EDGE/DM Governance Rulebook

EDGE/DM public documentation

PROPRIETARY & CONFIDENTIAL INFORMATION © Idneo Technologies S.A.U. All Rights Reserved

EDGE/DM

Governed Data Space for Medical-Device Innovation

EDGE/DM Governance & Rulebook Guide

Public Summary of Governance, Rulebook, DUA/DUP and Evidence

A formal public summary of the governance model, Rulebook scope, usage policies, evidence and traceability framework.

Document code	EDGEDM-PUB-GR
Version	v1.0 - Final pilot public edition
Date	9 June 2026
Owner	Idneo Technologies S.A.U.
Audience	Governance, compliance, legal, providers, consumers and executive stakeholders

Publication note: *This document describes the final pilot operating model of EDGE/DM for public website download. It is not an implementation-status report and should not be read as a legal, medical or regulatory approval instrument.*

Table of contents

Governance overview

Document control

Field	Value
Purpose	Summarise the final pilot governance model and Rulebook in a public, participant-readable form.
Audience	Participants, governance bodies, legal/compliance stakeholders, providers, consumers and executives.
Classification	Public downloadable document
Final pilot assumption	The document describes the target/final EDGE/DM pilot operating model and deliberately omits implementation-progress indicators.
Clinical boundary	EDGE/DM documentation must not be interpreted as clinical decision support, medical diagnosis or regulatory clearance.

This document summarises the governance and Rulebook framework that makes EDGE/DM a trusted data space rather than a collection of informal bilateral data-sharing arrangements.

Governance principles

- Data sovereignty: providers retain control over the Data Products they publish and define conditions of use within the common framework.
- Verified trust: participants operate under approved roles and identity conditions.
- Purpose limitation: access and use are limited to authorised purposes.
- Controlled access pathway: access is mediated through approved components and policies.
- Evidence by design: publication, access and relevant events can be traced and reviewed.
- Interoperability: metadata, policies and evidence use common profiles and versioned concepts.
- Controlled evolution: changes to rules and policies are governed.

Governance functions and responsibilities

Governance functions

Function	Responsibility
Governance authority	Maintains governance model, reviews participation and handles escalation.
Rulebook owner	Controls updates to operational rules and public summaries.
Data Product steward	Maintains metadata, evidence and policy alignment for each product.
Technical operator	Operates catalogue, connectors, policy interfaces and evidence infrastructure.
Audit/review function	Reviews traceability, decisions, incidents and compliance evidence.

Rulebook scope

The Rulebook defines operational rules for participation, Data Product publication, access, usage, policy compliance, AI governance, traceability, security and incident handling.

Rulebook scope

Area	Rulebook function
Participation	Admission, role approval, permanence and offboarding.
Data Products	Publication, classification, policy linkage and evidence requirements.
Access and use	Allowed purposes, prohibited purposes, actions, obligations and restrictions.
DUA/DUP	Product-specific usage conditions.
AI governance	Model cards, inference records, limitations and

	traceability.
Incidents	Misuse, breach handling, corrective actions and revocation.

DUA/DUP usage-policy framework

Data Usage Agreements / Data Usage Policies attach permitted purposes, prohibited purposes, obligations and constraints to each Data Product.

DUA/DUP contents

Field	Explanation
Target Data Product	The asset, service or capability governed by the policy.
Allowed purposes	The purposes for which access may be requested.
Prohibited purposes	Purposes that must be denied.
Allowed actions	Actions compatible with a purpose.
Obligations	Duties such as logging, traceability, no redistribution or no re-identification.
Constraints	Conditions such as geography, identity, role and organisation authorisation.

Governed lifecycle

The governance lifecycle gives participants predictability and enables review.

1. Participant onboarding and role approval.
2. Data Product preparation and policy definition.
3. Evidence attachment and governance review.
4. Catalogue publication for public discovery.
5. Access request preparation by consumer.
6. Policy evaluation and AccessDecision.
7. Usage monitoring, evidence and audit.
8. Incident handling, revocation or offboarding where needed.

Prohibited use boundaries

The final pilot public framework excludes uses that would undermine trust, safety or the intended scope.

- Real clinical diagnosis.
- Autonomous medical decision-making.
- Clinical decision support outside an approved future framework.
- Unauthorised redistribution.
- Re-identification attempts.
- Model weight extraction or dataset download when the Data Product is offered as a controlled service.
- Processing outside applicable geography or policy scope.

Evidence and traceability

Evidence categories

Evidence	Role
Anonymisation evidence	Supports safe treatment of Class1 or sensitive datasets.
Minimisation evidence	Shows that only necessary data or outputs are used.
Model Card	Documents model purpose, limitations, inputs, outputs and risk boundaries.
InferenceRecord	Records controlled inference use for traceability.
AccessDecision	Records GRANT/DENY outcome and reasons.
Audit log	Supports review, incident investigation and accountability.

Economic and value-governance principles

The governance model allows economic conditions and value-creation models to be defined without treating sensitive data as an uncontrolled commodity.

- Commercial terms are linked to participation, Data Product terms and applicable agreements.
- Providers may define controlled access, licensing, service, benchmarking or validation models.

- Consumers receive clarity about permitted use, obligations and constraints.
- Any monetisation pathway must remain compatible with governance, law, data protection and the Rulebook.