

Livre Blanc RGPD

Enjeux et opportunités dans les banques et assurances

DE LA MISE EN CONFORMITE A LA MISE EN ŒUVRE
OPERATIONNELLE. LA DONNEE, CHALLENGES ET
OPPORTUNITES POUR LES ORGANISATIONS FACE A LEURS
CLIENTS. UN ENJEU DURABLE ET A VALEUR COMMERCIALE
BIEN AU-DELA DE L'ASPECT REGLEMENTAIRE.

Préambule

L'objectif de ce Livre Blanc n'est pas simplement de retracer les grands principes du Règlement à la Protection des Données (RGPD), mais de partager le positionnement d'ACI partners sur le sujet. En effet, si cette réglementation est sujette à remettre en cause une grande partie des process et infrastructures existantes au sein des grands organismes bancaires et assurantiels, elle peut être une réelle source de valeur ajoutée – à condition de mesurer l'ampleur des transformations à l'œuvre. La confiance entre les différentes parties prenantes, incluant le consommateur, dans le traitement des données personnelles est un axe déterminant dans la réussite de ce processus de mise en conformité.

La problématique qui se pose dans ce contexte est la suivante : au-delà de la mise en conformité, comment puis-je en tirer un profit commercial et/ou améliorer mon image ?

Dans ce Livre Blanc, il nous semble ainsi bénéfique d'exposer les points structurants permettant de transformer cette contrainte réglementaire en un atout, participant à la qualité de la relation clientèle et à la confiance que chaque client doit avoir en sa banque, son assureur ou plus généralement son prestataire de service. L'accompagnement du changement et le besoin d'une solide gouvernance de la donnée sont deux aspects déterminants de la démarche.

De façon plus générale, la valorisation de la donnée est un axe majeur qui découle directement de cette réglementation et qui touche, compte tenu des bouleversements technologiques à l'œuvre, toutes les entreprises.

Table des matières

1. Les principes clés du RGPD	4
1.1 QU'EST-CE QUE LE RGPD ?	4
1.2 DEFINITIONS ET PERIMETRE D'APPLICATION	4
1.3 LE RGPD EN PRATIQUE	9
1.4 LES ETAPES DE MISE EN CONFORMITE	12
1.5 LES SANCTIONS EN CAS DE NON-RESPECT	13
2. Les problématiques RGPD chez nos clients	14
2.1 LES CHALLENGES AUXQUELS ILS FONT FACE	14
2.2 LES POINTS D'ATTENTION A NE PAS NEGLIGER	14
3. Notre approche pour les accompagner	15
3.1 UNE APPROCHE TRANSVERSE BASEE SUR UNE SOLIDE EXPERTISE	15
3.2 UN CABINET PLURIDISCIPLINAIRE APPUYE PAR DES PARTENARIATS D'EXPERTS	16

1. Les principes clés du RGPD

1.1 QU'EST-CE QUE LE RGPD ?

Le Règlement Général sur la Protection des Données (RGPD)¹ est entrée en vigueur le 25 mai 2018 au niveau européen, retranscrit par la CNIL au niveau national. Il fait suite aux problématiques de protection des données personnelles qui n'étaient pas inscrites dans les précédentes réglementations; son objectif principal étant de définir les contours d'une réglementation commune en matière de protection des données au sein des Etats de l'Union Européenne.

Il impose aux organismes de renforcer la protection des Données à Caractère Personnel (DCP) des personnes physiques concernées par la collecte ou le traitement de données personnelles.

Les objectifs de cette réglementation peuvent ainsi se résumer en trois mots : confiance, transparence, responsabilité.



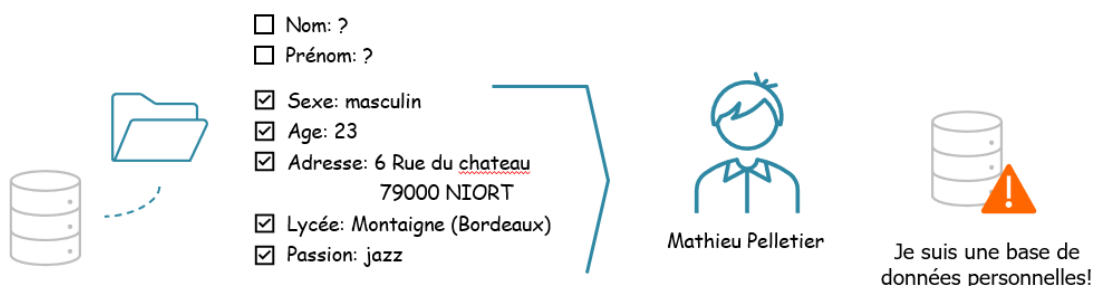
- **Confiance** | Le respect du RGPD est un gage de confiance dans les relations avec les différentes parties prenantes
- **Transparence** | Le respect du RGPD permet aux organismes concernés de gérer les données de façon totalement transparente et encadrée par un cadre strict aux yeux du régulateur au niveau national et européen
- **Responsabilité** | Le respect du RGPD implique une responsabilisation des organismes traitant des données personnelles vis-à-vis des parties prenantes

1.2 DEFINITIONS ET PERIMETRE D'APPLICATION

• Donnée à Caractère Personnel

On définit une *Donnée à Caractère Personnel* (DCP) comme toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

*Toute information se rapportant à une **personne physique identifiée ou identifiable** (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.²*



¹ En anglais « General Data Protection Regulation » ou GDPR

² Source : CNIL

La notion d'identification est cruciale ; elle peut en effet se faire de deux façons :

- **De façon directe** | Exemple : nom, prénom
- **De façon indirecte** | Exemple : identifiant (n° client), numéro (de téléphone), donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image

Il existe différentes catégories de données à caractère personnel en fonction du niveau de sensibilité de la donnée; on distingue ainsi :

- Les données personnelles « standard »
- Les données personnelles dites « sensibles » aussi appelées données « à risque »

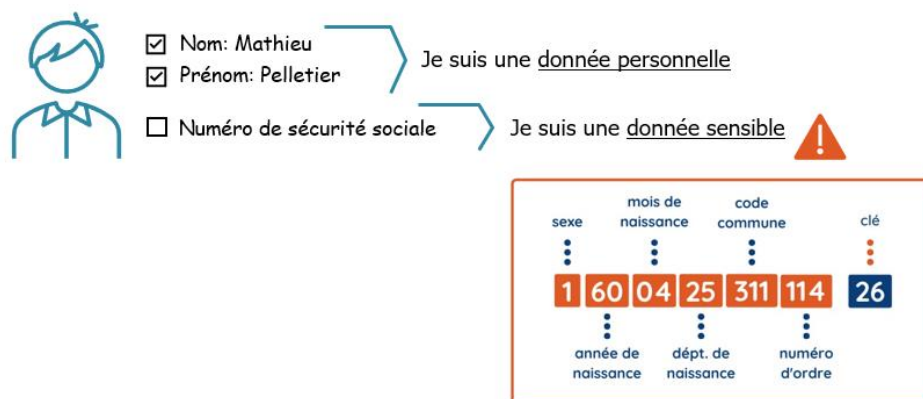
*Les **données sensibles** sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.*

Exemple : Le nom/prénom sont des données personnelles, tandis que le numéro de sécurité sociale est une donnée caractérisée comme sensible.

Point d'attention Le RGPD interdit de recueillir ou d'utiliser ces données sensibles, sauf dans les cas suivants :

- Si la personne concernée a donné son consentement dans le cadre du traitement de ses données sensibles (démarche active, explicite, écrite, qui doit être libre, spécifique, et informée) ; il s'avère nécessaire de structurer les processus afin de collecter le consentement de la personne concernée – ce qui ne relève pas simplement de la « non-opposition » au traitement mais bien de la formulation d'un consentement explicite
- Si les informations sont manifestement rendues publiques par la personne concernée
- Si elles sont nécessaires à la sauvegarde de la vie humaine
- Si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL
- Si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale

Dans le cas où des données sensibles seraient collectées dans le cadre de l'activité, un traitement particulier leur est réservé. Le Numéro de Sécurité Sociale en est l'exemple le plus parlant. En effet, il est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE. Dans la mesure où il est unique à chaque personne, particulièrement identifiant et signifiant, son utilisation présente d'important risques quant à l'identification d'un individu.



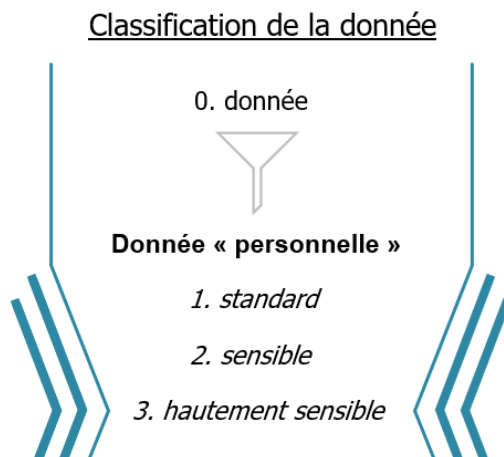
Des mesures sont ainsi mises en œuvre pour encadrer strictement son usage, selon les deux grands principes suivants établis par la CNIL :

- Son usage est essentiellement limité à la sphère « santé-social-travail »
- L'utilisation du NIR doit systématiquement faire l'objet d'une autorisation préalable de la CNIL

Point d'attention Il existe dans les outils informatiques utilisés des « Zones de Texte Libre » (ZTL) qui permettent d'assurer notamment la gestion des dossiers clients ou le suivi de la relation avec un prospect. Il est strictement interdit de faire apparaître dans ces zones des données dites « sensibles » ! En effet, il est nécessaire de garder en tête que la personne dont les données ont été collectées peut demander à tout moment à avoir accès au contenu de ces zones. Il est par ailleurs interdit d'y inscrire tout commentaire à caractère désobligeant, insultant, raciste, sexiste..

• Cartographie des DCP

De façon plus approfondie, les données personnelles peuvent se décomposer finement en plusieurs macro-catégories en fonction de leur niveau de criticité ; chaque catégorie de données définie faisant ainsi l'objet d'un traitement spécifique. On peut aisément différencier 3 niveaux de criticité : « *standard* », « *sensible* », « *hautement sensible* ».



Vous trouverez ci-dessous une extraction de la cartographie des différentes catégories³.

Type d'informations données à titre d'exemples		Niveau de classification DCP		
Type de données	Description	DCP1 Standard	DCP2 Sensible	DCP3 Hautement Sensible
Données de gestion clients	Données administratives (assurances, garanties) : - Données de gestion administrative (n° de contrat,...),	X		
Données de gestion clients	Données administratives incidents : - Gestion des sinistres, - Rapport d'expert,...		X	
Données de gestion clients	Données médicales clients			X
Données de gestion interne	Intranet	X		
Données de gestion interne	Clés cryptographique		X	
Données de gestion interne	Mot de passe		X	
Données PCI-DSS	Données monétiques, Données d'identification sensibles - Données complètes de piste magnétique (ou équivalent sur une puce) - Tout type de cryptogramme, piste, puce, visuel (CAV2/CVC2/CCV2/CID...) - Code/bloc PIN			X
Données PCI-DSS	Données monétiques, Données du titulaire : - PAN (numéro de carte)		X	
Données PCI-DSS	Données monétiques, Données du titulaire : - Nom, Prénom - Date de validité / d'expiration - Code Service	X		
Données personnelles	Données d'identité Nom et prénom	X		
Données personnelles	Régime matrimonial		X	
Données personnelles	Données biométriques ou génétiques			X
Données personnelles RH	Responsable hiérarchique	X		
Données personnelles RH	Contrat		X	
Données personnelles RH	Donnée de santé salarié			X

³ Ces catégories de DCP sont données à titre d'exemple ; un référentiel complet est fourni par la CNIL.

En fonction de la classification et de l'utilisation des données personnelles dans le cadre de l'activité, il est nécessaire de fixer des règles de gestion de la donnée. On pense nécessairement à la suppression irréversible de ces données personnelles, principe premier du RGPD, mais également au processus d'anonymisation ou de pseudonymisation ou encore à une définition des habilitations (i.e. les personnes qui peuvent avoir accès directement à ces données au contraire des personnes qui doivent en faire la demande à une personne référente).



Vous trouverez ci-dessous le détail de chaque moyen de traiter la conservation des données personnelles :

- ✓ **Pseudonymisation** : on la définit comme un « *traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire* » – on peut remonter à la personne concernée via une clé de rapprochement
- ✓ **Anonymisation** : on la définit comme « *un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible* » – on ne peut plus remonter à la personne concernée
- ✓ **Purge** : on peut définir la purge comme la « *suppression physique de l'ensemble des données personnelles* » à l'issue de la durée de conservation définie en amont – on ne peut plus remonter à la personne concernée

Ce travail est nécessairement en lien avec la gestion des habilitations. Par exemple, si les départements métiers n'ont plus d'utilité à consulter la donnée personnelle, elle peut être gardée en cas de potentiel recours au sens du RGPD. Dans ce cas, cela oblige l'organisme à la conserver plus longtemps, mais il est possible de restreindre les accès aux départements métiers et de structurer une démarche d'accès à la donnée dans les procédures internes.

• Traitement DCP

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé.

On définit un **traitement de données à caractère personnel** comme une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).⁴

Le RGPD impose que tout traitement de DCP ait une finalité identifiée et répertoriée i.e. l'objectif poursuivi par la collecte et la conservation de données personnelles. Il est en effet nécessaire de définir la légitimité i.e. le fondement qui sert d'appui à la collecte de la donnée, qu'on peut désigner sous le terme de « base légale ». De manière plus spécifique, il est également nécessaire de gérer les habilitations reliées à cette même donnée – quelle est la procédure d'accès ? Qui a accès à la donnée ? Est-elle réservée à une population bien précise au sein de l'organisation ? Tous ces points sont autant de questions à traiter et retranscrire dans les procédures internes.

Les éléments principaux à garder en tête sont les suivants : au-delà de la tenue d'un référentiel des traitements et la définition d'une durée de conservation et finalité pour chaque traitement de données personnelles, il est nécessaire de veiller à la mise en œuvre d'habilitations en fonction de la criticité des données personnelles. Il faut également toujours avoir à l'esprit que les personnes disposent de droits qui leur permettent à tout moment d'avoir une vue sur le traitement de leur données personnelles stockées chez un tiers.

Exemple : Les données candidat sont conservées par les ressources humaines durant tout le processus de recrutement (du premier contact au choix définitif des candidatures); elles n'ont ensuite plus de raison d'être conservées et doivent donc être supprimées. Les personnes en charge des recrutements peuvent accéder aux CV durant cette période.

⁴ Source: CNIL

Autre exemple : Les personnes qui n'ont plus de produits d'assurance chez leur ancien assureur, et dont les données personnelles doivent être supprimées à l'issue de la durée définie.

Le processus de contrôle est un axe déterminant, le contrôle permanent étant une des briques de la démarche de mise en conformité.

Périmètre d'application

Le Règlement RGPD a vocation à s'appliquer aux traitements de données à caractère personnel qui ont lieu sur le territoire de l'Union Européenne, à ceux qui touchent des ressortissants européens, mais aussi à ceux pour qui le responsable de traitement (i.e. « *data controller* ») et/ou le sous-traitant (i.e. « *data processor* ») sont établis sur le territoire de l'Union européenne ; que le traitement de données personnelles soit effectué de façon automatisée, semi-automatisée ou manuelle.

Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. [...] Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ; un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union seulement dans le cadre de certaines activités ; un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.⁵

Principe d'Accountability

L'accountability est un principe issu de l'Article 5 du RGPD désignant « *l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* »⁶.

Concrètement, ce principe s'inscrit à travers des livrables documentaires qui doivent être classés par thème, centralisés et conservés sous forme électronique et/ou papier par le DPO dans un dossier conformité ou « dossier d'accountability », décrivant de manière circonstanciée la gouvernance appliquée par l'entreprise sur les données qu'elle traite. Ce dossier structuré de livrables est destiné aux audits réalisés par les autorités auprès des organismes concernés par le RGPD, afin de prouver la mise en place de mesures adéquates et pertinentes au sein de ces mêmes organismes.

Exemple : Tenir à jour un registre des traitements avec la finalité et la durée de conservation retenue pour chaque traitement, rédiger et conserver une procédure de gestion des violations de données ou une procédure sur la gestion des droits d'accès RGPD...

Les documents de gouvernance sont ainsi un prérequis dans la démarche de mise en conformité. On peut distinguer trois grands niveaux de gouvernance : la politique générale, les procédures et outils utilisés et enfin les adhésions métiers. C'est cette dynamique descendante qui permet d'engager une transformation à tous les niveaux au sein de l'organisation.



⁵ Source: CNIL

⁶ Source: CNIL

Il est ainsi nécessaire de définir un schéma descendant qui permette de traiter les éventuelles problématiques, tant au niveau des procédures/dispositifs définis que de la mise en œuvre au n des départements métiers.

1.3 LE RGPD EN PRATIQUE

Après avoir défini les différents éléments qui constituent le RGPD, nous allons nous attarder sur les grands principes qui définissent le RGPD ainsi que les droits des personnes concernées vis-à-vis du traitement de leur données personnelles.

Les grands principes Il existe 6 grands principes qui définissent le RGPD dans son application effective au sein des organismes.



Principe de minimisation Les données personnelles doivent être adéquates, pertinentes et limitées au strict nécessaire au vue de la finalité visée par leur traitement

Exemple: La collecte et la conservation du statut marital d'un salarié n'apparaît pas nécessaire à l'activité du service des ressources humaines

Principe de limitation à la conservation Collecter les données personnelles qu'à des fins spécifiques et ne conserver les données que pour une durée nécessaire

Exemple: Les données d'un candidat non retenu seront conservées pendant 2 ans maximum (sauf s'il en demande l'effacement) par le service des ressources humaines

Principe de responsabilité Le responsable de traitement se doit de respecter les principes fondamentaux et le démontrer, être transparent au regard de la personne concernée

Exemple: La constitution d'un registre des traitements de données personnelles fait partie de la documentation minimale requise

Principe de l'exactitude des données Garantir l'exactitude et la mise à jour des données personnelles

Exemple: La mise à jour d'une adresse dans un dossier client à la suite d'une procédure de déménagement

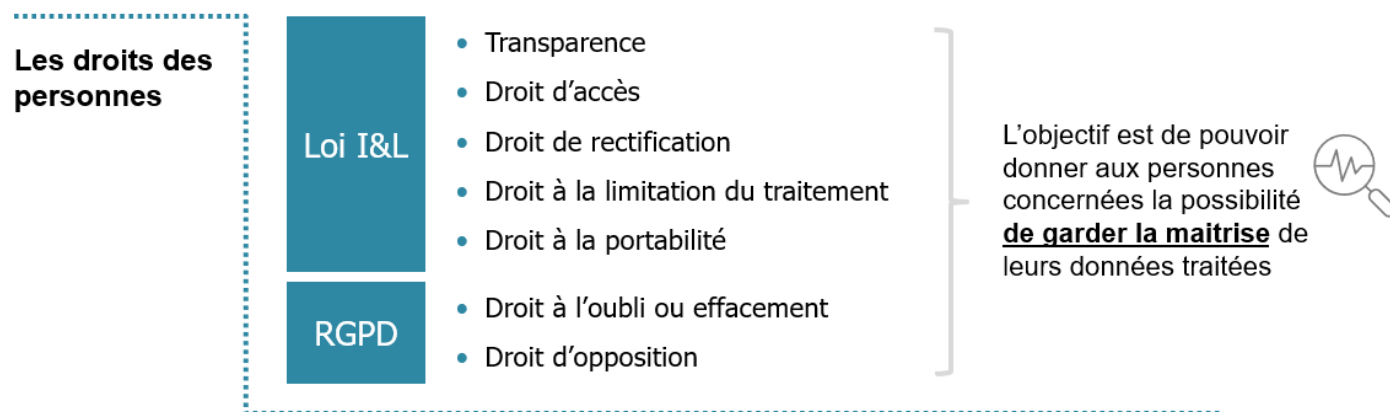
Principe de légitimité, de loyauté et de transparence Traiter de manière licite, loyale et en toute transparence les données personnelles au regard de la personne concernée

Exemple: La personne donne son accord à un organisme d'assurance pour la collecte des données de santé

Principe d'intégrité et de confidentialité Garantir une sécurité du traitement des données appropriée

Exemple: Le système de gestion des données est sécurisé via des habilitations aux personnes ayant accès aux données

Les droits des personnes Il existait initialement dans la Loi Informatique et Libertés cinq droits que les personnes pouvaient exercer vis-à-vis du traitement de leur données personnelles ; auxquels s'ajoutent désormais deux nouveaux droits instaurés par le Règlement RGPD, que sont le *droit à l'oubli* ainsi que le *droit à la portabilité*.



- **Transparence** – Toute personne a le droit de connaître la raison de la collecte des différentes données les concernant, de comprendre le traitement qui sera fait de leurs données, d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits
Exemple: une personne peut demander lors de la souscription à une assurance auto combien de temps sera conservé le permis de conduire, document obligatoire pour effectuer la souscription
- **Droit d'accès** – Toute personne peut demander à avoir accès aux données personnelles traitées par un organisme, qui doivent ainsi être communiquées sous un délai d'un mois dans un format compréhensible
Exemple: une personne souhaite contrôler l'exactitude des données utilisée dans le cadre de son assurance habitation
- **Droit de rectification** – Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite
Exemple: une personne peut demander la modification de son adresse postale à sa banque en cas de déménagement sur présentation d'un justificatif de domicile
- **Droit à la limitation du traitement** – Toute personne peut demander à un organisme de geler temporairement l'utilisation de certaines de ses données personnelles
Exemple: une personne demande de rectifier certaines de ses données personnelles à son assurance, l'organisme devra ainsi geler les données le temps de la procédure de vérification
- **Droit à la portabilité** – Toute personne a la possibilité de récupérer une partie de ses données personnelles dans un format ouvert et lisible par machine, lui permettant ainsi de les stocker ou les transmettre facilement d'un système d'information à un autre, en vue de leur réutilisation à des fins personnelles ; à noter que cela ne concerne que les données faisant l'objet d'un traitement automatisé
Exemple: une personne peut demander l'extraction des données personnelles collectées à sa banque
- **Droit à l'oubli ou effacement** – Toute personne peut demander expressément par voie électronique ou papier la suppression de données personnelles qu'elle ne juge pas utile dans le cadre de l'activité d'un organisme
Exemple: demander la suppression de données bancaires lorsqu'il n'y a pas lieu à une facturation
- **Droit d'opposition** – Toute personne peut s'opposer à tout moment à ce qu'un organisme utilise certaines de ses données

Exemple: une personne qui reçoit des e-mails à des fins publicitaires sur sa boîte personnelle et ne souhaite plus figurer dans la base de prospection peut demander à ne plus être dans cette base et destinataire des e-mails

Cas particulier de la fuite ou violation de DCP

On définit une violation des données au sens du RGPD comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. »⁷

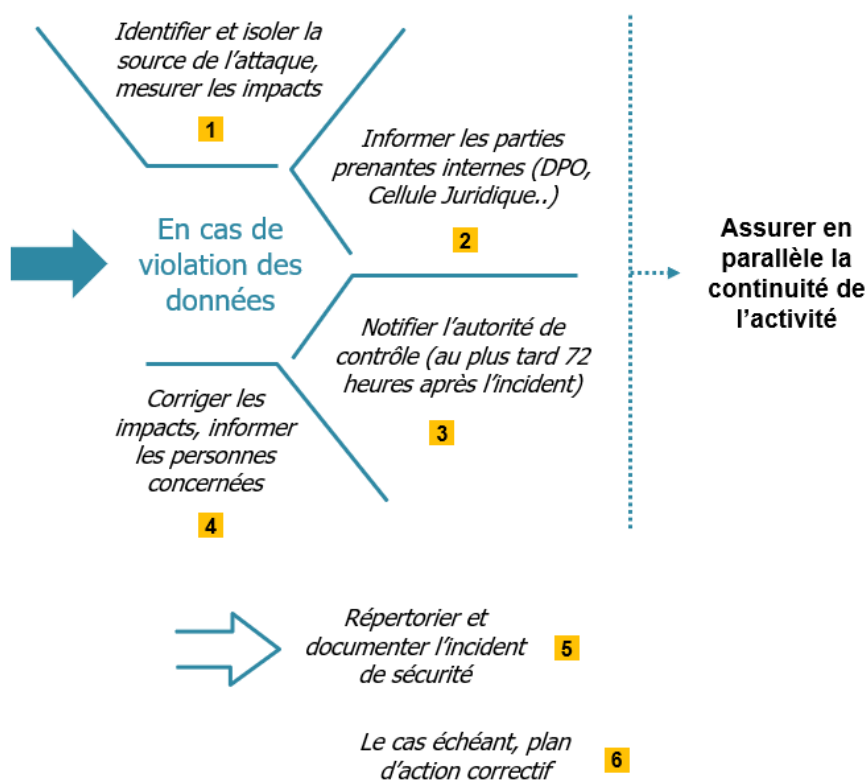
« Dans ce cas, et s'il est probable que la **violation engendre un risque pour les droits et libertés d'une personne**, votre entreprise/organisation doit notifier l'autorité de contrôle dans les meilleurs délais, et au plus tard 72 heures après avoir pris connaissance de la violation. Si votre entreprise/organisation est un sous-traitant des données, elle doit notifier chaque violation de données au responsable du traitement des données. Si la violation de données engendre un risque élevé pour les personnes affectées, ces dernières devraient alors également en être informées à moins que des mesures de protection techniques et organisationnelles efficaces ou d'autres mesures qui garantissent que le risque n'est plus susceptible de se matérialiser aient été prises. En tant qu'organisation, il est essentiel de mettre en œuvre des mesures techniques et organisationnelles appropriées pour éviter d'éventuelles violations de données. »⁸

Les mesures techniques et organisationnelles permettent d'éviter qu'un cas de violation des données personnelles ne se produise. Néanmoins, que faire en si un tel cas se présente ?

Les préconisations RGPD

- Documenter la mise en conformité au sein d'un registre des traitements
- Gérer les habilitations et accès au différentes briques informatiques
- Structurer le circuit de traitements des données personnelles
- Assurer un suivi des données personnelles de leur collecte jusqu'à leur destruction in fine
- Prévoir une procédure spécifique et un circuit de remontée d'alerte
- Maintenir une politique de sécurité
- Sensibiliser les départements métiers aux enjeux RGPD
- Former les départements métiers en cas de remontée d'alerte
- ...

Mettre en œuvre des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident



Nous voyons ainsi qu'il est impératif en amont de définir des process et procédures qui puissent palier un tel incident. Dans le cas où un tel incident de sécurité se produirait, il est essentiel d'une part d'identifier rapidement et de façon structurée les processus impactés ; d'autre part d'informer les différentes parties prenantes – que ce soit en interne (référénts DPO/Cellule Juridique) mais également en externe (CNIL et personnes concernées par l'incident). Un des éléments complexes est d'assurer en parallèle la continuité des activités, sans remettre en cause la sécurité ou la sensibilité des traitements de données personnelles. Enfin, il paraît nécessaire de catégoriser et répertorier l'incident dans les processus internes afin d'éviter qu'un même cas puisse se présenter dans le futur – le cas échéant appliquer un plan d'action correctif à la suite de cet incident.

⁷ Source: CNIL

⁸ « Qu'est-ce qu'une violation de données et que doit-on faire en cas de violation de données? » EC Europa

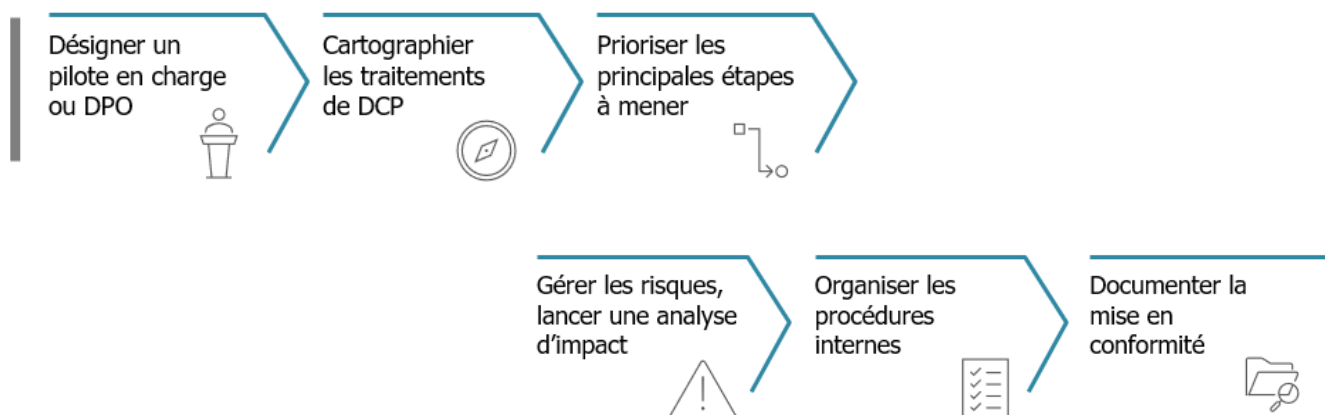
On voit bien que le RGPD en pratique suppose une adaptation de l'organisation à tous les niveaux en termes de gouvernance. Dans ce cadre, comment structurer la démarche de conformité ?

1.4 LES ETAPES DE MISE EN CONFORMITE

Le processus de mise en conformité ne peut se faire qu'en suivant un chemin défini d'étapes obligatoires afin d'assurer une mise en conformité globale de l'organisme.

Ce processus se décompose plus précisément en 6 grandes étapes, recommandées par la CNIL.

Processus défini par la CNIL



1. Désigner un « pilote » pour la gouvernance des données personnelles ou DPO

Le Délégué à la Protection des Données ou « DPO » est un véritable chef d'orchestre de la mise en conformité qui exercera une mission d'information, de conseil et de contrôle en interne; il est dans le prolongement du « correspondant informatique et libertés » chargé d'organiser les actions à mener pour être en conformité l'organisme.

La question du DPO est relié à une problématique de gouvernance ; il se doit en effet d'avoir une place en 1^{ère} ligne pour assurer ses différentes missions. C'est la raison pour laquelle, il est souvent directement rattaché au Secrétariat Général ou bien à la Direction Juridique, la Direction Conformité ou la Direction du Contrôle Interne.

Si l'entité n'est pas de taille conséquente, un DPO suffit à piloter le processus de mise en conformité. En revanche, si l'on a affaire à un grand groupe, il est préférable de nommer un DPO (ou Cellule DPO) au niveau groupe ainsi que des correspondants DPO dans les différentes entités du groupe afin d'établir une pyramide de transfert efficace.

• Data Protection Officer

Le DPO ou Délégué à la Protection des Données est en charge de conseiller de manière indépendante le responsable du traitement et s'assurer que le RGPD est bien respecté dans l'organisation. Il a donc un réel rôle d'accompagnement de l'organisme qui comprend notamment les missions suivantes:

- ✓ Informer et conseiller le responsable du traitement quant aux obligations en matière de protection des données personnelles ; cela implique de mener des actions de sensibilisation et de formation
- ✓ Contrôler le respect du RGPD – au travers d'audit de mise en conformité
- ✓ Dispenser des conseils sur demande – notamment en ce qui concerne la PIA
- ✓ Gérer les interactions avec la CNIL (ou toute autre autorité de contrôle) et à ce titre, il fait office de point de contact avec elle

Les organismes ont ainsi l'obligation de nommer un DPO dans les trois cas suivants :

- Si vous êtes un organisme public ou une autorité publique
- Si vous procédez à un suivi à grande échelle de personnes
- Si vous traitez des données sensibles (ex: données de santé) à grande échelle

2. Cartographier les traitements de données personnelles

Il s'agit de mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez ; ce qui commence par un recensement précis des traitements de données personnelles via la constitution d'un registre des traitements ainsi qu'une identification pour chaque traitement de la finalité visée.

Registre des traitements Le registre des traitements doit comporter une fiche pour chaque activité recensée répertoriant les informations suivantes relatives aux données personnelles :

- L'objectif poursuivi i.e. la finalité
- Les catégories de données utilisées
- La/les personne(s) qui ont accès aux données i.e. le destinataire
- La durée de conservation de ces données personnelles

3. Prioriser les étapes à mener

Sur la base du registre de traitements, il faut identifier les actions à mener pour être conforme aux obligations du RGPD ; cette priorisation s'établit au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées.

4. Gérer les risques et lancer une étude d'impact

Pour chaque traitement de données personnelles identifié comme susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il faut mener une Analyse d'Impact sur la Protection des Données (AIPD). Cette AIPD permettra notamment de définir le cadre du d'application traitement ainsi que l'objet de la collecte des données personnelles afin d'encadrer les risques identifiés.

5. Organiser les procédures internes

Pour assurer un haut niveau de protection des données personnelles en permanence, il faut mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles.

Exemple: faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire...

6. Documenter la conformité

Pour prouver la conformité au RGPD, il faut enfin constituer et regrouper la documentation obligatoire dans un dossier centralisé. Il est également nécessaire de réexaminer et actualiser à chaque étape les actions/documents réalisés afin d'assurer une protection des données en continu; cela rejoint le principe d'accountability évoqué plus haut en cas d'audit réalisé par les autorités.

1.5 LES SANCTIONS EN CAS DE NON-RESPECT

Des sanctions pécuniaires sont infligées aux organismes ne respectant pas le Règlement RGPD – jusqu'à **20 millions d'euros** ou dans le cas d'une entreprise jusqu'à **4% du chiffre d'affaires** annuel mondial ; sanctions qui peuvent être rendues publiques. De plus, ce processus de sanction a un fort impact sur l'image et la réputation des organismes, identifiés comme non-responsables vis-à-vis des données qu'ils traitent.

Exemple: Des sanctions ont été prononcées à l'encontre de Google et Amazon, pour leurs entités qui exercent des activités au sein de l'Union Européenne – 60 millions € à l'encontre de GOOGLE LLC, 40 millions € à l'encontre de GOOGLE Ireland Limited, 5 millions € à l'encontre d'AMAZON Europe Core⁹.

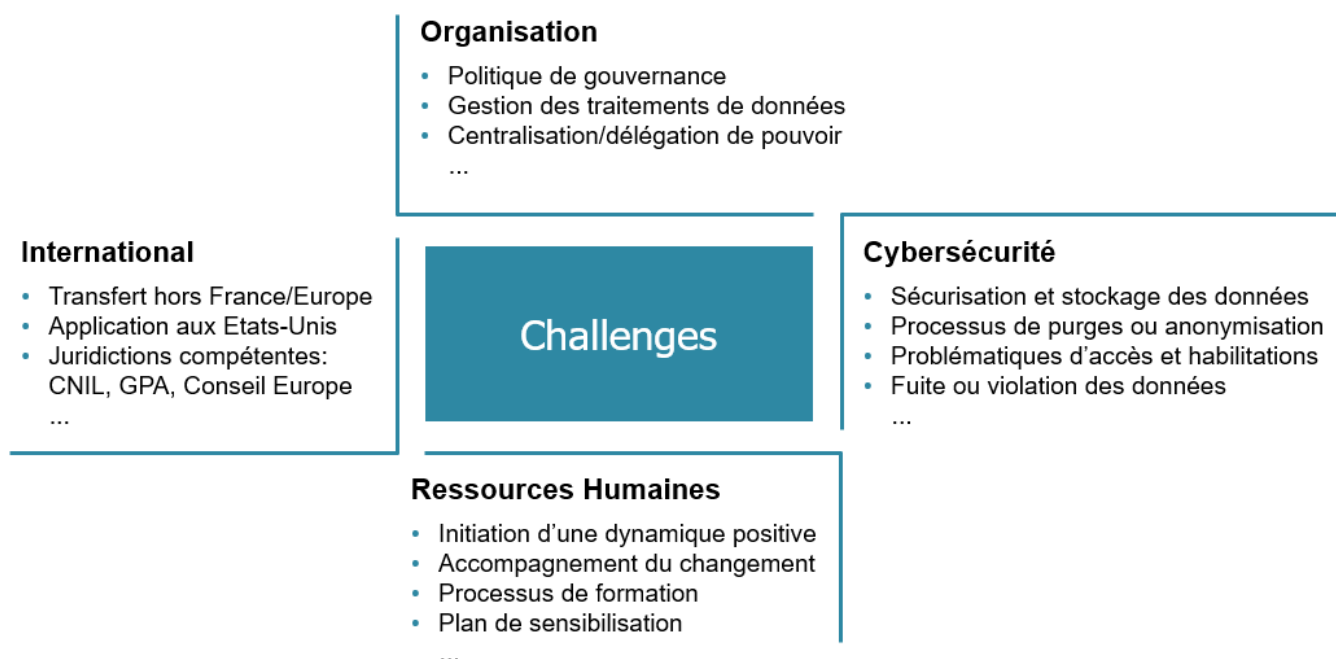
⁹ Pénalités prononcées en date du 10/12/2020 par la CNIL

2. Les problématiques RGPD chez nos clients

2.1 LES challenges auxquels ils font face

Le Règlement RGPD induit des enjeux qui dépassent le simple périmètre de la gestion de la donnée.

Parmi les principaux challenges auxquels sont confrontés les acteurs, nous pourrions par exemple citer les menaces de cybersécurité ou bien des problématiques organisationnelles, mais également la dimension internationale du traitement des données à caractères personnelles.



L'idée est de faire un tour d'horizon des principaux challenges liés à la gestion de la donnée ; cette représentation n'étant qu'une vue partielle des enjeux.

Les secteurs les plus exposés sont bien évidemment les organismes d'assurance (qui traitent notamment de la « donnée sensible » liée à la santé), les organismes bancaires ou encore les secteurs exposés sur le plan digital. D'une façon plus générale, tous les organismes qui traitent de données personnelles, que ce soit au sein des frontières nationales/européennes ou en dehors de l'Europe sont soumis à des règles strictes visant principalement à la protection de la vie privée des personnes.

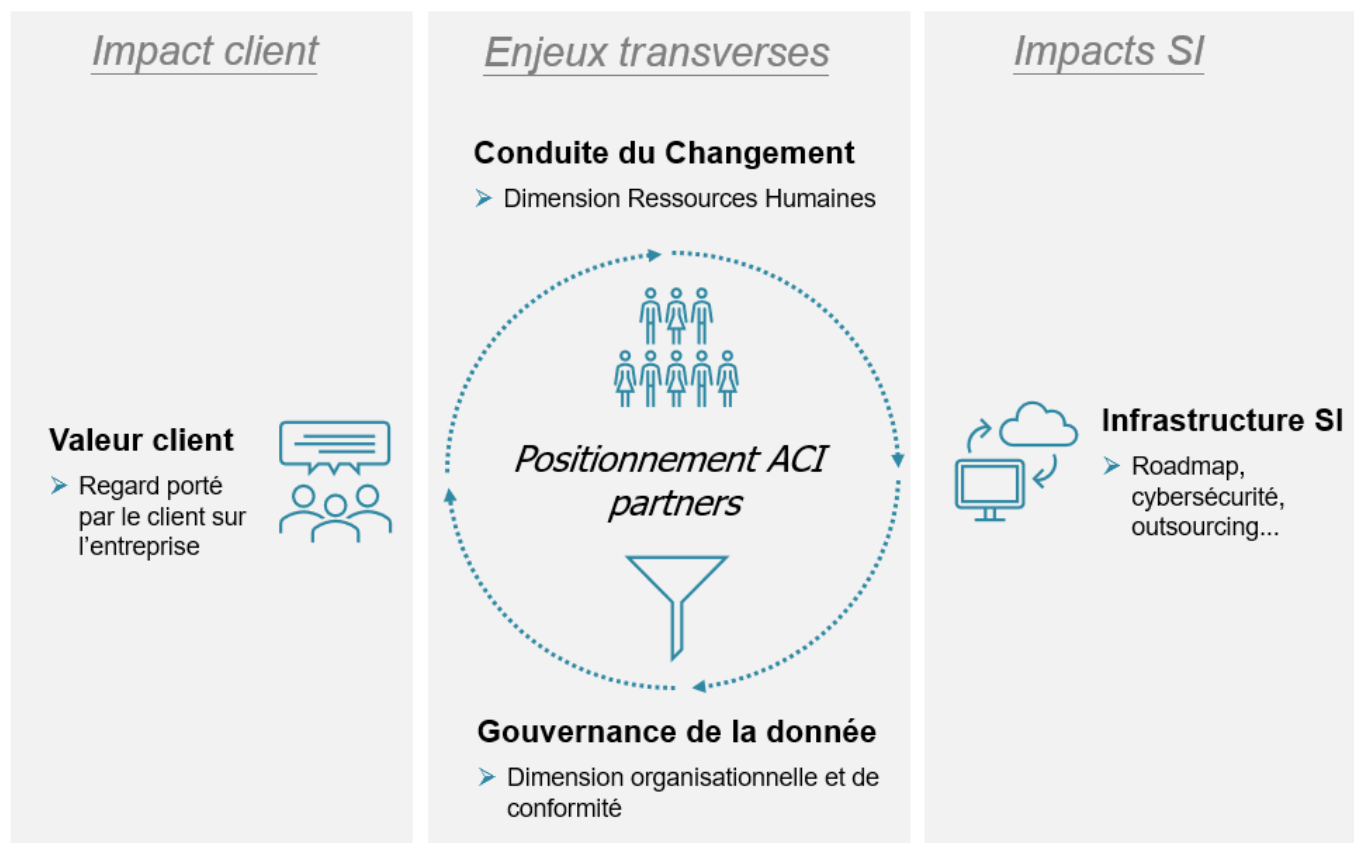
2.2 LES points d'attention à ne pas négliger

Le Règlement RGPD s'inscrit dans une approche transverse de mise en conformité, pour laquelle il ne faut pas négliger certains axes clés qui permettront d'avoir une approche complète du sujet.

On pense par exemple à la structure des systèmes d'information. En effet, plus cette structure est complexe et articulée, plus la mise en œuvre des processus sera complexe. L'aspect référentiel et documentation est également un axe primordial : la présence de procédures en cas de violation des données ou délimitant les habilitations en fonction des département/services métiers ou de l'échelle hiérarchique est nécessaire.

Vous trouverez ci-dessous une vision de l'articulation que peut apporter ACI partners en termes d'accompagnement du changement et de gouvernance de la donnée. Cette expertise d'ACI partners s'imbrique nécessairement entre, d'une part, les enjeux au niveau interne (infrastructure informatique, révision des procédures...) et d'autre part, le regard client – un des éléments constitutifs de la démarche.

Notre vision transverse s'attache à permettre une articulation fluide entre les différentes parties prenantes dans ce processus de mise en conformité.



3. Notre approche pour les accompagner

3.1 UNE APPROCHE TRANSVERSE BASEE SUR UNE SOLIDE EXPERTISE

Bien que le chantier de mise en conformité RGPD des organismes ai déjà été amorcés auparavant, il reste néanmoins encore des composantes spécifiques à mettre en œuvre – la plupart des organismes n'étant pas encore entièrement conformes à l'heure actuelle. Le chantier peut parfois s'avérer complexe, en fonction notamment de la taille de l'entreprise, de l'infrastructure informatique interne ou des ressources allouées.

La force de notre expertise est de partir d'une approche transverse du sujet, à savoir qu'il y a la gestion de la donnée qui est un élément central dans la mise en conformité RGPD, mais qu'elle s'inscrit dans un processus plus global qui doit impliquer l'ensemble de l'organisation – allant des fonctions centrales aux équipes métiers en passant par les supports constituant l'infrastructure informatique. La mise en conformité ne peut ainsi se faire qu'en mobilisant les différentes parties prenantes, avec une participation active et une coordination intelligente des ressources.

Cette démarche implique ainsi des évolutions de nature différente mais qui restent complémentaires :

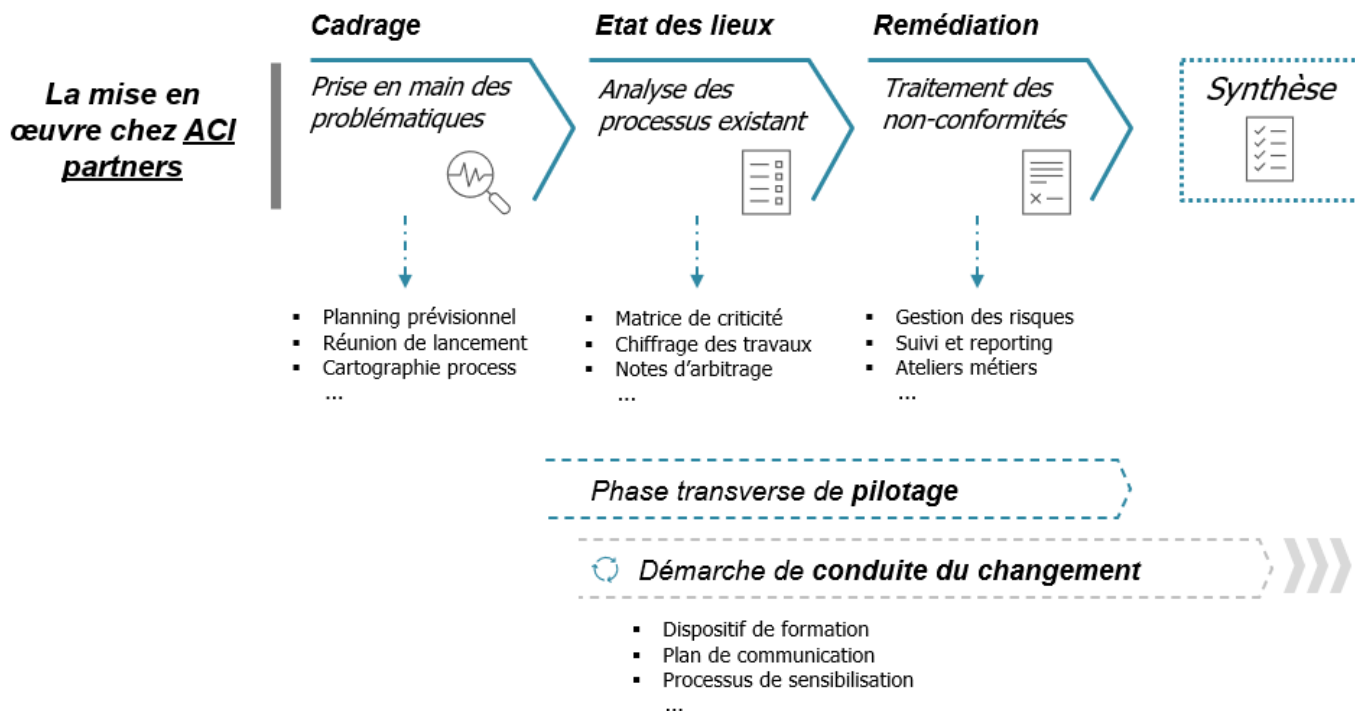
- Changements juridiques : contrats signés avec les clients et les sous-traitants, règles de consentement...
- Changements organisationnels : désignation d'un Data Protection Officer, chaîne de responsabilité, reporting...
- Changements technologiques : architecture des systèmes d'information, cybersécurité, datamining...

La mise en conformité à la réglementation RGPD implique donc la combinaison de plusieurs axes complémentaires, qui s'inscrivent dans une approche transverse et une expertise qu'ACI partners vous propose :

- ❖ **Conduite du Changement** | Sensibilisation et formation des collaborateurs sur les sujets conformité
- ❖ **Méthode Agile** | Mise en œuvre des dernières briques en s'insérant dans un processus déjà lancé
- ❖ **Data Gouvernance** | Cartographie et sécurisation des données via une réelle culture de la donnée
- ❖ **Cybersécurité** | Mise en cohérence des risques cyber avec la complexité de l'infrastructure informatique

Ces différentes composantes de notre approche sont des leviers clés pour accélérer la transformation agile des organisations, et ainsi veiller à la mise en conformité effective à la réglementation RGPD.

Notre démarche s'articule autour d'une structure initiale, qui s'adapte ensuite en fonction des problématiques et enjeux au sein des différents organismes – notamment en lien avec l'état de maturité du processus de mise en conformité.



Nous insistons également sur le fait que la conduite du changement est un axe clé de la démarche. En effet, comment initier de nouveaux processus et permettre aux différents acteurs de s'approprier les éléments, sans prendre en compte les potentielles résistances aux changements ?

Dans cette démarche, chaque étape est importante, que ce soit au niveau de la phase de cadrage à l'initiation, au niveau de la cartographie des process ou lors de la définition d'une matrice de criticité.

L'enjeu est ainsi de pouvoir réaliser une analyse de l'existant exhaustive qui permette ensuite d'initier une phase de remédiation, plus ou moins conséquente en fonction de la taille, de l'historique ou encore du secteur de l'entreprise.

La phase transverse de pilotage est également un des éléments déterminants, puisque qu'elle permet de mener de front les différents chantiers qui s'imbriquent – et notamment une gestion des adhérences métiers/informatiques.

Enfin, une démarche d'accompagnement du changement est essentielle afin de permettre aux collaborateurs, non seulement d'intégrer les nouvelles pratiques, mais surtout de devenir des acteurs du changement à l'œuvre au sein de l'organisation – l'adhésion des équipes métiers étant une condition sine qua non de la réussite de ce processus.

ACI partners propose un diagnostic complet sur certains points critiques pour vous aider à parachever la mise en conformité de votre entité, de par les missions menées au sein d'organismes de taille conséquente ainsi que l'expertise développée en interne au sein du cabinet. L'objectif principal est de générer une culture de la donnée au sein de votre organisme, qui permette ainsi d'être en conformité et de le rester.

3.2 UN CABINET PLURIDISCIPLINAIRE APPUYE PAR DES PARTENARIATS D'EXPERTS

L'équipe pluridisciplinaire composée de consultants et de senior consultants, qui peuvent s'appuyer sur l'expertise des partenaires et senior advisor spécialisés sur ces problématiques RGPD. Cette diversité nous permet ainsi d'accompagner nos clients en fonction de la maturité du processus de mise en conformité, en s'insérant dans les travaux amorcés depuis la mise en application du Règlement RGPD en mai 2018.

Nos consultants, de par leurs expériences sur des sujets conformité, sont à même de traiter les différentes problématiques conformité mais également plus généralement tout ce qui est relié à la gestion de la donnée ou l'accompagnement du changement.

Cette structure de travail s'inscrit d'une façon plus générale dans une dynamique de collaboration et de mobilisation des ressources afin de pouvoir répondre de façon efficace et réactive aux problématiques traitées dans le cadre de nos missions.

Equipe de rédaction

Julia Snidaro

Consultante ACI partners

Julia.snidaro@acipartners.fr

+33 (0)6 17 01 56 00

Francois Pineau

Associé ACI partners

Francois.pineau@acipartners.fr

+33 (0)6 61 97 47 27