RGPD : défis et proposition de démarche

Fédération des CPAS – Mars 2018

Dominique GREGOIRE

Le challenge

Le RGPD en Théorie…

Le contexte

La distance à parcourir: 100m

Le chemin à parcourir et le niveau de maturité

Ex: Echelle: CMMI

1
« Initial »
Imprévisible et réactif

2
« Géré »
Gestion élémentaire des projets

3
« Défini »
Standardisation des pratiques

4
« Géré quantitativement »
Pilotage par objectif quantitatifs

5
« Optimisé »
Optimisation des ressources, amélioration continue

1 ou 2
Niveau général des administrations

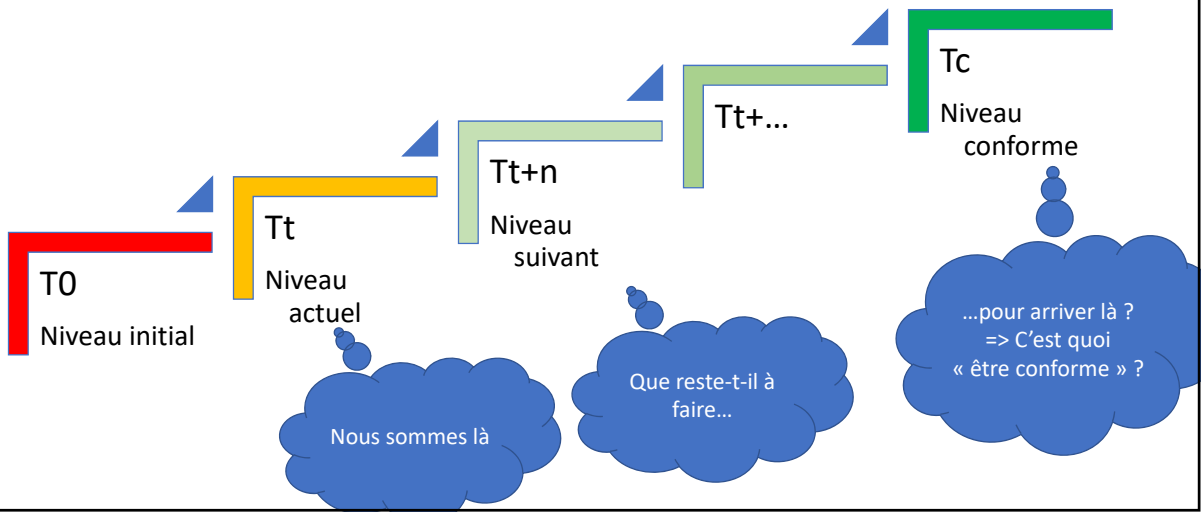
Niveau minimal pour s'assurer que TOUS les traitements sont bien gérés.

Le RGPD dans le contexte des administrations…

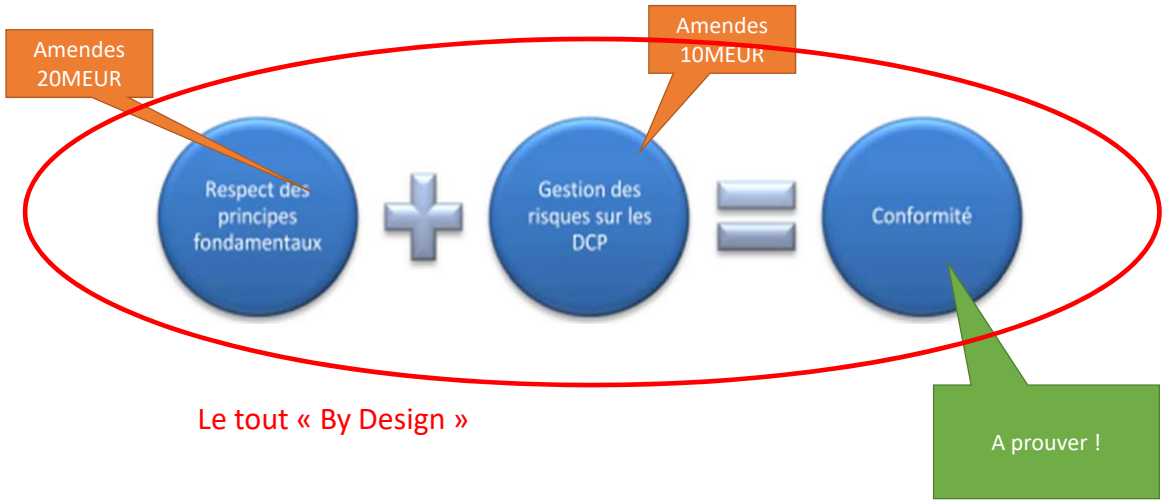
Le contexte

La distance à parcourir: 42,195 km

Le niveau de conformité atteint est relatif au niveau à atteindre



Les 2 piliers de la conformité



Le tout « By Design »

Source dessin: CNIL

Principes généraux

Licéité

Transparence

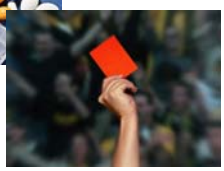
Loyauté

Finalité

Proportionnalité

Sécurité

Non-conformité ?



« Triche » => Disqualification

Niveau insuffisant => non qualification

Que signifie « être prêt » ?

Les 2 grands défis

1. Parvenir à faire du « **privacy by design** »…
2. Le **prouver** !

Défi 1: Privacy by Design

"**Data protection by design refers to the *existence of embedded safeguards and mechanisms* throughout the lifecycle of the application, service or product.**"

https://edps.europa.eu/sites/edp/files/publication/17-06-09_lina_jasmontaite_stefano_leucci_dpbddpbdf_ipen_en.pdf

"The challenge for privacy by design will be to achieve a **cultural**, **management**, **technological** and **regulatory** **environment** that can effectively address these problems [...] to protect privacy."

-- UK Information Commissioner's Office

« Difficultés probables » selon le cabinet Ulys

« Les deux nouveaux devoirs de *data protection by design and default* poseront **difficultés** dans l'implémentation en ce qu'ils impliquent une **prise en compte** de la protection des données **à tous les niveaux de processus** -et à **tous les métiers** participants audit processus- de traitement.

Ils imposent pour être correctement mis en œuvre **une étroite collaboration entre différents métiers** au sein de l'organisation du responsable du traitement et **une sensibilisation, voire un véritable enseignement** de chacun aux principes en cause : les métiers techniques des data (programmeurs, analystes, statisticiens, etc.), les métiers du legal et de la compliance et, le cas échéant, d'autres métiers opérationnels (marketing, etc.). Des processus spécifiques de contrôle devront être mis en place **dès la conception d'un projet data**.

La difficulté est d'autant plus ardue que l'on est face à des appréciations délicates (principes de nécessité, prise en considération du risque, etc.) qui exigent en réalité un savoir-faire et une pratique de longue date. »

https://www.gdpr-expert.eu/article.html?id=25#difficultesprobables

Quand la protection vient après le reste…

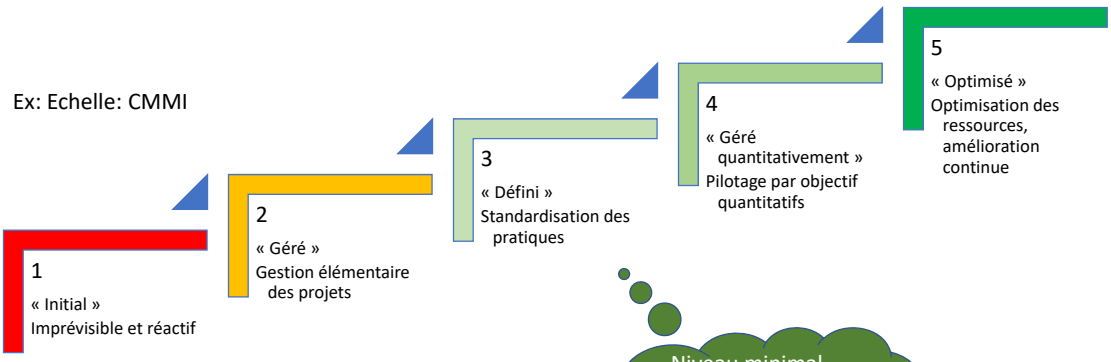
Quand la protection est intégrée au reste…

Le plus grand défi du RGPD pour les organisations ?

La **TRANSFORMATION** de l'organisation

Le chemin à parcourir pour atteindre un conformité RGPD

Ex: Echelle: CMMI



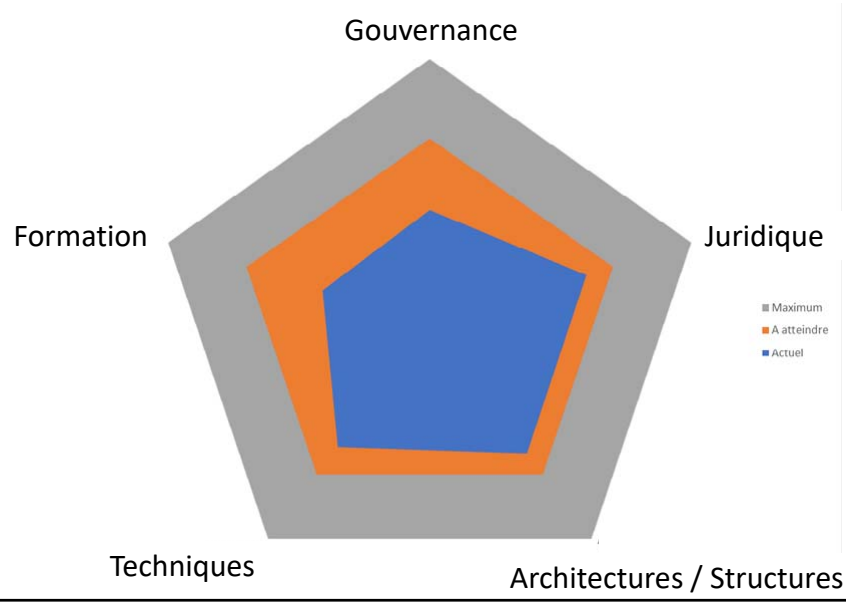
1 ou 2
Niveau général des administrations

=> D'abord mettre en œuvre une structure organisationnelle et des processus pour parvenir à standardiser les pratiques

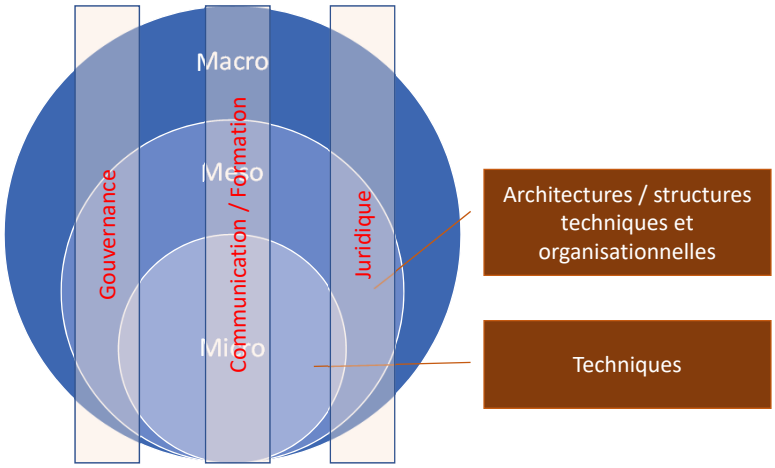
Niveau minimal pour s'assurer que TOUS les traitements sont bien gérés.

=> Insérer des checklists dans les pratiques standardisées

Privacy by Design: proposition de 5 axes



A tous les niveaux de l'organisation

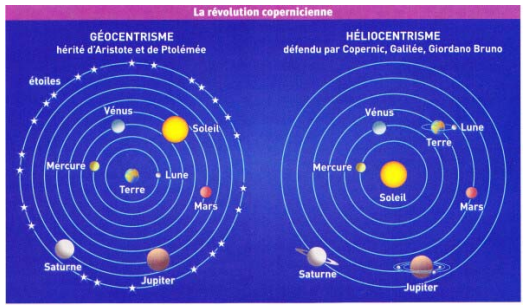


Gouvernance « Data Centric »

La gouvernance des données inclut *de facto* la protection des données => étendue à la sécurité de l'information

- Comité de gouvernance de données avec prérogatives en matière de sécurité de l'information;
- Architecte des données veille à créer une protection des données par conception;
- Data stewards en charge:
  - de veiller à l'utilisation légitime des donnée;
  - de l'analyse d'impact et du maintien du registre.

Data Steward est aussi un « Security Steward » !

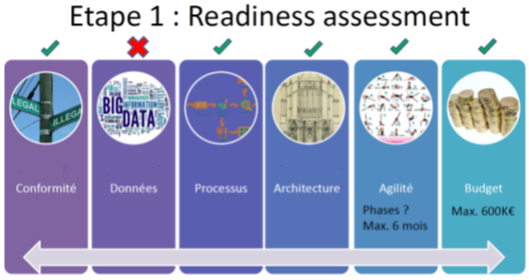


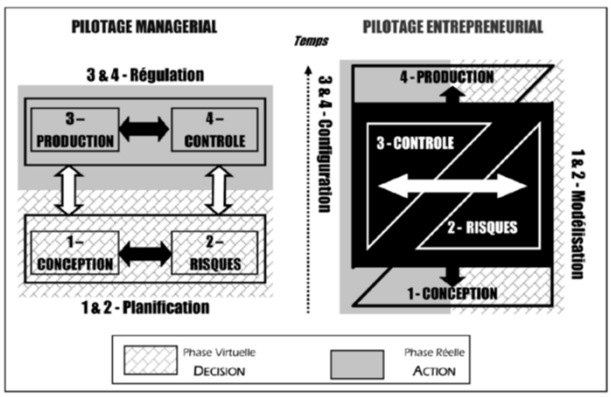
Une véritable révolution copernicienne !

Gouvernance des projets

Attention à ne pas limiter celle-ci à l'étape 1 « Readiness Assessment »

- Gestion centralisées des demandes;
- Intégration des dimensions risques dans le processus;
- Agilité !





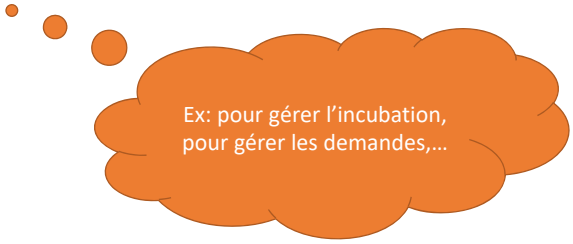
Architecture technique

Transformation de l'architecture des applications et des infrastructures afin d'intégrer les concepts de l'architecture des données:

- Gestion fine des accès;
- Traçage des transactions;
- Gestion des consentements des personnes;
- Authentification forte;
- Etc.

Architecture organisationnelle

La nouvelle gouvernance des données et la nouvelle gouvernance des projets devrait conduire à une nouvelle architecture organisationnelle.



Sensibiliser et former

Dans une logique de **confiance** et de **motivation**:

- Ex: communiquer aussi sur le **pourquoi** du RGPD

=> Viser la **coopération** et une **implication** des acteurs.

VS

Logique de peur => replis des ac[illegible] non-collaboration, délations, etc.

Réseautage

Identifier des relais dans l'organisation

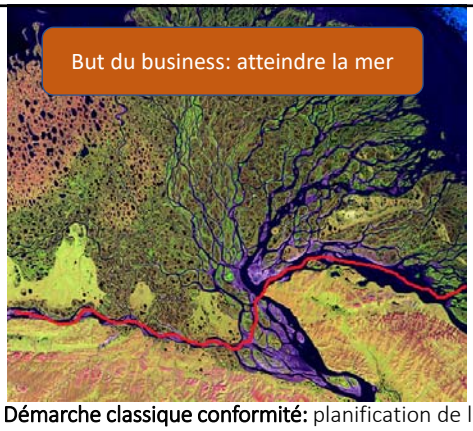
&

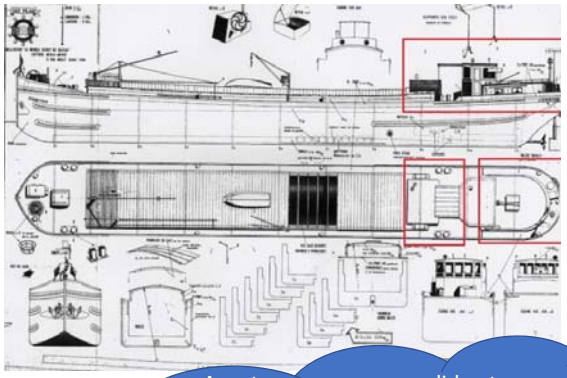
Etablir une **relation de confiance et de motivation**

Effet de levier (effet papillon)

&

Création d'émergences





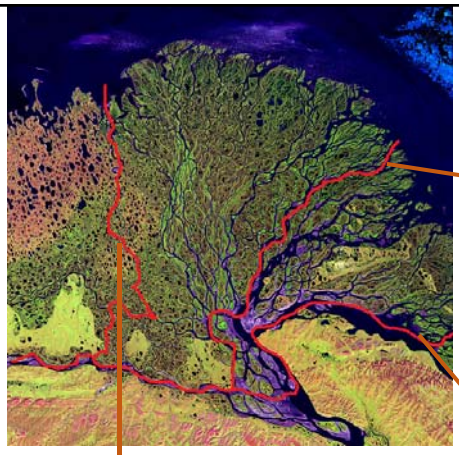
Démarche classique conformité: planification de la mise en conformité (trajet, structures, processus, procédures, etc).
et on fait entrer les acteurs dans l'embarcation lorsque c'est prêt…

Aucune autonomie laissée aux acteurs.
=> Nécessité d'un « chef de projet ».

La protection est le but de ce chef projet, pas l'atteinte de la mer.

Avantage: apparence solide et rassurante

Désavantage: long, couteux, fortes résistances au changement et surtout risque de ne plus être approprié lorsque le plan et la construction sont finis. (ex: passage devenu trop étroit pour faire passer le bateau, niveau de l'eau a baissé, etc…)
De plus la conformité RGPD n'est pas un « One Shot »: elle doit être continue.



Avantage: agile, s'adapte aux besoins présent, facilite l'atteinte des objectifs de l'organisation.

Désavantages: sentiment d'un moins bonne maitrise (pour les personnes en charge de la conformité, pas pour les acteurs !)

Démarche par émergence: Responsabilisation et marge de liberté laissée aux acteurs.
On accompagne les acteurs dans leur réalité quotidienne afin de gérer au mieux possible les risques. On les aide à trouver des solutions par eux-mêmes.

La protection est un facteur de succès, non l'objectif.

Pas besoin d'un chef de projet (il n'y a pas de projet…) mais il faut un facilitateur…

Une approche pas classique, mais qui repose sur les préceptes des spécialistes de la gestion de la complexité et du changement.

Il ne s'agit pas d'improvisation ou de *« laisser faire »,* mais d'une démarche intégrative, laissant une bonne marge de liberté. Les interventions sont réduites au maximum et vise principalement **à mettre l'acteur en capacité de gérer les risques dans leur contexte.**

Elle mise sur la puissance du collectif, repose sur la **confiance** et la prise en compte des **points de vue divergents.** Elle **rassemble et non divise.**

Les convergences des émergences sont obtenues par le partage de sens.

Cette démarche présente le gros avantage d'être foncièrement positive (vs logique d'opposition).

Les procédures de conformité sont inutiles dans une terre stérile

Transformer une organisation, c'est d'abord préparer un terreau propice.

Architecture: *structure, pentes…*

Gouv. Données:
qualité des nutriments…

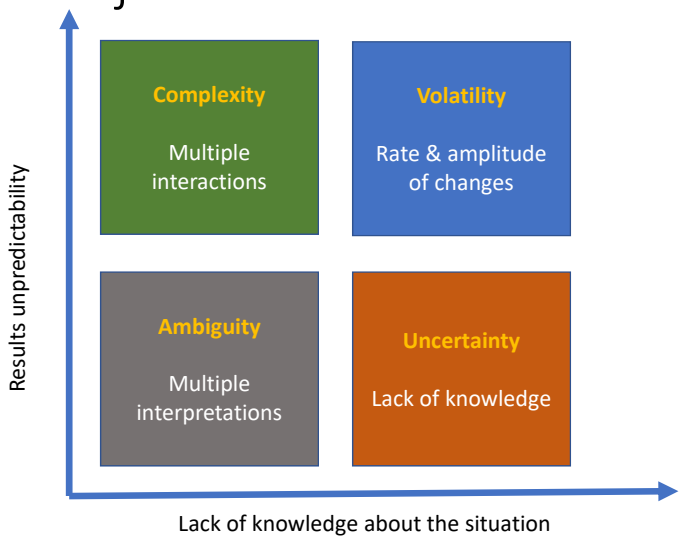
Gouv. projet:
Répartition des nutriments…

Techniques: *empierrement, digues…*

Réseautage: *irrigations, engrais…*

Règlements: *juste partage, garde fous…*

Une démarche compatible avec le « VUCA world » d'aujourd'hui



The « VUCA world »: les conséquences

''This is the era of « fluid strategy », and it means that companies have to act more quickly – and more agile – than ever before''

– Peter Hinssen - The network always win

Les organisation doivent se transformer pour plus d'agilité
⇒ le « privacy by design » étant par définition intégré dans l'organisation, il doit aussi être agile…

Défi 2: Prouver

Prouver que l'on fait suffisamment de choses.

Prouver que l'on fait bien les choses.

Prouver que l'on a:

- bien fait les choses;
- suffisamment fait de choses.

Critères de conformité « objectifs » et « subjectifs » du RGPD

- Points « objectifs »/ « binaires »: facilement contrôlables par CPVP (Commission Protection Vie Privée)
  - Existence documentations:
    - Registre des traitements;
    - Analyses d'impacts;
    - Décisions / choix de solutions;
    - Informations aux personnes;
    - Contractualisations.
  - Transfert hors UE;

Importance des « bonnes pratiques » et recommandations CPVP, G29, BCSS, ISO,…

- Points « subjectifs » : dépend du niveau d'exigence de l'évaluateur
  - Efficacité des mesures;
  - Gestion des risques.

Prouver: licéité, finalité, légitimité, loyauté, transparence, proportionnalité…

Justifier l'adéquation des mesures de protections.

Prouver que des choses sont mises en œuvre pour gérer les risques des personnes concernées.

Tactique de mise en œuvre proposée

Tactique proposée : pragmatisme !

Montrer que **l'organisation est en pleine transformation**.

Investir prioritairement sur la construction de **fondations solides** afin de mettre en œuvre **le « privacy by design » de manière effective.** Ce qui apportera à termes automatiquement un bon niveau de protection.

Plutôt que sur des changements cosmétiques couteux et inefficaces.

Pour les **anciennes applications:** logique de **« best effort »** et **migration progressive vers le nouveau système** en construction.

Tactique de mise en œuvre proposée

Miser prioritairement sur les fondations :

- Gouvernance des projets;
- Gouvernance des données;
- Architectures techniques.

et **formaliser les processus et allocation des ressources.**

⇒Permettra de garantir de manière structurelle et organisationnelle:

- La «**privacy by design** » pour les nouveaux projets et les modifications passant par ces gouvernances;
- Le maintien de la **documentation** y relative.

Par ex. : ce qui est cherché en priorité n'est pas d'avoir un registre des traitements pour mai 2018, mais un processus, une structure et des ressources qui garantissent que ce registre sera correctement maintenu.

Tactique de mise en œuvre proposée

- Du formalisme…utile… :
  - La documentation devrait aussi servir un maximum à autre chose (ex: « dictionnaire des données » utilisé par les architectes des données servira également de registre de traitement)

  ⇒« By design »;

  ⇒Formalisme spécifique RGPD, ne coute quasi rien.

De manière générale: vrai pragmatisme prenant en compte les conditions réelles et non un contexte idéal.

Tactique de mise en œuvre proposée

- La gouvernance des données et de projet vise notamment à systématiquement:
  - Maintenir un registre des traitements **utile pour le business** dont l'exhaustivité dépasse largement les prescrits du RGPD;
  - Analyser le respect des droits fondamentaux des personnes concernées;
  - Réaliser une analyse d'impact pour les personnes concernées, lors d'un nouveau traitement;
  - Déterminer les données strictement nécessaires, les personnes pouvant y avoir accès, la durée de conservation, les bases de légitimité, etc.
- L'architecture applicative vise à notamment:
  - Sécuriser techniquement les accès sur base de rôles et de classification des données;
  - Authentifier de manière forte les utilisateurs;
  - Tracer les usages des données;

Avantages de la tactique proposée

- Les coûts:
  - 90% de la conformité est obtenu sans investissements spécifiques:
    - Pas de « chef de projet » et autres ressources pour transformation RGPD (repose sur les acteurs et projets existants)
    - Ex: Data stewards = Securtity Stewards;
    - Authentification FAS (eID);
    - Architecture Données;
    - ESB;
    - Etc.
  - 10% plus « spécifiques » pour :
    - Gestion des incidents;
    - Monitoring (une bonne part devrait déjà exister pour simplement détecter des dysfonctionnements…)
    - Communication/formation/sensibilisation
    - Juridique
- Réaliste/pragmatique: ressources pouvant être allouées limitées, complexité, environnement changeant, etc.

Conclusion

- Pour les organisations avec un faible niveau de maturité, la conformité RGPD passe avant tout par une transformation de l'organisation.
- Cette transformation nécessite un terrain propice, un bon terreau.
- Ce terrain s'obtient par la **motivation (pas par la peur) et par une coopération des acteurs.**
- Le RGPD est une **opportunité pour les organisations d'améliorer la qualité de ce qu'elles produisent**. Vu comme cela, le coût spécifique du RGPD peut-être très faible.

Des questions ?

Merci !