Le GDPR ?
Une opportunité pour repenser notre fonctionnement interne et en améliorer la qualité

C. Scoubeau | 30/11/2018 (CIPIQs - La gestion du changement dans les projets d'amélioration de la qualité)

jj/mm/aaaa

Sommaire

Sommaire

- Contexte
- GDPR – principes, obligations et droits
- Fonctionnement interne et qualité
- Axes d'amélioration
- Gestion du changement dans les projets de la qualité
- Exemple d'un changement bien géré
- Quels gains retirer de la compliance au GDPR et donc de ces changements ?
- Conclusion

Exposé

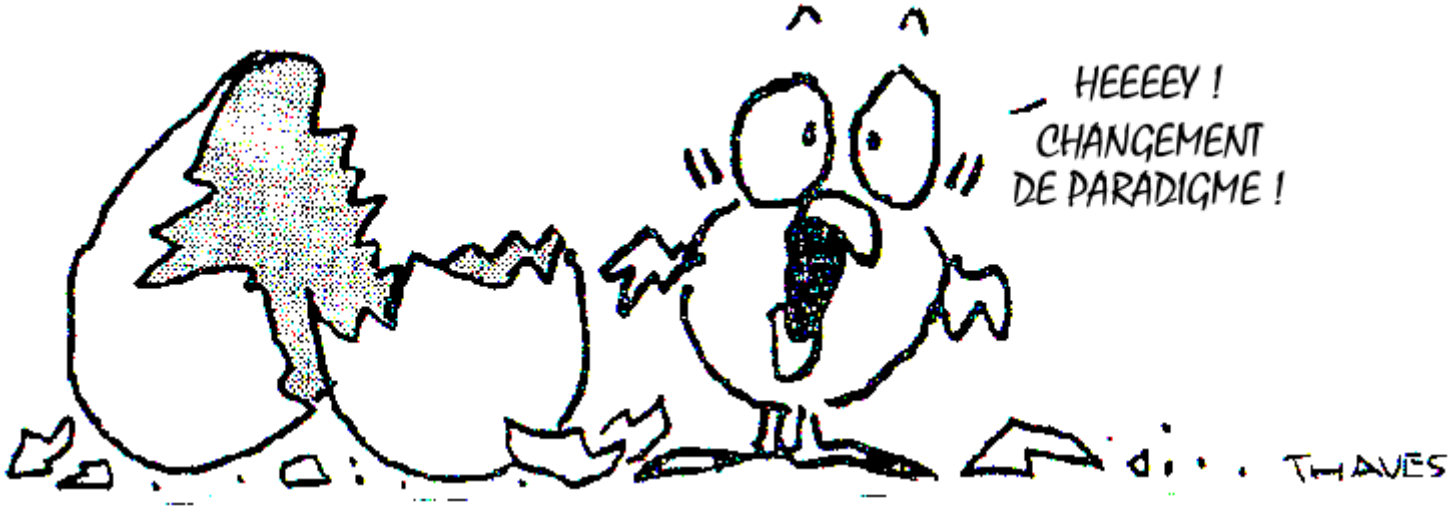
Contexte

Depuis le 25 mai 2018, le GDPR* est d'application.

* Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Contexte

- Tous les jours, nous devons faire face à des changements (vie privée, vie professionnelle).
- Ces changements peuvent être dus à l'évolution quasi normale de nos pratiques mais peuvent aussi être perçus comme déstabilisants, voire …



Contexte

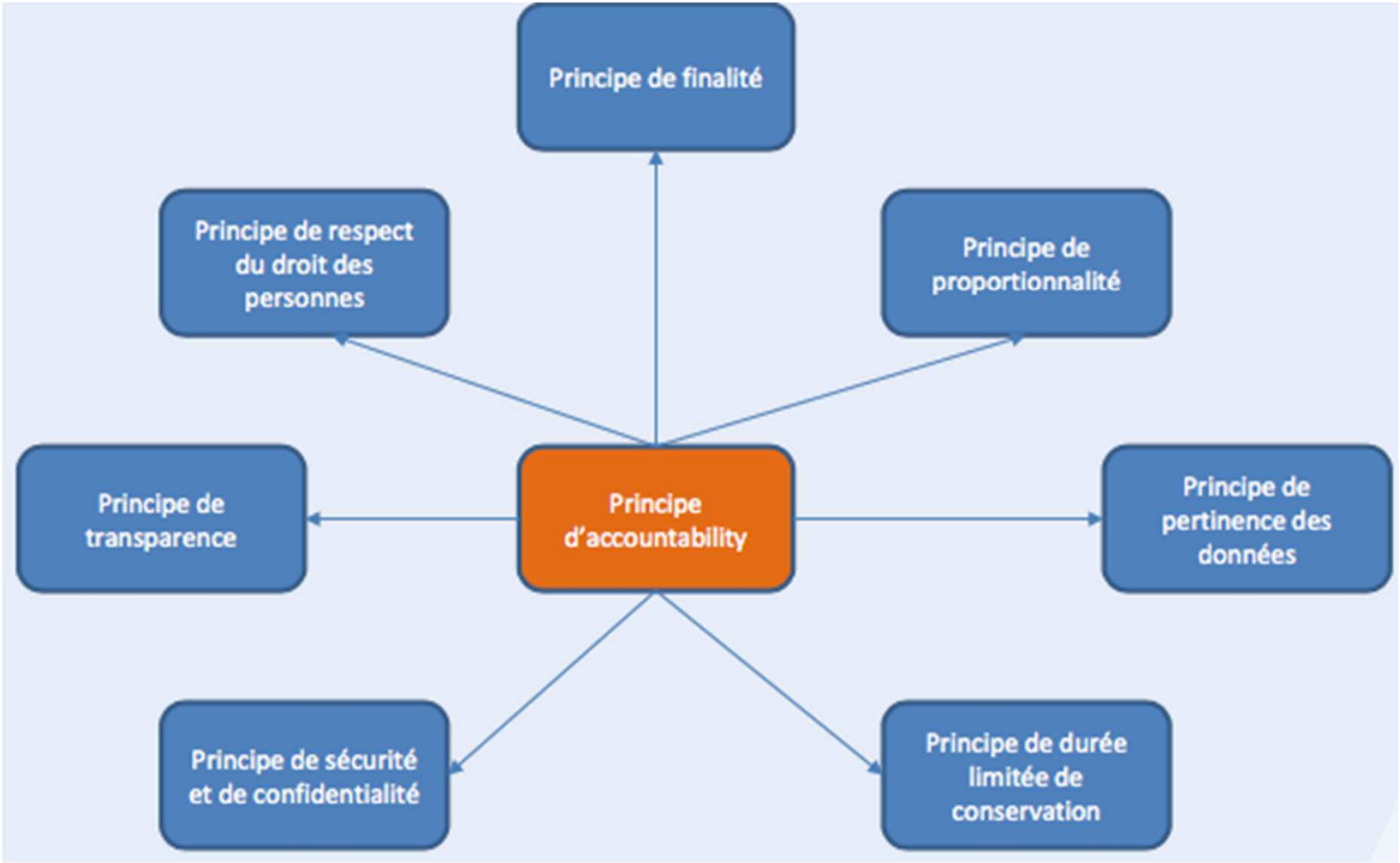
- Les changements ne sont, de plus, pas toujours désirés (comme c'est le cas avec les dispositions légales).
- Mais apprenons à vivre avec ces transformations, adaptons-nous à notre nouvel environnement.

Contexte

- Pour faire face aux changements que nous impose le GDPR (Règlement), commençons par le comprendre en quelques mots.

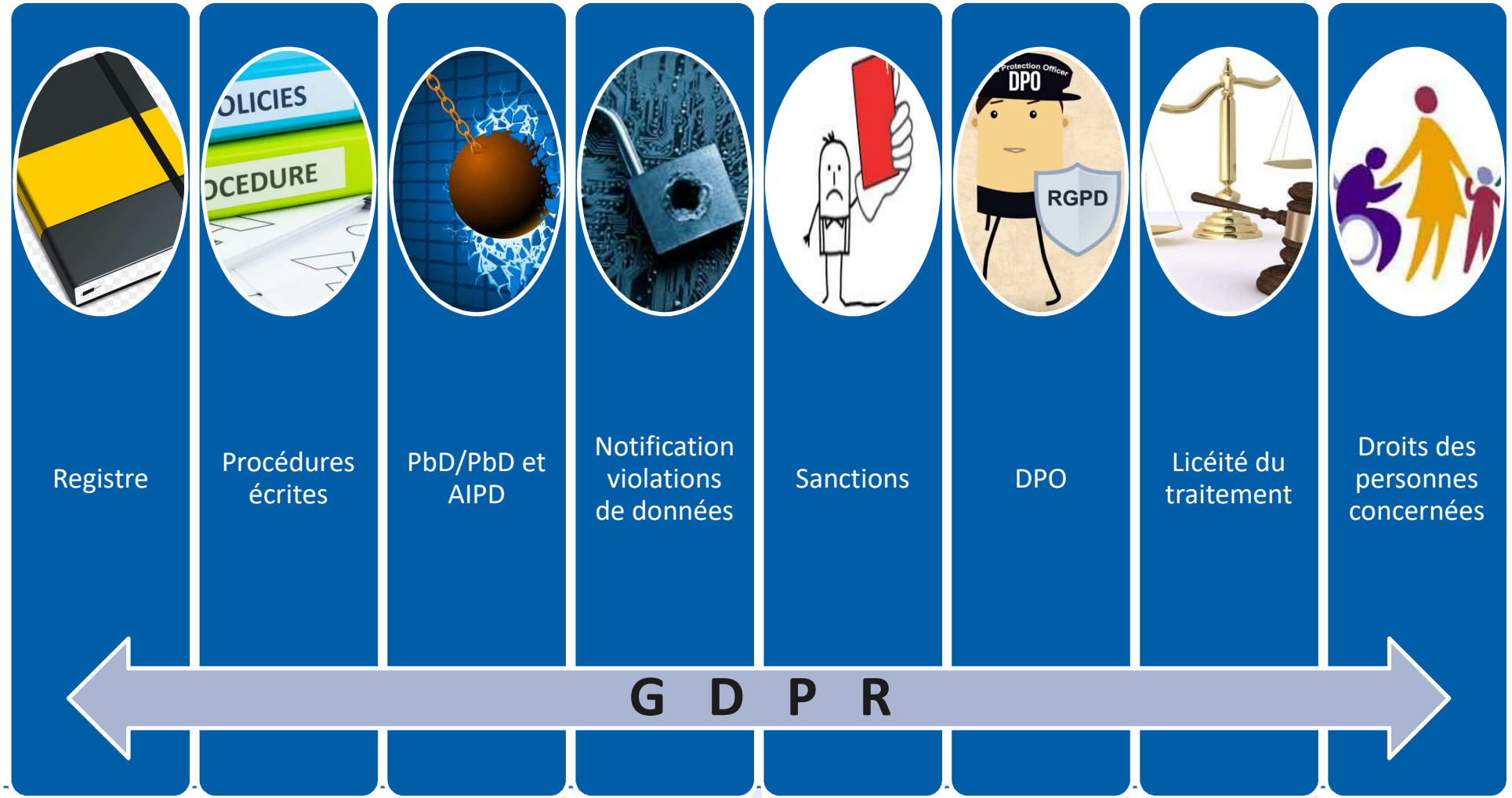
GDPR – principes, obligations et droits

Principes



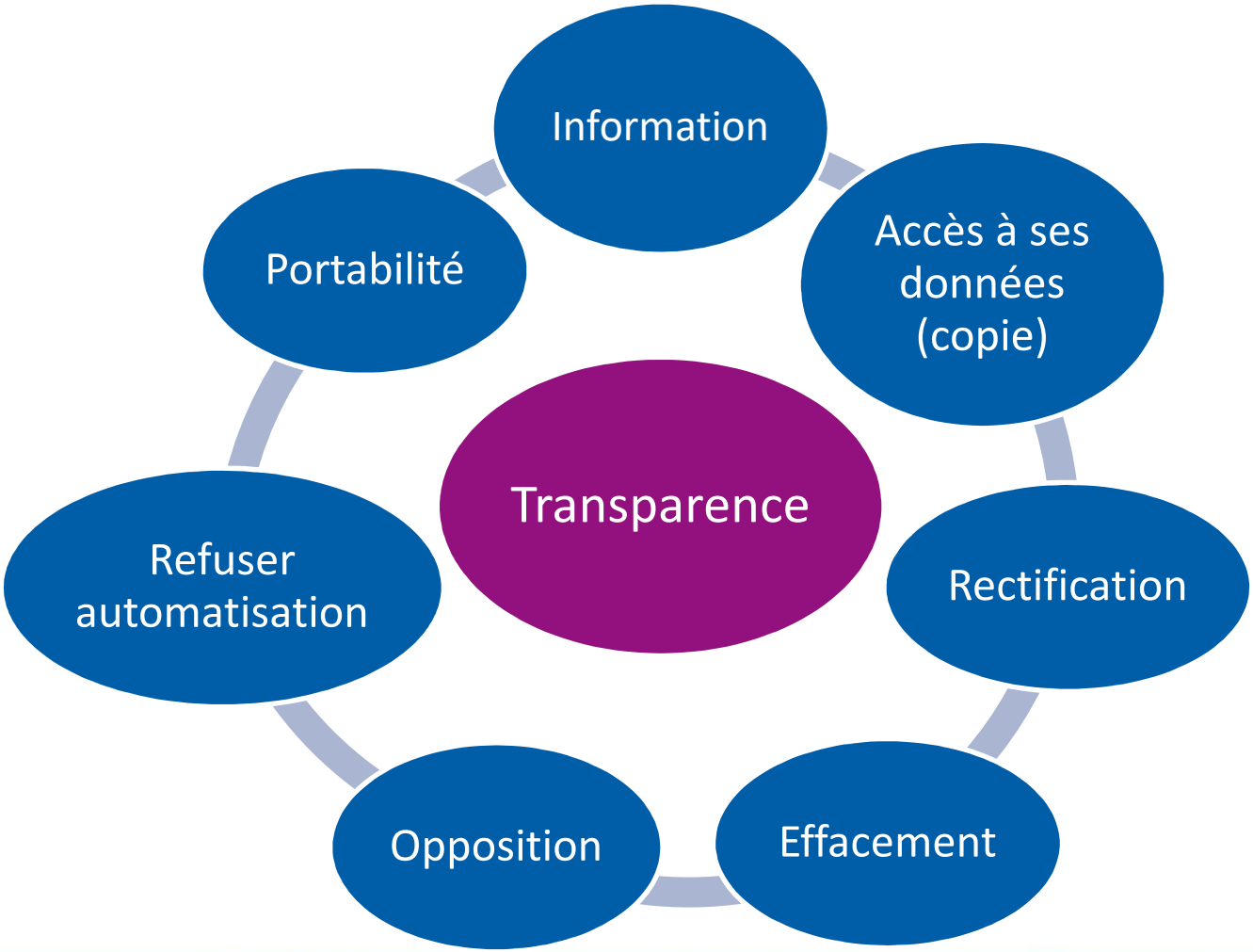
GDPR – principes, obligations et droits

Obligations



GDPR – principes, obligations et droits

Droits des personnes concernées



GDPR – principes, obligations et droits

Exigences du GDPR

Vers quels changements ?

Fonctionnement interne de la qualité

Faut-il en arriver à :

Fonctionnement interne et qualité

Quels **changements** ? Nous devons (mieux) :

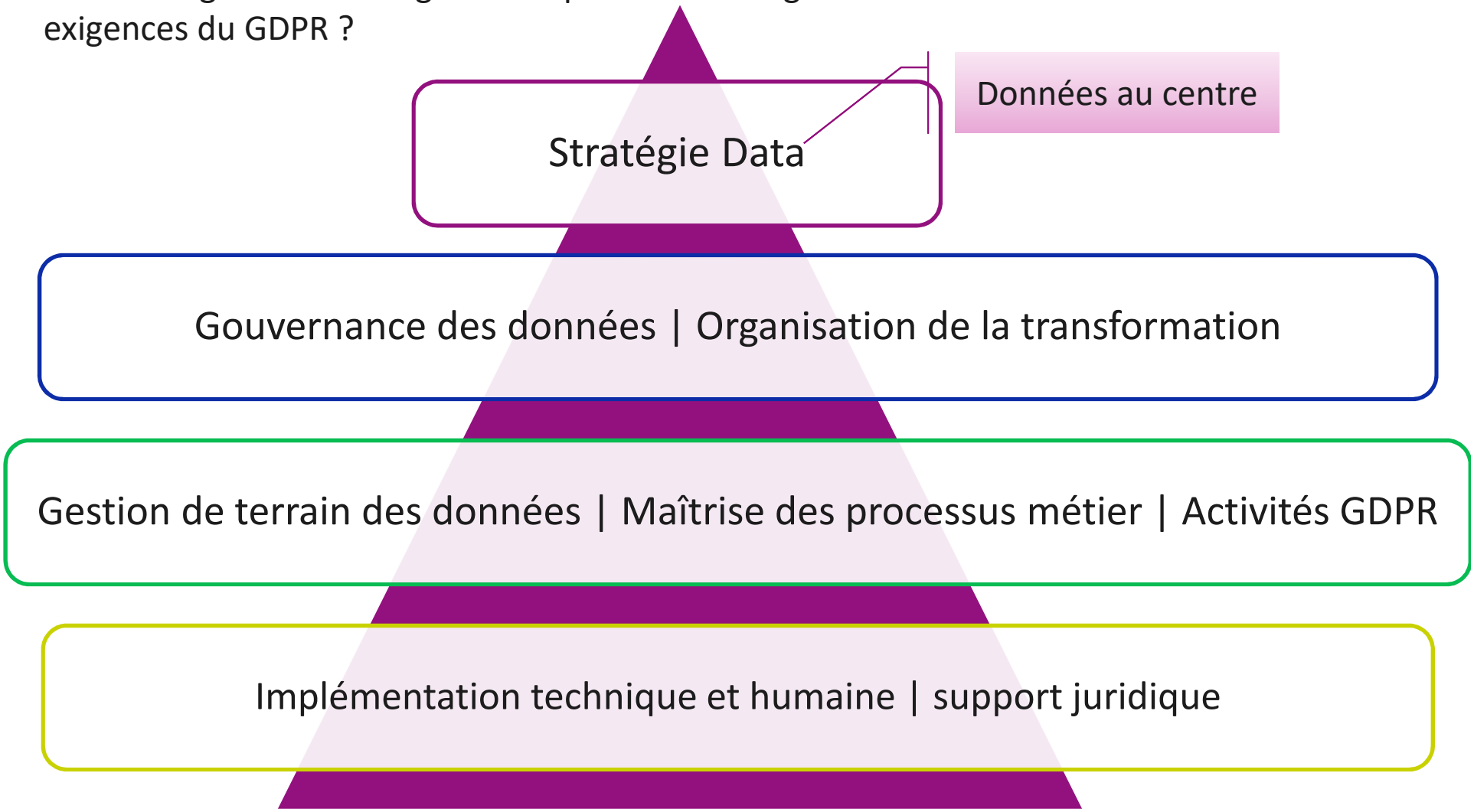
- Renforcer la **gouvernance des données**
- Maîtriser les **processus métier** et données associées
- Mettre en œuvre de bonnes **mesures technique et organisationnelle**

☞ = approche globale à déployer selon différents axes*

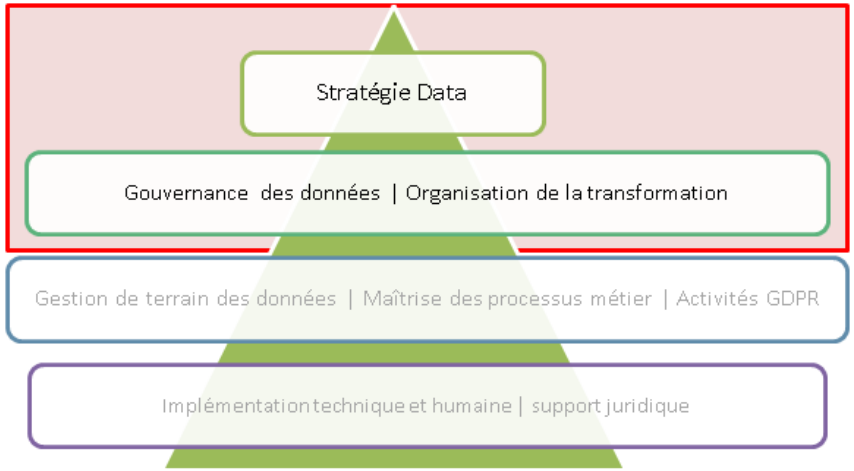
* Source : La Tribune

Axes d'amélioration

Comment gérer ces changements que sont les exigences renforcées et les nouvelles exigences du GDPR ?

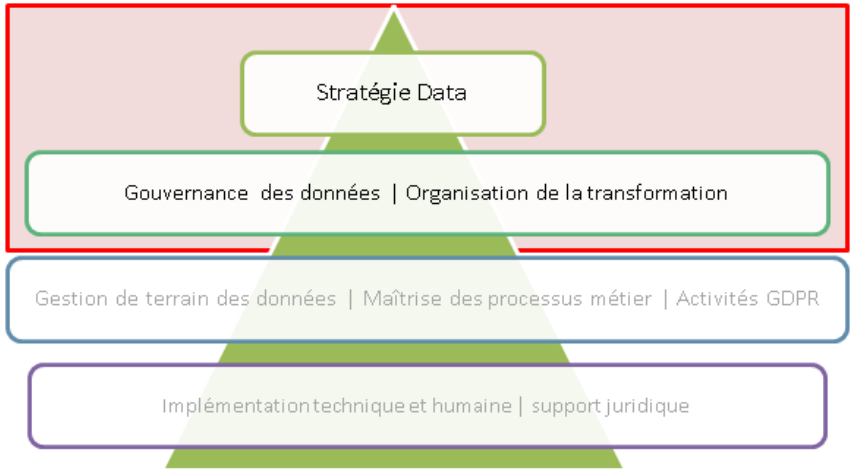


Axes d'amélioration



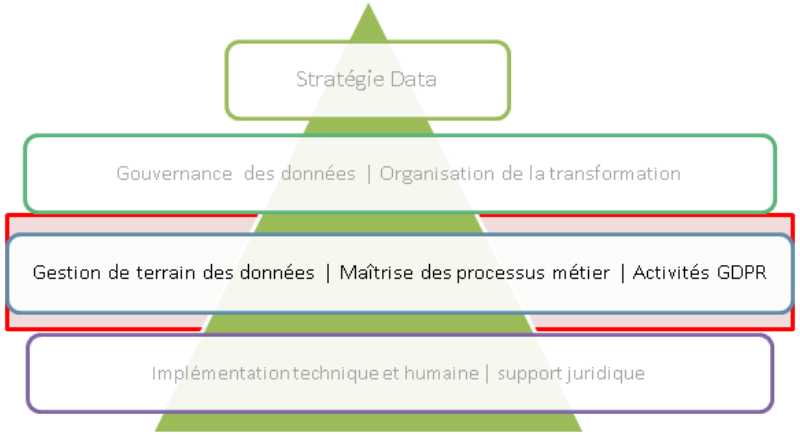
- **Stratégie Data** : créer une stratégie de création de valeurs en collectant et valorisant les données dans dans le cadre d'une finalité claire et transparente (données au centre)
- **Gouvernance des données** : doit être portée par le top management qui donne l'orientation à l'entreprise (via sensibilisation, politiques vie privée, implication des acteurs, principes à suivre)
- **Organisation de la transformation**

Axes d'amélioration



- **Stratégie Data**
- **Gouvernance des données**
- **Organisation de la transformation** : par l'intermédiaire du DPO. Sa position est clarifiée, son rôle bien défini, travaille en collaboration avec d'autres acteurs complémentaires et responsabilités bien définies, reçoit les moyens dont il a besoin (outils, formations, ressources, accompagnement)

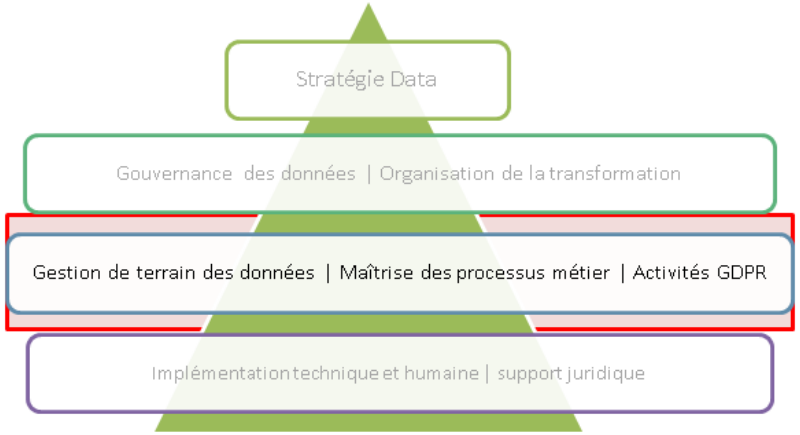
Axes d'amélioration



- **Gestion des données et de l'information sur le terrain** : cartographie générale des DCP, elles sont structurées, les modalités de stockage sont définies, traitements ciblés, indicateurs de suivi définis pour mise à jour, suivi des incidents formalisé
- **Maîtrise des processus métiers** : notamment par la rédaction et la mise à jour du Registre, les AIPD, PbD/PbD, contrôle d'accès, sécurité
- **Mener à bien les activités GDPR**

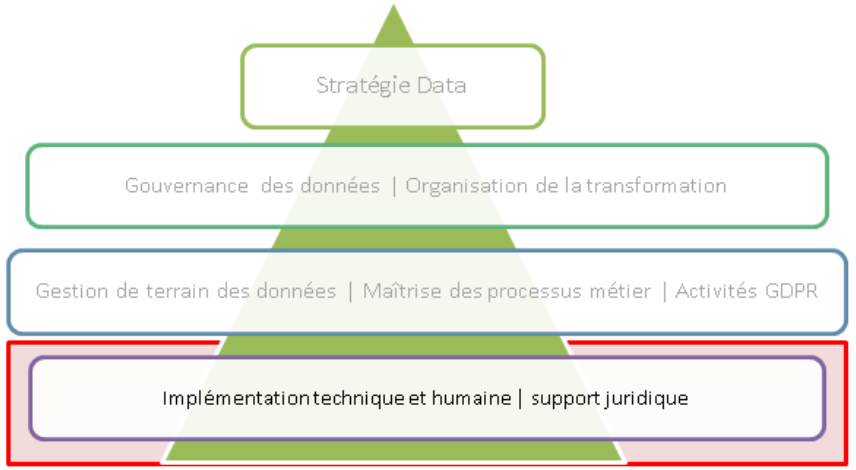
Axes d'amélioration

- **Gestion des données et de l'information sur le terrain**
- **Maitrise des processus métiers**



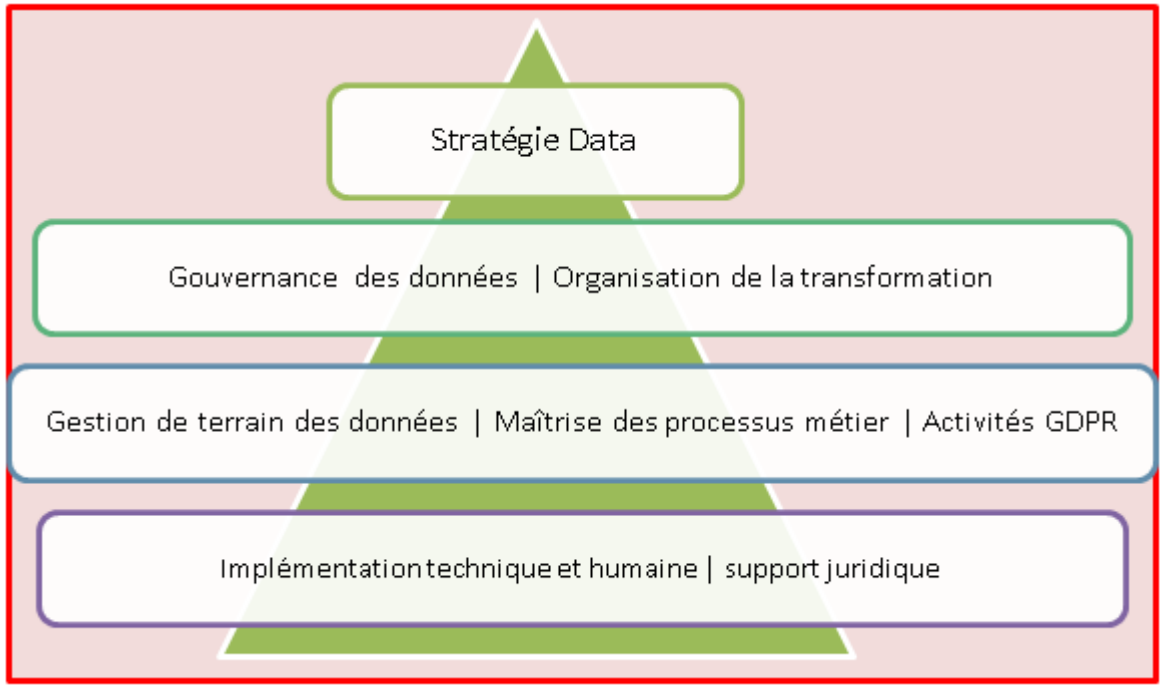
- **Mener à bien les activités GDPR** : à déployer dans tous les secteurs, opérationnel pur → répondre aux droits des personnes concernées, pilotage opérationnel au sein de l'entreprise, gestion des risques, audits, reporting, suivi des sous-traitants, communication, gestion des alertes

Axes d'amélioration



- **Implémentation technique et humaine** : intégration des exigences du GDPR dans l'architecture du SI → création d'outils pour faciliter l'audit, développement d'applications. Intégration des exigences du GDPR dans les habitudes par la formation du personnel.
- **Implication du service juridique** : établissement de contrats avec les partenaires et sous-traitants, coordonner, contrôler, valider les actions juridiques, veille juridique.

Axes d'amélioration



Pyramide de bonnes pratiques de gouvernance et de management de données → bénéfiques pour les données personnelles mais aussi, pour toutes les autres données de l'entreprise.

Axes d'amélioration

Ces bonnes pratiques permettent de digitaliser l'entreprise correctement, car elles amènent à :

- L'**amélioration** de la **gouvernance** et de la **culture** ;
- Une **meilleure maîtrise des risques**, l'augmentation de la **sécurité** et du **contrôle** ;
- Des données de **meilleure qualité** ;
- La bonne gouvernance impliquant une **optimisation des ressources techniques**.

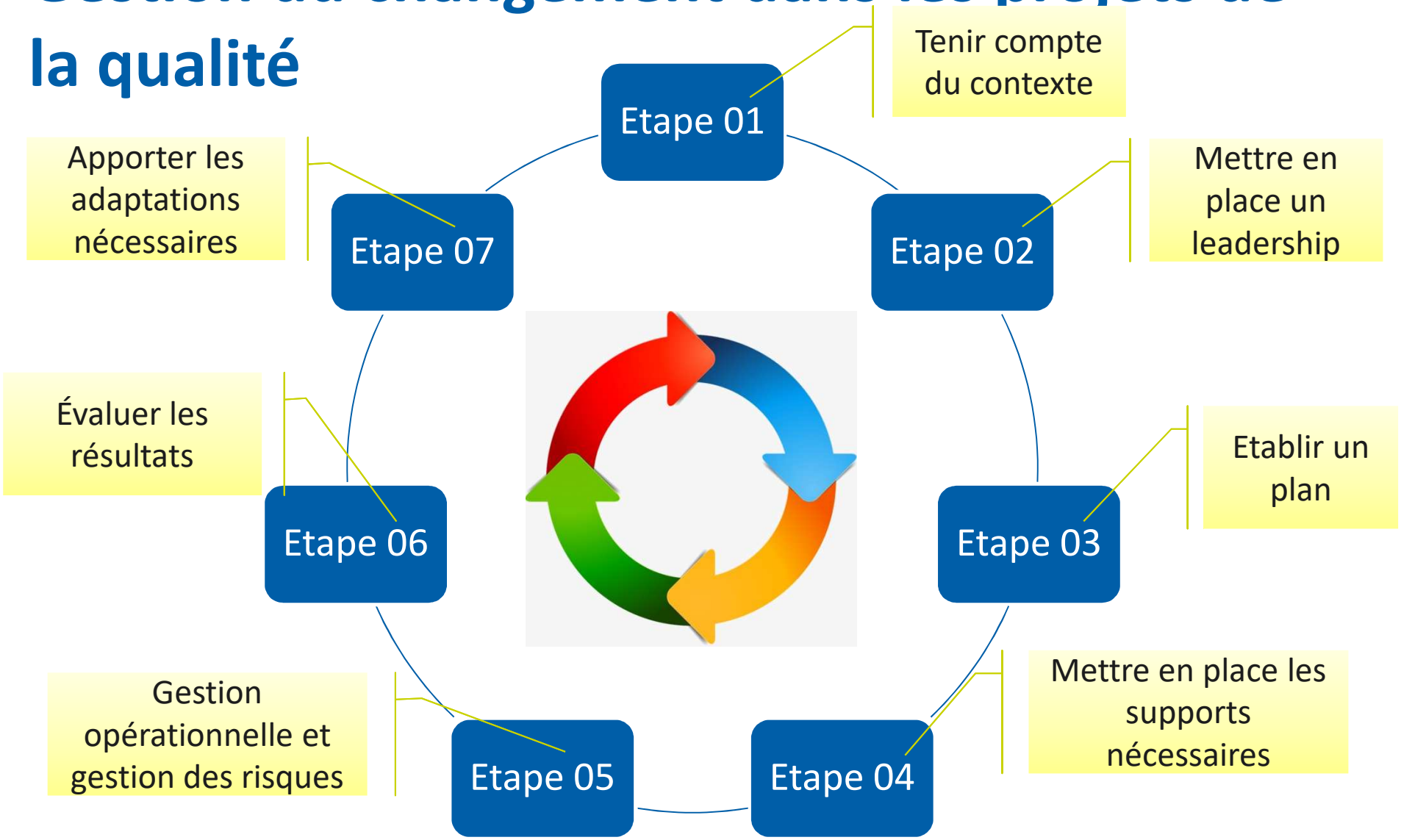
Gestion du changement dans les projets de la qualité

- Les axes d'amélioration permettent de **concrétiser le changement** du top management aux personnes de terrain, en passant par les supports techniques et humains ;
- « Faire le GDPR » selon les axes précités permet donc d'**améliorer la qualité du data management** mais pas uniquement ;
- « Faire le GDPR » est aussi une **opportunité** pour le processus d'**accréditation** puisque cela permet d'être en règle avec certains critères déterminants pour obtenir le label.

Gestion du changement dans les projets de la qualité

- Les axes d'amélioration permettant d'atteindre la mise en conformité GDPR peuvent être déployés selon la **norme ISO 27001** (Système de Management de la Sécurité de l'Information – SMSI, exigences).
- L'objectif est de **protéger** les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.
- Suivre la norme ISO est tout à fait **compliant** au GDPR 

Gestion du changement dans les projets de la qualité

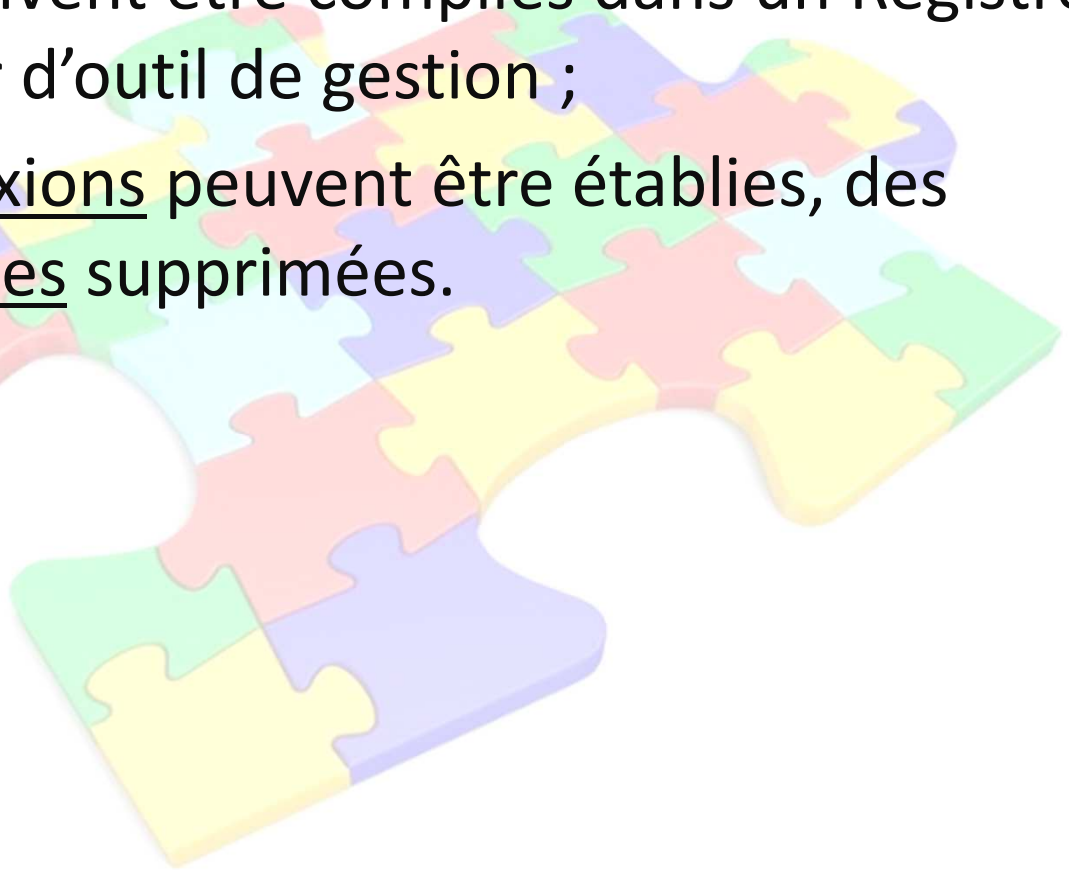


Gestion du changement dans les projets de la qualité

- Devoir étudier tout projet sous l'angle GDPR implique d'avoir une **vision faitière** de l'ensemble des projets de l'entreprise et d'établir des relations entre ceux-ci.
- Les changements qu'impose le Règlement dans nos procédures peuvent être mises à profit pour avoir une meilleure **vision globale** de la stratégie :
  - ✓ Les finalités doivent clairement être établies ;
  - ✓ Les principes doivent être respectés ;
  - ✓ Des analyses d'impact doivent potentiellement être réalisées ;

Gestion du changement dans les projets de la qualité

- ✓ Les flux doivent être compilés dans un Registre qui peut servir d'outil de gestion ;
- ✓ Des connexions peuvent être établies, des redondances supprimées.



Gestion du changement dans les projets de la qualité

- Un **plan de crise** doit être défini → que faire en cas de fuite de données et, plus largement, en cas de faille de sécurité ?
- Grâce à ce plan de crise, l'entreprise est capable de **réagir rapidement**, de prendre les mesures nécessaires pour limiter l'impact de la défaillance et corriger les faiblesses ; les rôles de chacun dans la gestion de la crise sont clairement définis.

Exemple d'un changement bien géré

- **Objet** : changement de fournisseur et de logiciel central
- **Objectif** : remplacer un logiciel existant par un autre plus performant, vendu par un autre fournisseur, tout en tenant compte des normes GDPR
- **Conséquences** :
  - ✓ Changement d'interface → adaptation de l'utilisateur ;
  - ✓ Changement dans les procédures → adaptation de l'utilisateur ;
  - ✓ Révision de l'architecture informatique → modifications et suppression de passerelles ;
  - ✓ Adaptation de programmes « satellites » .

Exemple d'un changement bien géré

- Les **métiers se parlent**, apprennent à mieux se connaître, raisonnent ensemble ;
- Réalisation d'une **analyse d'impact** : vérifier les principes et la sécurité des données à caractère personnel implique de revoir et contrôler le projet dans sa globalité, sur tous les plans :
  - ✓ principes GDPR,
  - ✓ obligations,
  - ✓ sécurité informatique,
  - ✓ sécurité organisationnelle,
  - ✓ sécurité juridique

Exemple d'un changement bien géré

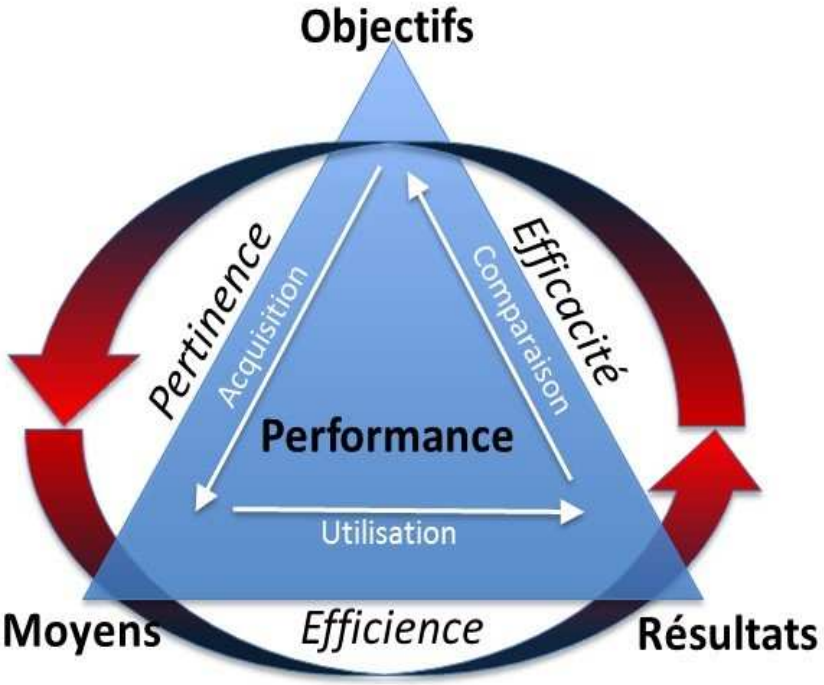
- Ces démarches permettent d'arriver à un **produit bien pensé, nettoyé, de qualité, optimum et efficace**.
- Des personnes de disciplines différentes auront dû se parler, se concerter et avancer dans le même sens.

Quels gains retirer de la compliance au GDPR et donc de ces changements ?

- Profitons du GDPR pour étendre le raisonnement la protection des données à caractère personnel à **toutes les données de l'entreprise** ;
- Les traitements de données sont **plus performants** ;
- L'entreprise connaît mieux ses données et sait mieux les exploiter → développe mieux ses **stratégies** ;
- Relation de **confiance** accrue avec ses clients grâce à la transparence → relation plus **durable** ;

Quels gains retirer de la compliance au GDPR et donc de ces changements ?

- L'entreprise renforce ainsi la **disponibilité** des données en les connaissant et en les maîtrisant mieux, en augmentant leur qualité, elle en contrôle l'**accessibilité** grâce à l'amélioration de la sécurité → gestion saine, efficace et efficiente.



Quels gains retirer de la compliance au GDPR et donc, de ces changements ?

- La notion de changement est indissociable de la performance, ce qui est démontré *in casus* si on profite de la **mise en conformité au GDPR** pour améliorer la gestion des données, davantage les sécuriser et leur donner une réelle plus-value.

Quels gains retirer de la compliance au GDPR et donc, de ces changements ?

- Les changements qu'implique la mise en conformité au GDPR touche l'**ensemble des dimensions de l'entreprise** : depuis l'implantation des équipements et la conception des postes de travail jusqu'aux orientations de stratégie, aux choix de structure, en passant par les dispositifs de coordination, d'information, de gestion et les relations avec les partenaires et l'environnement de l'entreprise
- Le GDPR est donc une belle occasion pour améliorer notre fonctionnement interne et en améliorer la qualité.

Conclusion

- La meilleure connaissance de nos flux de données (obligation GDPR) est favorable pour l'entreprise et le développement de sa stratégie ;
- La mise en conformité au GDPR implique une **rationalisation des procédures** et une **plus forte digitalisation** ;
- Selon une étude réalisée par la firme bruxelloise Megabyte*, les entreprises belges ont un **niveau d'avancement assez faible** dans la transformation digitale ;

* Source : Tendances Trends

Conclusion

- Le fait de devoir se conformer au **GDPR** peut **forcer** les entreprise **à se digitaliser** et, tant qu'à faire, correctement selon les axes précités.
- Le **GDPR** et tout ce qu'il implique est donc une **aubaine** pour ne pas louper l'adaptation des entreprises à nos sociétés toujours plus connectées et ce, de manière propre, qualitative et sécurisée.

* Source : Tendances Trends

Conclusion

- Un **risque** existe cependant : l'**alourdissement** des procédures et la forte documentation peuvent ralentir les processus, ce qui peut entraver le rendement ou augmenter les coûts de production.
- Un **juste équilibre** doit donc être trouvé entre respect des exigences et le bon fonctionnement de l'entreprise sans perdre de vue finalement que…

Conclusion

- …oui, le GDPR est une charge supplémentaire pour l'entreprise mais c'est aussi l'opportunité de **s'améliorer au niveau qualitatif et sécuritaire**, de s'investir dans la qualité via un projet global de révision des processus selon les principes et axes suscités.
- Et communiquer à ce sujet peut faire partie de la politique **concurrentielle** de l'entreprise.

Merci pour votre attention.

CHU
UCL
NAMUR

Dinant • Godinne • Sainte-Elisabeth

www.chuuclnamur.be

CHU UCL Namur asbl, Av. Docteur G. Thérasse, 1 - B5530 Yvoir (Belgique)