# Comment protéger ses données, si on ne sait même pas où elles sont ?

## Le lignage des données : un atout indéniable en matière de protection des données et des renseignements personnels

**Par Marie Dubernais et Cynthia Viau-Mainville, KPMG**

**Congrès annuel AAQ, virtuel, 28 mai 2021**


## Cynthia Viau-Mainville

Conseillère principale
Gouvernance de l’information

KPMG



## Marie Dubernais

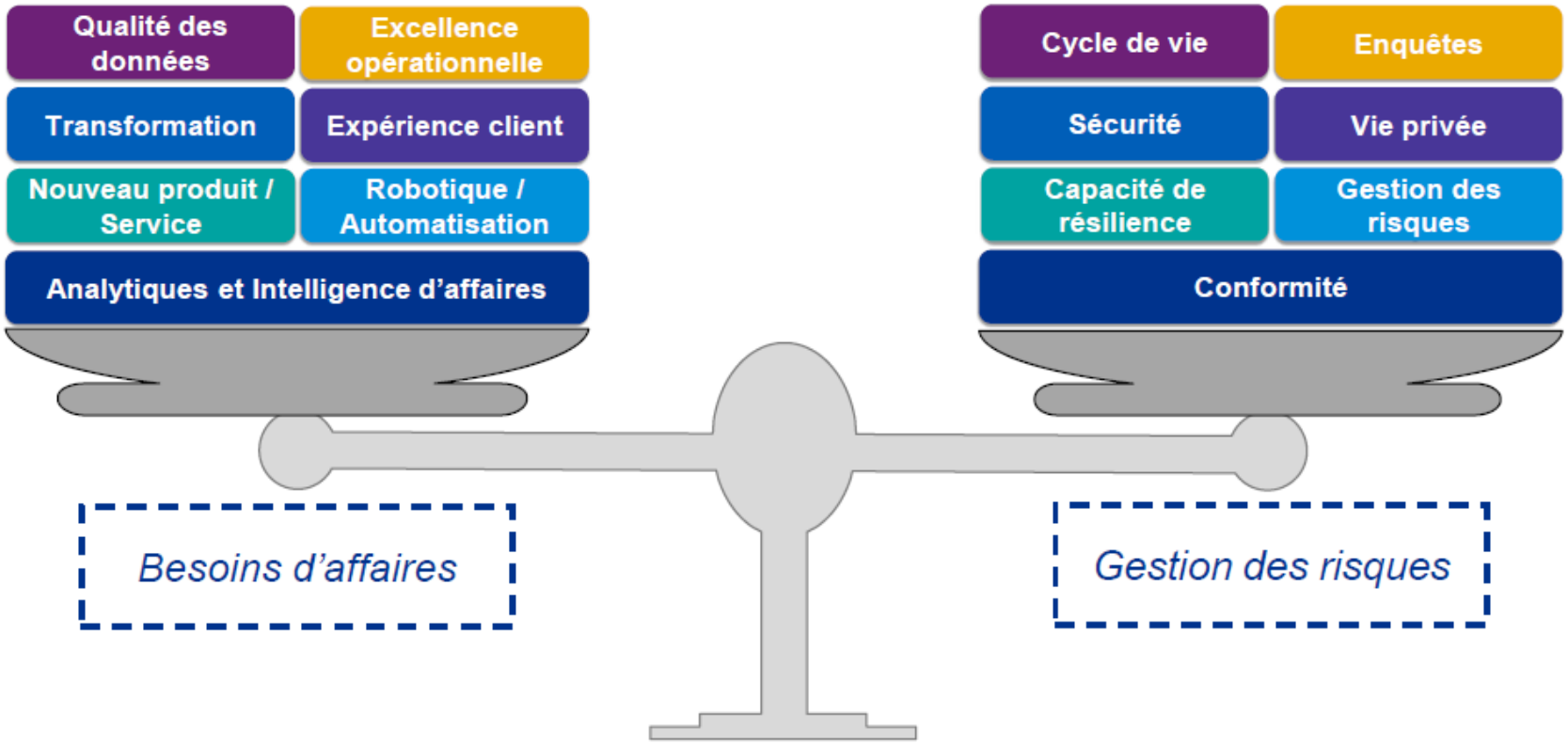
Conseillère principale
Stratégie digitale et
transformation technologique

KPMG

# Agenda

1. Introduction à la protection des renseignements personnels
2. Le lignage de données: un préambule à la protection des renseignements personnels
3. La protection des renseignements personnels est l'affaire de tous

# La densification de la donnée crée un jeu d'équilibre



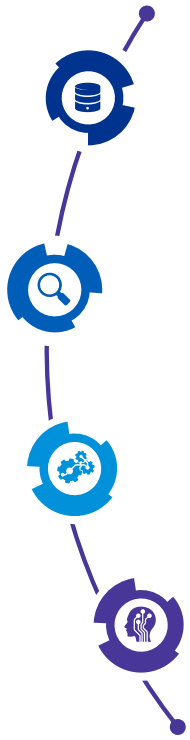
# Les données sont toujours plus présentes mais les différencions-nous?

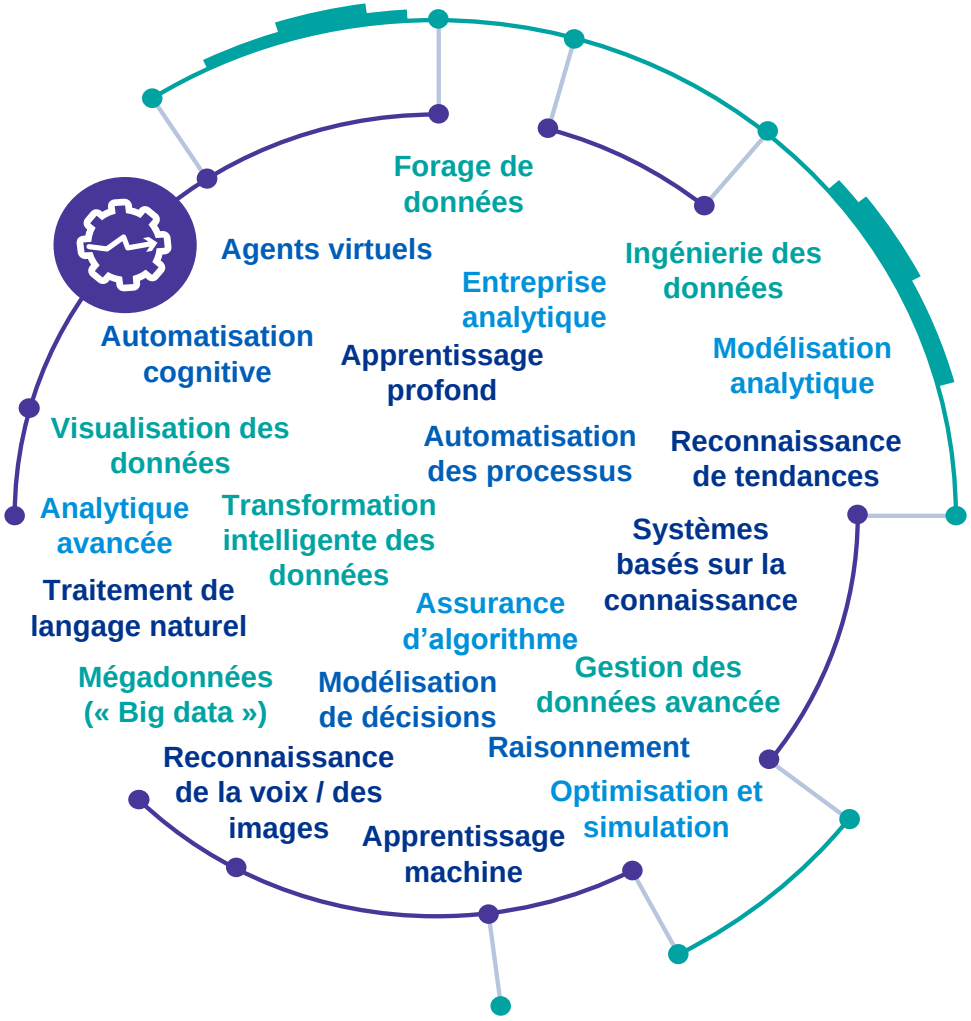
## Données
Un avantage compétitif significatif peut être acquis en valorisant les données internes et externes d'une organisation.

## Analytique
Le développement de solutions fiables supportent les dirigeants d'organisations dans l'acquisition de connaissances clés ainsi que dans leur capacité de prendre des décisions d'affaires éclairées avec confiance.

## Automatisation intelligente
Les organisations peuvent tirer d'importants bénéfices d'une amélioration stratégique de leurs opérations par l'automatisation de processus.

## Intelligence artificielle
L'IA peut paver la voie à l'optimisation, l'accélération, l'automatisation et une meilleure prise de décisions tout en conservant l'intervention humaine dans celles-ci.





# Les données que nous voulons protéger

La classification et la catégorisation de la donnée permettent de mettre en place des solutions adaptées en gestion des accès, en sécurisation de l'information et en protection des renseignements personnels.

**La plupart des informations personnelles sont confidentielles, mais toutes les informations confidentielles ne sont pas personnelles !**

## Renseignements personnels

**Les renseignements personnels sont des informations qui concernent ou sont liés à une personne identifiable.**

Des exemples **de renseignements personnels** inclus:

- Nom, adresse courriel
- Numéro d'assurance sociale
- Information bancaire et financière
- Race, sexe, opinions

Les informations des employés inclus:

- Identifiants gouvernementaux (ex. NAS, passeport)
- Numéros de compte (ex. comptes en banque)
- Informations RH (ex. Informations personnelles de santé, gestion de la performance, salaire)

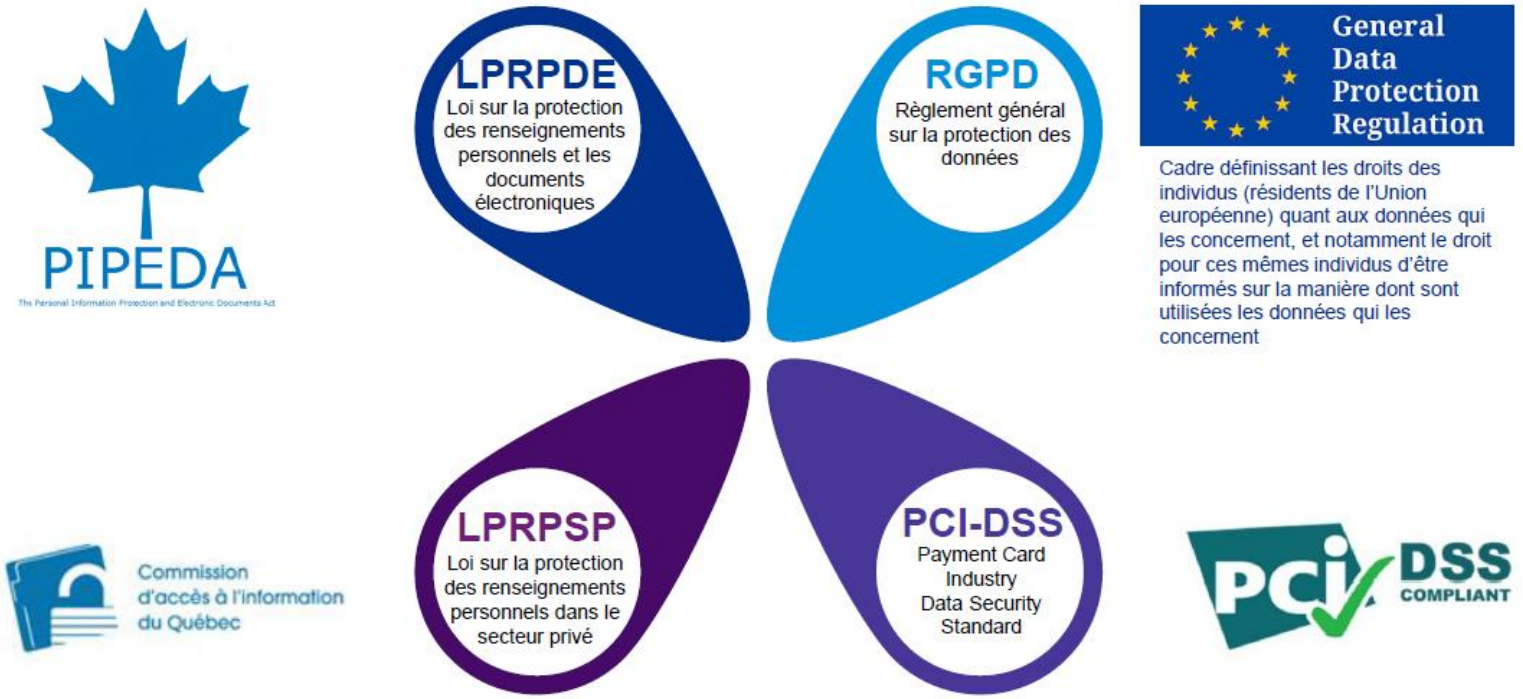
Des nouveaux types d'informations (biométrie, géolocalisation, tendances, informations sous-entendues, etc…

## Informations confidentielles

Contrairement aux renseignements personnels qui sont souvent définis par la loi ou la réglementation, il n'existe pas de définition unique et largement reconnue des informations confidentielles. Dans le cadre de la communication et des transactions commerciales, des informations ou des données sont souvent échangées et l'une ou l'autre partie exige qu'elles soient conservées selon le principe du "besoin de savoir". Ceci est généralement régi par un contrat.

Les informations confidentielles peuvent inclure des informations financières non publiées, des documents stratégiques, des documents juridiques et des plans d'affaires.

# Les cadres légaux en protection de ces données




Les cadres légaux ci-dessus régissent la protection des données dans les entreprises d'ici.

# Les attentes des régulateurs

| | |
|---|---|
| Responsabilité | Avons-nous une personne responsable de la conformité de l'organisation? |
| Détermination des fins de la collecte des renseignements | Pourquoi voulons-nous collecter des renseignements personnels? |
| Consentement | Avons-nous obtenu le consentement des clients et employés pour utiliser à des fins légitimes leurs renseignements? |
| Limitation de la collecte | Avons-nous recueillis des renseignements personnels pour la fin légitime établie? |
| Limitation de l'utilisation, de la communication et de la conservation | Sommes-nous au fait des renseignements personnels dont ont dispose, de l'endroit où ils se trouvent et de ce que l'on en fait? |
| Exactitude | Quelle est la qualité des renseignements personnels que nous détenons? |
| Mesures de sécurité | Avons-nous des mesures de sécurité en place? |
| Transparence | Avons-nous informé les clients et employés de nos politiques et pratiques de gestion des renseignements personnels? |
| Accès aux renseignements personnels | Sommes-nous en capacité de répondre aux demandes d'accès? |
| Possibilité de porter plainte à l'égard du non-respect des principes | Avons-nous en place un recours en élaborant des procédures simples de traitement des plaintes et d'enquête? |

# Les risques liés au défaut de protection des renseignements personnels

## Légaux

En cas de brèche de confidentialité, les organisations assujetties à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) doivent :

- déclarer au commissaire à la protection de la vie privée du Canada les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus;
- aviser les intéressés au sujet de ces atteintes;
- conserver un registre de toutes les atteintes.

## Réputationnels

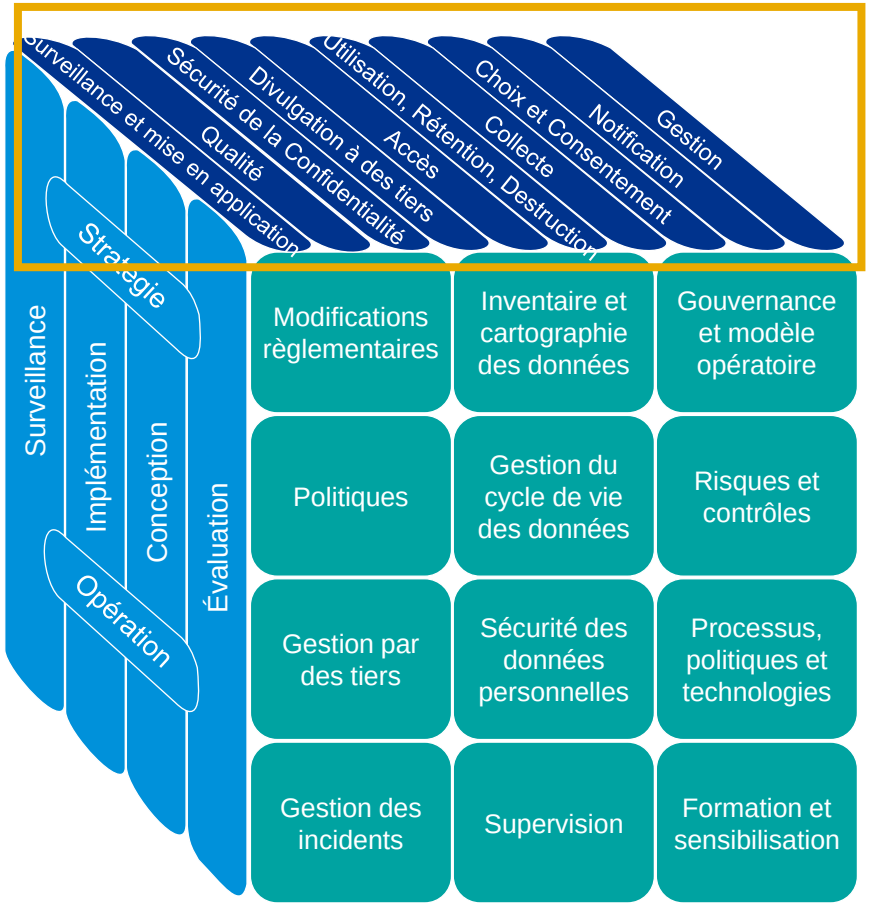
L'image de l'organisation étant victime d'une brèche de confidentialité voit son image de marque fortement dégradée. Une perte de confiance en l'organisation peut en découler.

## Financiers

Une étude portant sur 22 brèches canadiennes a révélé que le coût moyen était de 250 dollars par dossier perdu, pour un coût total moyen de 5,32 millions de dollars.*

**iapp : Combien coûte une fuite de données?*

# Le cadre de protection des renseignements personnels est soutenu par la gouvernance des données




**Cadre global de protection des renseignements personnels de KPMG**

# Le lignage de données: un préambule à la protection des renseignements personnels

# Périmètre des données

## Données structurées

Peuvent être affichées sous forme de rangées, colonnes au sein d'une base de données relationnelle

Données indexées, en colonnes, facilement exploitables par les organisations

Nombres, dates, séries, etc.

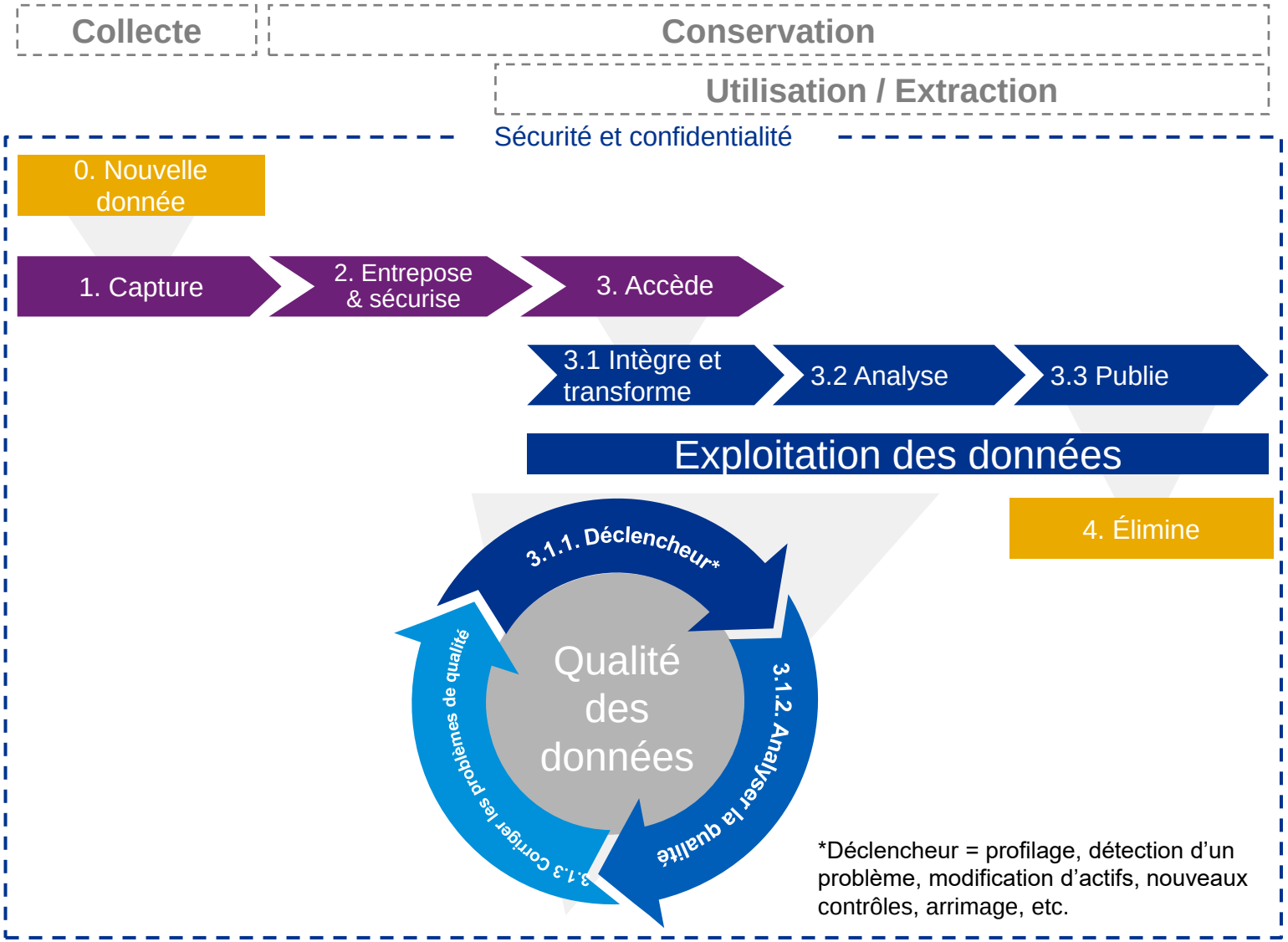
## Données non-structurées

Images, fichiers audio, fichiers texte, documents papier et électroniques, courriels, etc.

Nécessitent d'être bonifiées de métadonnées afin de rendre leur exploitation plus simple

Peuvent être affichées via des applications, des BDD NoSQL, des lacs de données ou des entrepôts de données

# Cycle de vie de la donnée



# Qu'est-ce que le lignage des données ?

**Le lignage des données permet de suivre le flux de données depuis leur origine jusqu'à leur destination finale.**

1 **«Who?»**

Qui collecte, reçoit, utilise les données

2 **«What?»**

Qu'est-ce que qui collecté, conservé, utilisé

3 **«When?»**

Quand est-il collecté, utilisé, transformé, etc.

4 **«Where?»**

Où est-il enregistré, Conservé, stocké

5 **«Why?»**

Pourquoi est-il collecté, conservé, utilisé

# Pourquoi le lignage des données est-il important?

Étant donné que les entreprises sont des structures organisationnelles complexes dans un environnement en constante évolution, il est important qu'elles se concentrent davantage sur le lignage des données pour les raisons suivantes :

### Technologie

Des données propres et concises issues du lignage aident à faire face aux changements de l'environnement technologique concernant la maintenance des données

### Assurance raisonnable


Un lignage complet des données fournit une assurance raisonnable de la qualité des données aux parties prenantes internes et aux régulateurs

### Reddition de compte plus fiable

Un processus complet et cohérent de lignage des données permet de réduire les incohérences et d'améliorer l'efficacité de la transmission des données

### Architecture de données

Une architecture de données efficace optimise le reporting internes et externes sur les risques, ce qui permet aux employés de se concentrer sur d'autres domaines tels que l'analyse des données ou les objectifs stratégiques

### Conformité aux lois et règlements

Une meilleure compréhension des exigences et des directives réglementaires en matière de reporting peut contribuer à la conformité et réduire le risque réputationnel

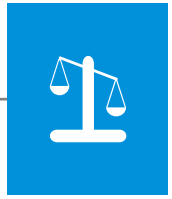
### Perspectives d'affaires

Le lignage des données facilite la génération d'analyses prédictives qui contribuent à la sensibilisation des clients et à l'augmentation de l'offre de produits afin de stimuler la croissance future des revenus

# Quels sont les principaux moteurs du lignage des données ?

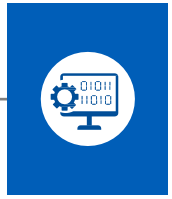
**Parmi les principaux moteurs de l'investissement dans le lignage des données figurent la conformité réglementaire, l'efficacité opérationnelle et l'efficacité commerciale.**

## La conformité réglementaire



- Garantit que les données déclarées sont conformes aux exigences réglementaires en ce qui concerne la compréhension de la provenance des données et de la manière dont elles sont arrivées
- Élimine toute ambiguïté quant à l'origine des données, à la date de leur collecte, aux personnes qui y ont eu accès et aux raisons pour lesquelles elles l'ont été

## L'efficacité opérationnelle



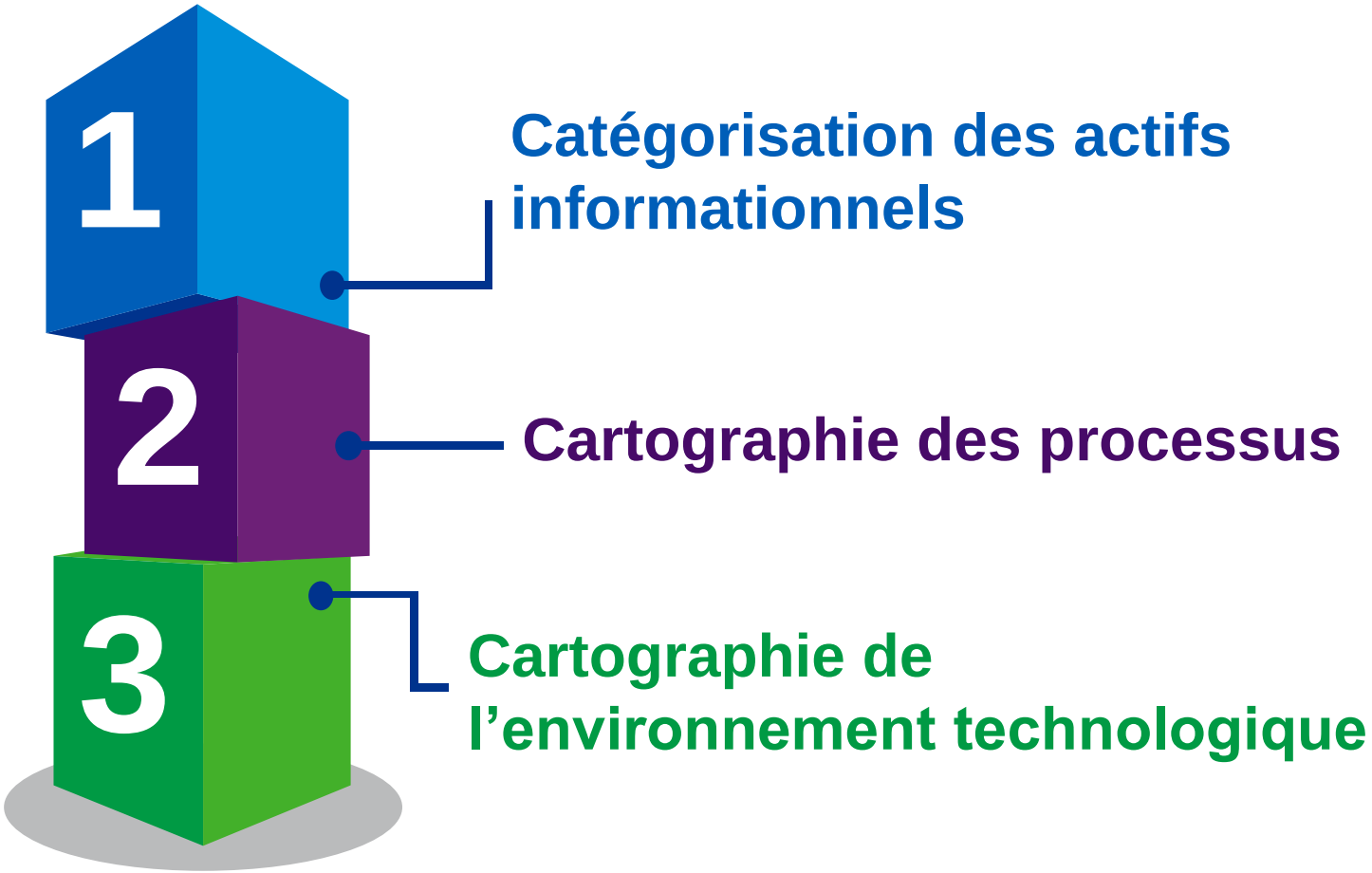
- Le suivi permet de réaliser des économies substantielles sur les activités de remédiation et d'améliorer l'efficacité des entreprises, qui peuvent ainsi se concentrer davantage sur leurs activités commerciales
- Fournit un moyen efficace d'identifier tout problème susceptible de se produire et d'affecter les données au cours de leur voyage de l'origine à la destination finale

## La compétitivité

- Offre de nouvelles possibilités aux entreprises qui suivent leur lignage en leur fournissant des perspectives d'affaires précieuses
- Rassemble toutes les informations qui peuvent être connues sur l'organisation afin qu'elle puisse réagir rapidement et de manière compétitive lorsque de nouvelles opportunités d'affaires se présentent, en traçant les données provenant de plusieurs systèmes TI

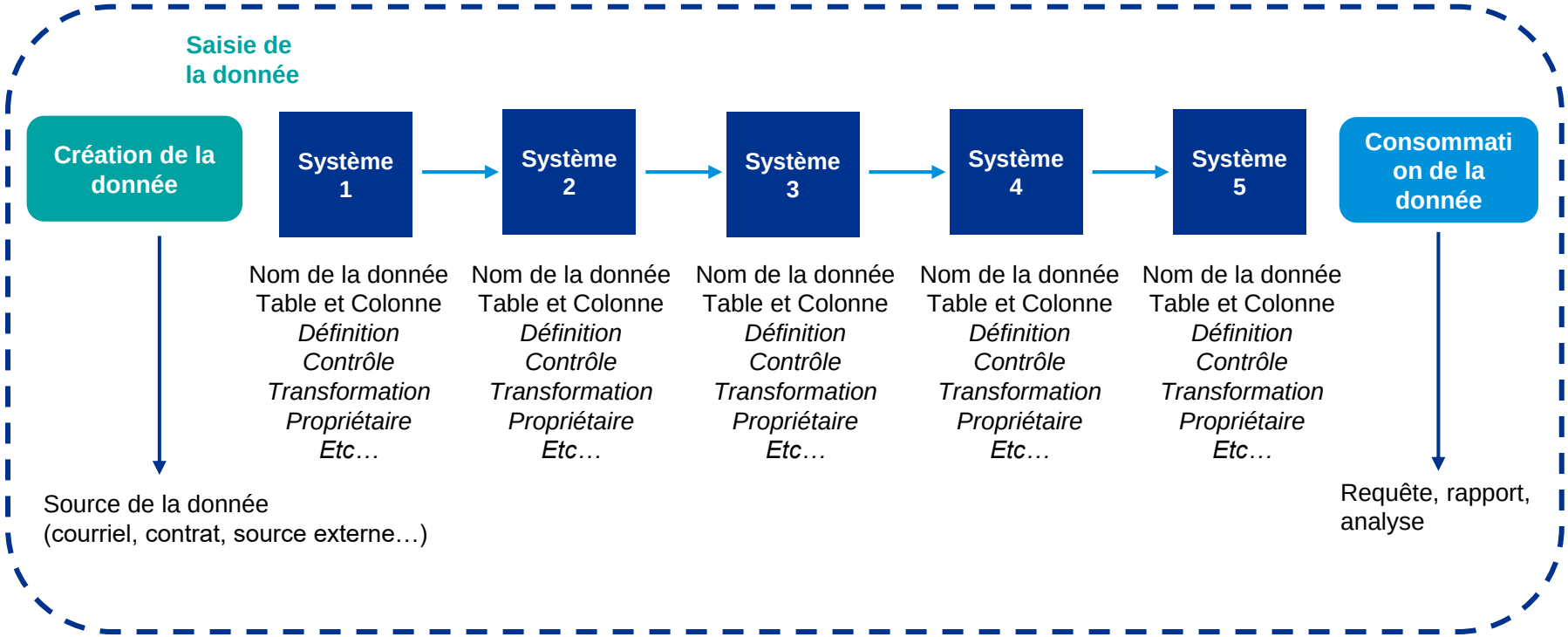
# Cartographie de données

Lors du démarrage d'une initiative de cartographie de données, trois outils peuvent être employés à titre d'intrants essentiels à la cartographie. Ils permettent de connaître le contexte documentaire, d'établir le périmètre de l'initiative et d'identifier les parties prenantes à considérer dans le projet.



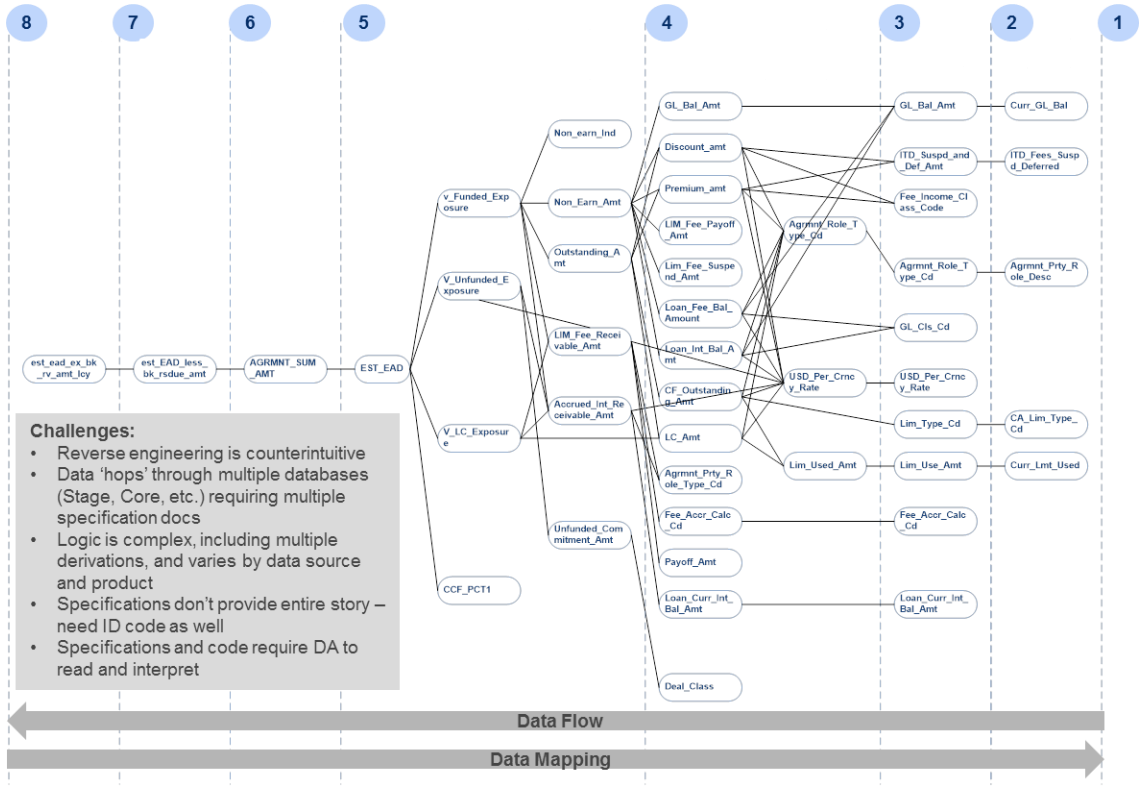
# Cartographie de données

## 1ÈRE FAÇON DE FAIRE : « WHERE »
## À PARTIR DES SYSTÈMES INFORMATIQUES



# Cartographie de données

## 2ème FAÇON DE FAIRE : « WHO »
## À PARTIR DES UTILISATEURS

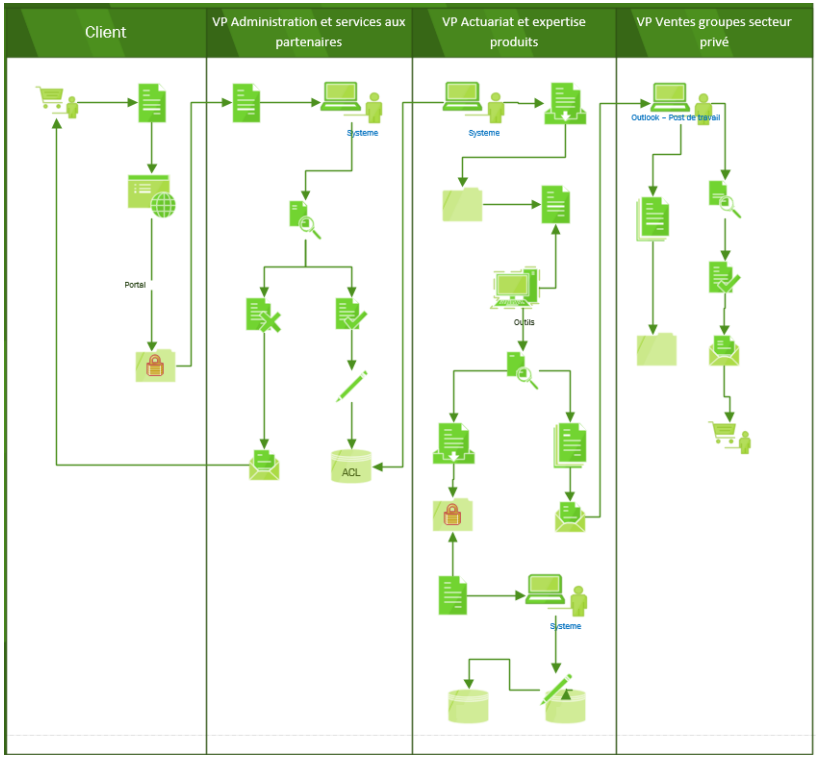



- Le lignage des données fournit des **informations sur le lieu de conservation des données physiques**
- De plus, il permet aux utilisateurs d'identifier **les relations en amont** (collecté comment, par qui, etc.)
- Il ne montre pas seulement le **flux de données**, mais il reflète également les **transfert et partages**, le cas échéant, qui débouchent sur de nouveaux éléments de données dérivés
- Le lignage des données est essentiel pour effectuer des **contrôles de qualité des données** et pour assurer le **suivi et la remédiation des problèmes**

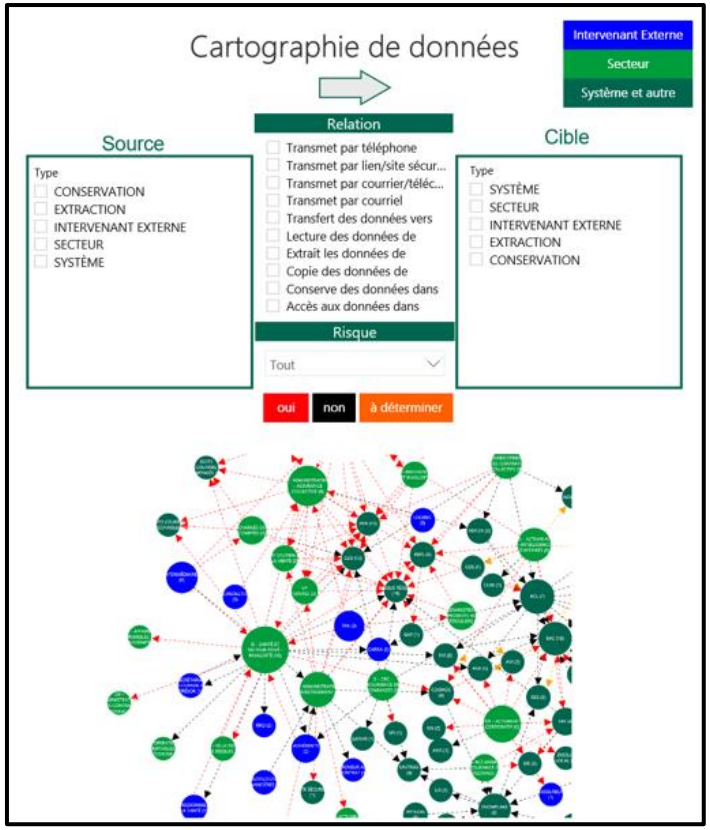
# Gabarit de cartographie

Le choix du format du gabarit de la cartographie doit être basé sur des critères de disponibilité de l'entreprise, de simplicité d'utilisation, de la qualité de l'interface utilisateur et de son caractère interactif ainsi que des possibilités d'actualiser les données facilement.

## Format Microsoft Visio




## Format Microsoft Power BI



# Identification de constats et établissement d'une feuille de route

Lors de la finalisation d'une initiative de cartographie des données, certains constats seront mis en évidence touchant différents aspects de la donnée ; sa gouvernance, sa protection, son accès, sa conservation, son partage, son utilisation non-adéquate, sa qualité, etc.

Cela pourrait donc engendrer d'établissement d'une feuille de route au sein de l'organisation.

# La protection des renseignements personnels c'est l'affaire de tous!

# Le rôle de l'organisation

La protection des renseignements personnels touche tous les secteurs d'affaires. Certains d'entre eux sont des acteurs importants dans la définition et l'établissement des cadres, politiques, procédures, etc. touchant à cette thématique. On en dénombre cinq principaux, soit la Conformité, les Services juridiques, l'Analytique de données, les Technologies de l'information puis l'Audit interne.

## Conformité

- Qu'est-ce que les concurrents font en matière de confidentialité ?
- Comment développe-t-on notre feuille de route de conformité ?
- Comment pouvons-nous convaincre la haute direction d'obtenir des ressources supplémentaires pour répondre aux exigences ?

## Services juridiques

- Quelles sont les exigences règlementaires auxquelles nous sommes soumis ?
- Quelle sera l'impact des projets de loi à venir (PL64 / C-11)

## Analytique de données

- Comment utilisons-nous les données personnelles pour générer de la valeur, tout en respectant les exigences règlementaires
- Comment pouvons-nous aborder la confidentialité dans nos initiales pour prévenir les risques

## Technologie de l'information

- Quels mécanismes technologiques sont nécessaires / disponibles pour automatiser les activités de conformité et confidentialité ?
- Comment peut-on améliorer notre environnement de sécurité actuel pour protéger nos actifs informationnels ?

## Audit interne

- Comment pouvons-nous inclure le volet Confidentialité aux mandats d'audit ?
- Existe-t-il des politiques, procédures, etc. pour soutenir la conformité et la confidentialité ?
- Est-ce que les secteurs d'affaires respectent les procédures définies ?

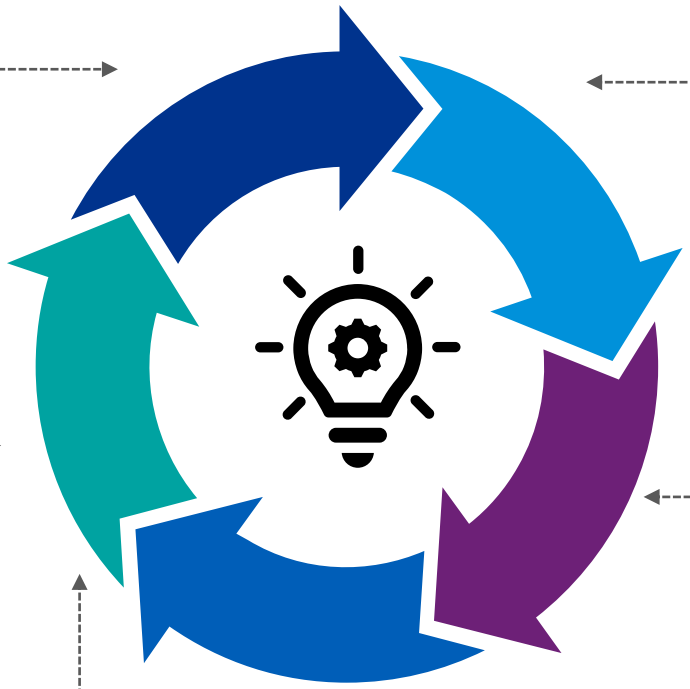
# Le rôle des individus

## DESTRUCTION

- Destruction les données sur support numérique, support papier, systems métiers, plateforme / solution de stockage sécurisée des données
- Destruction en temps opportun selon les normes et les standards

## COLLECTE

- Choix/ Consentement
- Limitation de la collecte
- Transferts sécurisés
- Sources /collecte fiables avec les tiers



## CONSERVATION

- Établissement de délais de conservation
- Transfert sécurisé vers la plateforme / solution de stockage sécurisée des données
- Sécurisation des données au repos
- Considérations sur la continuité des affaires, accessibilité et récupération des données

## UTILISATION

- Minimisation de données
- Utilisations secondaires
- Gestion des identités et accès (GIA)
- Gestion des mots de passe
- Journalisation
- Limitations de l'utilisation

## EXPLOITATION

- Anonymisation , minimisation
- Définition des limitations du traitement des données
- Gestion du programme de gestion des tiers
- Inventaire et transfert sécurisés

# Questions?

# Nous contacter

**Cynthia Viau-Mainville**
Conseillère principale
KPMG

cviaumainville@kpmg.ca

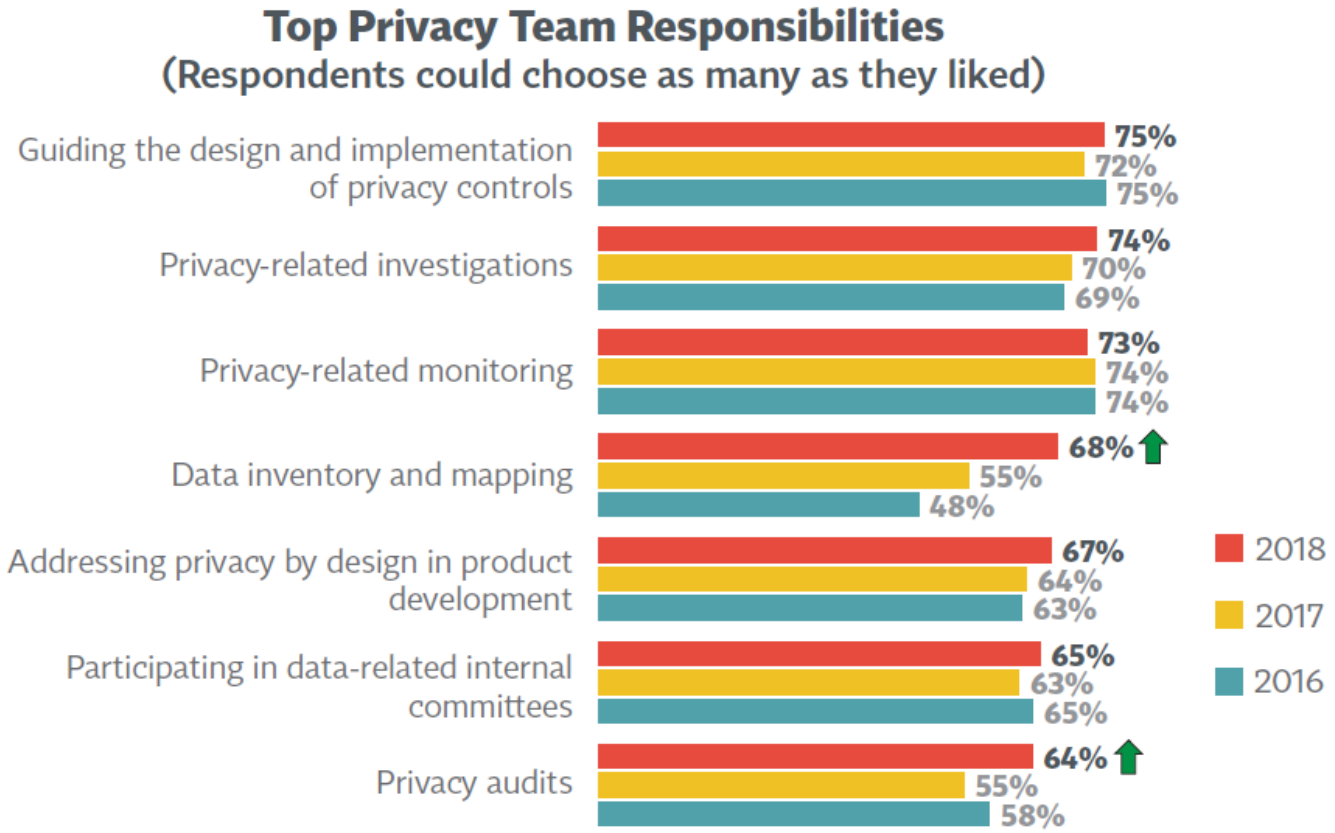
**Marie Dubernais**
Conseillère principale
KPMG

mdubernais@kpmg.ca

# Annexe

# Cartographie des données en hausse

**Privacy team responsibilities are expanding to include data mapping**




Source: IAPP Annual Privacy Governance Report 2018