IRON MOUNTAIN®

RGPD : LES RECETTES POUR DÉPLOYER UNE BONNE GOUVERNANCE DE L'INFORMATION

Un guide du forum virtuel
Physical Meets Digital

Au MENU

ENTREZ DANS UN MONDE EN PLEINE ÉVOLUTION

Le constat est unanime. Nous vivons dans un monde qui change. Les entreprises du XXI^{ème} siècle partagent volontiers l'idée selon laquelle le papier va disparaitre. Alors, comment garantir des processus documentaires uniformisés ?

Toute organisation réclame une information toujours plus disponible, un accès toujours plus rapide. Or cette idée ne touche pas uniquement les entreprises.

Il n'y a qu'à voir du côté des États. Dans le cadre de marchés publics, la facturation dématérialisée est obligatoire pour les grandes entreprises et les entreprises de taille intermédiaire, mais également pour les PME. Plusieurs avantages se dégagent : **plus de productivité, de sécurité, de transparence et de protection de l'environnement.**

Même au regard de l'administration française le raisonnement est : **pas d'archive physique mais de l'information !**

- Limiter la transmission de papier
- Faciliter l'accès à l'information
- Optimiser la prise de décision
- Réduire les temps de traitement

Autant d'objectifs qui ont besoin d'un cadre pour être accomplis. Les entreprises doivent trouver un nouveau cap et adapter leur gestion de l'information.

Dans la foulée du RGPD, il est temps de réfléchir aux flux d'informations pour déployer un programme garantissant la **fiabilité et l'accessibilité de l'information dans le strict respect de la réglementation en matière de conformité.**

Le but de ce cahier de recettes est de partager les bonnes pratiques du RGPD. Au menu : durée de conservation et confidentialité de l'information. Deux points importants qu'il est nécessaire de traiter.

Toujours dans le but d'améliorer vos performances, **retrouvez ici fiches recettes et fiches pratiques qui vous permettront de déployer une gouvernance de l'information conforme au RGPD.**

LES INDISPENSABLES POUR SE LANCER DANS UNE POLITIQUE RGPD

Fiche pratique pour une adaptation réussie des clients aux enjeux du RGPD

Se lancer dans la réalisation d'un bon menu peut parfois s'avérer plus complexe qu'il n'y parait. En effet, la gastronomie a des codes, qu'il convient de respecter. A-t-on les bons ustensiles ? Les règles de sécurité sont-elles respectées en cuisine ? Quel protocole suivre pour réussir sa mise en place ? Revenons ensemble sur les indispensables de la cuisine du RGPD.

L'aménagement de la cuisine et son équipement font partie des réflexions prioritaires. On ne fait pas de cuisine sans un plan de travail impeccable.

Il faut sortir du vrac numérique, de cette exposition de données, dans un environnement légal qui se durcit.

« Le but de la gastronomie est de veiller à la conservation des hommes au moyen de la meilleure nourriture possible » - Jean Vitaux

Evolution des méthodes de travail

Les ustensiles indispensables

- Externaliser les processus non stratégiques
- Automatiser les processus métiers clés
- Visibilité et prise de décisions

Gérer les risques

Les règles de sécurité de base

- Définir et appliquer une politique de gouvernance globale
- Maitriser les audits et les contrôles
- Eviter les failles de sécurité

Extraire la valeur des informations

Réussir son dressage

- Gérer le cycle de vie de l'information
- Assurer la restauration et la récupération des données
- Valoriser la data

LES DÉFIS DU RGPD POUR LUTTER CONTRE UNE MAUVAISE GOUVERNANCE DE L'INFORMATION

Fiche pratique pour une entreprise conforme au RGPD

Seuls 51% des entreprises ont signalé des incidents au cours des douze derniers mois.

Être conforme au RGPD du 25 Mai 2018

Simples, rapides et faciles à appliquer, les recettes proposées vous aideront à changer vos habitudes alimentaires.

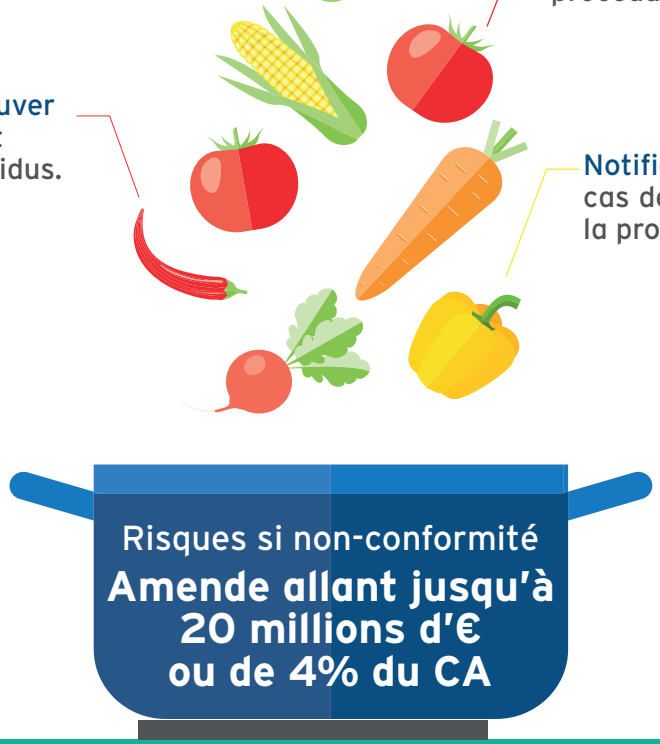
Garantir la sécurité de toutes les données collectées, traitées et stockées contre les risques de perte, de vol ou de divulgation.

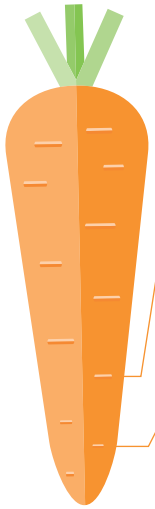
Recueillir et prouver le consentement éclairé des individus.

Garantir aux personnes physiques l'**accès**, la **modification**, la **restitution** et l'effacement de leurs données.

Documenter les mesures et procédures de protection.

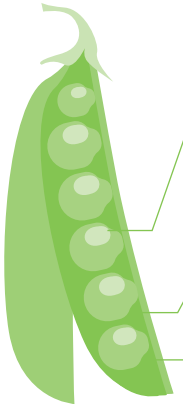
Notifier la CNIL sous 72h en cas de risque réel d'atteinte à la protection de la vie privée.





39% des entreprises décrivent leur gestion de messagerie comme « chaotique ». Pour 55% d'entre elles, le courrier électronique est considéré comme un contenu non étiqueté, non gouverné et à haut risque. Elles sont seulement 10% à archiver sélectivement leurs courriels.

20% des erreurs entrainant une perte de données sont dues à la négligence du personnel ou bien à une mauvaise pratique.



47% des entreprises ont une politique qui définit les périodes de conservation mais 51% comptent sur la suppression manuelle de contenu stocké.

15% utilisent une classification automatisée ou assistée.

Seuls **7%** des entreprises utilisent des outils d'analyse pour le nettoyage des données.

LE RGPD, UN GUIDE QUI CODIFIE LA PROTECTION DES DONNÉES

Mémo : Comment protéger vos données comme un chef

Changez de recette, il est temps de sublimer votre tambouille !
Avec l'application du RGPD concoctez quelque chose de simple, succulent et original.

Le RGPD, vrai Auguste Escoffier de la donnée

Le Chef Escoffier a développé le concept de brigade de cuisine, en rationalisant la répartition des tâches dans l'équipe et en veillant au comportement du cuisinier.

Le RGPD impose de nouvelles règles, fixe de vraies sanctions et détermine finalement une nouvelle manière de traiter les données personnelles.

Escoffier a modernisé et codifié la cuisine de Marie-Antoine Carême, créant ainsi de nombreuses recettes. De la même manière, le RGPD n'est pas un concept nouveau ! Il est hérité de la loi française de 1978 Informatique et liberté.

LA PROTECTION DES DONNÉES EN FRANCE

Se limiter au texte du RGPD serait une erreur !

La loi française apporte un cadre à l'entreprise. Ainsi, le RGPD s'applique en complément d'autres réglementations portant sur les données.

Par exemple le Contrat de Sécurisation Professionnelle pour les données de santé ou encore le Code des assurances.

CONFIDENTIALITÉ ET SÉCURITÉ : DEUX THÈMES PORTEURS DU TEXTE DU RGPD

Mémo : Comment bien respecter les DLC

De la même manière que chacun doit veiller à la propreté et à l'hygiène de la cuisine, chaque collaborateur doit être responsabilisé. Ne communiquons pas nos données personnelles à tout va, mais seulement quand cela est nécessaire !

Avis à chaque individu, et aussi au PDG !

Bien évidemment **le RGPD n'interdit pas d'avoir de la donnée personnelle.**
Mais celle-ci **doit être légitime pour la profession.**

Le **RGPD impose un niveau plus élevé de protection de la vie privée** pour les données collectées auprès de toute personne résidant dans l'UE.
De ce fait **la responsabilité des infractions peut atteindre le niveau du conseil d'administration**, en vertu des lois et de la jurisprudence en matière de violation de données.

Le risque de sécurité concerne tous les niveaux de l'entreprise. Attention aux pirates qui deviennent de plus en plus sophistiqués.

ATTENTION AUX DURÉES LIMITES DE CONSERVATION ET AUX DATES DE PÉREMPTION !

Le vrai challenge : se débarrasser de cette manie bien française de toujours tout conserver.

COMMENT FAIRE MONTER SA MAYONNAISE ?

Deux ingrédients phares : CONFIDENTIALITÉ et SÉCURITÉ.

- Se conformer aux politiques de conservation et de confidentialité.
- Ne pas conserver l'information plus longtemps que nécessaire (au risque d'encourir des coûts et des risques inutiles).
- Savoir retracer de manière fluide les changements de politiques aux propriétaires de contenu et à l'infrastructure.
- Prouver aux auditeurs que votre organisation est conforme.

On ne peut pas garantir de la sécurité si on maintient du vrac et l'incertitude ; il est nécessaire de savoir de quoi on parle.
Comment voir clair dans une cuisine si les inventaires ne sont pas dressés ? Pas question de partir au marché sans sa liste de courses !

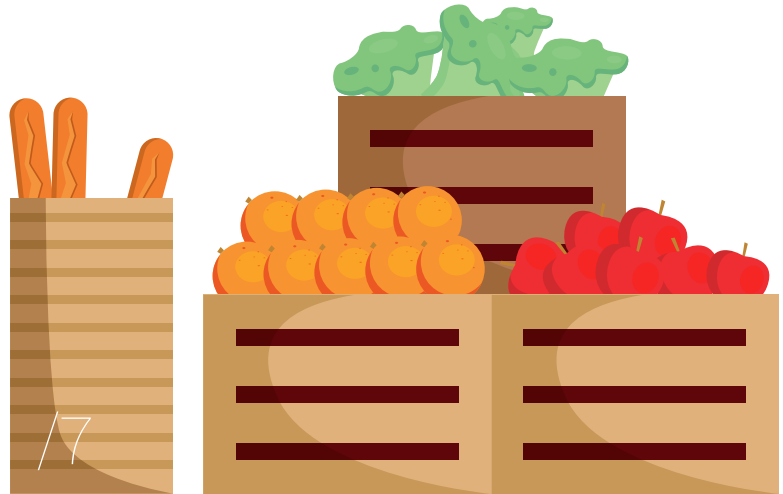
Le consentement au traitement est élargi

Il est **devenu nécessaire dans de nombreux cas**, notamment pour le **traitement de données sensibles.**
Telles que les données faisant apparaître : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques ou l'appartenance syndicale, données génétiques ou biométriques permettant d'identifier une personne physique de manière unique, médicales ou concernant la vie ou l'orientation sexuelle.

Le consentement doit être intentionnel (case dédiée à cocher, information spécifique, etc.)

Dès qu'une fonctionnalité logicielle, un progiciel, une application ou un programme traite des données personnelles dans le cadre de l'entreprise localisée dans l'UE et/ou traitant de données de personnes localisées dans l'UE, cette entreprise est concernée par le RGPD.

VOUS NE POUVEZ PAS SECURISER VOS DONNÉES SI VOUS NE SAVEZ PAS OÙ ELLES SE TROUVENT



LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT DES DONNÉES

Leçon pas à pas à l'égard du PDG, le responsable du traitement

S'il se passe quelque chose, l'entreprise est représentée au pénal par le PDG.
Qu'il s'agisse d'une PME ou d'une grande entreprise : le PDG est toujours la personne morale responsable devant les tribunaux.

1. **Changer tous les contrats** (clients et fournisseurs) et documents RH pour tenir compte du RGPD.
2. Avoir un **registre des activités de traitement.**
3. Désigner un **Data Protection Officer** (« DPO ») en cas de traitements nécessitant un suivi régulier ou en cas de traitements big data. Possibilité de désigner un DPO externe (avocats, etc...).
4. Tenir compte du RGPD dès la conception d'un programme ou d'un logiciel : **Privacy by design.** Dans le cadre d'un appel d'offres ou en cas de commande à un tiers : déterminer dès la conception ou l'achat d'une application, les données collectées, les traitements, les types de destinataires et la durée de conservation.
5. **Documenter toutes les procédures et liens contractuels** en vue de démontrer le respect du RGPD en cas de contrôle. Les contrats avec les tiers qui auront accès, ou à qui sont transférées des données personnelles, devront comprendre des mentions et thématiques obligatoires désormais.
6. Assurer une **sécurité informatique renforcée**, avec obligation, en cas de faille de sécurité, de la notifier à la CNIL dans les 72h et, dans certains cas, aux personnes concernées.
7. Être à jour dans **l'information et la sécurisation juridique** en cas de transfert de données hors de l'Union européenne.

ATTENTION AU COÛT DE VIOLATIONS DE DONNÉES

- Recours collectifs et recours dérivés des actionnaires
- Amendes et pénalités
- Perte de fidélité des clients
- Perte de revenus
- Érosion du cours des actions
- Publicité négative
- Dommages causés par le « capital de marque »
- Atteinte à la réputation de l'entreprise
- Augmentation des coûts d'exploitation
- Perte de propriété intellectuelle

LES DROITS DES PERSONNES DONT LES DONNÉES SONT TRAITÉES

Leçon pas à pas à l'égard du citoyen européen

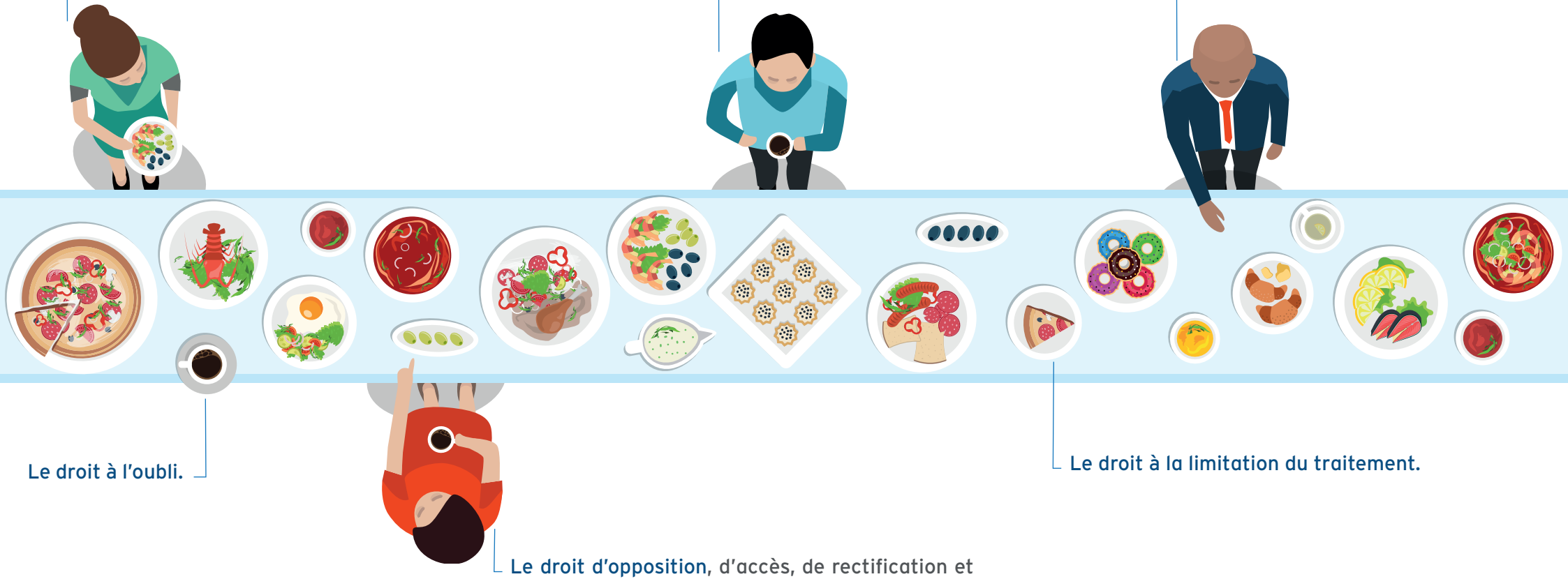
Un droit plein de vitamines pour booster vos défenses immunitaires ! On l'oublie bien souvent, mais le RGPD vise avant tout à protéger le citoyen européen ; bien plus qu'à contraindre les entreprises. Retour sur les ingrédients nécessaires du RGPD qui me protègent en tant qu'individu européen.

Le RGPD ajoute des droits à ceux existants sous la loi « informatique et libertés » et comprend ainsi :

Le droit à l'information (collecte loyale) sur les données collectées, la nature des traitements, les destinataires, les transferts éventuels hors UE, les droits dont dispose la personne, le droit de saisir la CNIL, etc.

Le droit à la portabilité des données personnelles pour les transférer ailleurs.

Le droit à une intervention humaine dans le cadre de prise de décision.



Le droit à l'oubli.

Le droit d'opposition, d'accès, de rectification et de suppression des données personnelles.

Le droit à la limitation du traitement.

LES SANCTIONS ENCOURUES

Fiche pratique pour éviter de passer à la casserole

De la même manière que le chef est responsable en cuisine de sa brigade, ici c'est bien le responsable de traitement qui est responsable. En effet, le RGPD précise qu'il appartient à chaque responsable de traitement de prouver qu'il respecte la réglementation et notamment les obligations de document.

Les tips pour passer à table en toute sérénité

Rester informé des sanctions qui tombent chaque semaine
Être à l'écoute, permet de se rendre compte plus vite des mutations et des transformations à venir.

Les observer afin de pouvoir proposer des services en conséquence.
Le RGPD a mis en œuvre un raisonnement de compliance ; les contrôles de la CNIL sont réalisés dans cet esprit.

Rendez-vous sur le site des organismes régulateurs de chaque pays pour se tenir informé des sanctions

3 ordres de sanctions prévus, souvent en concaténation

1. Les sanctions financières extrêmement dissuasives

Pour un manquement au	*Prévoir jusqu'à*
• Privacy by Design • Privacy by Default • PIA • etc...	10 millions d'€ ou 2% du CA annuel
• Droit des personnes (accès, rectification, opposition, suppression, ...)	20 millions d'€ ou 4% du CA annuel

2. Les sanctions pénales

Ces sanctions, moins bien maitrisées par les entreprises, peuvent conduire directement à la case prison sans passer par la case départ.

Jusqu'à 5 ans d'emprisonnement et 300 000€ d'amende

3. Le risque médiatique très fort

ÉTABLIR UNE STRATÉGIE DE GOUVERNANCE

Leçon pas à pas pour une cuisine saine

Chaque cuisine de restaurant doit mettre en place une stratégie pour respecter l'hygiène et la sécurité afin de réduire les risques pour ses clients. Préserver la salubrité des aliments en utilisant des techniques de conservation et de préparation des aliments, de nettoyages et de désinfection des ustensiles et des plans de travail... Autant d'enjeux qui imposent de générer une stratégie de manière rigoureuse.

1

Formaliser l'engagement de la Direction

2

Communiquer/ diffuser les éléments d'information du Règlement

3

Définir un plan de sauvegarde des données (P.S.D.)

4

Maintenir un registre des activités de traitement

5

Former et évaluer les collaborateurs

6

Evaluer et contractualiser les sous-traitants stratégiques

7

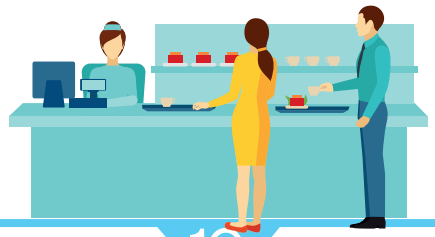
Respecter la vie privée dès la conception (P.B.D.)

8

Etudier l'impact sur la vie privée (P.I.A.)

9

Déterminer un plan d'audit des traitements



10

Respecter une procédure de signalement de violation des données à caractère personnel (data breach)

11

Respecter l'exercice des droits des personnes

12

Assurer le suivi de la politique générale de protection des données

LAISSEZ-VOUS SÉDUIRE PAR LES OPPORTUNITÉS DU RGPD

Pour conclure ce menu, voyez le RGPD comme une opportunité. Le RGPD ne doit pas être vu comme une sanction mais bien comme l'opportunité de développer le capital informationnel de son entreprise. Commencez votre farandole des desserts par le démêlement des durées de conservation. Puis brassez toutes ses notions pour définir votre propre référentiel.

Attention aux caries ! Le périmètre est très large, il suppose une démarche assez procédurale pour mettre en valeur le capital informationnel de votre entreprise.
Laissez-vous tenter par un dessert simple : c'est en allégeant le plus possible votre gâteau que vous serez le plus efficient.

Alors pour mettre en place une gouvernance de RGPD, c'est comme en pâtisserie, soyez précis dans vos pesées ! L'astuce est de suivre une méthodologie et de respecter la procédure définie.

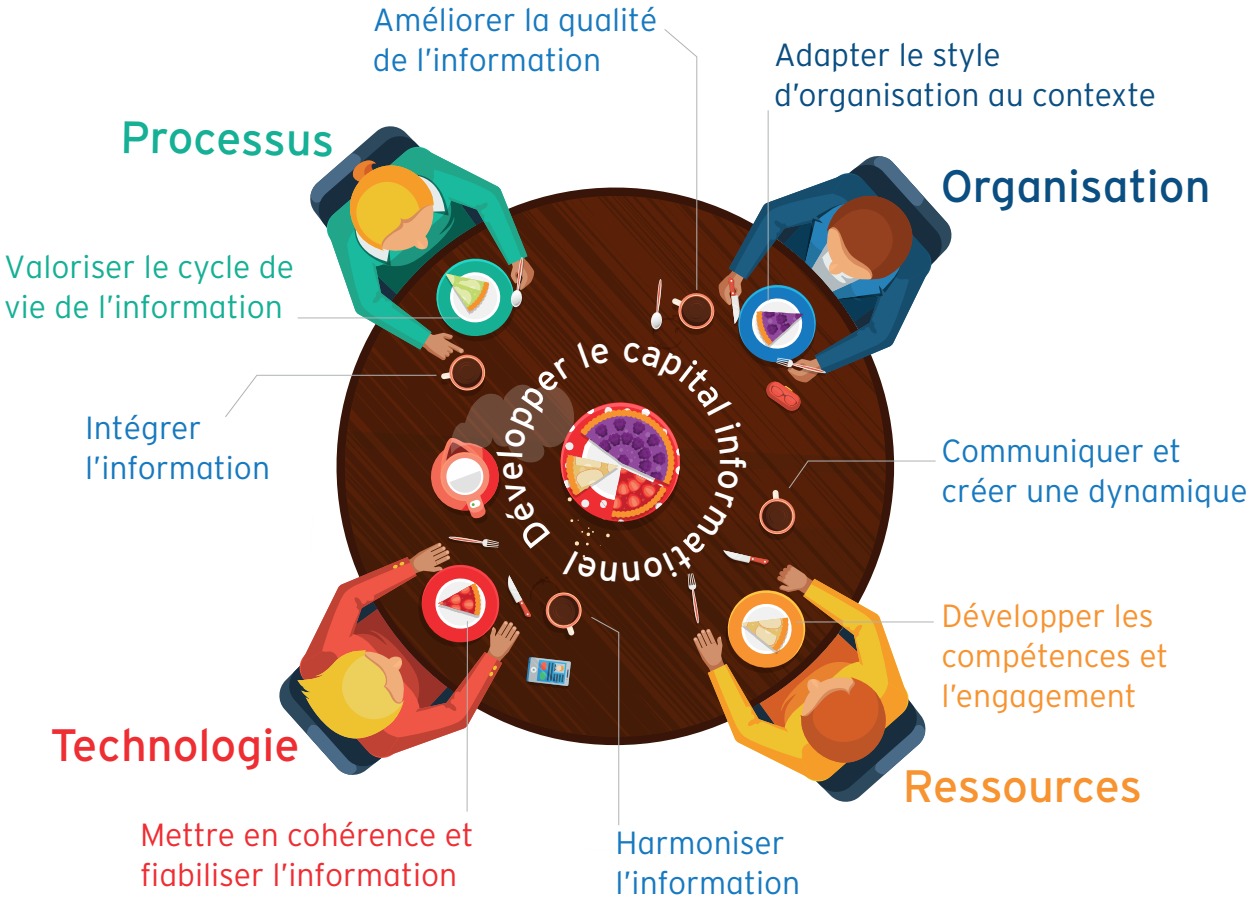
Et maintenant ?

Rassemblez les éléments nécessaires :

- Processus
- Technologie
- Organisation
- Ressources

Si vous respectez les recettes étape par étape, les dosages et les DLC, vous obtiendrez le développement de votre capital informationnel optimal.

A vous de jouer pour maîtriser le RGPD comme un chef !



IRON MOUNTAIN®

POUR ALLER PLUS LOIN...

Regardez le webinaire du forum virtuel Physical Meets Digital **intitulé « Le RGPD : une opportunité de déployer une gouvernance de l'information. »**

REGARDER LE WEBINAIRE MAINTENANT ▷

À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE : IRM) offre des services de gestion de l'information qui permettent aux entreprises de réduire leurs coûts, de limiter leur exposition aux risques et d'éliminer les inefficacités en matière de gestion des données numérisées et sur support physique. Fondée en 1951, la société Iron Mountain prend en charge la gestion de milliards d'actifs informationnels, tels que données de sauvegarde et d'archives, documents électroniques, imagerie documentaire, documents professionnels, destruction sécurisée, pour les entreprises du monde entier.

Visitez le site Web de la société à l'adresse www.ironmountain.fr pour obtenir des informations supplémentaires

Vous avez besoin de plus d'informations, d'aide ou de conseils?

CONTACTEZ NOUS AU : 0800 215 218 ou WWW.IRONMOUNTAIN.FR/CONTACT-US

IRON MOUNTAIN®