DATA MATURITY ASSESSMENT	NIVEAU GARTNER	FORCE	FAIBLESSE	PLAN D'ACTION
Data Governance	2 Reactive	Reconnaissance de l'importance de la gouvernance ; présence d'un DPO et CDO ; volonté managériale d'amélioration : conscience des enjeux et volonté d'agir.	Absence de framework formel unifié ; pas de politique documentée ; rôles et responsabilités flous ; absence de Data Stewards identifiés ; pas de comité de gouvernance ; processus décisionnels ad-hoc. Les départements gèrent leurs données de façon indépendante, créant des silos et un manque de responsabilité partagée	Établir une politique de gouvernance formelle ; créer un **Data Governance Committee** ; définir et documenter rôles/responsabilités (Chief Data Officer) ; nommer des Data Stewards par domaine ; implémenter un cadre décisionnel structuré
Data Quality	3 Proactive	Utilise activement les données pour améliorer les recommandations. Conscience de l'importance qualité pour les recommandations et les analyses. Culture de l'amélioration	Processus non standardisés et ad-hoc ; incohérences cross-départements ; métadonnées potentiellement obsolètes et erreurs (métadonnées et préférences utilisateurs) : pas de Data Quality metrics formels, absence de data profiling systématique, impact direct sur l'expérience utilisateur	Implémenter un **Data Quality Framework** (profiling, cleansing, monitoring) ; définir des **DQ KPIs mesurables** ; automatiser les contrôles qualité ; établir des data quality rules par domaine ; prioriser les datasets critiques (user data, content metadata)
Data Architecture	3 Proactive	Infrastructure technique sophistiquée (data lakes, cloud, bases relationnelles) ; capacités temps réel ; scalabilité démontrée ; architecture moderne	Silos architecturaux entre départements ; fragmentation des sources ; manque d'intégration globale ; absence d'architecture de référence documentée ; pas de data catalog centralisé	Définir une **architecture de référence enterprise** ; implémenter un data catalog ; standardiser les patterns d'intégration ; documenter les flux de données ; créer une cartographie des systèmes sources
Compliance (GDPR, CCPA, PCI-DSS)	2 Reactive	DPO en place ; conscience des obligations réglementaires ; présence d'une équipe Legal	Risques de non-conformité majeurs sur 180+ juridictions ; processus de consentement non standardisés ; mécanismes DSAR (Data Subject Access Requests) immatures ; documentation des traitements insuffisante ; exposition à amendes RGPD (20M€ ou 4% CA) ; délais breach (72h) non garantis	**Audit de conformité immédiat RGPD/CCPA** ; standardiser les processus de consentement ; implémenter un système DSAR automatisé ; documenter le registre des traitements ; formation compliance ; mettre en place des privacy impact assessments (PIA). S'orienter vers un **Privacy By Design**
Data Usage & Accessibility	3 Proactive	Usage extrêmement proactif et sophistiqué des données pour améliorer produits/services, culture data-driven ancrée, exploitation ML/IA avancée ; appétit pour l'exploitation data	Silos départementaux bloquant l'accès ; données fragmentées et difficiles d'accès ; absence de self-service BI ; pas de data catalog ; inefficacité opérationnelle ; duplication des demandes ; délais d'accès aux données pénalisants	Implémenter une plateforme de **data catalog** ; développer des capacités **self-service BI** ; définir une politique d'accès aux données ; créer des data products réutilisables ; briser les silos par des data domains transverses
Data Security	3 Proactive	Mesures de sécurité existantes ; infrastructure cloud sécurisée ; sensibilisation aux risques	Standards de sécurité non uniformes ; absence de politique centralisée ; classification des données non formalisée ; contrôles d'accès hétérogènes ; risques de breach non quantifiés ; pas de data loss prevention (DLP) systématique	Définir une politique de **sécurité data unifiée** ; implémenter une classification des données (public, internal, confidential, restricted) ; standardiser les contrôles d'accès (RBAC) ; déployer des solutions DLP ; conduire des audits de sécurité réguliers. s'orienter vers **Zero Trus Model**
DATA LITERACY	3 Proactive	Culture data-driven forte ; équipes techniques compétentes ; appétence pour les données ; capacités analytiques avancées	Compréhension limitée des principes de gouvernance ; formation compliance insuffisante ; awareness privacy variable ; pas de programme de formation structuré ; compétences data governance faibles au-delà de la tech	Créer un programme de **Data Literacy structuré** ; former aux principes de gouvernance et compliance ; sensibiliser à la privacy by design ; certifier les Data Stewards ; communication régulière sur les enjeux data
Data Integration	2 Reactive	Reconnaissance du problème ; volonté d'améliorer les synergies ; capacités techniques d'intégration	Fragmentation majeure cross-départements ; vue parcellaire du user journey (discovery → conversion) ; duplication des efforts ETL ; absence de stratégie d'intégration formelle ; pas de MDM (Master Data Management) ; données non réconciliées	Définir une **stratégie d'intégration enterprise** ; implémenter un MDM pour entités critiques (users, content) ; standardiser les processus ETL/ELT ; créer une golden record strategy ; **développer des API data standardisées**
Analytics & BI	3 Proactive	Capacités ML/IA avancées ; moteur de recommandation world-class ; exploitation analytique forte ; mesure de performance établie ; culture data-driven	Analyses limitées par les silos de données ; manque de vue 360° utilisateur ; potentiel analytique non pleinement exploité ; insights fragmentés ; collaboration analytique entravée	Créer des **data products intégrés pour vue 360°** ; développer des analytics cross-fonctionnels ; **implémenter une gouvernance des modèles ML** ; standardiser les metrics business ; favoriser le partage d'insights. Pourquoi **AI Governance Framework** (compliance)