IBM – Isabelle Renard Avocat – Parker Williborg

Livre blanc

GDPR

Protection des données personnelles

Se mettre en conformité : Pourquoi ? Comment ?

Une nouvelle réglementation européenne sur la protection des données personnelles va entrer en vigueur en mai 2018. Les sanctions peuvent aller jusqu'à 4% du chiffre d'affaires annuel mondial. Parker Williborg, Maître Isabelle Renard et IBM proposent une démarche opérationnelle outillée de mise en conformité GDPR développée dans ce livre blanc.

Sommaire

1. La GDPR : une vraie révolution !

La GDPR (General Data Protection Regulation / Règlement sur la Protection des Données Personnelles) est le fruit d'un compromis. Elle donne les moyens aux personnes de se replacer au centre du contrôle de leurs données personnelles. Corrélativement, les entreprises doivent adopter un comportement responsable quant à l'usage qu'elles font de ces données, dans une logique d'autorégulation encadrée.

1.1 La GDPR : un changement de paradigme

La GDPR constituera le cadre réglementaire européen de la protection des données personnelles à compter du **25 mai 2018**. Il s'agit d'un règlement et non d'une directive : la GDPR sera donc directement applicable dans les états membres, sans délai de transposition[1].

La GDPR ne constitue pas une modification « à la marge » de la Loi Informatique et Libertés. Elle représente un véritable changement de paradigme dans la façon dont les entreprises devront désormais prendre en compte la dimension « données personnelles » inhérente à leurs activités.

Jusqu'ici, la conformité à la réglementation sur les données personnelles se bornait à s'assurer que les déclarations ou les demandes d'autorisation imposées par la Loi Informatique et Libertés avaient été faites. C'est souvent en cas de contrôle de la CNIL que les non conformités apparaissaient : données non effacées à l'issue de leur durée utile, mal sécurisées, diffusées de façon inappropriées, ou détournées des objectifs pour lesquels elles avaient été collectées. Ces non-conformités faisaient l'objet de corrections a posteriori plus ou moins complètes, sans entraîner de réflexion de fond sur l'organisation et la gestion de la donnée dans l'entreprise.

Avec la GDPR, l'ère des déclarations de pure forme et des justifications a posteriori est terminée.

[1] En pratique, la Loi Informatique et Libertés actuelle sera remplacée par la GDPR, qui constitue un socle minimum de protection des données. La future Loi Informatique et Libertés comprendra, en plus du socle de la GDPR, des dispositions complémentaires sur les points où la GDPR laisse aux Etats Membres un degré de liberté.

1.2 Deux idées-forces : protection de la donnée personnelle dès la conception & auto-responsabilité de l'entreprise

La nouvelle réglementation repose sur deux idées-forces. La première est d'amener les entreprises à intégrer la protection de la donnée personnelle dans la conception même des applications et des processus métiers[2]. La seconde est d'imposer à l'entreprise d'être en mesure de **démontrer à tout moment** qu'elle a pris les mesures juridiques, organisationnelles et techniques nécessaires pour respecter les objectifs poursuivis par le règlement. Ces mesures ne sont pas uniformes. Elles dépendent du type de données traitées et du type de traitement considéré : elles doivent être **proportionnées au risque**, c'est-à-dire au préjudice qui résulterait pour les personnes de leur utilisation inappropriée *(voir Encadrés 1 et 2)*. Cette seconde idée est le principe dit d'« **Accountability** », littéralement de « capacité à rendre compte », traduit de façon moins parlante en français par le « principe de responsabilité ».

L'auto-responsabilisation a un prix : l'ignorer pourra coûter une amende pouvant atteindre la somme la plus élevée entre 20 millions d'euros et 4% du chiffre d'affaires total annuel.

Reste à savoir de quelle façon l'entreprise va réaliser en pratique sa mise en conformité, dans un délai qui est finalement très court compte tenu du changement de perspective radical introduit par la GDPR. La réponse tient dans la mise en œuvre d'un plan de progrès continu et itératif selon trois axes : analyse juridique, méthode et outillage.

Encadré 1 : Les données particulières (ex-données sensibles)

Les données particulières :
- Origine raciale ou ethnique
- Opinions politiques
- Convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques
- Données biométriques aux fins d'identifier une personne physique de manière unique
- Données concernant la santé
- Données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Encadré 2 : Le numéro de sécurité sociale (NIR)

Le traitement du NIR (Numéro d'Inscription au Répertoire) est laissé à l'appréciation de chaque pays. En France, le régime actuel sera vraisemblablement reconduit, l'autorisation étant remplacée par une validation de l'analyse d'impact par la CNIL.

[2] « Privacy by design »

1.3 La mise en œuvre d'un plan de progrès : 3 axes

1.3.1 L'analyse juridique

L'analyse juridique est un préalable structurant à toute démarche de conformité. Elle permet, sur la base d'une connaissance approfondie de la réglementation, **d'identifier les zones sensibles** tant dans les applications back office que dans les opérations cœur de métier de l'entreprise, d'évaluer le risque afférent, et de prioriser leur encadrement.

Elle permet également d'évaluer le **positionnement de l'entreprise dans la chaîne de traitement des données**. Selon que l'entreprise est responsable de traitement, sous-traitant, ou co-responsable *(voir Encadré 3*) avec un ou plusieurs tiers, il faudra mettre en place des organisations et des structures contractuelles différentes.

Encadré 3 : Définitions

Responsable de traitement Entité qui détermine, seule ou conjointement avec d'autres, les finalités et les moyens du traitement.	**Responsabilité conjointe** Lorsque plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement, ils sont responsables conjointement. Ils doivent définir par contrat leurs obligations respectives, notamment en matière de respect des droits des personnes et d'information des personnes.
Sous-traitant Entité qui traite des données personnelles pour le compte d'un responsable de traitement.	

1.3.2 La méthode

La façon méthodique de traduire en mesures pratiques les résultats de l'analyse juridique consiste en la réalisation d'une analyse d'impact, ou « **PIA** » **: Privacy Impact Assessment**. Cette opération consiste à identifier méthodiquement, pour chaque traitement ou type de traitement, les risques que les données personnelles soient diffusées et utilisées à tort, conservées sans limite, gérées de façon incontrôlée, etc. Face à ces risques, le PIA identifie les mesures d'ores et déjà mises en place, et/ou celles devant être mises en place.

La GDPR rend le PIA obligatoire dans certains cas *(voir Encadré 4)*, et il doit alors être soumis à la CNIL avant que le traitement puisse être mis en œuvre : dans ce cas, la GDPR maintient un contrôle a priori comparable à celui de l'actuelle procédure d'autorisation mais de façon plus interactive, dans le cadre d'un dialogue pragmatique avec la CNIL sur le caractère suffisant des mesures proposées dans le PIA.

Encadré 4 : Traitements à risque : Le PIA est obligatoire dans certains cas

Certains traitements à risque rendant obligatoire une analyse d'impact
Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

- Evaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire
- Traitement à grande échelle de « catégories particulières » de données
- Traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions
- Surveillance systématique à grande échelle d'une zone accessible au public.

La liste de ces traitements sera établie de façon précise et publiée par la CNIL.

Lorsque le PIA n'est pas obligatoire, il reste néanmoins nécessaire pour démontrer la conformité de l'entreprise aux principes de la GDPR : **le PIA est le tableau de bord de la conformité de l'entreprise et de son respect du principe d'« Accountability ».**

En cas de contrôle, la CNIL pourra s'appuyer sur deux bases documentaires : l'une est le « registre des activités de traitement », répertoriant de façon détaillée tous les traitements effectués dans l'entreprise[3] ; la seconde est constituée des PIA qui auront été effectués. **L'absence de ce socle documentaire minimum sera, en soi, une infraction à la GDPR susceptible d'entraîner des sanctions** s'il n'y est pas remédié rapidement, et ce en l'absence même de toute faille ou de tout préjudice avéré.

1.3.3 L'outillage

Les systèmes d'information des entreprises sont maintenant d'une grande complexité et comportent de multiples gisements de données non structurées qui constituent des failles béantes dans la gestion de la sécurité des données. La conformité reste alors un concept théorique en l'absence de mesures pratiques permettant de savoir où sont les données personnelles de tel ou tel type dans le système d'information. La mise en œuvre d'un outillage permettant de repérer ces données est le complément indispensable de l'analyse juridique et de la mise en œuvre d'une méthode adaptée.

[3] La tenue du registre des activités de traitement est obligatoire au-dessus de 250 employés. Dans tous les cas il doit être tenu en cas de traitements comportant des risques ou portant sur des données particulières.

1.4 Le Data Protection Officer (DPO)

Le « Délégué à la Protection des Données », ou « Data Protection Officer », est l'héritier de l'actuel Correspondant Informatique et Libertés (CIL). Il peut être salarié de l'entreprise ou lié par un contrat de service à celle-ci. Il rapporte directement au niveau le plus élevé de la direction de l'entreprise et ne doit recevoir aucune instruction dans l'exercice de ses missions, dont le socle minimum est défini par le règlement : information de l'entreprise sur l'étendue de ses obligations ; contrôle du respect de la règlementation ; formation du personnel et gestion des audits internes ; conseil pour la conduite des études d'impact ; coopération avec la CNIL et point de contact…

Aux termes du règlement, la nomination d'un DPO est a minima obligatoire dans le secteur public, en cas de traitement à grande échelle de données particulières, et en cas de traitement exigeant le suivi régulier et systématique de personnes, étant précisé qu'il est possible de nommer un seul DPO pour un groupe d'entreprises. Ces conditions seront précisées dans le cadre de la mise à jour de la Loi Informatique et Libertés.

1.5 La GDPR s'applique aux entreprises en dehors de l'Europe

La GDPR s'applique à toute entreprise ayant des activités impactant des personnes sur le territoire européen, même si l'entreprise est établie en dehors de l'Europe. L'objectif recherché est de ne pas créer de distorsion de concurrence entre les entreprises européennes, tenues par principe à la GDPR, et des entreprises étrangères opérant sur le territoire européen au travers de réseaux virtuels.

1.6 La GDPR prend en compte la situation des groupes

La GDPR introduit la notion d'autorité de contrôle « chef de file », qui est celle de l'établissement principal d'un groupe établi sur plusieurs pays en Europe. Les différentes autorités de contrôle devront coopérer pour leurs prises de décision, notamment les sanctions, concernant les opérations transfrontalières du groupe. Corrélativement, la GDPR met en place un contrôle de cohérence entre les autorités de chaque état membre.

1.7 La GDPR donne les moyens aux personnes de se placer au centre du contrôle de leurs données

Par principe, un traitement de données personnelles n'est licite que si la personne y a consenti de façon claire, indubitable et démontrable a posteriori, ce qui imposera aux entreprises de mettre en place une traçabilité efficace de l'existence de ce consentement. Il existe un certain nombre d'exceptions à ce principe de consentement, telle que par exemple l'exécution d'un contrat entre la personne et le responsable du traitement, dont le contour sera précisé par la CNIL.

Chaque personne doit être informée de ses droits (droit d'accès, droit de rectification, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité, droit d'opposition) par l'entreprise qui les traite, que les données aient été collectées directement par l'entreprise ou indirectement.

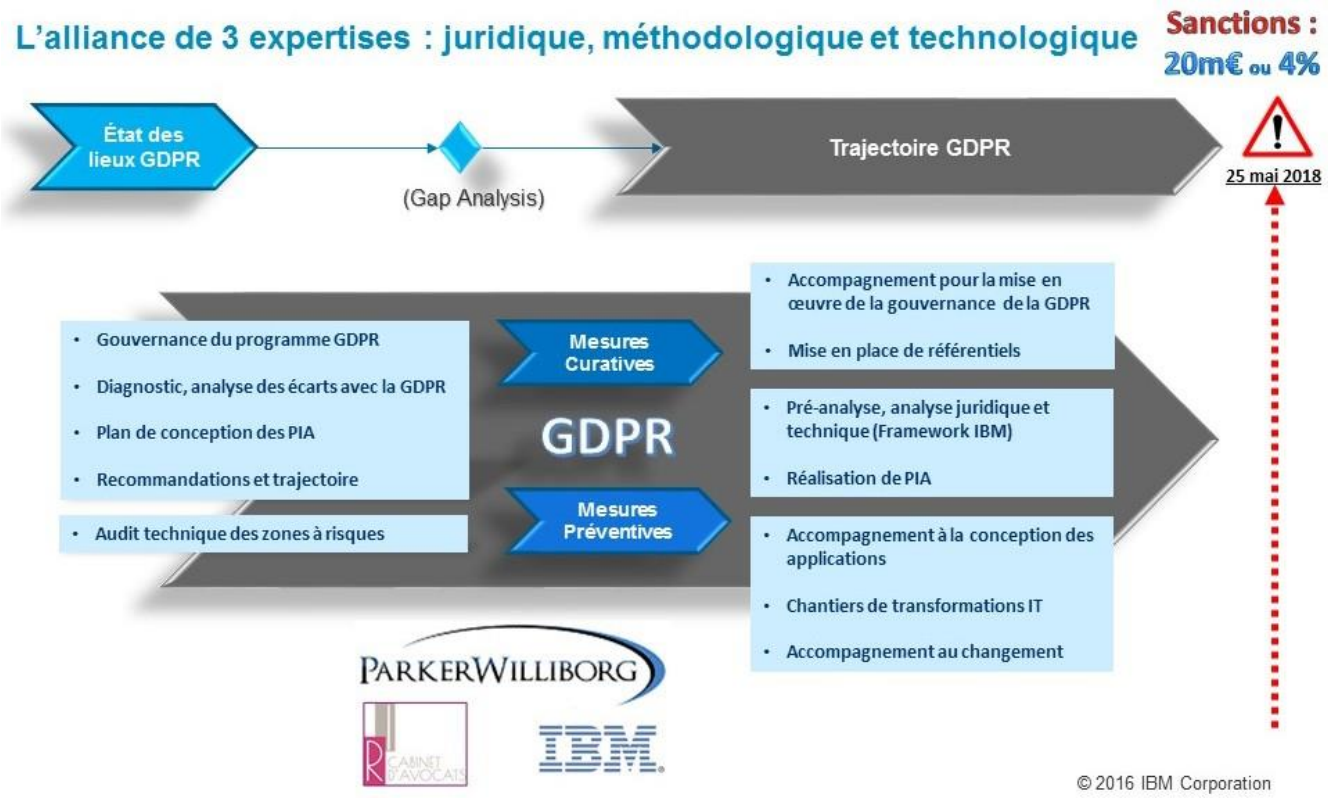
Enfin, le délai de réponse à une demande d'information d'une personne est enfermé dans un délai d'un mois, ce qui est très court en l'absence d'une organisation adéquate.

De façon générale, la GDPR renforce et précise de façon très substantielle les droits des personnes sur leurs données, de même que les contraintes mises à la charge des entreprises pour répondre aux demandes.

2. Démarche opérationnelle de mise en conformité

La GDPR est aussi un « voyage » vers la conformité qui nécessite une démarche opérationnelle outillée fondée sur un **état des lieux** relevant les écarts pour mieux les réduire dans une **trajectoire** dont la cible pourra être une certification de l'organisation. *(voir Figure 1)*

Figure 1 : Etablir un diagnostic GDPR et définir une trajectoire



2.1 Pilotage de la GDPR

Les enjeux de la GDPR sont multiples. Très rapidement se pose la question du meilleur positionnement du pilotage et du contrôle de la GDPR dans l'organisation. Pour y répondre, les dispositifs mis en place sont assez variés, au regard de l'importance accordée à la maîtrise des données en général et aux données personnelles en particulier, ainsi qu'aux efforts déjà déployés dans cette direction.

Le pilotage peut se rapprocher de celui mis en œuvre pour le suivi de la politique Informatique et Libertés, des CIL et des relations avec l'autorité nationale de contrôle. Il est aussi légitime de le positionner dans les structures de mise en conformité à la réglementation, de maîtrise et de gouvernance de l'information et des données voire de la sécurité ; sans oublier la mise en place d'un pilotage spécifique de la GDPR.

La nomination d'un DPO devient une obligation pour les entreprises de plus de 250 salariés. Cependant, la structure de pilotage reste à définir au cas par cas, avec des référents des différents métiers les plus exposés aux risques de la GDPR et en pensant à bien mettre en place les liaisons avec les programmes et politiques présentant des adhérences[4].

[4] Exemples : Sécurité, Suivi de la réglementation, Gouvernance des données, …

Ces structures doivent être à même de cadrer l'installation et le déploiement de la GDPR mais être capables également de gérer des situations de crise. Par exemple, en cas de fuite ou de perte de données personnelles, la structure doit être à même de garantir une réactivité certaine pour respecter les délais inscrits dans la réglementation[5] .

2.2 Un large champ d'application

Avec la GDPR, le champ d'application des mesures de protection des données personnelles se trouve élargi :

- **Le consentement des personnes doit être explicite** : l'autorisation doit impérativement être accompagnée d'une action d'autorisation de la personne et ne plus laisser la place à l'autorisation « par défaut » (ex. : case à cocher pré-remplie, positionnement sur une page web valant office d'autorisation, …)

- **Droits des citoyens : le devoir d'échange d'informations avec les personnes physiques est renforcé** ; les personnes ayant confié leurs données personnelles sont en droit de demander à tout moment un état des lieux ou de faire opposition à l'exploitation de ses données, voire de demander leurs destructions[6] dans des délais resserrés[7].

- **Le principe de responsabilité de la mise en conformité est étendu aux sous-traitants**, partenaires (ex. : hébergeur, prestataire de services e-marketing, …) responsables de tout ou partie de l'exploitation des données personnelles de ressortissants de l'Union Européenne. Il appartient au responsable des traitements de s'assurer qu'ils sont conformes ou en voie de mise en conformité à l'aide des moyens de contrôle qui lui paraîssent appropriés (ex. : audit, demande de révision des dispositifs d'information pour les clients, …). La compréhension de la réglementation européenne et le délai de réactivité n'étant pas toujours au rendez-vous, il est fortement recommandé d'anticiper cette demande.

- **Il est exigé une maîtrise des données personnelles et de leurs traitements dans le Système d'Information** (SI) à divers titres : une durée de rétention doit pouvoir être appliquée aux données personnelles, elles doivent pouvoir être restituées ou détruites sur demande ou à l'issue de leur durée de conservation, les données sensibles au regard de la loi ou perçues comme telles, doivent faire l'objet d'un traitement spécifique (ex. : pseudonymisation, anonymisation, cryptage, …). Le périmètre est étendu au « Shadow IT »[8] car il n'est pas rare d'y retrouver la génération plus ou moins spontanée de référentiels de données personnelles sur les serveurs et les postes de travail. Sans aller jusqu'à la réécriture des applications concernées, la démarche demande a minima la maîtrise de la localisation numérique (et des échanges) de ces données.

- Nul n'est censé ignorer la loi, il est indispensable de **pouvoir informer au plus tôt les personnes** qui confient leurs données personnelles de même que les personnes en charge de leur traitement. Le champ du possible est très large, de la publication des notices d'information à la formation au diagnostic GDPR des applications. A noter que les collaborateurs internes sont aussi bien concernés que les personnes physiques externes.

[5] 72 heures pour alerter l'autorité de contrôle

[6] Procédure de « droit à l'oubli »

[7] Un mois

[8] L'IT échappant au contrôle direct de la Direction des Systèmes d'Information

- **La sécurité des données également**. La maîtrise des données personnelles et de leur confidentialité est un enjeu majeur, l'actualité est riche en nouvelles de fuite massive de données personnelles confidentielles, parfois suivies de leur publication sur des sites publics, voire de leur revente. Il faut donc pouvoir prévenir ces risques, ce qui est dans le champ d'application de la politique de sécurité, mais, devant le fait établi, il faut pouvoir rapidement alerter les autorités de contrôle voire les personnes, ce qui, là, est dans le champ d'application de la GDPR.

2.3 Préparer la mise en oeuvre

L'étendue des nouvelles actions à entreprendre et, en conséquence, des moyens à engager, peut être très importante ; elles nécessitent des **compétences multiples,** du pilotage à l'accompagnement au changement, en passant par l'expertise SI et sécurité numérique. Il est donc indispensable de :

- **Mesurer les écarts de conformité GDPR**. Cet exercice nécessite en tout premier lieu une interprétation de la réglementation, le champ d'application et les priorités ne seront pas les mêmes pour une entreprise de vente en ligne avec une forte activité en liaison avec les personnes physiques que pour une entreprise essentiellement en liaison avec les entreprises. Il s'avère ensuite nécessaire d'identifier les écarts GDPR sur différents axes : le réglementaire, la maîtrise du cycle de vie des données personnelles et de leurs traitements, le devoir d'information auprès des personnes, l'accompagnement au changement, l'appropriation de la politique et le contrôle de son application.

- **Pouvoir très rapidement répondre aux questions concernant la nature des données personnelles traitées, leur localisation et les volumes en jeu**. Cet exercice demande la maîtrise des processus et des référentiels de données « embarquant » les données personnelles et leurs traitements ; il demande souvent aussi un exercice d'examen des sources numériques de données « à risque »[9] pour analyser la présence des patterns de données personnelles et les volumes associés.

- **Evaluer les risques et les priorités**. Il y a nécessité d'ordonnancer les actions à entreprendre ; la mise en œuvre de la GDPR demande la constitution d'une trajectoire dans la durée, nécessitant une estimation des risques déterminée principalement par la criticité des données personnelles[10], leur volume, et leur localisation dans des sources numériques « à risque ». La préparation de la mise en œuvre permet de situer les priorités, voire les urgences, réparties entre des **mesures préventives**[11] et **des mesures curatives**[12].

[9] Exemples : bases clients, infrastructure cloud pour l'hébergement des données, cookies, ...

[10] Données identifiées comme sensibles au niveau de la loi ou perçues comme telles

[11] Exemples.: actualisation de la conception des applications avec le principe de « Privacy by Design », formations, …

[12] Exemples : insertion des mentions obligatoires dans les sites existants en ligne, mise en place de processus de destruction des données personnelles, …

2.4 Renforcer la documentation et le contrôle

Le principe d'« Accountability » (ou de responsabilisation), apporté par la GDPR, nécessite le renforcement de plusieurs démarches :

- **La création et le maintien de la documentation** des données personnelles et de leurs traitements, documentation qui doit être ouverte et auditable par l'autorité de contrôle. Le PIA, véritable tableau de bord des données personnelles, en constitue l'élément majeur, avec la description du cycle de vie, des risques et des mesures de mise en conformité.

- **Le diagnostic GDPR et le contrôle de la mise en œuvre des mesures** de mise en conformité, à appliquer à soi-même ou à diligenter auprès de ses partenaires et sous-traitants.

- **L'audit Flash / GDPR Assessment :** compte tenu des échéances rapprochées, la trajectoire de mise en conformité et le plan des premières actions à entreprendre deviennent des outils indispensables. Un premier exercice doit permettre d'établir deux livrables déterminants pour la suite des opérations : le **plan des PIA** et le **plan des mesures complémentaires**.

Dans un premier temps, l'exercice doit pouvoir réunir les principaux référents et s'effectuer dans un périmètre prioritaire[13]. Le diagnostic et les recommandations doivent pouvoir être établis dans un temps comprimé[14], tout en réunissant les expertises appropriées[15]. L'approche doit combiner une analyse des processus embarquant des données personnelles et l'examen technique des zones de données numériques « à risque ».

Tous les services et directions du responsable de traitement sont concernés, de près ou de loin, par les données personnelles. Elles demandent des actions de fond, mais aussi des gestes, des formules qui doivent accompagner l'organisation dans ses relations quotidiennes avec les clients, les nouveaux collaborateurs, les fournisseurs, etc. L'accompagnement au changement prend ici une dimension toute particulière, applicable à tous les niveaux de responsabilité, pour intégrer les enjeux et les actions à entreprendre.

Ici, comme pour d'autres enjeux réglementaires, la conformité induit d'autres valeurs ajoutées comme le renforcement de l'image de probité, la maîtrise de ces données numériques du client qui apporteront, si nécessaire, d'autres arguments pour la mise en œuvre de la GDPR.

La démarche opérationnelle de mise en conformité nécessite de répondre à des exigences d'exploration, de traitement des données personnelles, d'enregistrement des règles dans des délais contraints, ce qui rend l'usage d'outillages indispensable dans ce programme GDPR.

[13] L'évaluation de la priorité peut prendre en compte le niveau de criticité des données à examiner, les métiers gérant les relations avec les personnes, la densité des données personnelles dans la zone étudiée, l'exposition aux risques des traitements effectués…

[14] De 3 mois à 6 mois

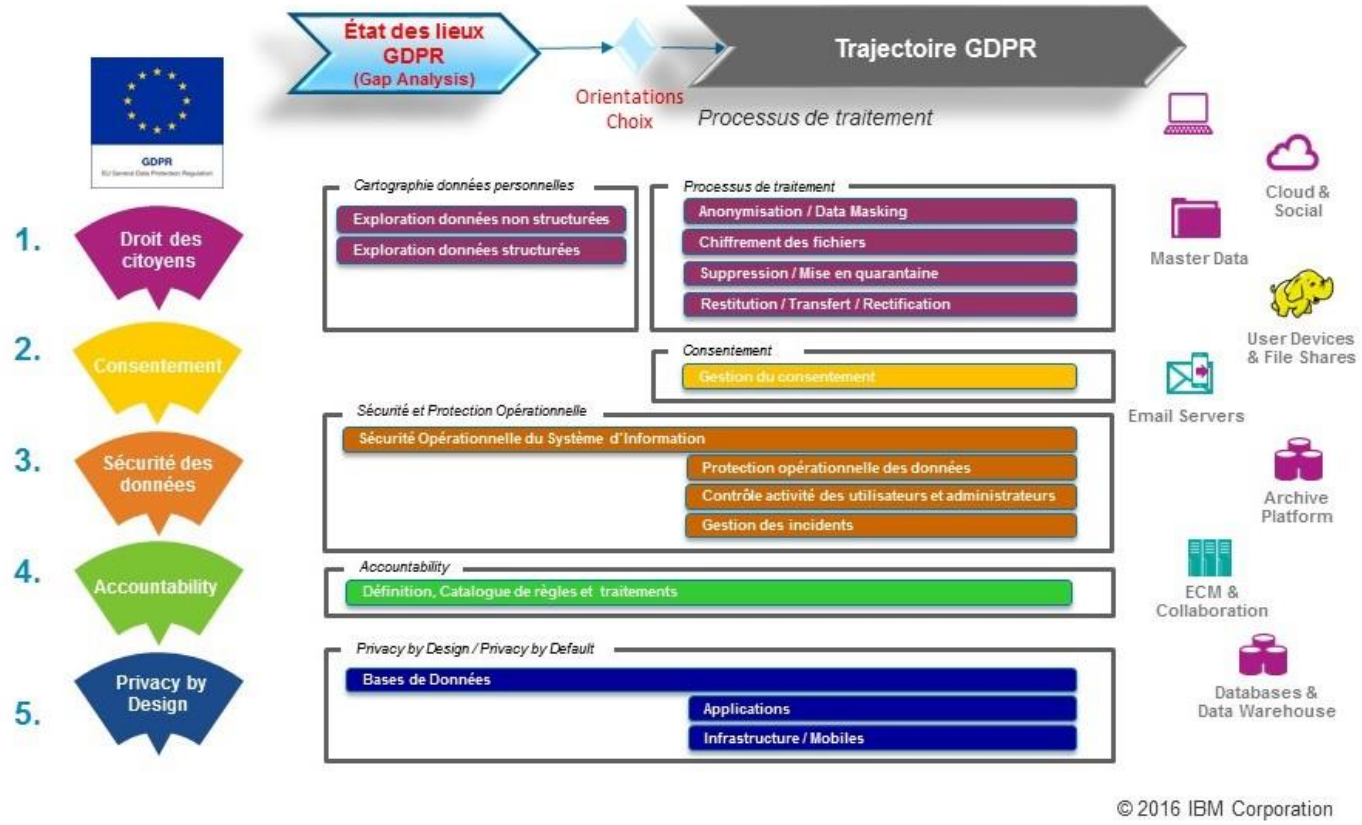
[15] Réglementaire, organisationnelle, fonctionnelle, technique et sécurité

3. De l'état des lieux à la mise en place des outillages d'une conformité durable

Du point de vue de la mise en œuvre de la GDPR, l'application de la réglementation se traduit, selon IBM, par cinq domaines de transformation *(voir Figure 2*) : le droit des citoyens, la gestion du consentement, la sécurité des données personnelles, le principe d'« Accountability » et celui de « Privacy by Design ».

Pour chacun de ces principes nous avons identifié des fonctions essentielles à la fois dans la phase d'état des lieux (analyse d'écart) et dans la phase de trajectoire de mise en conformité. Chacune de ses fonctions pourra ensuite être appuyée ou accélérée par la mise en œuvre d'une solution technologique.

Figure 2 : Cinq domaines de la transformation pour une conformité GDPR durable : Les fonctions technologiques répondant aux exigences -selon IBM



1. **Droit des citoyens -** En phase d'état des lieux, la cartographie a pour objectif de localiser les endroits où pourraient se trouver des données particulières (données personnelles / sensibles…). En effet un des sujets des projets de mise en conformité GDPR est de savoir où se trouvent les données, notamment en explorant les zones à risque. Par exemple, des informations sensibles au sens GDPR se trouvent fréquemment dans des emails ou des serveurs de fichiers (Shadow IT, données non structurées, commentaires de textes, ...). Des solutions d'exploration de données à base de reconnaissance de catégories (numéro de sécurité sociale, appartenance syndicale, …) aident à la cartographie.
   En phase de Trajectoire de mise en conformité GDPR, des processus de traitement nécessaires à cette mise en conformité pourront être définis. Les principaux processus impactés sont :

   - ✓ **Anonymisation ou Data Masking -** Surtout utilisé lorsque des données quittent un environnement sécurisé servant au métier pour aller vers des environnements techniques autres. Il s'agit par exemple des données de production recopiées en environnement de test pour mener des tests de non-régression logiciels. La problématique de ce processus est de transformer les données afin qu'elles soient représentatives (pour la qualité des tests) mais pas réelles (pour respecter les obligations). Il s'agira également de transformer les données de manière à préserver l'intégrité du jeu d'essai (par exemple sans casser les liens d'intégrité référentiels dans une base relationnelle).

   - ✓ **Chiffrement -** Il s'agit de l'encryption des supports de stockage au niveau du stockage physique. La GDPR insiste sur l'importance de chiffrer les informations pour les protéger. En effet, une fuite de données chiffrées n'est pas réellement une fuite puisque ces données sont illisibles et ne pourront donc pas être exploitées. Le règlement GDPR mentionne même explicitement ce cas comme une exception à l'obligation de communication d'un incident (Article 34 - 3a). Le chiffrement des fichiers, des bases de données ou des environnements Big Data est donc une des pratiques de base de la protection de l'information.

   - ✓ **Suppression -** Il s'agit de répondre à la demande d'un citoyen d'effacer les données le concernant de manière cohérente et auditable. De plus, si une donnée ne peut pas être conservée plus d'un certain temps (carte de crédit après un achat) ou si on a découvert qu'elle était présente à tort, il faudra l'effacer de manière cohérente (sans mettre en péril le comportement de l'application) auditable (démontrer qu'un effacement a eu lieu) et permanente (irréversible).

   - ✓ **Mise en quarantaine des données -** Ce processus permet de limiter l'accès à un document dont le contenu est soupçonné d'être en écart de conformité du point de vue GDPR, le temps de l'analyser pour décider du traitement qui doit lui être associé.

   - ✓ **Restitution & Transfert -** Un citoyen peut faire valoir son droit à l'oubli, son droit de rectification ou celui de portabilité des données personnelles. Des processus doivent être mis en place pour collecter les informations puis les mettre à jour ou les transférer vers un tiers (nouvel opérateur téléphonique par exemple) afin de pouvoir effectuer les traitements qui dérivent de l'exercice de ces droits. Ces processus doivent être auditables.

2. **Gestion du consentement -** Le consentement d'un citoyen pour la collecte, l'utilisation (dans un but déterminé) et la détention de ses données doit être explicite et démontrable. Des processus de recueil et de suivi de ce consentement doivent être mis en place.

3. **Sécurité des données -** Pendant l'état des lieux on analysera la sécurité des données : Il faudra vérifier que les processus de protection sont bien définis et mis en œuvre puis contrôler leur bon fonctionnement.
   En phase de trajectoire de mise en conformité, on devra organiser la sécurité opérationnelle :

   - ✓ **Mettre en place une protection opérationnelle des données** : suivre en temps réel l'accès aux données et empêcher les accès non-conformes.

   - ✓ **Gérer les incidents** : à chaque incident détecté un processus d'alerte doit être déclenché (selon le cas : vers l'autorité de contrôle, la victime et/ou les services concernés pour remédier au problème).

   - ✓ **Contrôler l'activité des utilisateurs** : il faudra vérifier que les utilisateurs de données, y compris les utilisateurs privilégiés, ont un accès aux données qui soit adéquat vis-à-vis de règles définies et des fonctions de cet utilisateur. Par exemple, on ne pourra pas accepter d'un administrateur de bases de données qu'il s'attribue des droits pour effectuer des actions qui n'entrent pas dans son champ d'action.

4. **Accountability -** Les règles définies pour la protection des données doivent être formalisées dans un référentiel. Ce référentiel peut être non seulement un outil d'enregistrement des règles mais peut aussi être un outil d'exécution automatisée de ces mêmes règles. En phase d'audit, on vérifiera l'existence et la documentation des règles alors qu'en phase de trajectoire on pourra aussi s'intéresser à leur automatisation.

5. **Privacy by Design -** Les applications doivent être conçues de manière à intégrer la protection des données personnelles. Les développeurs doivent être sensibilisés au sujet, de plus l'outillage de développement et de test pourra prendre en compte les problématiques de failles de sécurité. De la même manière, les données et l'infrastructure (par exemple les terminaux) doivent faire l'objet d'une protection permanente dès la phase de conception du système.

Le délai pour se conformer aux exigences de la nouvelle règlementation est très bref. Pour accompagner les entreprises et organisations dans leurs projets, Parker Williborg, Maître Isabelle Renard et IBM proposent une offre unique, associant trois expertises - juridique, méthodologique et technologique- et qui est à ce jour une des plus développée sur le marché français.

Pour en savoir plus sur la GDPR, vous pouvez contacter :

Parker Williborg est une entreprise de consulting spécialisée dans les nouvelles technologies informatiques et la gouvernance de l'information, l'analyse des processus.
Contact : Marc NOEL - 01 42 92 07 82 - mnoel@parkerwilliborg.fr

Maître Isabelle Renard intervient dans tous les domaines liés aux nouvelles technologies et à la transformation digitale. Elle est Docteur Ingénieur de formation, ce qui lui permet d'avoir une vision claire et pragmatique des sujets techniques.
Contact : Maître Isabelle RENARD - 01 85 08 44 87 - irenard@irenard-avocat.com

IBM, leader technologique au service de l'innovation, accompagne les entreprises et organisations dans leur transformation. IBM innove en permanence et propose, entre autres, une offre de services et des technologies pour adresser les problématiques de la GDPR et plus largement celles de la gouvernance des données.
N'hésitez pas à consultez notre site Internet : ibm.biz/GDPR_fr
Contact : Thierry BRUN - 01 49 75 26 75 - thierrybrun@fr.ibm.com

Compagnie IBM France
17 Avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Imprimé en France
Novembre 2016