Guide technique EDGE/DM

EDGE/DM public documentation

EDGE/DM | Medical-Device Data Space

Guide technique EDGE/DM

Data Products, politiques, ontologie et accès de confiance

Document public EDGE/DM pour téléchargement web · État final du pilote

Code documentaire	EDGEDM-PUB-TG-FR
Version	v1.0
Date	2026-06-09
Périmètre	Modèle opérationnel final du pilote
Audience	Intégrateurs techniques, data spaces, gouvernance technique, équipes plateforme

Note de publication : ce document décrit le modèle opérationnel final du pilote EDGE/DM pour téléchargement public depuis le site web. Il ne remplace pas les accords contractuels spécifiques, les évaluations réglementaires ni les revues juridiques applicables à des participants concrets.

Table des matières

Contrôle documentaire

Champ	Valeur
Responsable	Idneo Technologies S.A.U. / EDGE/DM
Statut	Version publique formelle
Confidentialité	Document public pour parties prenantes
Usage prévu	Information, onboarding, participation et revue technique de haut niveau

Vue d’ensemble

Ce guide décrit l’architecture finale du pilote EDGE/DM à haut niveau pour les participants techniques, intégrateurs et réviseurs de gouvernance.

Architecture de référence

Couches

Couche	Fonction
Portail public	Découverte, documentation, participation et catalogue.
Catalogue et métadonnées	Description des Data Products et conditions.
Sémantique	Ontologie, profils et alignement.
Politiques	DUA/DUP, ODRL-lite, bundle et enforcement.
Connecteurs	Canal contrôlé fournisseur-consommateur.
Preuves	Enregistrements de publication, demande, décision et usage.

Fondation sémantique et ontologie

L’ontologie fournit un langage commun pour participants, rôles, Data Products, politiques, finalités, preuves et décisions d’accès.

- Participant, fournisseur, consommateur, opérateur technique et autorité de gouvernance.
- DataProduct, Dataset, InferenceService, ComplianceService et AIModel.
- Permission, Prohibition, Obligation et Constraint.
- Evidence, AnonymisationEvidence, ModelCard et InferenceRecord.

Spécification de Data Product

Chaque Data Product comprend métadonnées obligatoires, politique applicable, preuves, sensibilité, risque fonctionnel et cycle de vie.

Champs

Champ	Description

identifier/title/provider	Identité, titre et organisation responsable.
type	Dataset, service d’inférence, agent IA, tâche fédérée ou traçabilité.
allowed purposes	Finalités permises.
prohibited purposes	Usages exclus.
evidence	Documentation et preuves de soutien.

Modèle de politiques : DUA/DUP, ODRL-lite et bundle

DUA/DUP exprime les conditions d’usage dans un langage compréhensible. ODRL-lite permet une représentation lisible par machine. Le bundle opérationnel alimente l’évaluation des politiques.

AccessRequest et AccessDecision

AccessRequest décrit le demandeur, l’organisation, la finalité, l’action, la géographie et l’acceptation des termes. AccessDecision renvoie résultat, raisons, obligations et preuves liées.

Flux

Entrée	Sortie
demandeur, organisation, finalité, action, géographie, acceptation DUA/DUP	GRANT/DENY, motif, politique appliquée, obligations, trace

Connecteurs et accès contrôlé

Les connecteurs constituent le canal contrôlé pour les interactions fournisseur-consommateur. Ils évitent les routes parallèles et permettent identité, politiques et preuves.

Services IA et collaboration fédérée

Les services IA sont des capacités gouvernées. Un agent IA ou service d’inférence peut être un Data Product si la tâche, les limites, les entrées/sorties, les journaux et obligations sont définis.

Sécurité, confidentialité et usage responsable

- Limitation de finalité.
- Périmètre UE/EEE si applicable.
- Pas de redistribution.
- Pas de ré-identification.
- Pas d’extraction non autorisée de poids ou données.
- Traçabilité et audit des décisions.