## **Respectez les obligations en termes de données personnelles à l'heure du RGPD**

La protection des données à caractère personnel est une des facettes du **droit au respect de la vie privée**. Ce droit est garanti et protégé par des textes à valeur constitutionnelle. De surcroît, ces textes sont supra nationaux :

* la **Convention européenne de sauvegarde des droits de l'Homme**. Son article 8 dit que "*toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance*".
* la **Charte européenne des droits fondamentaux**. Son article 7 indique que "*toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications*". Surtout, son article 8, Protection des données à caractère personnel, dit que :
  + "*toute personne a droit à la protection des données à caractère personnel la concernan*t" ;
  + "*Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification*";
  + "*Le respect de ces règles est soumis au contrôle d'une autorité indépendante*".

Le droit français a été **pionnier** en la matière : la loi dite *informatique et libertés*, adoptée le 6 janvier 1978, est l'une des premières législation qui traite de manière globale les questions qui naissent du rapprochement de l'informatique, des fichiers et des libertés !

C'est également en 1978 qu'est créée la **CNIL**, la *Commission nationale de l'informatique et des libertés*, qui est l'autorité chargée de veiller au respect de cette législation.

La protection des données à caractère personnel a progressivement pris une dimension toute particulière avec l'avénement de l'ère du numérique. :o Les illustrations abondent :

* Les *wikileaks*, l'affaire Snowden, les vols de données personnels contenus dans les fichiers d'Uber, l'affaire Facebook-Cambridge Analytica...
* Le marketing qui développe des outils de *profiling* grâce aux multiples données que les utilisateurs laissent lors de l'utilisation des services.
* Les utilisations possibles désormais du *big data*, le traitement de données en masse.

Il y a donc un besoin de mieux encadrer et d'assurer la protection des données personnelles. Les règles qui s'appliquent sont issus du **paquet européen de protection des données**, adopté par le Parlement européen le 27 avril 2016.

* Le règlement (UE) 2016/679 dit règlement général sur la protection des données (**RGPD**) ;
* La directive (UE) 2016/680 relative aux traitements de données personnelles mis en œuvre à des fins de prévention et de détection des infractions pénales.

|  |  |  |
| --- | --- | --- |
| **Instrument** | **entrée en vigueur** | **abroge et remplace** |
| Règlement (UE) 2016/679 | 25 mai 2018 | directive 95/46/CE |
| Directive (UE) 2016/680 | 6 mai 2018 | décision-cadre 2008/977/JAI |

Le Parlement français a adopté une nouvelle loi afin d'adapter le droit et les institutions nationales à ce nouveau dispositif, la **loi relative à la protection des données personnelles**.

**Synthèse du RGPD**

Les **sources** du régime juridique applicable en France sont :

* le règlement (UE) 2016/679 ;
* la loi Informatique et libertés de 1978 (modifiée par la loi de 2018). Cette loi est augmentée d'un nouveau chapitre rassemblant l'ensemble des règles applicables aux **traitements de données à caractère personnel en matière pénale** (issues de la directive 2016/680).

Le nouveau dispositif cherche à concilier la protection des droits fondamentaux des individus, sans entraver la libre circulation des données, considérée comme un levier de croissance.

Cet objectif est atteint par un changement de paradigme, abandonnant le régime gradué d'autorisation *a priori,* pour y substituer un contrôle *a posteriori* avec une **obligation de documenter la conformité** du traitement des données aux principes protecteurs inscrits dans le règlement.

Quant aux**droits substantiels**, le règlement maintient et conforte les droits des personnes physiques sur leurs données à caractère personnel, tels que le droit d'information. Il en créé de nouveaux tel que le droit à l'effacement des données ("droit à l'oubli") ou le droit à la portabilité des données.

**Le champ d'application du RGPD**

**Le champ territorial**

Comme il s'agit d'un règlement européen, **tous les États membres** appliquent le même texte.

Il restera néanmoins des **différences entre les législations** des États membres car le règlement prévoit certaines marge d'aménagement.

Par exemple, le règlement dispose que l'âge à partir duquel un mineur peut consentir à une offre directe de services de la société de l'information est fixé à 16 ans, mais il offre la possibilité aux États membres d'abaisser cet âge jusqu'à 13 ans.

La protection des données personnelles bénéficie donc de **règles harmonisées**au sein de l’Union européenne lesquelles sont :

* applicables à tous les acteurs sur le territoire de l’Union européenne,
* et applicables aux opérateurs installés hors de l'Union européenne dès lors qu'ils offrent des biens et des services aux citoyens européens.

S'ajoutent des règles imposant une coopération plus étroite entre les autorités nationales des États membres pour appliquer ce jeu de règles unique.

Par exemple, les entreprises présentes dans plusieurs marchés (européens) ne doivent plus faire face à des décisions potentiellement contradictoires des autorités nationales.

**Le champ matériel**

Le nouveau régime s'applique aux **traitements** de **données à caractère personnel**, que ce traitement soit automatisé en tout ou en partie, ou non automatisé, dès lors qu'elles seront contenues dans ou appelées à figurer dans un **fichier**.

Chaque terme est important et explique que le champ d'application du régime de protection est extrêmement large.

**Traitement** : toute opération (procédé automatisé ou non) telle que la collecte, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion, toute mise à disposition, le rapprochement et l'interconnexion, la limitation, l'effacement ou la destruction.

*Concrètement* : les informations utilisées par la fonction RH, la géolocalisation d'un véhicule employé par un salarié, un fichier client, la tenue des comptes clients, le partage d'une base de contacts...

**Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement. Ce peut être un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, un élément d'identité physique, physiologique, génétique, psychique, économique, culturel ou social.

*Concrètement* : la couleur des yeux, de la peau ou des cheveux, une infirmité, la taille, le poids, les croyances religieuses, l'appartenance politique, le niveau de vie, la fonction professionnelle, les pratiques sexuelles, les goûts alimentaires, le passe-temps...

**Fichier** : tout ensemble structuré (de données personnelles) accessible selon des critères déterminés, centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique.

L'action (traitement de données à caractère personnel) est mise en œuvre par une *personne*, qui est qualifiée de **responsable du traitement**. Là encore, la notion est très large : une personne physique (un individu) ou morale (société, association, fondation... ), une autorité publique, un service ou un organisme qui, seul ou conjointement avec une ou plusieurs autres personnes, détermine les finalités et les moyens du traitement.

Dès lors que l'action consistant à traiter des données à caractère personnel est mise en œuvre par une entité, le régime de protection s'applique.

**Les principes du RGPD**

**Principes directeurs**

Le traitement des données à caractère personnel doit se conformer à des **principes directeurs**, au nombre de 7 (art. 5, règlement 2016/679).

**1° Licéité, loyauté et transparence**

Les données doivent être traitées de manière**licite, loyale et transparente**.

Par conséquent, vous devez informer la personne concernée du traitement des données, obtenir son consentement, exclure la pratique de l'*opt-out*.

**2° Limitation des finalités**

Les données sont collectées pour des**finalités déterminées**, explicites et légitimes.

Nuance : le traitement ultérieur à des fins d'archivage dans l'intérêt public, de recherche scientifique, historique ou statistique est considéré comme compatible avec les finalités initiales.

**3° Minimisation des données**

Les données à caractère personnel qui font l'objet du traitement doivent être adéquates, pertinentes et **limitées à ce qui est nécessaire**au regard de la finalité du traitement.

C'est une exigence de proportionnalité, qui vous oblige, en tant que responsable du traitement, à ne viser que le "strict minimum" selon la finalité de votre traitement des données.

**4° Exactitude**

Les données doivent être **exactes** et, le cas échéant, **tenues à jour**.

Cette obligation de mise à jour vous oblige à prendre toutes les mesures raisonnables pour que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées.

**5° Limitation de la conservation**

Les données sont nécessairement conservées sous une forme permettant l'identification des personnes concernées **pendant une durée n'excédant pas celle nécessaire** au regard des finalités pour lesquelles elles sont traitées.

Si, à des fins d'archivage, une durée plus longue de conservation est possible, c'est à la condition que vous mettiez "en œuvre les mesures techniques et organisationnelles appropriées (respect du principe de minimisation, pseudonymisation) afin de garantir les droits et libertés de la personne concernée".

**6° Intégrité et confidentialité des données**

Le traitement est effectué de manière à **garantir une sécurité** appropriée des données.

Ce principe vous oblige à prendre les mesures, notamment techniques et organisationnelles, qui garantissent contre un accès ou une utilisation non autorisés ainsi que contre la perte et la destruction accidentelle.

**7° Responsabilité**

Enfin, il est prévu que vous, en tant que responsable du traitement, devez être en mesure de démontrer le **respect de ces principes directeurs**.

C'est bien en cela qu'il y a une obligation de documenter la conformité de votre traitement au regard des principes généraux.

**Licéité du traitement**

Il ne suffit pas de mettre en œuvre un traitement qui satisfasse aux principes directeurs que l'on vient de voir ; encore faut-il que le traitement soit **licite**.

Il sera licite dès lors qu'il **répond à l'une au moins** des conditions suivantes :

* la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
* le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
* le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
* le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
* le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
* le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

**Mettez en œuvre le RGPD**

Le RGPD s'applique à vous dès lors que vous communiquez en ligne, gérez des données de clients, clients potentiels ou fournisseurs ou lorsque vous conservez des données.

C'est une **logique de contrôle *a posteriori***  qui s'applique, et le respect des droits des personnes repose principalement sur une logique de responsabilisation des entreprises.

**Respectez le règlement**

Vous devez tout d'abord respecter le règlement, c'est-à-dire que vous devez respecter les droits des personnes protégées (concernées par les données).

Cela signifie que vous devez alors :

* fournir une **information extensive** sur le traitement des données aux personnes concernées ;
* organiser un **droit d'accès** à ces informations ;
* organiser un **droit de rectification et d'effacement** (droit à l'oubli) ;
* tenir compte du **droit à la limitation du traitement** ;
* organiser la **portabilité des données**.

Par principe, les traitements portant sur des catégories particulières de données à caractère personnel (données portant sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses... ; données génétiques ou biométriques, données concernant la santé ou la vie sexuelle d'une personne physique) sont interdits.

Ces données ne peuvent être traités qu'à certaines conditions énoncées à l'article 9 du RGDP.

**Documentez la mise en œuvre du traitement**

Ensuite, vous devez documenter la mise en œuvre de votre traitement afin de garantir et démontrer que vous vous conformez aux principes directeurs.

En pratique, l'enjeu essentiel est donc celui de l'identification des **obligations de documentation** de sa propre conformité : le règlement prévoit des outils de conformité.

Pour faciliter cette identification (et donner une plus grande sécurité juridique aux acteurs du secteur) vous pouvez vous appuyer sur diverses sources et outils :

* La **Commission européenne** publie des questions/réponses et des analyses.
* Le **CPDP**, Comité de la protection des données personnelles, publie des lignes directrices.
* La **CNIL**, au niveau national, développe des analyses et offre des outils de conformité.

Par exemple, le [logiciel PIA](https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) (privacy impact assessment) est un logiciel libre d'utilisation (open source) que la CNIL met à disposition des responsables de traitement, afin de faciliter votre conduite d'une analyse d'impact qui est une des modalités exigée par le régime RGDP.

Dès lors que vous mettez en place un traitement de données à caractère personnel, il vous faut identifier l'outil de conformité à mettre en place. Ils sont au nombre de trois.

**(1) Le registre des activités de traitement (art. 30 du RGPD)**

Cet outil doit être mis en place dès que l'on met en œuvre un traitement et le RGDP indique les éléments qui doivent y figurer.

**(2) Le délégué à la protection des données (art. 37 du RGDP)**

Dès lors que vous êtes dans l'un des trois cas ci-dessous, vous devez désigner un DPD (**DPO** en anglais, pour *Data Protection Officer*, qui est l'acronyme que tout le monde utilise) :

* Le traitement est effectué par une autorité publique (sauf les juridictions) ;
* Les activités de base du traitement consistent en des opérations qui exigent un suivi régulier et systématique à grande échelle des données personnelles ;
* Les activités de base du traitement consistent en un traitement à grande échelle de catégories particulières de données (celles de l'article 9 du RGPD).

Le **DPO** peut être membre de l'organisation (salarié, par exemple) ou un tiers (contrat de service). Il est désigné en fonction de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

Il doit accomplir les missions suivantes :

* informer et conseiller le responsable du traitement sur ses obligations ;
* contrôler le respect du RGPD ;
* dispenser des conseils concernent l'analyse d'impact qui doit éventuellement être réalisée ;
* coopérer avec l'autorité de contrôle ;
* faire office de point de contact pour l'autorité de contrôle.

**(3) L'analyse d'impact (art. 35 du RGPD)**

Dès lors que le traitement que vous envisagez est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, il est exigé d'effectuer, **avant** la mise en place du traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Ce risque s'identifie notamment à raison du recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

L'évaluation doit porter sur l'origine, la nature, la particularité et la gravité du risque que le traitement fait naître. La loi européenne précise le **contenu** de cette analyse en indiquant que l'on doit y retrouver *a minima* les éléments suivants :

* une description systématique du traitement et de ses finalités, ainsi que la précision de l'intérêt légitime poursuivi ;
* l'évaluation de la nécessité et de la proportionnalité du traitement par rapport aux finalités poursuivies ;
* une évaluation des risques pour les droits et libertés (des personnes physiques concernées) ;
* les mesure envisagées à cet égard, afin de protéger les données à caractère personnel.

Si votre analyse d'impact révèle un **risque élevé** à défaut de mesures prises par le responsable du traitement, vous devez consulter l'autorité de contrôle (en France : la CNIL).

**Assurez votre conformité au RGPD**

Aspects pratiques : la check-list de conformité (ou les [6 étapes de la RGPD](https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes))

|  |  |  |
| --- | --- | --- |
| **Étape** | **Action** | **Ressources** |
| 1. | Désigner un pilote (un DPO) | Guide CNIL : [Devenir DPO](https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees) |
| 2. | Établir un registre des activités (cartographie des traitements de données personnelles) | [Modèle de registre](https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx) |
| 3. | Prioriser les actions à entreprendre |  |
| 4. | Gérer les risques | [Guides CNIL étude d'impact (PIA, *privacy impact assessment*)](https://www.cnil.fr/fr/PIA-privacy-impact-assessment) |
| 5. | Organiser les processus internes | Téléservice de notification de violation (site CNIL) |
| 6. | Documenter la conformité |  |

Si vous êtes concerné, vous devez impérativement envisager 4 actions principales :

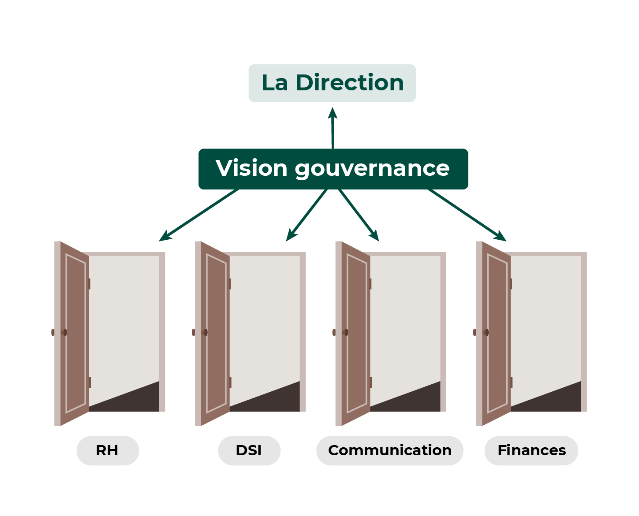
1. **Constituer un registre de vos traitements de données** (étape 2 ci-dessus, en vous aidant du modèle de registre), ce qui suppose de formaliser l'objectif poursuivi, les différentes catégories de données utilisées, d'identifier qui a accès aux données et de préciser la durée de conservation.
2. **Faire le tri dans vos données**, en déterminant quelles sont les données réellement nécessaires et si, parmi celles-ci, il y en a qui relèvent de la catégorie des données dites sensibles.
3. **Respecter les droits des individus** en mettant en œuvre une politique de transparence (au moyen de mention ou de renvoi à un document de politique de confidentialité) et en permettant aux personnes d'exercer leurs droits (accès, rectification, opposition, effacement, portabilité).
4. **Sécuriser vos données** en adoptant les mesures raisonnables et nécessaires afin de garantir la sécurité des données. En l'absence de risque zéro, ce seront les process mis en place, la surveillance constante et l'efficacité des mesures qui permettent de contenir votre risque juridique.

**GOUVERNANCE DES DONNEES**

Définition :

Mettre la donnée au cœur de l’entreprise au service de toutes les entités en vue d’aider à la stratégie d’entreprise.

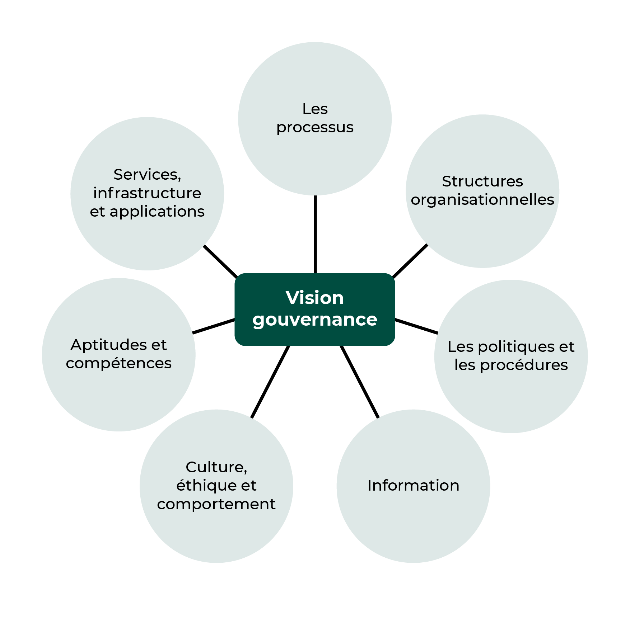
On a donc besoin d’une stratégie DATA au service de la stratégie des différents services au service de la stratégie d’entreprise

MDG : **master data governance** : c’est « piloter » les données au service d’une stratégie plus globale : éthique personnelle et professionnelle, stratégie commerciale plus globale, etc

* + **Le MDM et la MDG sont ainsi parfaitement complémentaires, mais la MDG vous ouvre les portes d’une vision plus large, plus complète, plus maîtrisée des données de votre entreprise.**

1. **Les grands principes de la gouvernance**

La gouvernance des données est la concrétisation de ce que l’on appelle **l’alignement stratégique** : **L’alignement stratégique**, c’est la mise en place de processus uniformisés au sein de l’entreprise, qui vont permettre de faire concorder les objectifs et la volonté politique de la direction avec les actions des services opérationnels et du métier. La stratégie data est au service des stratégies métiers, qui sont au service de la stratégie d’entreprise !

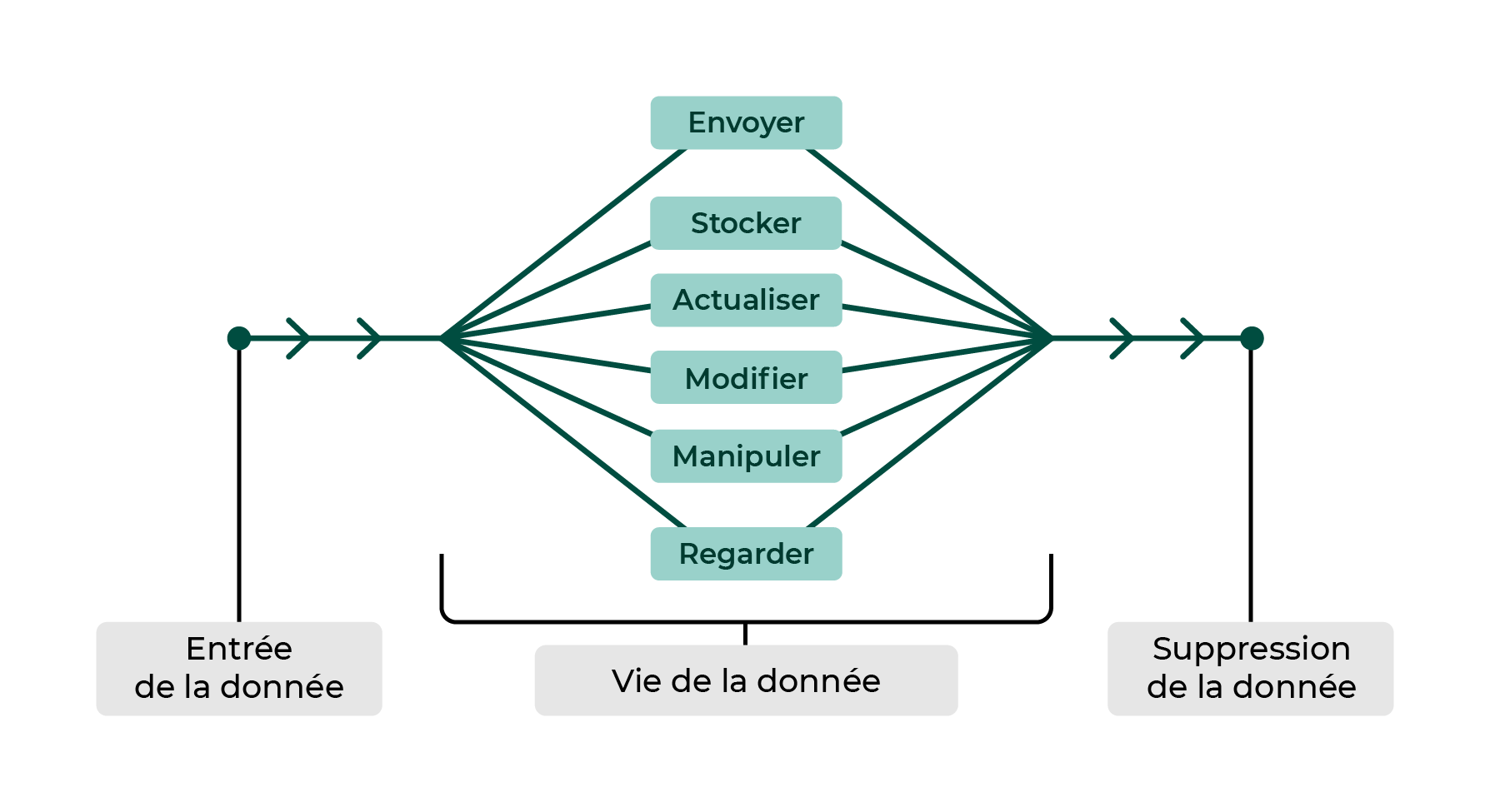
* + 1. **Démarche globale de gouvernance :**

**Les objectifs de la gouvernance des données :**

* **Définir et communiquer les stratégies**, les politiques, les normes, l'architecture, les procédures et les paramètres relatifs aux données ;
* **Suivre et assurer le respect des réglementations** et de la conformité aux politiques, normes, architectures et procédures en matière de données ;
* **Augmenter la confiance en interne**;
* **Encourager et superviser la réalisation de projets** et de services de gestion des données ;
* Gérer et **résoudre les problèmes** liés aux données plus facilement ;
* Comprendre et **promouvoir la valeur** des données.
  + **La stratégie de gouvernance des données est dans l’alignement direct de la stratégie d’entreprise et des objectifs. C’est ce qu’on appelle l’alignement stratégique.**

**L’objectif de la gouvernance des données est de créer de la valeur !**

1. **CARTOGRAPHIE ET CYCLE DE VIE DES DONNEES**

****

***Projet 7 :***

***Service RH : données qui proviennent du SIRH à l’embauche de l’employé***

***DRH : ils ont accès aux informations (salaires, nom et prénom, sexe, adressse, email, numéro de téléphone***

***Mort des données : diagnostic par an***

1. **Bien connaitre les portes d’entrée par lesquelles vos données entrent dans l’entreprise afin de bien les répertorier en tenant compte des contraintes**
   * **3 sources d’informations principales qui vont alimenter nos systèmes de données :**

* **Outils internet : site web, application mobile etc**
* **Partenaires : qui délivrent des données de manière contractuelle**
* **Données externes : open data délivrées par l’INSEE ou acheter à des concurrents etc**

**Exemple :**

**Les informations qui sont issues des sites internet** :

* Données qui viennent des « devices » utilisés directement par les clients (site internet, mobile, pc) qui envoient les données aux serveurs,
* Et des données qui arrivent quand il y a interaction entre le client et le site web

Ces 2 sources d’informations ne vont pas nous remonter le même nombre de clients sur le site web selon si les users acceptent ou non les cookies, un portable derrière un pare-feu, etc

Il est important de comprendre comment est faite la collecte en prenant en compte les contraintes.

****

1. **Répertorier les données de l’entreprise**

**3 grandes catégories de données :**

1. **Les données personnelles**

Elles permettent d’identifier une personne : nom, prénom, date de naissance, photo, email, adresse postale, coordonnées bancaires, adresse IP, données de consommation, etc

1. **Les données publiques**

Toutes les données produites par une administration dans l’exercice de ses missions de service public (dossier, rapports, stats, codes sources, etc). Ce sont les **informations publiques**

1. **Les données privées**

Données protégées par d’autres types de droits (ex : droit d’auteur, secret des affaires)

**SUPPRIMER LES DONNEES DE VOTRE ENTREPRISE**

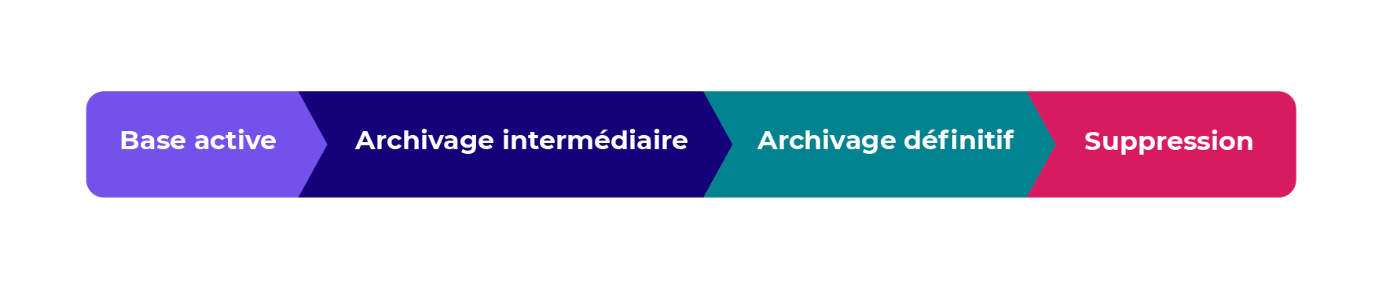
Ça vous est sans doute déjà arrivé : en fouillant dans vos archives, vous retrouvez plusieurs anciennes bases de données qui ne vous ont pas servi depuis des années, et vous vous dites : **« Je la garde, au cas où »**. Voilà exactement le type de réaction à éviter !

Oups… 😨

Si chaque donnée paraît essentielle aux équipes métiers (qui veulent souvent tout garder !), déterminer une durée de vie à vos données fait partie de l’action de tri et de classification nécessaire à une bonne gouvernance. Sous peine d’être enseveli très rapidement par des millions de données inutiles !

Une donnée n’a souvent pas une fin de vie brutale, et sa disparition peut s’étaler dans le temps :

* Elle est d’abord dans ce qu’on appelle la **base active**, et répond à une utilisation courante : elle est nécessaire à vos activités quotidiennes ;
* Elle peut ensuite passer dans une phase d’**archivage intermédiaire** : la donnée ne vous est plus utile tous les jours, mais elle conserve encore un intérêt administratif pour votre société (gestion d’un éventuel contentieux, par exemple) ;
* L’**archivage définitif**est une étape supplémentaire : parce qu’elle a une certaine valeur et un intérêt pour l’entreprise, la donnée peut être archivée de manière pérenne ou définitive ;
* Enfin, la donnée peut être **supprimée** définitivement.

Fin de vue de la donnée, de la base active à la suppression

La suppression d’une donnée peut également prendre plusieurs formes. Par exemple, plutôt qu’une suppression sèche, on pourra préférer un **processus d’anonymisation**.

Un processus d’anonymisation ?

**L'anonymisation** d’une donnée personnelle est le fait, par la suppression d’autres informations ou par un degré de précision moindre, de rendre totalement impossible l’identification d’une personne.

**PLAN D’ACTION DE GOUVERNANCE**

**Identifier les actions de conformités au RGPD au droit des données personnelles.**

**Plan d’action : Identifier qui fait quoi, comment et dans quel ordre.**

**Pk fait-on tout ça ?**

**Respecter le RGPD est une obligation légale, c’est aussi une stratégie de communication et d’éthique de l’entreprise.**

**Notre Cartographie des données c’est un tableau excel, ou un logiciel simple d’utilisation**

**Plan d’action un doc word partagé en interne connu de tous librement accessible qui explique pourquoi on mène ces actions de gouvernance et comment elles sont réalisées.**

**La Gouvernance des données est un travail collectif et partagé.**