EDGE/DM Technical Guide

EDGE/DM public documentation

EDGE/DM

Governed Data Space for Medical-Device Innovation

EDGE/DM Technical Guide

Data Products, Policies, Connectors and Trusted Access

A high-level technical guide to the final pilot architecture, semantic model, policy layer, access decisions, connectors and evidence records.

Document code	EDGEDM-PUB-TG
Version	v1.0 - Final pilot public edition
Date	9 June 2026
Owner	Idneo Technologies S.A.U.
Audience	Technical integrators, data-space architects, platform teams and governance engineers

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

Overview

Document control

Field	Value
Purpose	Provide a high-level technical guide for EDGE/DM final pilot participants and technical reviewers.
Audience	Technical integrators, data-space architects, platform teams, governance engineers and advanced participants.
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 technical guide explains the final pilot architecture of EDGE/DM at a high level. It is intended to help participants understand how Data Products, policies, ontology, connectors, access requests, access decisions and evidence fit together.

Reference architecture

Reference architecture layers

Layer	Purpose
Public access point	Website, catalogue, participant information and documentation downloads.
Participant layer	Provider, consumer, governance and technical operator workspaces.
Catalogue and metadata	Data Product discovery, semantic metadata and

	DataHub/catalogue mapping.
Policy layer	DUA/DUP, ODRL-lite, policy bundle and decision logic.
Connector layer	Provider/consumer integration and controlled access mediation.
Evidence layer	Logs, access decisions, inference records, validation evidence and audit records.
Governance layer	Rulebook, participation agreement, review workflows and incident handling.

Semantic foundation and ontology

The semantic foundation provides a common language for participants, Data Products, policies, purposes, evidence and access decisions. It supports interoperability across catalogue, governance and technical enforcement components.

Ontology concepts

Concept	Meaning
Participant	An organisation or actor approved to operate in the data space.
Role	Provider, consumer, governance authority, technical operator or model provider.
Data Product	A governed asset prepared for discovery, request and controlled reuse.
Purpose	The declared and permitted reason for requesting or using a Data Product.
Policy	Permission, prohibition, obligation or constraint linked to a Data Product.
Evidence	Documents or records supporting publication, validation, traceability or audit.

AccessDecision	A traceable outcome of a policy evaluation for a request.

Data Product specification

Each Data Product is described by a specification containing mandatory metadata, usage conditions, policy references, evidence and lifecycle information.

- Stable identifier, title, description and provider.
- Data Product type and stakeholder summary.
- Sensitivity and risk classification.
- Allowed purposes and prohibited purposes.
- Allowed purpose-action use cases.
- DUA/DUP policy link and evidence references.
- Catalogue access, connector interface and technical profile where applicable.
- Version and lifecycle status.

Policy model: DUA/DUP, ODRL-lite and bundle

DUA/DUP policies define product-specific usage conditions. ODRL-lite provides a semantic representation of those policies; the policy bundle provides a deterministic projection for access-decision logic.

Policy mapping

Human concept	Machine-readable counterpart
Allowed purpose	Permission / allowed use case.
Prohibited purpose	Prohibition.
Obligation	Duty returned or enforced with the access decision.
Constraint	Condition evaluated against requester, purpose, action or geography.
Data Product target	Policy target identifier and catalogue ID.
Evidence requirement	Evidence references linked to Data Product or access decision.

AccessRequest and AccessDecision

The access-decision flow converts a request into a traceable outcome. The final pilot model is designed for policy-consistent GRANT/DENY decisions with reasons and obligations.

1. Requester selects a Data Product.
2. Requester declares role, organisation, purpose, action and geography.
3. Requester accepts applicable DUA/DUP terms.
4. Policy layer evaluates permissions, prohibitions, obligations and constraints.
5. AccessDecision records result, matched policy, obligations and reasons.
6. Evidence and logs support review and audit.

Connector and controlled access layer

The connector layer mediates provider/consumer interactions. It is the controlled pathway for operational use, replacing parallel or informal access routes.

Connector responsibilities

Responsibility	Description
Identity and context	Carry requester, organisation and role context.
Policy interaction	Route requests through policy decision points.
Data/service mediation	Expose approved Data Products, services or endpoints under governance.
Logging	Support traceability of requests and decisions.
Obligations	Communicate or enforce usage obligations where applicable.

AI services and federated collaboration

AI Agents and federated tasks can be represented as Data Products when their purpose, inputs, outputs, limitations, policy conditions and evidence are defined.

AI technical patterns

Pattern	Technical meaning
AI Agent	A governed automated capability operating

	within defined task and policy boundaries.
Inference service	A controlled model interface with output logging and no model-weight exposure.
Federated learning	Local training/evaluation with controlled exchange of updates or results.
Federated distillation	Sharing derived knowledge outputs rather than raw datasets.
Traceability agent	Assisted evidence retrieval, explanation or audit support.

Security, privacy and responsible-use controls

- No direct public download of sensitive Data Products.
- EU/EEA processing and operational scope where required by policy.
- Requester identity and organisation context are required for governed access.
- Clinical decision-making purposes are excluded from default pilot use.
- Model weights and underlying datasets are protected when service access is offered.
- Access, inference and policy decisions are traceable.