceive or contest, transparency (see Table 15 and Table 16) in 6G-DALI is interpreted as ensuring visibility of the presence, objectives, assumptions, and boundaries of AI-driven behaviour. The aim is to make system logic intelligible for governance and trust without requiring exposure of unnecessary technical internals.

Table 15. High-level requirement "Transparency"

EL-HLR-TR "Transparency"	
The 6G-DALI framework shall ensure that AI mediation of network behaviour is not invisible and that the presence, role, and general objectives of AI-driven components are intelligible to relevant stakeholders at an appropriate level of detail. Transparency shall support accountability and governance by making visible the high-level optimisation commitments, trade-off preferences, normative assumptions and validity limits under which AI-mediated behaviour is produced, without requiring disclosure of technical internals or implementation details beyond what is necessary for oversight and trust.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-01 Silent policy change* • *EL-RSK-06 Lack of metadata*
KVIs	• KVI-1, KVI-6

Table 16. Medium-level requirements for Transparency

EL-MLR-TR.1 "Appropriate Disclosure"

The framework shall support appropriate disclosure to authorized stakeholders of the system information and AI-driven behaviour, ensuring that such information is accessible for the duration of the system's lifecycle. Appropriate mechanisms (e.g., multi-level access to system information) shall be defined at design level to respect security, privacy, safety or confidentiality requirements. Personal Identifiable Information shall be limited to what is necessary for accountability, security, and compliance purposes, and shall be specified in accordance with data minimisation, purpose limitation, and storage limitation principles.	
System Requirements	*FR-MO-27, NFR-MLOPS-1, FR-DS 9, FR-MO-15, NFR-MO-2*
Evidence Artefacts	• A - System Information • B - System Control Record • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task • Triggered by specific event
EL-MLR-TR.2 "Operational Information Specification"	
During its operation, system information and AI-driven behaviour shall include, but is not limited to: intermediate processing outputs (generated during data/ML experiments), general objectives, assumptions, decisions optimisation rules, training datasets metadata and lineage, Operational Design Domain (ODD) parameters, guardrail zone violations, architectural/algorithmic rationale, and real-time internal state telemetry.	
System Requirements	*FR-MLOPS-4, FR-DS 14, NFR-MO-3*
Evidence Artefacts	• A - System Information • B - System Control Record • C - System Control Report
Trigger Mechanisms	• At system design/revision • Triggered by every data practice task • Triggered by specific event
EL-MLR-TR.3 "Non-deceptive Transparency"	
The framework shall be designed to ensure non-deceptive transparency by exposing, rather than concealing, internal failures or performance degradation (honest approach). The framework shall not employ optimisation techniques or interface designs that 'smooth over' or mask such events. All failure, degradation, and recovery events shall remain explicitly observable and traceable to ensure that governance, audit, and accountability processes reflect the true operational state of the system without bias or obfuscation.	
System Requirements	*NFR-MO-6, FR-TAI-5, NFR-MLOPS-4, NFR-DATAOPS-6*
Evidence Artefacts	• A - System Information • B - System Control Record • C - System Control Report
Trigger Mechanisms	• At system design/revision;

	• Triggered by specific event

6.5 Explainability

In response to explainability failure and limits in reconstructing anomalous or degraded behaviour, explainability (see Table 17 and Table 18) is treated as a capacity to understand the system's governing logic and aggregate operational effects. Rather than focusing on real-time micro-decisions, the project prioritises explanations that support lifecycle management, audit, and corrective action.

Table 17. High-level requirement "Explainability"

EL-HLR-EX "Explainability"	
The framework shall support explainability of AI-driven behaviour at the level of decision regimes and governing logic, and through analysis of aggregate operational effects, in order to support lifecycle management, troubleshooting, auditing, and informed trust in AI-native 6G infrastructures. Explainability shall be provided at an appropriate temporal and structural granularity, reflecting the fact that real-time explanation of individual microsecond-level decisions is neither feasible nor necessary in large-scale autonomous systems. The effectiveness of explainability shall be assessed using task-based and outcome-oriented metrics and, where appropriate, structured stakeholder feedback linked to concrete operational, troubleshooting, or audit events.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-04 Explainability failure*
KVIs	• KVI-1, KVI-3, KVI-6

Table 18. Medium-level requirement for "Explainability"

EL-MLR-EX.1 "Explainability Mechanisms"	
The framework shall support explainability mechanisms that enable operators to investigate, detect and understand the system behaviour (e.g., identification of influential input factors, aggregate effects, contextual conditions, model configurations, reliance on spurious correlations or unintended proxies) contributing to observed outcomes.	
System Requirements	*NFR-TAI-4, FR-MO-35*
Evidence Artefacts	• A - System Information • C - System Control Report
Trigger Mechanisms	• At system design/revision • Triggered by specific event
EL-MLR-EX.2 "Stakeholders-targeted metrics"	
The framework shall support stakeholder-targeted explainability metrics and corresponding satisfaction thresholds, reflecting the explainability needs of different roles (e.g. operators, auditors, governance bodies). Failure to meet these thresholds shall trigger an automated assessment of the explainability mechanisms in place, with the purpose of informing troubleshooting, auditing, or governance review. Explainability metrics and thresholds shall be defined through governance processes and may evolve over time as system behaviour, stakeholder needs, or regulatory expectations change.	

System Requirements	*FR-MO-29, FR-MO-27, FR-TAI-3*
Evidence Artefacts	• A - System Information • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by specific event
EL-MLR-EX.3 "Explainability Information Specification"	
The framework shall provide clear information about the scope, assumptions, and limitations of available explanations, including uncertainty and known blind spots, to avoid overconfidence or misleading interpretations.	
System Requirements	*FR-TAI-1, FR-TAI-3, NFR-DT-1*
Evidence Artefacts	• A - System Information • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by specific event

6.6 Fairness

Considering risks of bias amplification, and structural differentiation emerging over time, fairness (see Table 19 and Table 20) is interpreted as the need to govern how differential effects arise, persist, and accumulate. The focus is therefore on explicit criteria, monitoring of systemic patterns, and the possibility of revising optimisation choices.

Table 19. High-level requirement "Fairness"

EL-HLR-FA "Fairness"	
The 6G-DALI framework shall ensure that autonomous AI-driven behaviour does not produce unjustified differential effects at system level, and that fairness-related risks are addressed through explicit governance processes rather than implicit assumptions. Decisions concerning acceptable differentiation, prioritisation, or differential impact shall be explicitly defined, assessed against predefined governance criteria, and subject to documentation, review, and revision over time. The framework shall further ensure that fairness indicators are designed to detect emergent, cumulative, and feedback-driven differential effects that may arise over time and may not be attributable to any single design choice or decision.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-07 Bias amplification* • *EL-RSK-13 Unfair processing of personal data*
KVIs	• KVI-1, KVI-7

Table 20. Medium-level requirement for Explainability

EL-MLR-FA.1 "Intentional Differentiation"
The framework shall support explicit documentation of where and why AI-driven behaviour differentiates between predefined classes (e.g., service classes, contexts, device capability tiers). While this requirement concerns intentional and design-time differentiation.

System Requirements	*FR-DS 10, FR-MO-7*
Evidence Artefacts	• A - System Information • C - System Control Report
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task
EL-MLR-FA.2 "Monitoring differentiation indicators"	
The framework shall support monitoring of aggregate and structural indicators that may signal unjustified differential effects across predefined, non-sensitive classes, rather than individual-level or demographic monitoring.	
System Requirements	*FR-MO-28, FR-MO-19*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-FA.3 "Mitigation of differentiation"	
The framework shall support governance processes through which disparities exceeding predefined thresholds trigger review of underlying policies, configurations, or optimisation strategies; corrective action shall focus on reassessment of system-level choices rather than real-time intervention in individual decisions. Governance reviews shall assess observed disparities against explicit criteria addressing alignment with declared differentiation, necessity, proportionality over time, structural persistence, and systemic impact, and shall result in documented decisions and actions.	
System Requirements	*FR-MO-22, FR-MO-23*
Evidence Artefacts	• A - System Information • C - System Control Report • D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by specific event

6.7 Societal and Environmental Well-Being

Given cumulative and long-term risks such as environmental sustainability and broader societal impact, well-being (see Table 21 and Table 22) is framed as a governance responsibility to identify, monitor, and periodically reassess impact signals. The framework supports structured attention to these dynamics even where direct measurement of harm is not feasible.

Table 21. High-level requirement "Societal and Environmental Well-Being"

EL-HLR-SEW "Societal and Environmental Well-Being"
The 6G-DALI framework shall ensure that potential societal risks arising from large-scale, autonomous AI-native 6G operation are identified and addressed through explicit governance

processes, rather than assumed to be absent or negligible. The framework shall not be expected to directly measure societal harm, but shall support the identification, documentation, and review of indicators that may signal cumulative or structural societal impact in order to inform governance oversight and system-level review over time.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-14 Environmental sustainability*
KVIs	• KVI-4

Table 22. Medium-level requirements for "Societal and Environmental Well-Being"

EL-MLR-SEW.1 "Ethics and Societal Risk Identification"	
Societal risk factors relevant to the operation of AI-native 6G infrastructures shall be identified and defined ex ante as part of the project's governance framework. Such factors shall reflect agreed societal concerns associated with large-scale autonomous operation and shall provide the normative reference against which system behaviour is monitored.	
System Requirements	*FR-TAI-6, FR-MO-17*
Evidence Artefacts	• A - System Information
Trigger Mechanisms	• At system design/revision
EL-MLR-SEW.2 "Ethic and Societal Risk Monitoring and Governance"	
The 6G-DALI framework shall support monitoring of system operation against the predefined societal risk factors (e.g., environmental impact signals associated with AI-native 6G operation, such as energy consumption and resource intensity), using aggregate and longitudinal indicators.	
System Requirements	*NFR-EH-3, NFR-TAI-1*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-SEW.3 "Human Autonomy"	
The 6G-DALI framework shall support the identification, monitoring, and governance of structural conditions through which AI-native 6G operation shapes, constrains, or pre-configures the space of human choices, potentially eroding meaningful human autonomy. This requirement concerns the conditions under which choices are made—such as availability of alternatives, defaults, reversibility, visibility of influence, and opt-out capacity—rather than the monitoring or evaluation of individual human behaviour or preferences.	
System Requirements	*FR-MO-30, FR-MO-27*
Evidence Artefacts	• B - System Control Record • C - System Control Report

Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event

6.8 Autonomy

In light of risks connected to silent policy change, policy bypass, drift, and expansion of machine authority, autonomy (see Table 23 and Table 24) is treated as a property that shall remain bounded, observable, and reversible at system level. The requirement therefore focuses on detecting patterns through which optimisation processes may gradually undermine human steering capacity.

Table 23. High-level requirement "Autonomy"

EL-HLR-AU "Autonomy	
The 6G-DALI framework shall explicitly recognise large-scale autonomous decision-making as a defining property of AI-native 6G and ensure that such autonomy remains governable over time through ex-ante constraints and continuous monitoring of aggregate autonomous behaviour. Rather than monitoring individual decisions, the framework shall support monitoring of autonomy-specific, system-level patterns whose emergence, persistence, or escalation may undermine control, reversibility, or accountability, including the ability of human actors to meaningfully intervene at system or policy level. This includes autonomous operational behaviours such as orchestration, experimentation, optimisation, and lifecycle management that may cumulatively expand system authority or reduce effective human control, even in the absence of security violations.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-01 Silent policy change* • *EL-RSK-02 Policy bypass through autonomous model behaviour* • *EL-RSK-03 Loss of governance in model drift*
KVIs	• KVI-1, KVI-2

Table 24. Medium-level requirements for Autonomy

EL-MLR-AU.1 "Autonomy Related Risks Identification"	
Autonomy-related risk patterns (e.g. escalation, persistence, boundary exploitation, convergence, irreversibility) shall be explicitly defined ex ante within governance processes. Furthermore, the framework shall prevent implicit drift driven solely by optimisation incentives or data availability.	
System Requirements	*FR-TAI-5, FR-MO-21*
Evidence Artefacts	• A - System Information
Trigger Mechanisms	• At system design/revision
EL-MLR-AU.2 "Autonomy-Related Risks Monitoring and Governance"	
The framework shall support monitoring of aggregate indicators reflecting autonomy-specific properties, such as stability, diversity, boundary proximity, and reversibility, without requiring interpretation of individual decisions.	
System Requirements	*FR-AR-2, NFR-MO-8*
Evidence Artefacts	• B - System Control Record • C - System Control Report

Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-AU.3 "Autonomy-Related Safeguard Mechanisms"	
The framework shall support safeguard mechanisms, escalating to governance review and enabling governance bodies to intervene at system or policy level where autonomy-related patterns threaten ethics and regulatory principles (e.g., loss of control, accountability, or reversibility).	
System Requirements	*FR-AR-4, FR-MO-22, FR-MO-30, FR-IDD-3*
Evidence Artefacts	• C - System Control Report • D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task • Triggered by specific event

6.9 Epistemic Integrity

Responding to risks such as validation mismatch, misapplied transfer, and limits of simulation environments, epistemic integrity (see Table 25 and Table 26) concerns the quality and validity of the knowledge base guiding AI behaviour. This requires traceability of assumptions, provenance of data, and visibility of generalisation limits.

Table 25. High-level requirement "Epistemic Integrity"

EL-HLR-EI "Epistemic Integrity"	
The 6G-DALI framework shall ensure that learning, validation, simulation, reinforcement learning, and data augmentation processes - carried out through AI and DTT systems - are governed so as to prevent or mitigate epistemic risks that could undermine the reliability and appropriate use of AI-driven behaviour in operational contexts.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-08 Misapplied transfer* • *EL-RSK-09 Validation mismatch*
KVIs	• KVI-3, KVI-5

Table 26. Medium-level requirements for Epistemic Integrity

EL-MLR-EI.1 "Epistemic Risk Identification"	
The framework shall support identification and documentation of epistemic risks. Documentation shall include information about provenance (e.g., synthetic or simulated through AI or DTT), validation environments, assumptions (e.g., scenario, model, algorithm, constraints, limitations), and reward structures used, underrepresented, or excluded in learning, validation and optimisation processes and in reinforcement learning.	
System Requirements	*FR-DS 4, FR-DT-2, FR-MO-37*
Evidence Artefacts	• A - System Information
Trigger Mechanisms	• At system design/revision

EL-MLR-EI.2 "Epistemic Risk Monitoring and Governance"	
The framework shall monitor and govern epistemic risks during validation processes, considering diversity of scenarios, data nature (e.g., synthetic or simulated through AI or DTT) and specified out-of-domain (OOD) parameters reflecting operational contexts and use cases. The framework shall support notification of range of limits to validity and generalisation of models.	
System Requirements	*FR-AR-4, FR-AR-6, FR-MO-20, FR-TAI-6*
Evidence Artefacts	• B - System Control Record • C - System Control Report • D - System Configuration
Trigger Mechanisms	• 2 - Triggered by every data practice task • 3 - Triggered by specific event
EL-MLR-EI.3 "Epistemic Risk Safeguard Mechanisms"	
The framework shall support safeguards against validation-induced distortion, including overfitting to narrow scenarios or amplification of bias through reward design.	
System Requirements	*FR-AR-4, FR-MO-9, FR-MO-13, FR-DA-2, NFR-DA-5*
Evidence Artefacts	• A - System Information • C - System Control Report • D - System Configuration
Trigger Mechanisms	• At system design/revision; • Triggered by every data practice task • Triggered by specific event

6.10 Bias

Given that bias may be introduced across multiple stages, from intent translation to training and adaptation, the project interprets bias (see Table 27 and Table 28) as a distributed lifecycle risk rather than a single defect. Governance shall therefore enable identification, monitoring, and intervention across interconnected components.

Table 27. High-level requirement "Bias"

EL-HLR-BI "Bias"	
The 6G-DALI framework shall ensure that bias risks arising across the AI lifecycle are explicitly identified, documented, and governed, so as to prevent their silent introduction or propagation into AI-driven behaviour.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-05 Bias/Intent Mismatch* • *EL-RSK-07 Bias amplification*
KVIs	• KVI-3, KVI-7

Table 28. Medium-level requirements for Bias

EL-MLR-BI.1 "Bias Risk Identification"

The framework shall support identification and documentation of bias risks that may introduced through data selection, transfer mechanisms, application to new domain, translation of user intent, processing, labelling, or aggregation steps used in model training, validation, simulation, or optimisation.	
System Requirements	*FR-IDD-6, FR-DS 4*
Evidence Artefacts	• A - System Information
Trigger Mechanisms	• At system design/revision
EL-MLR- BI.2 "Bias Monitoring and Governance"	
The framework shall monitor and govern bias that may be introduced during validation processes, simulation and operations. The framework shall support traceability and notification of identified bias and corresponding effects across datasets, models, simulations, and derived artefacts.	
System Requirements	*FR-MO-26, FR-TAI-5*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-BI.3 "Bias in Intent-based Translation"	
The framework shall support explicit and traceable interpretation of user intent, distinguishable from the original user request, including the identification and notification of ambiguity, under specification, or assumptions introduced during intent translation. The framework shall clearly distinguish between retrieved, generated, and hybrid datasets, including the recording of generation triggers where relevant, in order to enable governance and assessment of biases that may emerge or be reinforced through intent translation, data retrieval or generation, and associated learning, optimisation, or feedback processes.	
System Requirements	*FR-IDD-3, FR-DATAOPS-8, FR-IDD-6*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event
EL-MLR-BI.4 "Bias Mitigation Mechanisms"	
The framework shall support safeguard mechanisms against identified biases, escalating to governance review, enabling governance bodies to intervene at system or policy level and applying appropriate de-biasing techniques.	
System Requirements	*FR-ELT-4, FR-MO-23, NFR-ELT-3*

Evidence Artefacts	• A - System Information • C - System Control Report • D - System Configuration
Trigger Mechanisms	• At system design/revision • Triggered by every data practice task • Triggered by specific event
EL-MLR-BI.5 "Feedback on Intent Translation"	
The framework shall support verification and validation of intent fulfilment for every data retrieval or generation request, in order to assess whether the outcome corresponds to the user's declared intent. Such verification shall be performed through structured feedback mechanisms linked to accountability reports, capturing user assessment of intent fulfilment dimensions such as accuracy, relevance, completeness, ease of use, and outcome adequacy. The collection of intent-fulfilment feedback shall serve verification, validation and monitoring purposes. The use of such feedback to modify models, optimisation strategies, intent translation mechanisms, or governance criteria shall be treated as a significant action for accountability purposes.	
System Requirements	*FR-IDD-3, FR-IDD-6, NFR-DATAOPS-4, NFR-IDD-4*
Evidence Artefacts	• B - System Control Record • C - System Control Report
Trigger Mechanisms	• Triggered by every data practice task • Triggered by specific event

6.11 Security and Safety

Considering risks of data leakage, API exposure, and unsafe experimentation, security and safety (see Table 29 and Table 30)are interpreted as continuous boundary conditions for autonomous operations. Protection mechanisms shall remain active throughout system evaluation and support traceability of violations and anomalies.

Table 29. High-level "Security and Safety"

EL-HLR-SaS "Security and Safety"	
The 6G-DALI framework shall operate within enforceable security and safety boundaries to identify, monitor, prevent and mitigate potential threats, unauthorised, unsafe, or out-of-scope actions. APIs of the components - that provide and access data and functionalities - are a key element to be considered. The experimentation of 6G-DALI framework shall be carried out in a controlled and isolated environment from the operational context, considering the maturity level of technologies, the levels of autonomy of AI-driven components, the level of confidentiality of data belonging also to critical infrastructures, and potential side effects. Security and safety aspects shall be identified and governed during the whole 6G-DALI framework lifecycle.	
Addressing Challenge(s)/Risk(s)	• *EL-RSK-11 Data Leakage* • *EL-RSK-12 API Security*
KVIs	• KVI-1, KVI-2

Table 30. Medium-level requirements for Security and Safety

EL-MLR-SaS.1 "Authorisation and Governance"	
The 6G-DALI Framework experiments shall be explicitly authorised through governance processes and remain attributable to identifiable organisational actors or governance bodies. The authorisation and the governance processes shall be informed about operational assumptions and effects (e.g., potential operational scope, policy, or safety impact).	
System Requirements	*NFR-MLOPS-1, FR-DS 8, FR-DS 9*
Evidence Artefacts	• E – Authorisation
Trigger Mechanisms	• At system design/revision • At Pilot Planning
EL-MLR-SaS.2 "Experimentation Sandbox"	
The 6G-DALI Framework experiments shall be carried out in a controlled and isolated environment (sandbox), replicating operational context and characteristics.	
System Requirements	*FR-MO-42, FR-DT-1*
Evidence Artefacts	• E – Authorisation
Trigger Mechanisms	• At system design/revision • At Pilot Planning
EL-MLR-SaS.3 "API Security"	
The 6G-DALI Framework components shall implement security mechanism to ensure data protection and security through its APIs. The security mechanism shall (i) grant access to identified users (identity and permission management); (ii) monitor and trace API calls; (iii) limit rate of invocations. Security mechanism shall ensure confidentiality, integrity, and availability of data.	
System Requirements	*NFR-DS 6, FR-MLOPS-3, NFR-DS 7, FR-MO-15, NFR-MO-2*
Evidence Artefacts	• A - System Information • B - System Control Record • C - System Control Report • D - System Configuration
Trigger Mechanisms	• At system design/revision • Triggered by every data practice task • Triggered by specific event

6.12 Analysis and Insights

Drawing upon the established ethical and legal frameworks, the initial analysis categorised 14 primary risks into four distinct groups. To mitigate these risks and ensure regulatory compliance, the 6G-DALI team defined 11 high-level (core) requirements that embody fundamental ethical and legal principles. These core requirements are closely linked to the identified risks, while medium-level requirements establish the necessary constraints to integrate the system specifications elicited in[9] .

The relationship between these elements is two-fold: first, Table 31 illustrates how specific high-level requirements directly address the identified risks. Second, these requirements are mapped to the broader Key Value Indicators (KVIs) of 6G-DALI, as shown in Figure 5, ensuring that ethical safeguards are translated into measurable indicators for ethics, regulatory and societal aspects.

Table 31. Ethics and legal Risks - High-level Requirements Matrix

		High-Level Requirements										
		Privacy and Data Governance	Accountability	Reliability, Robustness, Resilience	Transparency	Explainability	Fairness	Societal & Env. Well-Being	Autonomy	Epistemic Integrity	Bias	Security and Safety
RISKS	1. Silent policy change	X			X				X			
	2. Policy bypass through autonomous model behaviour		X						X			
	3. Loss of governance in model drift		X	X					X			
	4. Explainability failure					X						
	5. Bias/Intent Mismatch										X	
	6. Lack of metadata	X			X							
	7. Bias amplification						X				X	
	8. Misapplied transfer									X		
	9. Validation mismatch									X		
	10. Lack of robustness			X								
	11. Data Leakage											X
	12. API Security											X
	13. Unfair processing of personal data	X					X					
	14. Environmental sustainability							X				

The distribution of requirements for the identified risks demonstrates a strategic shift from managing individual errors to governing systemic, emergent behaviours inherent in AI-native 6G networks, and contextualised in the specific 6G-DALI framework and the three PoCs.

“Validation Mismatch” is the highest-ranked risk and it is addressed through the high-level requirement “Epistemic Integrity” and its three medium-level requirements, mandating strict governance over provenance and the valid scope of generated data to prevent "false confidence" in operational contexts.

A recurring theme across the risks (e.g., Silent Policy Change, Policy Bypass, and Model Drift) is the potential hidden degradation or autonomous changes in data policies (e.g., change of consented purpose). The analysis counters this through a "Governance of Silence" approach. The Transparency and Accountability requirements are designed to force these implicit changes into the open. By treating "significant actions" (e.g., changes in autonomy scope) as events requiring tamper-evident

accountability receipts, the framework ensures that autonomous optimisation does not quietly rewrite safety rules in pursuit of efficiency.

The framework introduces novel safeguards for Intent-Driven DataOps. Risks like Bias/Intent Mismatch highlight the likelihood that AI might misinterpret a human operator's high-level request. The Bias requirement explicitly targets "intent translation," ensuring that the gap between what a user asks for (natural language) and what the system executes is verifiable and traceable, preventing the "black-box" distortion of command. Moreover, the requirements identify mechanisms to enable user feedback and therefore human oversight in the loop.

Ultimately, the comprehensive risk-requirement matrix and the KVIs-Requirements radar (Figure 5) reveal a proactive governance model, as well as full coverage of the KVIs with specific requirements. Rather than waiting for a failure to occur, requirements such as Autonomy and Reliability enforce continuous monitoring of aggregate patterns (e.g., escalation or boundary exploitation) to detect potential loss of control before it results in a critical system failure.

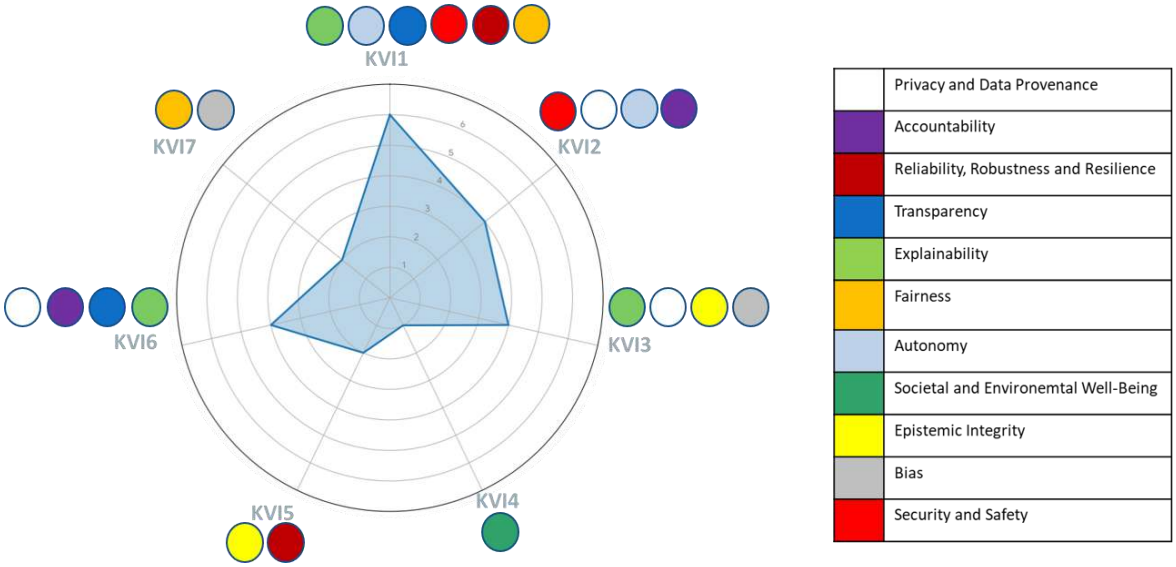


Figure 5. KVIS and High-Level Requirements radar

7 Conclusions

Deliverable D2.4, "6G-DALI compliance with data legislation and ethical requirements - Initial", establishes the governance and methodological architecture for operationalising ethical principles and regulatory obligations throughout the 6G-DALI technology lifecycle. While 6G-DALI operates at a preparatory stage of 6G development (focusing on dataset retrieval, curation, and generation to support future AI-native network architectures), this deliverable defines a framework applicable across all project phases, ensuring that compliance is embedded from initial design through subsequent architectural and technical evolution.

The work relies primarily on the Ethics of AI (ETHAI) model as a structured, iterative methodology for translating ethical norms and regulatory requirements into concrete system-level constraints. In framing relevant concerns and contextual considerations, the project also draws upon insights generated through the Social Acceptance of Technology (SAT) methodology in previous initiatives. In particular, empirical findings and analytical results produced in earlier projects (e.g., 6G4Society) informed the broader contextual understanding within which risks and requirements were analysed.

Through this ethics-by-conception approach, interdisciplinary collaboration between Social Sciences and Humanities (SSH) and Technology and Engineering (STEM) experts is operationalised as a continuous and structured process. This ensures that ethical principles, regulatory safeguards, and governance mechanisms remain systematically integrated into technological innovation as the 6G-DALI architecture evolves.

The framework is anchored in a comprehensive European ethical and regulatory background, integrating binding instruments such as the GDPR, AI Act, Data Act, and Data Governance Act. Furthermore, the methodology leverages emerging harmonised standards (e.g., ISO/IEC 42005, CEN/CLC prEN 18286) to support the translation of high-level principles into structured and auditable technical requirements.

Within this architecture, seven stable Key Value Indicators (KVIs) function as verifiable value-claims that reflect the successful embedding of ethical and legal principles into the system. Each KVI is linked to the identified risks and corresponding requirements across the hierarchy. While requirements operationalise values at the design and implementation level, the KVIs provide a structured mechanism to assess whether those values have been effectively realised. In this sense, the satisfaction of the relevant requirements should be reflected in the measurable fulfilment of the corresponding KVIs, thereby enabling verification of value integration within the technological architecture.

A structured risk analysis involving the full consortium identified and prioritised 14 primary ethics and regulatory risks, ranging from technical vulnerabilities such as Validation Mismatch (the highest-ranked risk) to governance-related challenges including Silent Policy Change and Model Drift.

To address these risks, D2.4 maps them to a three-level hierarchy of requirements:

- 11 High-Level Requirements (EL-HLRs): Core governance objectives and expected system properties (e.g., Accountability, Transparency, Epistemic Integrity), grounded in relevant ethical and legal principles.
- 37 Medium-Level Requirements (EL-MLRs): Requirements that contextualise and operationalise the EL-HLRs within specific 6G-DALI architectural layers, components, and use cases.
- 70 Low-Level Requirements (EL-LLRs): Requirements aligned with functional and non-functional technical specifications defined in Deliverable D2.2. They are distributed across architectural domains such as MLOps, DataOps, RLOps, Data Space, Trustworthy AI, and Digital Twins. Furthermore, they act as a feasibility check for ongoing technical development and its alignment with the ethics and regulatory aspects.

These requirements are linked to the seven KVIs and to five categories of evidence artefacts, ensuring that ethical and regulatory commitments can be systematically verified and traced.

At this stage while the mapping between risks, requirements, KVIs, and technical specifications provides a coherent governance model, further refinement and empirical verification are required as system

components mature. In particular, medium-level requirements will require targeted collaborative development.

The next phase of work will therefore focus on three interrelated streams. First, in close collaboration with the technical partners, the evidence artefacts will be further specified: for each requirement, the structure, content, delivery mechanisms, and feasible degree of automation of the corresponding artefact will be elaborated and fine-tuned. Second, the requirement hierarchy itself will be collaboratively refined.

The EL-MLRs will be reassessed in terms of clarity, feasibility, and architectural coherence, while the alignment between EL-MLRs and the technical EL-LLRs will be examined in greater depth. Where further alignment is needed, particularly as medium-level requirements are mapped against the evolving technical specification and development, iterative refinements or extensions will be introduced to ensure full coverage.

Third, as implementation progresses, a first ETHAI compliance cycle will be conducted. This will involve assessing the degree to which requirements are effectively embedded into the system specifications, implemented and reflected in the corresponding KVIs and evidence artefacts. Consistent with the iterative nature of ETHAI, the outcomes of this compliance assessment may trigger further refinement of requirements, artefact specifications, or implementation strategies.

Through this structured and collaborative process, 6G-DALI progressively aligns system specifications with ethical constraints, regulatory safeguards, and qualitative thresholds, ensuring that value integration remains an active and evolving component of technological development. The forthcoming Ethics Reports and the final consolidated version of the ethics and regulatory requirement framework foreseen for 2026 will mark the maturation of this ethics-by-conception model within the evolving landscape of AI-native 6G development.

8 References

[1] "Social Acceptance of Technology (SAT) methodology," CyberEthics Lab. [Online]. Available: https://sat.cyberethicslab.com/ [Accessed: 16-Feb-2026]

[2] M. Bezzi, L. Pereira Carwile, L. Briguglio, C. Occhipinti, and K. Petersen, "Societal aspects in 6G technology: concerns, acceptance models and sustainability indicators," 2024, doi: 10.5281/zenodo.14747637

[3] 6G4Society project. Available online https://cordis.europa.eu/project/id/101139070/

[4] L. Briguglio, P. -J. Nesse, A. Di Giglio, C. Occhipinti, P. Durkin and I. Markopoulos, "Business Value and Social Acceptance for the Validation of 5G Technology," in *IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2021, pp. 132-137, doi: 10.1109/MeditCom49071.2021.9647485

[5] 5G-SOLUTIONS project. [Online]. Available: https://cordis.europa.eu/project/id/856691/

[6] SNS JU, "Smart Networks and Services Joint Undertaking Working Groups," 2025. [Online]. Available: https://smart-networks.europa.eu/sns-ju-working-groups/

[7] S. Shafaei et al., "Toward AI in 6G: Concepts, Techniques, and Standards," in *IEEE Access*, vol. 13, pp. 143843–143874, 2025, doi: 10.1109/ACCESS.2025.3595752

[8] 6G-DALI Project, "D2.1 - 6G-DALI Business approach and use-cases assessment," 2025

[9] 6G-DALI Project, "D2.2 - Initial Report on Functional and Non-Functional Requirement of the 6G-DALI Architecture," 2025

[10] L. Volpini, V. Prosseda, F. Morpurgo, Š. Glišovic Krivec, D. Krivec, "The ETHAI Methodology," in *Artificial Intelligence Applications and Innovations. AIAI 2025 IFIP WG 12.5 International Workshops. AIAI 2025*, 2025, vol. 754, Springer, doi: 10.1007/978-3-031-97313-0_19

[11] MeSCobraD project. [Online]. Available: https://cordis.europa.eu/project/id/965422/

[12] COMFORTage project. [Online]. Available: https://cordis.europa.eu/project/id/101137301

[13] PRESERVE project. [Online]. Available: https://cordis.europa.eu/project/id/101168392

[14] AI-HLEG, "EU Guidelines for Trustworthy AI," 2019. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 [Accessed: 16-Feb-2026]

[15] European Parliament and the Council, "Artificial Intelligence Act (EU Regulation 2024/1689)," 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[16] UNESCO, "Recommendation on the Ethics of Artificial Intelligence," 2021. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000381137

[17] European Commission, "Living guidelines on the responsible use of generative AI in research," second version, April 2025. [Online]. Available: https://research-and-innovation.ec.europa.eu/document/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en

[18] M. Mert, "AI Ethics for 6G: Governance, Global Alignment, and Responsible Innovation," in *Journal of Industrial Policy and Technology Management*, vol. 8, no. 2, pp. 103-116, 2025, doi: 10.5281/zenodo.17866478

[19] P. Radanliev, "AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development," in *Applied Artificial Intelligence*, vol. 39, no. 1, 2025, doi: 10.1080/08839514.2025.2463722

[20] S.B. Chetty et al. "Sovereign AI for 6G: Towards the Future of AI-Native Networks", 2025. [Online]. Available: https://arxiv.org/html/2509.06700

[21] F6G IA SNVC-SG, "What societal values will 6G address?," 2022, doi: 10.5281/zenodo.6557534

[22] P. Tripathi e A. Malik, "Ethical and Social Dimensions of 6G Deployment", 2025, pp. 401–434. doi: 10.4018/979-8-3373-2220-9.ch014.

[23] United Nations, "The 17 Goals," 2025. [Online]. Available: https://sdgs.un.org/goals

[24] European Parliament and of the Council, "General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[25] B. Friedman, D.G. Hendry, "Value Sensitive Design: Shaping Technology with Moral Imagination," The MIT Press, doi: 10.7551/mitpress/7585.001.0001

[26] G. Wikström, et al., "Key value indicators: A framework for values-driven next-generation ICT solutions," in *Telecommunications Policy*, vol. 48, no. 6., 2024, doi: 10.1016/j.telpol.2024.102778

[27] SNS JU TMV WG, "6G KVIs – SNS Projects Initial Survey Results 2025," 2025, doi: 10.5281/zenodo.15220945

[28] M. Borghi, B. White, "Data extractivism and public access to algorithms: Mapping the battleground of international digital trade," in *Law, regulation and governance in the information society*, pp. 105–125, 2022, Routledge.

[29] R. Kitchin, "The data revolution: Big data, open data, data infrastructures and their consequences," 2014, Sage.

[30] E. Winsberg, "Science in the age of computer simulation," 2010, University of Chicago Press.

[31] European Parliament and the Council, "Data Act (EU Regulation 2023/2854)," 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

[32] European Parliament and the Council, "Data Governance Act (EU Regulation 2022/868)," 2022. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/868/oj

[33] Future Network Services, "The relevance of the AI Act to 6G: The Safety Component," 2024. [Online]. Available: https://futurenetworkservices.nl/publish/pages/6271/fns6g_20241211_ai_act_6g_safety_component_v1-0.pdf

[34] CEN/CLC TR 18115:2024 "Data governance and quality for AI within the European context"

[35] CEN/CLC prEN 18286 "Artificial Intelligence – Quality Management System for EU AI Act Regulatory Purposes"

[36] ISO/IEC 42005:2025 "Information technology — Artificial intelligence (AI) — AI system impact assessment"

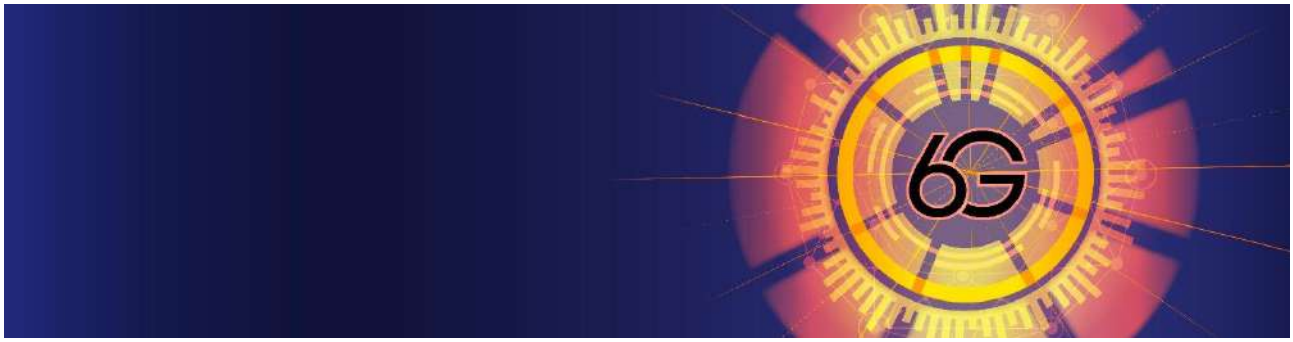
[37] ISO/IEC TS 6254:2025 "Information technology — Artificial intelligence — Objectives and approaches for explainability and interpretability of machine learning (ML) models and artificial intelligence (AI) systems"

[38] ISO/IEC DIS 25059 "Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality models for AI systems"

[39] ETSI TS 104 008 "Methods for Testing & Specification (MTS); Continuous Auditing Based Conformity Assessment for AI-enabled systems," 2026. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/104000_104099/104008/01.01.01_60/ts_104008v010101p.pdf

[40] ISO/IEC, "ISO/IEC CD TS 22443 - Artificial intelligence — Guidance on addressing societal concerns and ethical considerations", under development. https://www.iso.org/standard/87119.html

Annex I: Risk Assessment Questionnaire and Answers



6G-DALI Ethics and Legal Risk Questionnaire

CyberEthics Lab (CEL) , playing the role of ethics manager in the 6G-DALI project, is performing an initial assessment with respect to ethics and legal aspects.

This step is identifying an initial list of potential risks, based on the document review (i.e., D1.1, D2.1, D2.2).

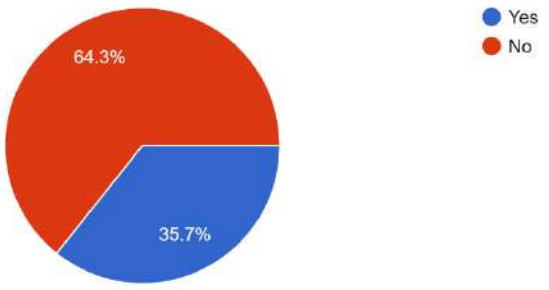
Based on these risks, CEL is eliciting ethics and legal requirements to be embedded into the development process.

Risks reflect the intrinsic characteristics of AI, data-intensive processing, autonomous optimisation, and intent-based abstractions.

It is fundamental the feedback of the partners to better fit the risks, to fine-tune the appropriate specific countermeasures and to elicit requirements.

It is enough just one questionnaire per partner.

Thanks for your cooperation

Email	*Valid email of the responder*
Partner	*Select from dropdown list*
Select your main thematic area(s) in 6G-DALI project	*Checkboxes* MLOps, DataOps, DTT, TestBed, Adaptation, Coordination, Compliance, Impact
<u>Personal Identifiable Information in Dataset</u> ***Does your dataset contain any information that identifies or may identifies individuals?*** ***<u>Personal information</u>*** in the context of GDPR means "*any information relating to an identified or identifiable living natural person ("data subject"). It covers direct identifiers (e.g., name, ID number) and indirect identifiers (e.g., location data, IP address, IMSI, or factors specific to physical, mental, or social identity).*"	Yes / No 

RISKS

For each risk in this questionnaire, please, select the relevance (low, med, high) for the following thematic areas (MLOps, DataOps, Adaptation, DTT, TestBed)

! Risk is not an issue, but an uncertain event or condition that, if it occurs, has a negative (threat) effect on at least one project objective.!

EL-RSK-01 Silent policy change

Significant changes in data processing practices (e.g. retention, reuse, access, or sharing) may be introduced without notification, explicit review, or formal approval, resulting in data use that deviates from the originally defined policy constraints.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

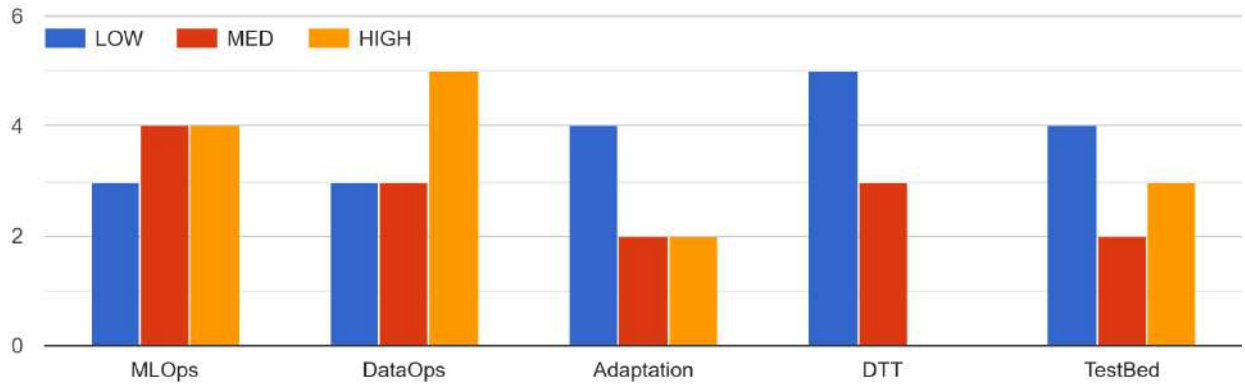


Figure 6. Answers for EL-RSK-01

EL-RSK-02 Policy bypass through autonomous model behaviour

The autonomous operation of AI/ML models may unintentionally bypass or circumvent predefined usage, access, or governance policies, leading to data processing or system behaviours that fall outside the intended policy constraints.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

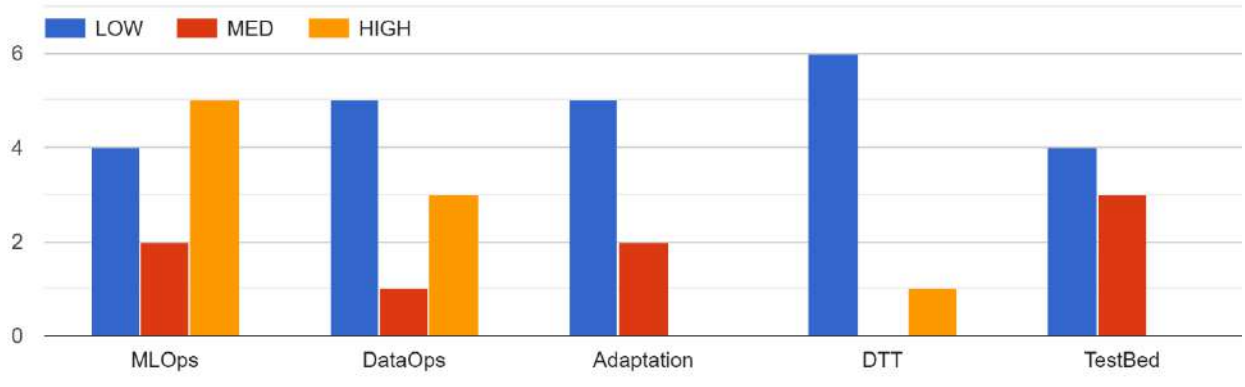


Figure 7. Answers for EL-RSK-02

EL-RSK-03 Loss of governance in model drift

The absence of adequate procedures or monitoring data may prevent the detection and assessment of model drift over time, leading to loss of control over model behaviour and performance.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

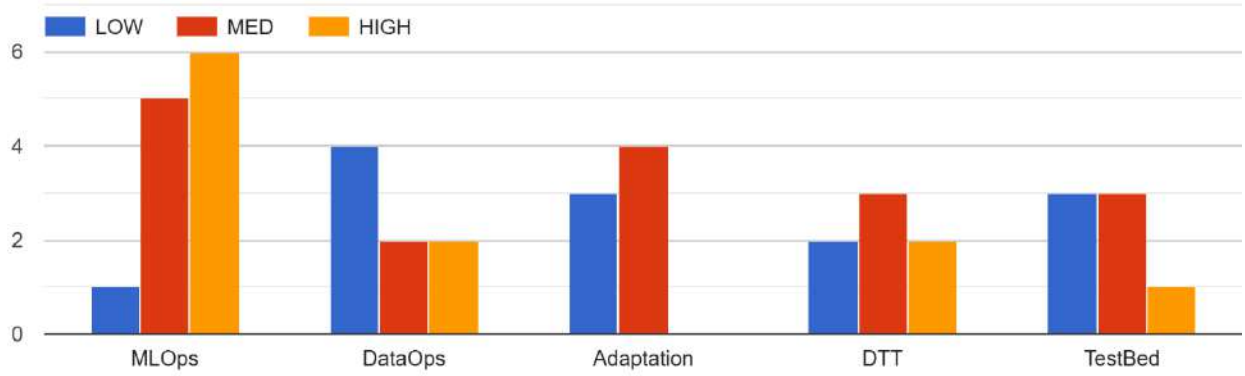


Figure 8. Answers for EL-RSK-03

EL-RSK-04 Explainability failure

Limited explainability may prevent the reconstruction of the causes underlying degraded, unexpected, or anomalous system or model behaviour.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

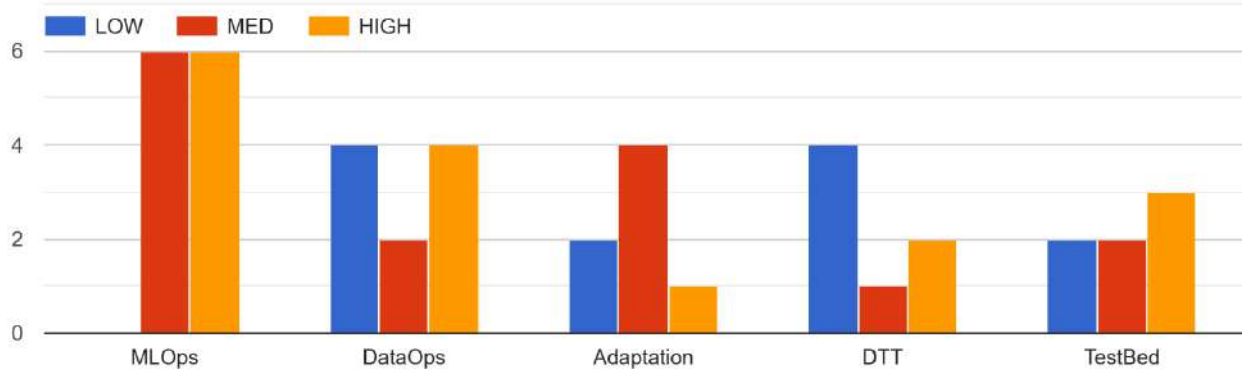


Figure 9. Answers for EL-RSK-04

EL-RSK-05 Bias/Intent Mismatch

Datasets generated or extracted from user-expressed intent (e.g. natural-language descriptions) may not accurately reflect that intent, while metadata describing the dataset may be insufficient to reveal such mismatches, leaving users without effective means to detect deviations between the requested and the actual dataset content.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

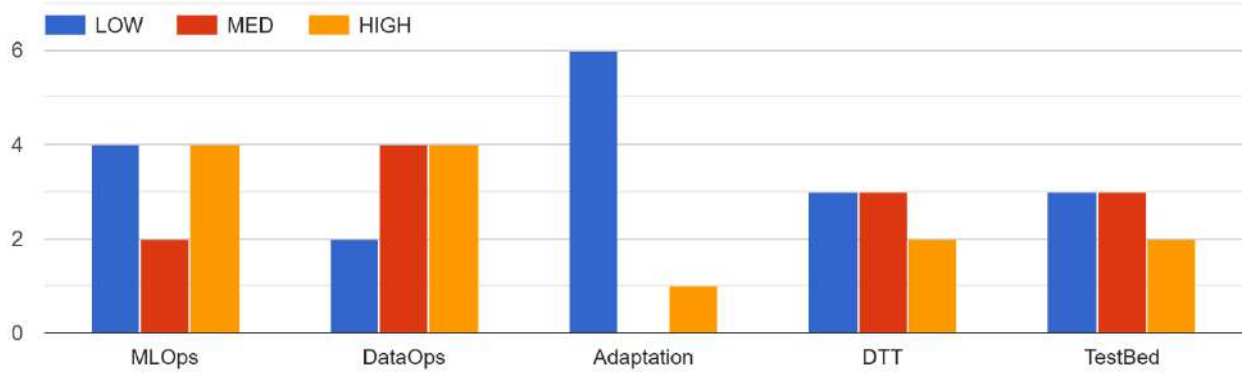


Figure 10. Answers for EL-RSK-05

EL-RSK-06 Lack of metadata

Insufficient or missing metadata may prevent users from effectively checking and validating datasets, models, decisions, or applied policies (e.g. provenance, integrity, or contextual information).

[Select the relevance (low, med, high) of the risk for at least one thematic area]

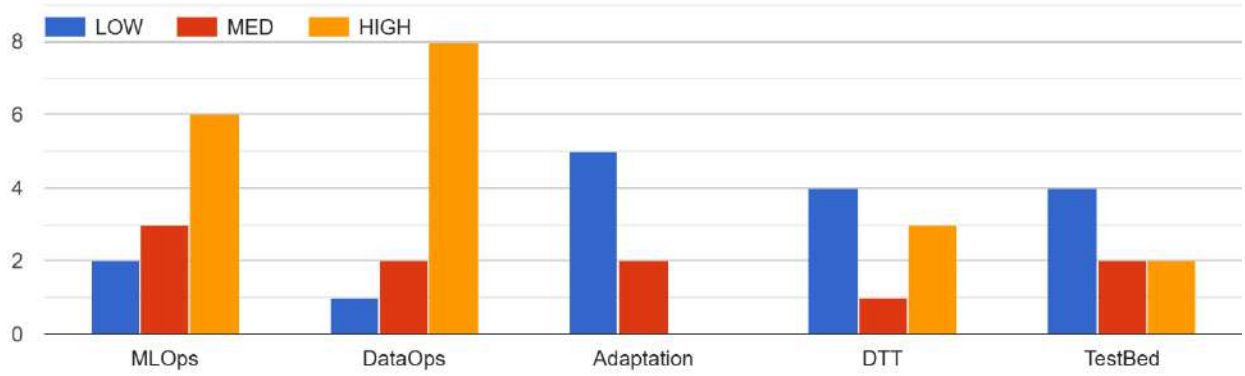


Figure 11. Answers for EL-RSK-06

EL-RSK-07 Bias amplification

Reward structures or optimisation loops may amplify dominant patterns or systematically suppress rare, edge, or under-represented conditions, leading to skewed model behaviour or degraded performance under atypical or low-frequency operating conditions.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

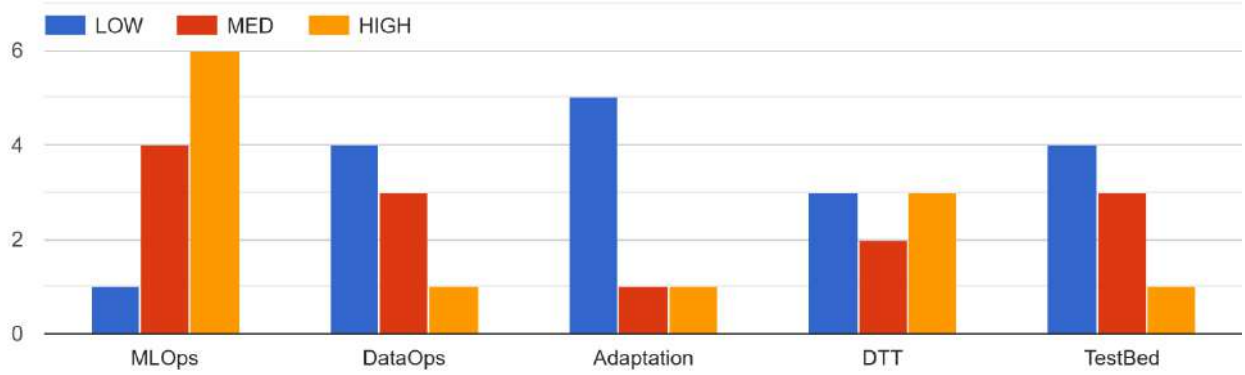


Figure 12. Answers for EL-RSK-07

EL-RSK-08 Misapplied transfer

Transfer learning or zero-shot learning (ZSL) may be applied with insufficient, incomplete, or misleading contextual information, leading to inappropriate model adaptation or degraded performance in the target domain.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

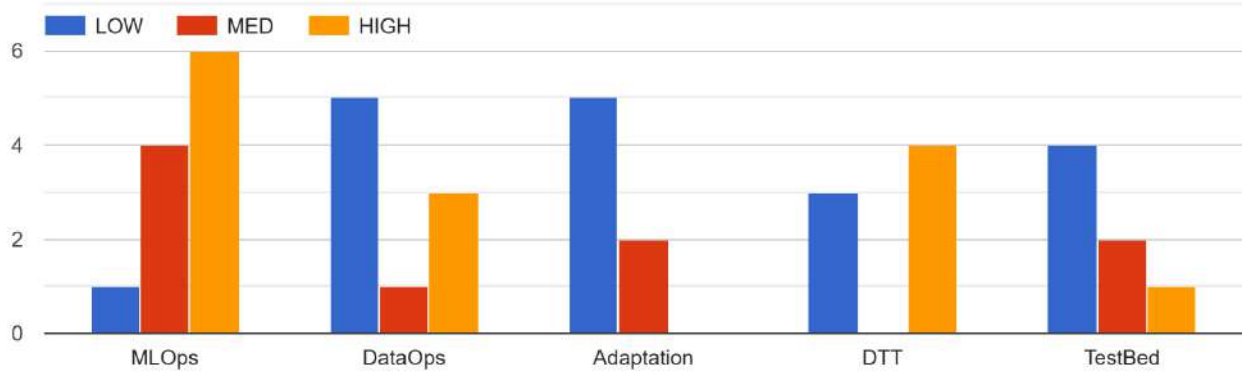


Figure 13. Answers for EL-RSK-08

EL-RSK-09 Validation mismatch

Validation and simulation environments may fail to adequately reflect real deployment conditions, creating false confidence in model performance, robustness, or policy compliance.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

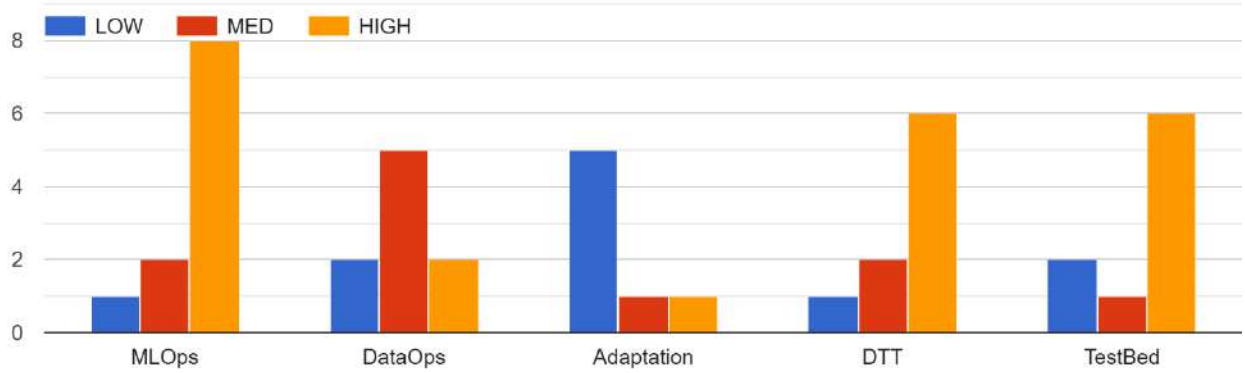


Figure 14. Answers for EL-RSK-09

EL-RSK-10 Lack of robustness

Datasets, models, or system components may not achieve the required level of robustness, resulting in unstable or unreliable behaviour, including non-graceful failure modes, under varying or adverse operating conditions.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

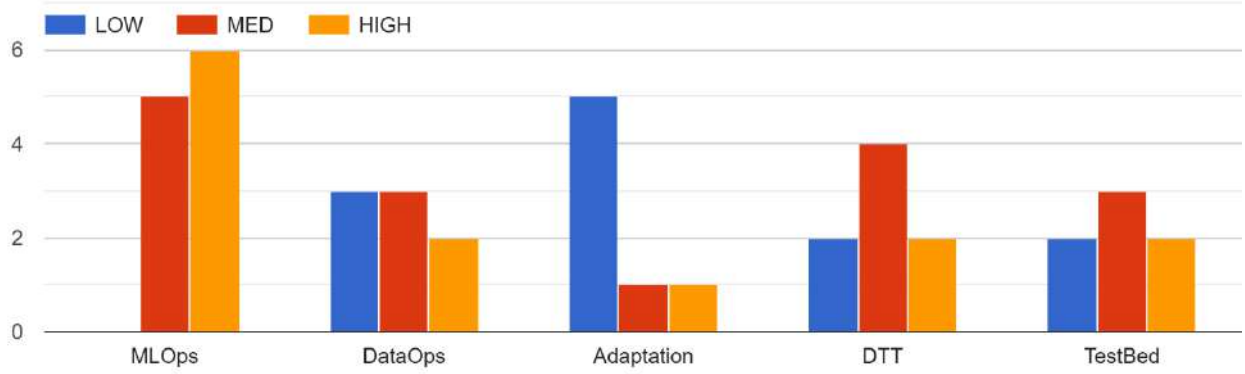


Figure 15. Answers for EL-RSK-10

EL-RSK-11 Data Leakage

Unintentional or unauthorised exposure or inference of data by external or unauthorised parties may occur during data generation, processing, storage, exchange, or model training and adaptation.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

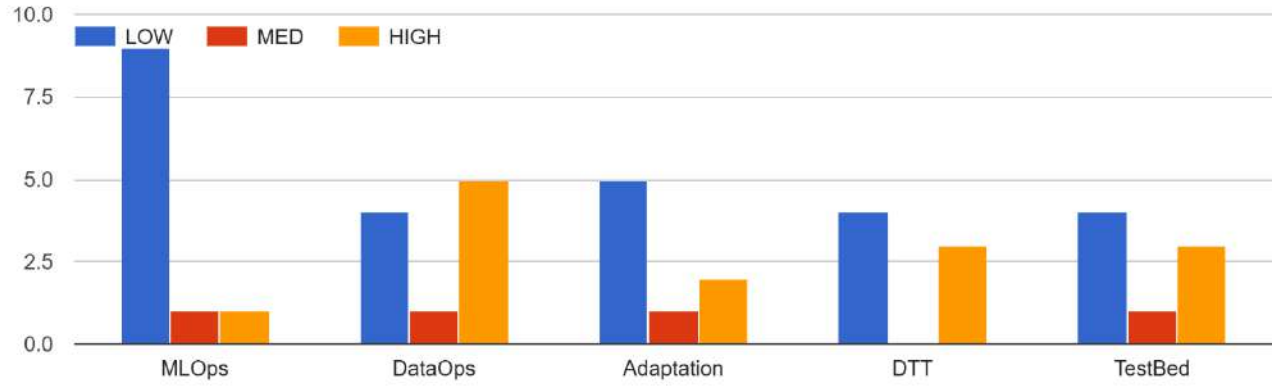


Figure 16. Answers for EL-RSK-11

EL-RSK-12 API Security

APIs exposed or consumed by internal components, autonomous AI/ML systems, or unauthorised third parties may be inadequately protected, potentially compromising system behaviour, integrity, or control.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

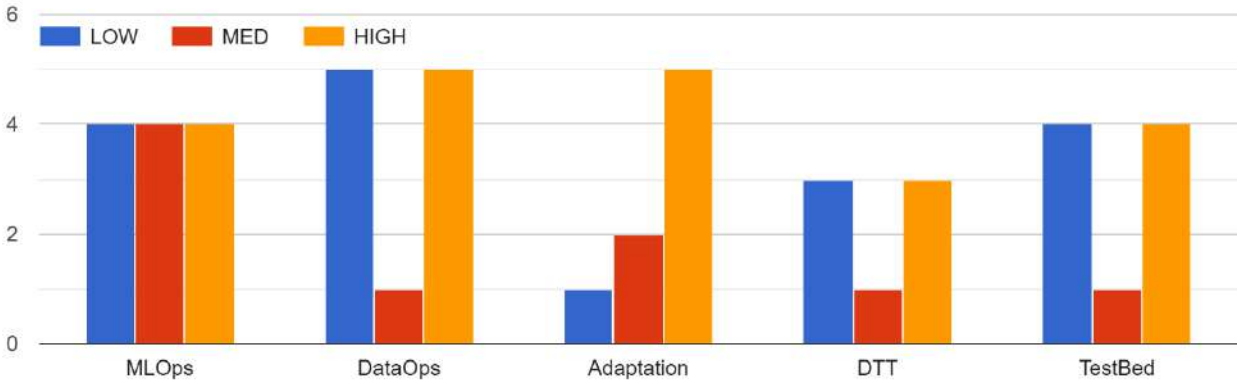


Figure 17. Answers for EL-RSK-12

EL-RSK-13 Unfair processing of personal data

Where datasets contain personal data, the applied technical and organisational measures may be insufficient to ensure fair and appropriate data processing and protection.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

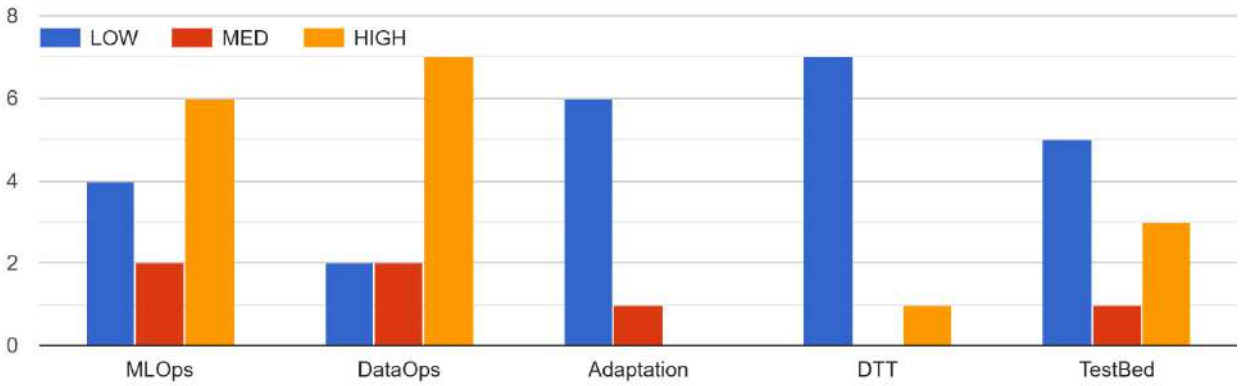


Figure 18. Answers for EL-RSK-13

EL-RSK-14 Environmental sustainability

The cumulative environmental impact of data generation, storage, processing, and model training (e.g. energy consumption and CO_2 emissions) may be significant if not adequately monitored or optimised.

[Select the relevance (low, med, high) of the risk for at least one thematic area]

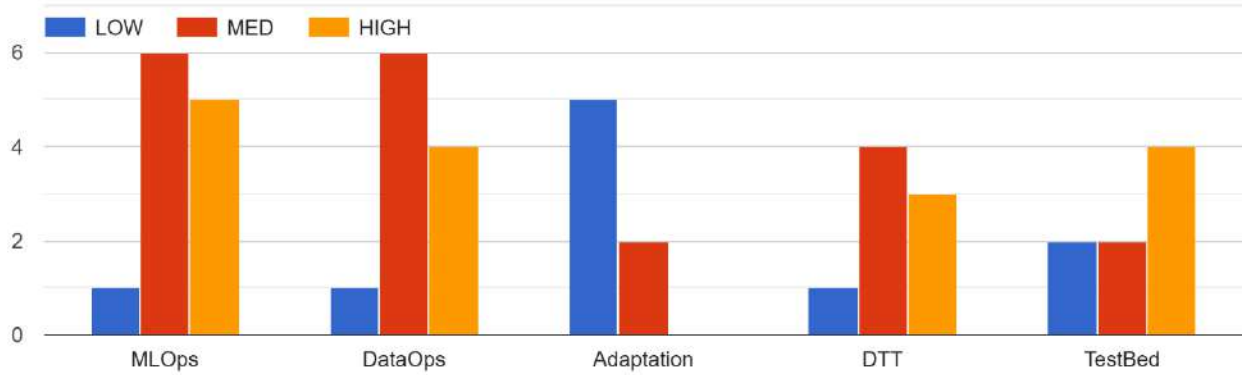


Figure 19. Answers for EL-RSK-14

Comments

Here you can provide comments for your answers

Table 32. Analysis of the answers for risks

RISKS	Description	H	M	L	Total	Score
EL-RSK-09	Validation mismatch	12	4	1	73	4.3
EL-RSK-10	Lack of robustness	7	8	2	61	3.6
EL-RSK-04	Explainability failure	7	8	2	61	3.6
EL-RSK-06	Lack of metadata	8	5	4	59	3.5
EL-RSK-01	Silent policy change	7	5	4	54	3.4
EL-RSK-07	Bias amplification	7	4	4	51	3.4
EL-RSK-08	Misapplied transfer	6	6	4	52	3.3
EL-RSK-12	API Security	9	1	7	55	3.2
EL-RSK-14	Environmental sustainability	4	10	3	53	3.1
EL-RSK-03	Loss of governance in model drift	5	7	5	51	3.0
EL-RSK-13	Unfair processing of personal data	7	2	8	49	2.9
EL-RSK-05	Bias/Intent Mismatch	5	3	6	40	2.9
EL-RSK-11	Data Leakage	6	1	10	43	2.5
EL-RSK-02	Policy bypass through autonomous model behaviour	4	4	8	40	2.5

Annex II: A template for System Information

ISO/IEC FDIS 42005[36] provides practical guidelines and illustrative examples to describe the fundamental characteristics of an AI system. These examples are suitable candidate proposals for implementing relevant data structures of the evidence artefacts, defined for documenting and assessing the 6G-DALI framework. These examples refer to tables in Annex and sections of the standard.

Table E.1 — General AI system information

AI system name or identification	Information to identify the AI system under assessment
Other AI system identifiers	Alternative means to identify the AI system under assessment
AI system life cycle stage	Information of the life cycle state at which the AI system impact assessment is to be conducted

Table E.2 — Revision history

Author	Name of the person or team responsible for the AI system impact assessment
Date last modified	Last modification date of the AI system impact assessment (more rows can be added as appropriate)

Table E.3 — Review and approval

Reviewed by	Name of the person or team responsible for a review of the AI system impact assessment
Date of review	Review date
Approved by	Name of the person or team responsible for a approval of the AI system impact assessment
Date of approval	Approval date

Table E.5 — Description of AI system functionalities and capabilities

	AI system functionality or capability	**In current version?**	**Planned or scheduled?**
1	Description of the functionality or capability as described in 6.3.2	Yes or No	In a planned version? Estimated version and date
2	Description of the functionality or capability as described in 6.3.2	Yes or No	In a planned version? Estimated version and date
3	...	...	...

Table E.7 — Description of the purpose of the AI system

Information on the purpose of the AI system as described in 6.3.3

Table E.8 — Description of intended uses of the AI system

	Intended use name	**Intended use description. Include information about the intended end user of the AI system, where and when the AI system can be used.**
1	Identification of the intended use	Description of the intended use of the AI system as described in 6.3.4
2	Identification of the intended use	Description of the intended use of the AI system as described in 6.3.4
3	...	...

Table E.9 — Description of unintended uses of the AI system

	Unintended use name	Unintended use description. Include whether this unintended use is a reasonably foreseeable misuse of the AI system.
1	Identification of the unintended use	Description of the unintended use of the AI system as described in 6.3.5
2	Identification of the unintended use	Description of the unintended use of the AI system as described in 6.3.5
3	...	..

Table E.10 — Data information

Dataset name, version, size	Identification of the dataset and additional information as needed
Dataset owner	Owner of the dataset, where applicable
Dataset access rights	Information related to access control
Description of the contents of the dataset	Can include information on the data's temporal scope and whether the datasets are real, synthetic and semi-synthetic, geographies covered by the dataset, etc.
Intended and unintended purposes of this dataset, including if it is approved to be used for AI systems	As indicated
Details about data collection, where from, by whom, etc.	Information on data provenance
Known or reasonably foreseeable risks of unwanted bias in the dataset and geographies covered.	As indicated
Processes applied to the dataset for quality purposes	Description of data quality processes as applied to the data set
Is a data protection impact assessment necessary?	Yes or No, depending on the presence of PII in the data set

Annex III: Linked system requirements from D2.2

This section provides the list of linked system requirements (both functional and non-functional) from D2.2[9] for the benefit of the reader.

Requirement ID	Requirement Title
AI-as-a-Service (AIaaS) and Hyperparameter Optimization (HPO) for RLOps	
FR-AR-2	6G-DALI shall provide monitoring and observability of ML task status and performance through dashboards.
FR-AR-4	6G-DALI shall offer unified support for searching, serving, optimizing, finetuning, and testing ML models.
FR-AR-6	6G-DALI shall support continuous model testing and validation across the 6G stack, adapting to latency and resource constraints.
Data Augmentation	
FR-DA-2	Data augmentation shall ensure that augmentations hold valuable information and do not merely add noise to the data.
NFR-DA-5	Data augmentation shall provide comprehensive documentation of implemented data augmentation techniques.
DataOps	
FR-DATAOPS-8	DataOps shall include logging capabilities for data access.
NFR-DATAOPS-2	DataOps shall align experiments' results with users' objectives and priorities.
NFR-DATAOPS-4	DataOps pipelines shall satisfy users from intent-based data requests up to 90%.
NFR-DATAOPS-6	DataOps shall execute DataOps workflows reliably and provide meaningful error messages in case of failure.
Data Spaces, Data Lake & Data connectors	
FR-DS 4	The system shall include rich metadata annotation for all data sets, ML models and services in the Data Space
FR-DS 7	The system shall ensure metadata for all available datasets is registered and searchable in the Data Space Catalogue
FR-DS 8	The system shall authenticate clients before granting access to the Data Space and Data Lake
FR-DS 9	The system shall verify that clients have necessary permissions to discover and retrieve data sets
FR-DS 10	The system shall enforce identity, trust, and security policies based on predefined user roles and data set classifications
FR-DS 12	The system shall require explicit acceptance of presented policies before allowing data set retrieval

FR-DS 14	The system shall include Gaia-X compliant rich metadata annotation for all data sets
FR-DS 15	The system shall include backend components to support metadata matching and access decisioning
NFR-DS 3	The system shall comply with applicable data protection, trust, and security regulations (e.g., GDPR, Gaia-X policies)
NFR-DS 4	The system shall use backup mechanisms and disaster recovery plans to maintain data integrity and availability in case of system failures
NFR-DS 6	The system shall use strong authentication and authorization mechanisms (e.g., multi-factor authentication, OAuth)
NFR-DS 7	The system shall use audit logs and activity tracking for monitoring user actions and ensuring data security
NFR-DS 15	The system shall provide comprehensive logging and monitoring capabilities to track its health, performance, and data transfer activities
Digital Twin & Reinforcement Learning (RL)	
FR-DT-1	6G-DALI shall define a Northbound API accessible via the enablers to configure and manage experiments, generate datasets, and deploy ML models and RL agents for MLOps and RLOps processes
FR-DT-2	6G-DALI shall define a consistent data model that the Digital Twin will adhere to and ensure compliance with the requisite Data Spaces and Catalogues.
NFR-DT-1	6G-DALI shall provide extensive documentation on usage of the Digital Twin aspects of the 6G-DALI project
Experiment as a Service and HPO	
NFR-EH-1	The system shall inform users about the status and outcome of the optimization job, including access to outputs or logs.
NFR-EH-3	The system shall aim to optimize the amount of computing resources used for the experiments.
Data Transformation	
FR-ELT-4	ELT pipelines shall allow experimenters to search for available data transformation (e.g., data imputation, outlier detection algorithms, etc.) and augmentation algorithms in the federated catalogue.
FR-ELT-7	ELT pipelines shall include data validation and integrity check mechanisms.
NFR-ELT-3	ELT pipelines shall align experiments results with user objectives and priorities.
Intent-Driven DataOps	
FR-IDD-3	The system shall include a chat interface for iterative interaction until correct ELT formulation is finalized.

FR-IDD-6	The system shall validate user intent using Semantic Role Labeling (SRL) and Knowledge Graph (KG) techniques.
NFR-IDD-4	DataOps shall achieve over 90% user satisfaction with intent-based data requests, validated via user surveys.
MLOps	
FR-MLOPS-3	The system shall allow secure and policy-driven access to models and orchestration resources.
FR-MLOPS-4	The system shall enable reproducibility, observability, and auditability of all ML operations.
NFR-MLOPS-1	The MLOps system shall enforce access control, ensuring only authenticated and authorized users can access models, functionalities, and execution environments.
NFR-MLOPS-4	In case of failures, the system shall notify users and offer diagnostic information.
MLOps Orchestration	
FR-MO-7	The system shall allow users to define the model combination policy, such as using equal weights, performance-based weighting, or learned aggregation.
FR-MO-9	The system shall allow users to define the evaluation protocol, including cross-validation, hold-out, or task-specific schemes.
FR-MO-13	The system shall allow users to select a validation strategy, either from the catalogue, user-defined, or auto-selected based on model/task.
FR-MO-15	The system shall allow users to define the result sharing policy, such as keeping results private or sharing only with some testbeds.
FR-MO-16	The system shall allow users to select an attack method and test scenario (black-white-gray box) to test the model's robustness.
FR-MO-17	The system shall allow users to define a robustness metric, which may be selected from a catalogue, custom-defined, or auto-selected.
FR-MO-18	The system shall allow users to configure a defense strategy, choosing a catalogue, including none.
FR-MO-19	The system shall allow users to define the drift metric to be evaluated during drift detection.
FR-MO-20	The system shall allow users to define the validation dataset to be evaluated during drift detection.
FR-MO-21	The system shall allow users to define the detection frequency to be used for drift detection.
FR-MO-22	The system shall allow users to define the trigger policy for re-training upon drift detection.

FR-MO-23	The system shall allow users to define the re-training strategy upon drift detection.
FR-MO-26	The system shall allow users to benchmark available models in the 6G-DALI framework using pipelines for model evaluation and comparison.
FR-MO-27	The system shall include an interface for verticals to define tasks and review results.
FR-MO-28	The system shall allow verticals to express requests for continuous monitoring of machine learning models.
FR-MO-29	The system shall allow verticals to configure model monitoring metrics and thresholds.
FR-MO-30	The system shall include the essential infrastructure for model monitoring and re-training
FR-MO-35	The system shall inform users about the pipeline execution and make the adapted model and evaluation outputs available.
FR-MO-37	The system shall allow providers/ML developers to annotate models with metadata attributes.
FR-MO-39	The system shall allow providers/ML developers to configure the lifecycle rules of their model.
FR-MO-42	The system shall allow experimenters/ML developers to run experiments in the 6G-DALI facility or in the testbed that allows experiment execution.
NFR-MO-1	The system shall ensure that MLOps tasks are reproducible by storing all relevant metadata, parameters, and runtime environment details.
NFR-MO-2	Sharing policies shall be enforced via the underlying access control layer and support fine-grained scoping by user role, project, or organization.
NFR-MO-3	The system shall inform users about the status and outcome of the training job, including access to outputs or logs.
NFR-MO-6	The system shall inform the user of the information about the detected drift and the triggered re-training.
NFR-MO-7	The system shall include a notification/ alerting system.
NFR-MO-8	The system shall include a dashboard so that verticals can review/control the monitoring.
Trustworthy AI	
FR-TAI-1	Trustworthy AI (in terms of Uncertainty Quantification (UQ)) shall be integrated within the MLOps pipeline to provide probabilistic predictions with specific confidence intervals to ensure trust for deployed models.
FR-TAI-3	Trustworthy AI shall provide specific uncertainty metrics (Expected Calibration Error, prediction interval coverage).

FR-TAI-5	Trustworthy AI shall monitor distributions of uncertainty over time (logs) to detect performance degradation or model drift.
FR-TAI-6	Trustworthy AI shall define specific actions based on the level of uncertainty: reject low confidence predictions, request more data for calibration, trigger model retraining.
NFR-TAI-1	Trustworthy AI solutions shall be computationally efficient or optimized through GPU use or batch inference, to not introduce significant latency overhead in the overall pipeline.
NFR-TAI-4	Trustworthy AI shall be interpretable and provide explanations of why the predictions are uncertain or why there is model drift.