Contexte

Etat des lieux

Expliquer la problématique - silo, rgpd, ccpa

Mauvais élèves, amendes, mauvaises réputations

Description

Center of excellence

Montrer les problématiques

Les solutions

—-

## Principes de data gouvernance.

*Use the****Governance Principles Guide****to outline key principles for data stewardship, quality, and security.*

### Gestion des données.

**Responsabiliser** en définissant des rôles clairs pour la gestion des données, comme la mise en place de Data Stewards, de DPO, CDO, afin de garantir le respect des normes organisationnelles et légales.

Mettre en place de la **transparence** vis à vis des utilisateurs sur la collecte, l’utilisation et la protection des données via la **construction d’une charte de confidentialité**.

S’assurer du **respect des différentes réglementations** en vigueur comme la **RGPD** en Europe, le **CCPA** en Californie avec la mise en place d’une vérification régulière de la conformité avec ces règles.

Mise en place d’**amélioration continue** sur la gouvernance des données permettant de suivre les évolution légales et technologiques.

Garantir une utilisation **éthique** des données. Les systèmes d’IA et d’automatisation doivent être compréhensible pour **éviter l’effet boîte noire**. L’utilisateur doit pouvoir **contrôler ses données** (accès, suppression, consentement). De plus pour **minimiser l’empreinte carbone**, il est possible d’utiliser des data centers à faible empreinte carbone.

### 2. Qualité des données

S’appliquer à maintenir des données précises, complètes et cohérentes permettant d’avoir des **données fiables**.

**Minimiser** la collecte et le traitement des données aux seules informations nécessaires pour des objectifs spécifiques, permettant la réduction des risques de sécurité, en montrant un respect pour la vie privée (amélioration réputation et confiance), baisse des coûts nécessaire au stockage et l’amélioration de la qualité des données.

### 2. Sécurité des données

**Protéger les données** afin de sécuriser les informations sensibles (données personnelles, données de paiements) via l’utilisation de firewall, du chiffrement et l’utilisation de protocoles de sécurité avancés comme la PCI-DSS.

Mettre en place du **contrôle d’accès** pour restreindre les données aux seules personnes autorisées.

## Technologies & Outils.

### Data Cataloging Tools.

Objectif : Centraliser et standardiser l’accès aux données pour favoriser une gouvernance efficace et une meilleure collaboration entre les équipes.

Exemple d’application :

* Alation (Documentation et organisation des données)
* Collibra
* Apache Atlas (meta données)

### 2. Data Quality Tools

Objectif : Optimiser la qualité des données utilisées pour la personnalisation des playlists et la publicité ciblée.

* Talend
* Informatica Data Quality

### 3. Compliance Monitoring Tools

Objectif : Assurer la transparence et la protection des données des utilisateurs à l’échelle mondiale.

* OneTrust
* TrustArc

### 4. Data Security Tools

Protéger les données sensibles (paiements, comptes utilisateurs) contre les cyberattaques et par conséquent, renforcer la confiance des utilisateurs en sécurisant leurs données personnelles et bancaires.

* Splunk
* Vormetric

Permettre aux utilisateurs d'accéder, modifier ou supprimer leurs données et de gérer leur consentement.

1. Niveau de maturité
2. Conception du cadre de gouvernance des données.
3. Plan de mise en oeuvre

Mise en conformité RGPD, CCPA et PCI-DSS.

Les avantages à long terme comprennent des flux de données plus fluides, une meilleure prise de décision et une protection plus forte contre les violations de données contre les violations de données.

L’investissement dans la data gouvernance permet :

* Réduction des coûts
* Etre en conformité avec les organismes de régulation
* Améliorer la transparence et la confiance des utilisateurs
* Avoir une infrastructure scalable

Ils visent le center of excellence (CoE)

Phase pilot avec un département (3 à 6 mois)

12 à 18 mois supplémentaire pour tous les départements.

Cout : investissement technique, formation des membres

L’embauche de rôles clés (Data stewards DPOs..)

Il faut un framework adpatable dans le temps

Mise en place de la sécurité (chiffrement, firewall, secure data storage)