38 2018 : une année pour se préparer au changement de paradigme sur la protection des données à caractère personnel


Étude rédigée par :

Yohann Brossard,
correspondant Informatique et Libertés
Grand Poitiers Communauté d'agglomération

Thomas Gaillard,
Wavestone

Le compte à rebours est lancé et les administrations comme les entreprises doivent se mettre en ordre de marche. À environ un an de l'entrée en vigueur (mai 2018) du nouveau règlement européen sur le traitement des données personnelles, les administrations doivent prendre la mesure de la marche à franchir. Si les grands groupes du secteur privé ont bien anticipé, beaucoup moins les administrations, pas assez préparées. Petit tour d'horizon sur les évolutions engendrées et les actions à engager.

1. De la loi Informatique et Libertés au règlement général de protection des données : un changement de paradigme

Cette évolution réglementaire est un véritable changement de paradigme : le modèle actuel, basé sur la déclaration, évolue vers une obligation de prouver la conformité du traitement des données à caractère personnel au regard du règlement.

A. - La loi informatique et libertés (LIL) : rappel des principes et obligations

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite loi Informatique et Libertés), a fixé en France, il y a presque 40 ans, le socle des exigences relatives à la protection des données personnelles.

> *Constitue une donnée à caractère personnel (DCP) toute information relative à une personne physique identifiée ou pouvant être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (LIL, art. 2)*

Ainsi, les 5 grands principes que tout traitement de données personnelles doit respecter sont :

- Finalité (*art. 6*) :
  - les données ne doivent être traitées que pour des finalités déterminées, explicites et légitimes ;
  - les données doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.
- Transparence :
  - les traitements automatisés de données à caractère personnel doivent être déclarés à la CNIL (*art. 22*), sauf en cas de désignation d'un Correspondant informatique et libertés (CIL) au sein de l'organisme, lui permettant une simplification des formalités administratives à accomplir ;
  - les personnes concernées par les données collectées doivent être informées par écrit et leurs droits doivent être respectés (*art. 32 et 38 à 40*) ;
  - consentement exprès de la personne dont les données sont collectées (*art. 7*) : par principe, la personne concernée doit avoir consenti au traitement de ses données, sauf dans l'un des 3 cas suivants : respect d'une obligation légale du responsable traitement, sauvegarde de la vie de la personne concernée, exécution d'une mission de service public par le responsable ou le destinataire du traitement

• Sécurité (*art. 34*) :
La confidentialité et l'intégrité des données doivent être assurées, par le responsable de traitement, qui prend toutes mesures appropriées afin de préserver la sécurité des données qui lui sont confiées ;
• Conservation (*art. 6*) :
Les données doivent être conservées pour une durée définie en cohérence avec la finalité du traitement. Pour les collectivités territoriales, cette durée est généralement définie par les textes réglementaires, en particulier par le Code du patrimoine et le Code général des collectivités territoriales.
• Transfert (*art. 32*) :
- les transferts de données à des tiers doivent être identifiés et encadrés ;
- les transferts de données internationaux (en particulier hors UE) doivent être encadrés : ils font l'objet d'un régime juridique de formalité spécifique.

B. - Les apports de la loi pour une République numérique, dite loi Lemaire

Du point de vue des sanctions, il faut retenir qu'avec la nouvelle loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (V. à ce sujet, *M. Bourgeois et A. Bounedjoum, Les apports de la loi pour une République numérique en matière d'accès et de réutilisation d'informations publiques : JCP A 2016, 2307*), **les sanctions financières de la CNIL** sont dès aujourd'hui plus sévères et **peuvent aller jusqu'à 3 millions d'euros** (*art. 64*). De plus « *lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte de la CNIL peut prononcer, sans mise en demeure préalable et après une procédure contradictoire, des sanctions* ».

Sans attendre l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en 2018, la France a déjà renforcé les obligations des organismes publics et privés, par la loi Lemaire, qui ajoute notamment de **nouvelles informations dans les mentions d'information**, telles que la durée de conservation des donnée personnelles de la personne concernée (*art. 32*) et la possibilité d'organiser le sort de ses données personnelles après la mort (*art. 40-1*).

Par ailleurs, la loi Lemaire va obliger les administrations à rendre publiques toutes leurs données : **par principe, tout document administratif est donc publiable**.

En revanche, elle pose l'interdiction de publication de documents portant atteinte à la vie privée et limite la publication de documents comportant des données personnelles à des conditions alternatives strictes :
• dispositions législatives expresses ;
• accord des personnes concernées ;
• ou procédé d'anonymisation des données rendant impossible l'identification des personnes concernées.

C. - Le RGPD : une nouvelle régulation, plus dure et plus ambitieuse, entre en vigueur dans un an, le 25 mai 2018

Le RGPD ou autrement appelé le « General Data Protection Regulation (GDPR) », après quatre années de négociations législatives, a été adopté par le Parlement européen le 14 avril 2016 et **sera directement applicable à partir du 25 mai 2018**. Il unifie le cadre et la régulation du traitement des données personnelles dans l'Union – notamment le traitement transfrontalier. Il fixe les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et à la libre circulation de ces données. **Les sanctions du RGPD seront applicables à partir de cette date.**

> Le RGPD prévoit un niveau de sanction plus élevé en cas de non-conformité, avec des amendes allant jusqu'à 20 millions d'euros pour une administration, applicable dès le 25 mai 2018.

D. - Un périmètre d'application élargi (*art. 3*)

Le règlement européen prévoit un champ d'application territorial très vaste (dans une démarche de protection du citoyen européen) en s'appliquant à la fois :
• auprès de **tout responsable de traitement ou sous-traitant établit sur le territoire de l'Union Européenne**, que le traitement de données ait lieu ou non au sein de l'Union ;
• auprès de **tout responsable de traitement ou sous-traitant établit hors Union, s'il traite des données personnelles d'un citoyen européen** et que le traitement se rapporte à une offre de bien ou services ou encore au suivi du comportement de la personne concernée.

Les exigences se durcissent. Si les grands principes resteront ceux de la loi informatique et libertés, le règlement renforce les droits des personnes, avec un droit à la portabilité de leurs données : elles doivent pouvoir récupérer les données fournies « *dans un format structuré, couramment utilisé et lisible par machine* » *(art. 20)*. Toutefois, tout ne peut pas être récupéré par l'administré ou l'usager. Les administrations devront aussi donner plus formellement la preuve du consentement préalable quand elles récoltent des données.

Toutefois, la vraie révolution est « avant tout culturelle ». On passe d'un système qui repose en grande partie sur les formalités préalables, avec des déclarations et des autorisations, à une logique de responsabilisation et de transparence des administrations dans le traitement et dans la sous-traitance des données. C'est le « deal » du règlement : moins de formalités juridiques contre plus de formalisation interne du traitement, pour faciliter les contrôles.

Cela implique un changement d'échelle, avec « la prise en compte de la protection des données dès la conception d'un service ou d'un produit » et « une organisation et des outils internes adaptés » (registre des traitements, études d'impact, etc…). Cela a un coût, mais il s'avérera un bon investissement

alors que les administrés ou l'usager sont de plus en plus sensibles à la maîtrise de leurs données.

Il faut **sortir d'une approche purement administrative et juridique de la gestion des données et la considérer comme un enjeu stratégique** de la vie de l'administration, qui sera impactée dans tous ses compartiments.

2. Le renforcement des principes édictés par la loi Informatique et Libertés

A. - Des définitions précisées

Ajout des notions de données biométriques et génétiques et de données de santé (*art. 7*) :

- Les données biométriques sont « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques* ».
- Les données génétiques sont « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ».
- Les données de santé sont « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

Pour les données biométriques et génétiques, le règlement européen intègre ce type de données dans la catégorie des **données dites sensibles** (*art. 9*), par rapport à la loi française, **dont la collecte est par principe interdite** (sauf exceptions prévues à l'article 9-2). Le règlement européen vient également combler un manque important de la loi de 1978 pour les praticiens en apportant une définition de la notion de « données de santé ».

B. - Le renforcement du principe de transparence avec l'ajout de nouveaux droits

- **Renforcement de l'information des personnes dont les données sont collectées :**
  - sur le droit d'exercer une réclamation (*art. 13-2-d*) : le responsable de traitement informe la personne sur « le droit d'introduire une réclamation auprès d'une autorité de contrôle », en l'espèce la CNIL pour la France ;
  - sur les coordonnées du DPO (*art. 13-1-b*) : le responsable de traitement fournit « le cas échéant, les coordonnées du délégué à la protection des données » ;
  - sur l'intérêt légitime du responsable de traitement (*art. 13-1-d*) : cela signifie que « lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f) », soit l'intérêt légitime, il devra être précisé « les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers » comme par exemple le traitement à des fins de préventions de la fraude ;
  - sur le droit à l'effacement, ou « droit à l'oubli » (*art. 17*) : ce nouveau droit signifie que toute personne concernée pourra demander à ce que les données traitées par un responsable de traitement soit effacées dans les meilleurs délais (Cf. détail *infra*) ; sur le droit à l'opposition de la personne (*art. 21*) : au plus tard au moment de la première communication avec la personne, les droits suivants lui sont communiqués.

    Art. 21 -1 « *La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice* ».

    Art. 21-2 « *Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection* ».
- **Droit à la limitation du traitement** *(art. 18) :* il s'agit d'un nouveau droit pour la personne concernée, qui diffère du droit à l'effacement en ce sens où la personne concernée souhaite conserver le traitement de ses données mais pour un usage limité, selon les cas, dans la durée ou les modalités d'utilisation. Dans ce cas, la personne devra donner son consentement au traitement des données qui ont fait l'objet d'une limitation et sera tenue informée par le responsable de traitement avant la levée de cette limitation.
- **Droit à la portabilité des données** *(art. 20)* : ce droit a pour objectif de redonner à la personne la maîtrise de ses données, en facilitant le transfert de données à caractère personnel d'un fournisseur de services à un autre, par exemple d'un réseau social, à un autre. Ainsi, la **personne récupère la main sur ses données** (sous une forme facilement réutilisable) et décidera elle-même de sa transmission, ou non, à une autre entité, sans limitation possible du fournisseur initial.

C. - La charte DATA

Officialisée en mai 2016, elle s'engage à :

- **Droit à réparation** *(art.78 à 82) :* le RGPD renforce les droits à réparation du citoyen en introduisant pour la personne concernée un :

  « *Droit à un recours juridictionnel effectif contre une autorité de contrôle* » : par exemple contre une décision juridiquement contraignante rendue par la CNIL ;

« *Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant* » : par exemple contre une société de service ou une administration ;

« *Droit à une représentation des personnes concernées* » : il s'agit là d'une possibilité nouvelle permettant à la personne concernée de se faire représenter, par exemple par une association reconnue dans le domaine de la protection des droits et libertés. C'est l'introduction en droit européen de la notion de class action (action de groupe) déjà existante aux États-Unis.

« *Droit à réparation et responsabilité* » : le règlement européen reconnait à toute personne qui a subi un dommage matériel ou moral du fait d'une violation du texte, le droit à obtenir réparation du préjudice subi (par le responsable de traitement ou le sous-traitant).

- **Conditions particulières pour le traitement des données des enfants** *(art. 8)* : lorsqu'un enfant peut accéder directement à une offre de services de la société de l'information (exemple : réseaux sociaux, application en ligne), le consentement doit être recueilli auprès du titulaire de l'autorité parentale d'un **enfant de moins de 16 ans** (chaque État-membre pouvant abaisser cet âge à 13 ans minimum, par la voie législative). De même, l'information sur les traitements de données doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre.

D. - Les 5 grands principes du RGPD

1. Le DPO : le nouvel acteur fort en matière de protection de données à caractère personnel (*art. 39*)

Avec l'application du règlement européen concernant la protection des données, le Correspondant Informatique et Libertés (CIL) va devenir le Délégué à la protection des données (ou DPO, équivalent de Data Protection Officer). Plus qu'un changement d'habillage, cette évolution marque une étape importante dans la stratégie de protection des données personnelles. Au regard des critères du RGPD, le DPO sera de facto obligatoire dans chaque administration, il sera **bien plus qu'une fonction, un métier à part entière** (cf détail *infra*).

2. Responsabilité (*art. 24*)

Comme évoqué précédemment, il s'agit là de la principale inversion de paradigme avec un système qui reposera désormais sur une logique de responsabilisation et de transparence. **L'administration devra être en mesure de démontrer à tout moment sa conformité à l'égard du règlement**, ce qui impose de fortes contraintes de documentation et de traçabilité. Il ne s'agira plus uniquement de faire reposer son organisation sur les formalités préalables faites de déclarations et d'autorisations.

3. Privacy by design (*art. 25, 35*)

Il s'agit de garantir dès la conception le plus haut niveau de protection des données. **Avant la mise en place d'un traitement de données** pouvant présenter des risques pour la protection des données personnelles, l'administration devra réaliser une « analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel » il s'agit de l'**Étude d'impacts sur la Vie Privée (EIVP)**[1] (notamment en cas de traitement de données personnelles à grande échelle et de profilage).

Pour se faire, les collectivités devront élaborer une procédure d'analyse d'impacts définissant la méthodologie et les étapes à suivre et identifiant les parties prenantes à l'analyse d'impacts. Il est recommandé de s'inspirer de la méthodologie publiée par la CNIL.

Que faut-il prendre en considération?	Comment faut-il le mettre en œuvre?	Quels sont les avantages?
L'état de l'art et le coût de mise en œuvre	Concentrer les efforts sur **les traitements sensibles**	**Les problèmes potentiels sont identifiés** à un stade précoce (simplicité et réduction des coûts)
La **nature**, la **portée**, le **contexte** et les **finalités** du traitement de données	Créer des **documents cadres réutilisables**	Les organisations sont plus susceptibles de **respecter leurs obligations**
Les risques, dont le degré de probabilité et la gravité varie, pour **les droits et libertés des personnes**	**Répartir les efforts** sur l'ensemble du cycle de vie du projet	La **sensibilisation** envers le respect de la vie privée et la protection des données **est accrue** au sein de l'organisation

4. Notification des violations de données (*art. 33 et 34*)

En cas de fuite de données personnelles, l'administration a 72h pour prévenir l'autorité de contrôle (la CNIL en France). Les personnes physiques concernées devront aussi être informées

> *Violation de données personnelles : « 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 » (art. 4.12)*

Dans le cadre de la loi Informatique et libertés, seuls les fournisseurs de services de communications électroniques européens avaient à notifier les violations de données auprès de l'autorité. **Dans le cadre du RGPD, l'administration devra notifier la violation à :**

- **L'autorité de contrôle (*art. 33*), 72 heures au plus tard après en avoir pris connaissance**. Tout retard devra être justifié.

1. L'EIVP est également appelée "analyse d'impacts" ou Privacy Impact Assessment (PIA)

Le responsable de traitement devra décrire aux autorités la nature de la fuite de données, le nombre et la catégorie de personnes concernées, la nature ainsi que le volume des données et le plan de remédiation, « à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques » ;

• **La personne concernée (*art. 34*) sans délai** « *lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* »

5. Droit à l'effacement (*art. 17*)

L'administration doit être en mesure de répondre aux demandes d'effacement dans les meilleurs délais.

> *« La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant » (art. 17)*

Le « **droit à l'oubli** » cité dans la LIL implique la définition d'une durée de conservation et de traitement des données limitée. Le terme « **droit à l'effacement** » implique que la personne concernée par les données exerce son droit. **Les deux droits s'appliquent** mais l'expression « droit à l'effacement » a été privilégiée dans le cadre du RGPD afin **d'encourager les personnes concernées à faire valoir leurs droits.**

Cette obligation d'effacer les données dans les meilleurs délais s'applique lorsque :

• **les données ne sont plus nécessaires** au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

• **la personne concernée retire le consentement ou s'oppose** au traitement des données à caractère personnel ;

• les données ont fait l'objet d'un **traitement illicite ;**

• les données doivent être effacées pour **respecter une obligation légale.**

Afin de rendre applicable cette obligation, les administrations doivent anticiper un certain nombre de paramètres comme :

• définir la durée de conservation des données ;

• localiser les données à gérer et à supprimer ;

• revoir les modalités d'archivage électronique (et cela dès la conception des projets de GED ou de SAE).

3. Du CIL au DPO : perspective et retour d'expérience

Le délégué à la protection des données (DPO) ou autrement appelé Data Protection Officer aura une responsabilité accrue et devra être impliqué dans tous les aspects de la conformité de traitement de données à caractère personnel dès son élaboration : gestion des droits des personnes, définition des mécanismes de vérification de la conformité, audits, vérification de l'adéquation des mesures de sécurité, vérification de la bonne réalisation de l'analyse d'impact, maintien de la documentation, etc.

Pour répondre à ces nouvelles exigences, le DPO doit être positionné dans l'organigramme de sorte qu'il aura accès à toute information et pouvoir communiquer avec toute personne, quelle que soit sa hiérarchie, afin de pouvoir être en mesure d'exercer sa mission de façon effective et indépendante et de pouvoir faire directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant (*art. 38-3*).

Les compétences requises pour remplir pleinement le rôle de DPO supposent de solides bases juridiques, une expertise IT, une vision de la stratégie, la maitrise des processus métiers et de la gestion de crise.

Pour anticiper cette évolution, les CILs qui le souhaitent et qui répondent aux nouvelles exigences pourront être confirmés dans leur fonction en tant que DPO. Il s'agit là de capitaliser sur les travaux déjà réalisés, en permettant à l'organisme de mieux se préparer au nouveau cadre juridique, et au futur DPO de s'appuyer sur l'expérience pratique nécessaire

Pour être pertinente, l'organisation de la gestion des données personnelles doit s'inscrire dans un véritable « écosystème de protection des données personnelles ». Il s'agit là d'installer un dispositif de gouvernance/pilotage, dans lequel le DPO agit comme pilote, coordonnateur d'un ensemble de ressources : DGS, DSI, Direction Juridique, DRH, Directions métiers, Responsable des Traitements ».

Le DPO devra :

• être en capacité d'imposer le cadre réglementaire et de remonter l'importance des sujets de données personnelles au top management ;

• éviter d'être en position de conflits d'intérêt et d'agir indépendamment des personnes qui définissent les traitements ;

• être en mesure de comprendre la législation et ses principes clés ;

• identifier les nouveaux cas et anticiper les non conformités au plus vite ;

• comprendre les caractéristiques clés des activités de la collectivité pour pouvoir adapter ses actions ;

• être associé/informé dans tous les projets gérant des données personnelles (plateformes d'échange, portails, e-services, city-pass, applications sur smartphones…).

Le rôle de CIL aujourd'hui et perspective d'évolution – Retour d'expérience du Grand Poitiers

Poitiers a choisi de désigner un CIL mutualisé pour 3 entités juridiques distinctes (Grand Poitiers Communauté d'agglomération, la Ville de Poitiers et le CCAS de Poitiers). Ses missions sont très diversifiées, allant de la veille juridique et technologique à la rencontre de toutes les directions, décideurs comme agents, avec pour objectif de sensibiliser, accompagner, alerter ou vérifier la conformité des traitements de données personnelles.

À ce jour, environ **18 000 organismes ont désigné un CIL en France** (cette désignation revêt un caractère facultatif).

Demain, en réponse à l'article 34 du RGPD, ce ne sont pas moins a minima de **80 à 100 000 organismes** qui devront **obligatoirement** désigner un DPO auprès de la CNIL, soit déjà plus de 5 fois les nombres d'organismes actuels concernés.

Actuellement, les CILs ont des profils assez variés (archivistes, qualiticien/conformité, chargé de communication, avec malgré tout une tendance qui se dégage principalement autour de deux formations : informaticien (47 %) et juridique (19 %) - (source : CNIL : étude à l'occasion des 10 ans du CIL, 10/2015 : https://www.cnil.fr/fr/cil-un-metier-davenir)

Demain, le profil du DPO devra être en phase avec l'article 37 du règlement européen, qui précise que ce dernier est désigné sur la base de ses qualités professionnelles et, en particulier, « *de ses **connaissances spécialisées du droit et des pratiques en matière de protection des données**, et de sa capacité à accomplir les missions* » : le DPO sera donc juriste, mais devra également intégrer un profil de qualiticien (notamment au regard des obligations en matière d'EIVP et d'accountability).

En plus des sanctions financières applicables par l'autorité de contrôle, celle-ci peut saisir le juge pénal, qui pourra prononcer, dans le cas d'une infraction grave aux droits de la personne, une sanction pénale pouvant aller jusqu'à 5 ans d'emprisonnement (*C. pén., art. 226-16 à 226-22*) pour le responsable des traitements qui est responsable des manquements à la législation.

Le CIL aujourd'hui, comme le DPO demain, ne peut voir sa responsabilité pénale engagée dans le cadre de ses fonctions, sauf s'il enfreint intentionnellement la législation ou s'il aide le responsable des traitements à violer la loi.

Conclusion
2018 : quel rétroplanning opérationnel

Les principales actions qui peuvent être engagées dès à présent en anticipation du jalon du 25 mai 2018 couvrent à notre sens :

1. Le recensement des applications contenant des DCP
2. Les formalités déclaratives dans le registre CIL
3. L'analyse de risques à réaliser sur les applications contenant des DCP si l'administration n'a pas déjà opéré ces travaux
4. L'analyse d'impacts à réaliser lorsque les traitements sont susceptibles d'engendrer des risques élevés, notamment en cas de traitement de données personnelles à grande échelle et de profilage
5. La création d'un guide de mise en conformité à l'attention des MOEs et des métiers, afin d'intégrer les règles du RGPD dans les règles de la PSSI
6. Mise à jour du cadre de référence (règles techniques)
7. La mise en place de mécanismes / patterns de sécurité pour chaque règle (mécanisme qui permet de voir une perte d'intégrité de nos données, …)
8. La mise en œuvre des règles techniques pour protéger les DCP
9. La réalisation de contrôles / audits pour vérifier la conformité au RGPD, des solutions mises en place (bonne sécurisation mise en place pour protéger les DCP)

Face aux enjeux liés au développement des nouveaux usages et à la digitalisation des services, nous avons vu que l'administration doit prouver que tous les moyens ont été mis en œuvre pour protéger les données personnelles qu'elle collecte, et ce, dans le respect des droits des personnes. Les nouvelles obligations induites par la règlementation concernent toutes les applications actuellement existantes et à venir. Elles ont un spectre très large tant en terme d'organisation que de modifications des processus des systèmes d'information.

Or, le spectre d'analyse est large, et le travail de mise en conformité en conséquent. Ce projet doit mobiliser plusieurs expertises et métiers de l'administration, notamment les directions juridiques, informatiques ainsi que les fonctions opérationnelles. Par ailleurs, il conviendra de revoir l'analyse systématiquement tous les 3 ans, afin de s'assurer que les mesures en place sont encore suffisantes compte tenu des évolutions techniques.

Il est donc impératif de commencer au plus tôt afin d'éviter de s'exposer inutilement à des sanctions par faute d'anticipation et alors même qu'il s'agit là, pour chaque administration, d'une réelle opportunité pour prendre la main sur la gouvernance de ses données numériques.

Pour aller plus loin

- *https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes*
- *https://www.republique-numerique.fr/*
- *https://www.cnil.fr/sites/default/files/atoms/files/poster_fr-optimise.pdf*