MPG Overview - Regulation

Auteur

Equipe Publication

MPG PARTNERS

136 Boulevard Haussmann
75008 Paris
Tél : 01.53.05.98.52

GDPR – Une nouvelle gouvernance de la donnée

Une réglementation européenne

Contexte : Dans un nouvel environnement où la frontière entre vie publique et vie privée diminue et se fragilise, où la sécurité informatique devient un enjeu prioritaire, GDPR *« General Data Protection Regulation »* voit le jour. Le texte publié en 2016 entrera en application le 25 mai 2018.

Des enjeux revus et une autorité renforcée : GDPR c'est des sanctions renforcées pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires. Le contrôleur européen de la protection des données sera aussi remplacé par l'EDPB *« l'European Protection Data Board »* dont l'objectif est de veiller au respect de GDPR.

Des exigences impactantes

Principes clefs pour trois objectifs : Cette réglementation a trois objectifs. Le but principal est de renforcer le droit des personnes. Le texte dote les individus de nouveaux droits (droit de retrait, de portabilité, …) leur permettant de mieux contrôler la collecte, le traitement et l'utilisation de leurs données personnelles. GDPR est né aussi d'un besoin d'harmonisation des règles au sein de l'union européenne. Enfin, il entraine d'importants changements en matière de gouvernance de la donnée visant à responsabiliser les entreprises

Une nouvelle gouvernance de la donnée : GDPR va donc imposer une nouvelle gouvernance de la donnée aux entreprises avec notamment la mise en place d'un DPO *« Data Protection Officer »*. Celles-ci devront aussi appliquer les principes clés de la réglementation dès la conception de leurs processus.

Comment réussir son projet GDPR ?

Tous ces changements doivent être anticipés et intégrés au sein des entreprises. Ils nécessitent la mise en place d'un projet permettant l'identification des données, l'adaptation des processus, l'accompagnement des équipes et la normalisation des relations avec les autorités concernées comme la CNIL en France.

Une réglementation européenne

A l'heure du numérique, la donnée est reine. Et la donnée personnelle est devenue l'or noir de cette nouvelle ère. Le volume de données personnelles traité par les entreprises est en nette croissance et nécessite des règles adaptées afin d'assurer la liberté et les droits des personnes. C'est dans ce contexte que la réglementation GDPR voit le jour. GDPR *« General Data Protection Regulation »* ou RGDP « Réglementation Générale de la Protection des Données » en français, est la nouvelle réglementation européenne de référence en matière de protection des données. Bien que le projet débute en 2012, le texte final est publié le 26 avril 2016, pour une entrée en application le 25 mai 2018.

On peut distinguer trois objectifs à ce texte :

- **Droit des personnes**. Sans doute, la première motivation de ce texte est d'assurer et de renforcer le pouvoir des individus sur la collecte, le traitement et l'utilisation de leurs données personnelles.
- **Harmonisation**. GDPR se situe ici dans la continuité de la directive 95/46/CE sur la protection des données personnelles qu'elle remplace, en ayant pour but d'harmoniser les normes des différents États-membres.
- **Responsabiliser**. Les obligations induites par ce texte entrainent un changement important au sein des entreprises, notamment en matière d'organisation et de gestion de la donnée.

Cette réglementation dispose d'un pouvoir d'action large car elle concerne toute entreprise européenne collectant ou traitant des données personnelles. Il en est de même des entreprises non européennes qui ciblent le marché européen.

Des enjeux revus et une autorité renforcée

Auparavant, la loi « informatique et libertés » du 6 janvier 1978 prévoyait des sanctions ne pouvant pas excéder 150 000 euros, puis 300 000 euros en cas de récidive dans les 5 années suivantes. Bien que ce montant fût ramené à 3 millions d'euros en 2016 avec la loi pour une République numérique, il est loin des montants des sanctions possibles sous GDPR.

Ainsi, GDPR, c'est de nombreux acteurs (syndicats, associations de consommateurs, gouvernement, citoyens, …) pouvant intenter une action en justice et des sanctions administratives pouvant aller jusqu'à :

- 10 millions d'euros ou 2% du chiffre d'affaires mondial pour les entreprises en cas notamment :
  - De manquement ou d'absence en matière de protection des données dès la conception *« Privacy by design »* et *« by default »* ;
  - D'absence de tenue des registres des traitements ;
  - De manquement sur le rôle et les tâches du DPO *« Data Protection Officer »*.
- 20 millions d'euros ou 4% du chiffre d'affaires mondial pour les entreprises en cas d'infraction notamment :
  - En matière d'obtention du consentement et droits des personnes.
  - Sur un transfert de données à un destinataire situé dans un pays tiers.

En outre, il y a un réel risque d'image en cas de sanction. Il pourrait y avoir une perte de confiance des clients de l'entreprise qui aggraverait la sanction administrative.

Enfin, le risque opérationnel est aussi présent. En cas de non-respect de la norme, l'autorité de contrôle peut ainsi limiter temporairement ou définitivement le traitement de données personnelles. Elle peut suspendre le flux de données. Ces mesures peuvent s'avérer désastreuses, notamment pour les entreprises dont le cœur de métier est la donnée.

Afin de se donner les moyens de faire respecter cette réglementation, le texte prévoit une coopération des autorités nationales concernées, notamment pour les transferts de données transnationaux. Une nouvelle autorité européenne est aussi créée, à savoir l'EDPB, *« European Data Protection Board »*.

Des exigences impactantes

Principes clefs pour trois objectifs

On peut distinguer sur les trois objectifs mentionnés précédemment des principes clefs qui forment le cœur de cette réglementation.

Droit des personnes et transparence

Motivation première, le droit des personnes fait l'objet d'importants changements et se fonde sur le consentement de l'individu. Celui-ci doit être donné librement, de manière spécifique, informé et univoque. Pour renforcer les droits des personnes et la transparence des responsables de traitement, l'individu dispose d'un :

- Droit de retrait : L'individu peut à tout moment et de manière unilatéral, retirer son consentement *(Article 7 (3))*.
- Droit d'accès : Toute donnée personnelle traitée ou collectée peut être demandée par l'individu concerné, au responsable de traitement. Ce dernier doit alors fournir des informations connexes (finalité du traitement, destinataires, catégories de données concernées, la durée de conservation, …) et une copie des données à caractère personnel faisant l'objet du dit traitement *(Article 15).*
- Droit de rectification : Les données devront être complétées, rectifiées / mises à jour par le responsable du traitement dans le meilleur des délais, à la demande de l'individu *(Article 16).*
- Droit à l'oubli : L'individu peut demander à tout moment l'effacement de ses données personnelles *(Article 17).*
- Droit à la limitation du traitement : Dans certaines conditions comme en cas de traitement illicite ou d'inexactitude des données, l'individu peut obtenir la limitation du traitement. Ainsi, bien que l'entreprise puisse conserver les données personnelles, elle ne peut les traiter qu'avec le consentement de l'individu *(Article 18)*.
- Droit à la portabilité : Chaque individu pourra obtenir ces données personnelles d'un responsable de traitement dans un format spécifique structuré et lisible par machine afin de les transmettre. En outre, les responsables de traitement peuvent se voir imposer la transmission de ces données directement si cela est possible *(Article 20).*
- Droit d'opposition : L'individu peut, à tout moment, s'opposer au traitement de ses données personnelles *(Article 21)*.

Harmonisation

Un fort désire d'harmonisation fonde aussi la base de GDPR. Ainsi, le texte est une réglementation et non une directive. Il n'est donc pas transposé dans le droit national mais il est directement et totalement appliqué par les États-membres.

La portée territoriale est aussi renforcée. De ce fait, toute organisation disposant d'un ou plusieurs établissements en Europe traitant des données personnelles est impactée par GDPR, que ces données soient traitées ou non sur le sol européen.

De plus, les organisations non européennes traitant des données personnelles sur des citoyens européens, dont l'activité cible le marché européen, devront aussi respecter les principes de GDPR. Cette activité porte sur le suivi du comportement et sur l'offre de biens ou de services, qu'un paiement soit exigé ou non.

Mais qu'en est-il des données transférées à des filiales se situant hors de l'union européenne ?

Le ***« Binding Corporate Rule »*** désignant un code de conduite, vient compléter le dispositif d'harmonisation de GDPR en encadrant le transfert des données au sein d'un groupe, hors de l'union européenne. Il permet d'assurer un niveau de protection suffisant en prévoyant ce qui est possible ou non de faire.

Une nouvelle gouvernance de la donnée

Bien que ces principes impacteront de manière importante les entreprises, c'est bien la nouvelle gouvernance de la donnée qui formera un véritable challenge en matière d'organisation et de gestion de la donnée. GDPR implique en effet un changement dans le traitement de la donnée, de la conception à l'audit, l'un des buts de la réglementation étant de responsabiliser les entreprises sur le respect de la vie privée et le droit des personnes.

« Privacy by design »

Ainsi, les responsables des traitements devront intégrer une nouvelle méthode, le ***« Privacy by design »***. Les entreprises devront dès la conception de leurs procédures intégrer les principes de la vie privée. Cette notion née en 1990 repose sur 7 principes :

- Des mesures proactives et préventives. Le *« Privacy by design »* consiste à prévoir tout risque et non à réagir à un évènement. Dans un monde où la technologie évolue plus vite que la réglementation, il est nécessaire d'anticiper les possibles incidents.
- Une protection implicite et automatique. La protection de la vie privée est intégrée à minima dans les systèmes d'information et ne demande aucune action de la part des individus.
- Intégrer la protection de la vie privée dans la conception et dans les pratiques.
- Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle. La confiance fait partie intégrante du business. Le *« Privacy by design »* ne doit pas s'opposer à celui-ci mais il doit devenir un avantage concurrentiel de façon à concilier les intérêts.
- Assurer la sécurité de bout en bout. Les données personnelles collectées doivent être sécurisées jusqu'à leur destruction.
- Assurer la visibilité et la transparence. Comme il a été évoqué précédemment, le *« Privacy by desgin »* doit devenir un avantage concurrentiel, il doit instaurer un cadre de confiance dans les relations entre l'entreprise et les individus. Ainsi, assurer la visibilité et la transparence renforcera ce climat.
- Respecter la vie privée des utilisateurs.

Intégrée dans la notion de *« Privacy by design »*, la minimisation des données doit devenir la nouvelle philosophie en matière de gestion. Celle-ci doit être intégrée dès la conception des traitements. Ainsi, il est nécessaire, dans une optique de conformité et de réduction des risques, de concentrer et de rationaliser la collecte des données. Seules les données pertinentes et adéquates doivent être traitées.

L'entreprise doit avoir une bonne vision des données collectées, en distinguant, recensant les données par pertinence.

« Tenu de registres » et documentation

La charge de la preuve incombe aux responsables de traitement. Il est de ce fait de la responsabilité de ses derniers de prouver que leur organisation est en conformité avec la réglementation GDPR et qu'elle embarque ses principes. Via cette notion, la réglementation impose un travail important en matière de gouvernance de la donnée et de documentation aux entreprises concernées.

Ainsi, en vertu de l'article 30 de la réglementation, tout responsable de traitement doit tenir un registre des activités de ses traitements. Ce registre est en soit, un bon outil pour avoir une vision globale de la gestion des données, et intégrer les principes de GDPR.

PIA : *« Privacy Impacts Assesments »*

Le PIA *« Privacy Impacts Assesments »* n'est pas une nouvelle méthode, mais elle est explicitement mentionnée dans la réglementation. Toute entreprise devra effectuer une analyse d'impact relative à la protection des données (PIA), pour tout traitement susceptible d'engendrer des risques élevés pour le droit et liberté des personnes physiques. Cette analyse devra être effectuée avant la mise en place du dit traitement. Au minimum, cette analyse doit contenir :

- Une description des opérations de traitement et de leurs finalités ;
- Une évaluation de la nécessité et de la proportionnalité des opérations ;
- Une évaluation des risques pour les droits et libertés des personnes physiques ;
- Les mesures envisagées pour y remédier et assurer la conformité vis-à-vis de GDPR.

Désignation d'un DPO *« Data Protection Officer »*

La désignation d'un DPO n'est obligatoire que sous certaines conditions (organismes publics, ou organisations traitant des données sensibles à grande échelle). En revanche, véritable pierre angulaire d'un projet GDPR, il peut s'avérer indispensable pour réussir cette mise en conformité. Point de contact avec l'autorité, il aura pour mission d'accompagner l'entreprise dans son projet. Il devra donc piloter le projet, mais aussi sensibiliser et informer les équipes et dirigeants.

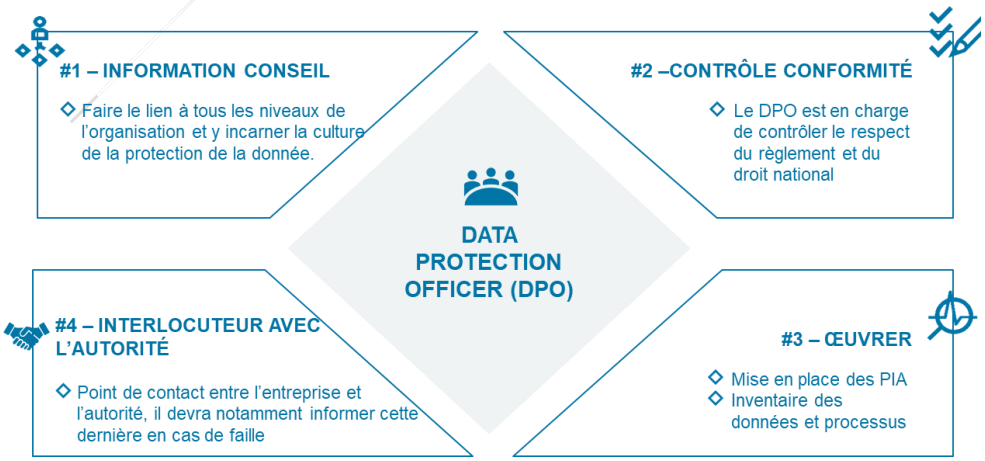


Figure : Rôle du DPO

Comment réussir son projet GDPR ?

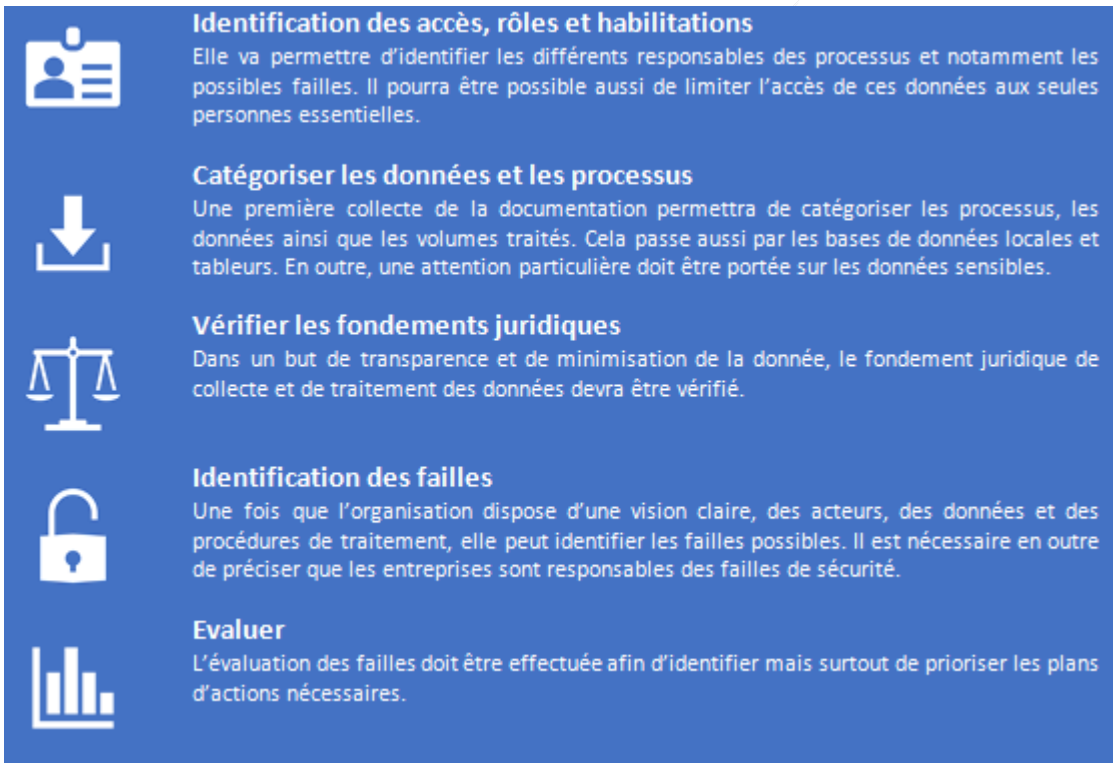
On peut distinguer trois méthodologies à appliquer pour se mettre en ordre de marche. Elles sont complémentaires et doivent être appliquées conjointement. Ainsi, il est nécessaire d'effectuer une approche par les risques afin d'assurer la mise en place de la nouvelle gouvernance. Le renforcement des droits des individus nécessite une approche juridique, quand la gestion des données intègre des outils qui requiert une approche technique.

La nouvelle gouvernance des données impose la mise en place d'un projet en plusieurs étapes :

- Identifier
- Adapter
- Accompagner
- Normer

Identifier

Les responsables de traitement vont devoir identifier les processus de gestion des données. Une cartographie des processus devra être réalisée avec une formalisation des registres des traitements.



Adapter

Comme évoqué précédemment, bien que la réglementation GDPR entre en application en 2018, elle reste dans la droite lignée de la directive de 1995. Les anciennes prérogatives continueront donc à être appliquées. Il est alors important de s'appuyer sur l'existant pour réformer son organisation et la mettre en conformité.

L'entreprise devra adapter sa gouvernance de la donnée compte tenu des prérogatives qui résultent de son analyse d'impact. Elle peut passer notamment par un DPO qui sera en

charge de la mise en place des plans d'action. Des outils de traçabilité des données ou la mise en place de pseudonymisation et d'anonymisation qui sont tous deux encouragés, pourront être nécessaires.

Enfin, des dispositifs de contrôle devront être mis en place pour permettre le maintien en place des bonnes pratiques et des processus en place.

Accompagner

La GDPR implique un changement de philosophie et de politique en matière de gestion des données personnelles. Ce changement doit passer par une sensibilisation des équipes aux principes de la vie privée. Les formations et e-learning seront notamment des outils indispensables pour permettre la diffusion des principes au sein de l'organisation.

Normer

Enfin, comme la charge de la preuve incombe au responsable de traitement, il est nécessaire de normer les relations de ce dernier avec l'autorité nationale, comme la CNIL. Cela passe par une formalisation des PIA, des notifications de *« data breach »* ou de la mise à jour de la documentation (glossaires, dictionnaires de données, documentations méthodologiques, …). La GDPR conseille notamment la mise en place d'un code de conduite.

Conclusion

Avec cette nouvelle réglementation et un calendrier intransigeant, l'Union Européenne engage un tournant dans la protection des données. Bien que certaines de ces notions comme le *« Privacy by design »* ne sont pas nouvelles, elles deviennent pour la première fois une obligation réglementaire. Ces nouveaux impératifs entrainent d'importants changements d'organisation et de culture qui n'ont pas été nécessairement anticipés par les acteurs.

GDPR ne devrait pas se voir comme une entrave au business mais comme une chance de se démarquer et de créer un avantage concurrentiel. A l'heure, ou les données personnelles sont de plus en plus utilisées dans la conduite du business, créer un cadre de confiance pourrait s'avérer stratégique et profitable pour les deux parties. La réglementation prévoit notamment la mise en place de certifications qui peuvent constituer un gage de respect de la sécurité des données et du respect de la vie privée des individus.