

Écosystème global de X-Corp

Architecture des flux de données et responsabilités



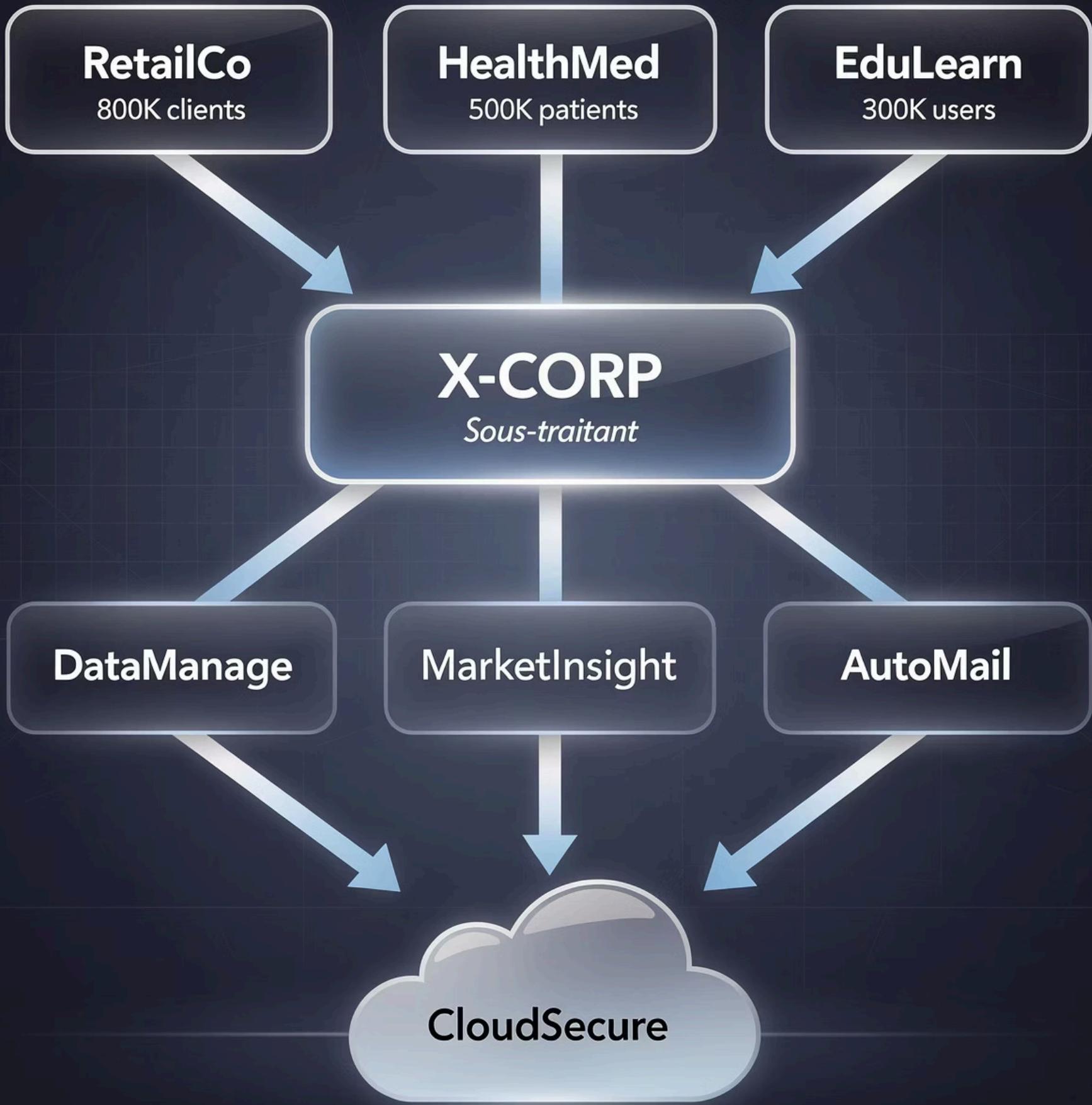
Données traitées

- Marketing comportemental et profilage
- Données de santé (art. 9 RGPD)
- Traitement algorithmique automatisé

Volume global

Plus d'1,5 million de personnes concernées
Complexité élevée et enjeux critiques de conformité





Méthodologie structurée

Démarche d'audit RGPD en 5 phases



Jour 1 : Analyse du cadre RGPD



Principes fondamentaux évalués

- Principes de l'article 5 RGPD
- Bases légales (articles 6 et 9)
- Droits des personnes concernées
- Sécurité technique (article 32)
- Accountability et documentation

✓ Sécurité technique
Infrastructure solide et robuste

⚠ Gouvernance
Partiellement formalisée

⚠ Consentement
Traçabilité insuffisante

📊 Volume élevé
50-100 demandes/mois

Jour 2 : Registre des traitements

Cartographie complète – Article 30 RGPD

Traitements à grande échelle

5 traitements principaux identifiés
couvrant 1,5M personnes

Profilage automatisé

Algorithmes marketing comportemental



Données sensibles

Données de santé HealthMed (article 9)

Conservation différenciée

Durées variables : 2 à 10 ans selon finalités

- Point stratégique :** Le registre constitue la preuve documentaire de conformité et facilite la démonstration de l'accountability

Registre des traitements – X-corp

Traitement n°1 — Gestion des clients RetailCo (via DataManage + AutoMail)	
	Description
Données traitées	Gestion de la base clients RetailCo
Finalité	Personnalisation des offres commerciales et amélioration de l'expérience client
Catégories de données	Nom, prénom, adresse email, numéro de téléphone, historique d'achats, préférences produits
Personnes concernées	Clients de RetailCo
Base légale	Consentement (article 6.1.a RGPD)
Durée de conservation	5 ans après le dernier contact
Destinataires / Sous-traitants	X-corp (sous-traitant), CloudSecure (hébergement)
Mesures de sécurité	Chiffrement AES-256, RBAC, authentification à deux facteurs, pseudonymisation
Transferts hors UE	Non
DPIA requise	Oui (profilage marketing à grande échelle)

Registre des traitements – X-corp

Traitement n°2 — Suivi des patients HealthMed (données de santé)	
	Description
Données traitées	Suivi médical et gestion des patients HealthMed
Finalité	Suivi des traitements, rappels de rendez-vous, conseils de santé personnalisés
Catégories de données	Données d'identification, données de santé, prescriptions médicales
Personnes concernées	Patients de HealthMed
Base légale	Consentement explicite (articles 6.1.a et 9.2.a RGPD)
Durée de conservation	10 ans après la fin du traitement médical
Destinataires / Sous-traitants	X-corp, CloudSecure
Mesures de sécurité	Chiffrement fort, pseudonymisation, accès restreint, journalisation
Transferts hors UE	Non
DPIA requise	Obligatoire (traitement de données sensibles à grande échelle)

 Traitement à risque élevé → DPIA obligatoire (ce sera notre focus Jour 3)

Registre des traitements – X-corp

Traitement n°3 — Analyse des usages EduLearn	
	Description
Données traitées	Analyse des parcours d'apprentissage
Finalité	Amélioration des parcours pédagogiques et recommandations de contenus
Catégories de données	Identifiants utilisateurs, emails, parcours d'apprentissage, résultats
Personnes concernées	Utilisateurs de la plateforme EduLearn
Base légale	Consentement (article 6.1.a RGPD)
Durée de conservation	1 ans après la fin d'utilisation
Destinataires / Sous-traitants	X-corp
Mesures de sécurité	Chiffrement, segmentation des accès, pseudonymisation
Transferts hors UE	Non
DPIA requise	Oui (profilage comportemental + analyse algorithmique)

Registre des traitements – X-corp

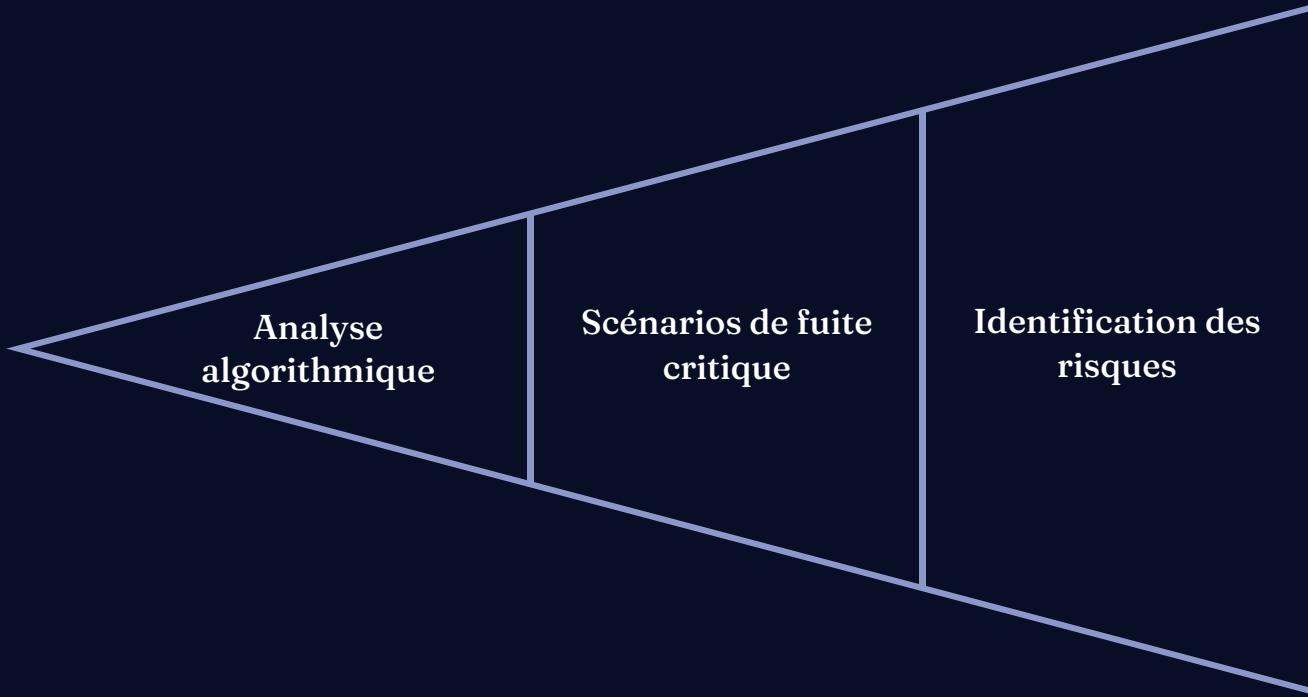
Traitement n°4 — Campagnes marketing automatisées (AutoMail)	
	Description
Données traitées	Envoi de campagnes emailing ciblées
Finalité	Marketing direct et communication commerciale
Catégories de données	Email, comportement utilisateur, préférences
Personnes concernées	Clients finaux
Base légale	Consentement
Durée de conservation	Durée du consentement + 3 ans maximum
Destinataires / Sous-traitants	X-corp, AdBoost
Mesures de sécurité	Gestion des accès, chiffrement, journalisation
Transferts hors UE	À vérifier (risque potentiel avec AdBoost)
DPIA	Recommandée (volume important + problématiques existantes)

Registre des traitements – X-corp

Traitement n°5 — Gestion des demandes d'exercice de droits (DSAR)	
	Description
Responsable	X-corp (pour son périmètre)
Données traitées	Identité du demandeur, données concernées, échanges
Finalité	Traitement des demandes d'accès, rectification, suppression
Catégories de données	Email, comportement utilisateur, préférences
Personnes concernées	Clients finaux des plateformes
Base légale	Obligation légale (art. 15 à 22 RGPD)
Volume	50 à 100 demandes par mois
Durée de conservation	3 ans à compter de la clôture de la demande
Mesures de sécurité	Procédure interne formalisée, traçabilité des réponses
Risques	Retard de traitement / réponse incomplète

Jour 3 : DPIA HealthMed

Analyse d'impact – Données de santé critiques



Périmètre du traitement

- **500 000 patients** concernés
- Données de santé sensibles (art. 9)
- Analyse algorithmique prédictive
- Risque critique en cas de violation

Mesures de protection

- SOC 24/7 opérationnel
- HSM (Hardware Security Module)
- Double validation humaine

Accès non autorisé

CRITIQUE – Chiffrement renforcé requis

Cyberattaque

CRITIQUE – Surveillance continue active

Erreur algorithmique

ELEVE – Validation humaine systématique

Jour 4 : Simulation d'incident

Test de conformité opérationnelle

Scénario simulé

Compte interne compromis

2 000 enregistrements exposés

Violation de confidentialité

Procédure de réponse testée

- Détection et confinement

Identification immédiate de la violation

- Notification CNIL

Délai de 72 heures respecté

- Information des personnes

Communication aux personnes concernées

- Documentation complète

Traçabilité interne assurée



Enseignement clé : Infrastructure technique solide confirmée, mais formalisation des procédures de gestion de crise à renforcer

Jour 5 : Audit final de conformité

Évaluation globale par domaine



Domaine évalué	Niveau
Sécurité technique	✓ Conforme
Gouvernance RGPD	⚠ Partielle
Gestion du consentement	⚠ Partielle
Droits des personnes	⚠ Partielle
Gestion des incidents	⚠ Partielle

85%

Sécurité technique

Infrastructure robuste et protection avancée

60%

Conformité documentaire

Formalisation à compléter

55%

Processus opérationnels

Procédures à standardiser



Plan d'amélioration stratégique

Feuille de route vers la conformité complète

Court terme (0-3 mois)

- Renforcer traçabilité des consentements
 - Formaliser plan de gestion incidents
 - Documenter procédures DPO

Moyen terme (3-12 mois)

- Automatiser gestion droits RGPD
 - Audits de sécurité réguliers
 - Formation continue des équipes

Long terme (12+ mois)

- Privacy by Design intégré produits
 - Revue annuelle conformité
 - Certification ISO 27701 visée

- ❑ **Objectif** : Passer d'une conformité partielle à une excellente opérationnelle en matière de protection des données