Règlement général sur la protection des données (RGPD)

Introduction :

Le Règlement général sur la protection des données (dit " RGPD ") adopté le 14 avril 2016 et entré en vigueur le 25 mai 2018 a été perçu et ressenti comme une véritable révolution dans la protection des données personnelles et, plus largement, de la vie privée.

Cependant, le GDPR remplace ou complète des textes déjà anciens dont les principes étaient déjà très proches : la directive 95/46/CE du 24 octobre 1995 au niveau européen ou, par exemple, la loi Informatique et Libertés en France datant du 6 janvier 1978.

Ce qui fait du GDPR un texte particulièrement innovant et impactant pour les entreprises au sens large, c'est d'une part sa volonté d'uniformiser le cadre réglementaire de la protection des données dans toute l'Union européenne, voire au-delà, et d'autre part le renforcement des obligations pesant sur les entreprises avec des sanctions très fortes.

Ce champ d'application étendu se traduit par le fait que le GDPR concerne toutes les entreprises et tous les organismes publics ou privés qui collectent ou traitent des données à caractère personnel en Europe : les cabinets d'avocats, mais aussi les professionnels du droit tels que les notaires ou les huissiers de justice sont donc tous concernés par le GDPR dans le cadre de leurs activités qui impliquent le traitement de volumes importants de données à caractère personnel.

En ce qui concerne nos obligations professionnelles et éthiques, nous devons être particulièrement vigilants et veiller à ce que nos activités soient conformes à ces nouvelles exigences.

Nouveautés du GDPR

1. Un champ d'application plus large

Les principaux objectifs du GDPR, à savoir l'harmonisation des réglementations nationales et le renforcement de la protection des données personnelles dans le contexte mondialisé dans lequel elles sont traitées, ont donné lieu à un champ d'application considérablement élargi :

La notion de "données à caractère personnel" est extrêmement large, puisqu'il s'agit de "*toute information concernant une personne concernée*" qui correspond à "*une personne physique identifiée* [...] *ou qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale [...]*". Ainsi, les données à caractère personnel ne sont plus définies uniquement en fonction du caractère identifiant de l'information détenue par le responsable du traitement lui-même, mais également en fonction de la possibilité que cette information soit croisée avec toute autre information détenue par un tiers et lui conférant un caractère identifiant.

En outre, la définition des données anonymes ou pseudonymes dans le cadre du GDPR est extrêmement restrictive. En substance, dès qu'une donnée est susceptible d'être individualisée, même sans identifier directement une personne, elle entre dans le champ des données à caractère personnel.

Par exemple, en faisant des statistiques pseudonymisées sur les préférences de ses clients ou en conservant des documents relatifs à une affaire qui ne font pas apparaître le nom ou le prénom d'une personne... on traite a priori des données à caractère personnel, et on doit respecter le GDPR.

Le champ d'application territorial du GDPR est étendu : dès lors qu'un traitement est effectué dans le cadre des activités d'un établissement situé sur le territoire de l'Union européenne, qu'il concerne un résident européen, ou qu'il est lié à une offre de biens ou de services à des personnes situées sur le territoire de l'Union européenne, le GDPR s'applique. De même, le transfert de données en dehors de l'Union européenne ou l'accès aux données depuis l'extérieur de ce territoire est soumis à des règles très strictes qui tendent à se renforcer sous l'influence de la Commission européenne.

On le comprend, dans le contexte de l'utilisation constante des outils numériques et des nouvelles technologies et où les données personnelles deviennent un enjeu économique fort : le GDPR s'applique partout et tout le temps !

2. Des obligations renforcées

Le GDPR impose aux entreprises de repenser l'organisation de la gestion et de la protection des données personnelles à travers, notamment :

L'obligation pour toutes les entreprises, sauf dans certains cas, **de tenir un registre** répertoriant les traitements qu'elles effectuent. Ce registre doit contenir un certain nombre d'informations qui nécessitent de savoir exactement quelles données sont traitées et comment. Ce travail peut sembler fastidieux mais permet souvent une analyse approfondie qui facilite la mise en conformité avec le GDPR par la suite.

L'obligation de définir la **répartition des responsabilités avec ses prestataires ou partenaires :** le GDPR prévoit différentes qualifications (responsable du traitement, co-responsable du traitement, ou sous-traitant) qui dépendent de qui décide des moyens et des finalités du traitement des données personnelles. La répartition de ces responsabilités doit être contractualisée dans un document respectant un certain nombre de dispositions imposées par le GDPR.

- Il peut être obligatoire ou recommandé de désigner un "délégué **à la protection des données**", le fameux "DPD" qui est la pierre angulaire de la conformité au GDPR.

- Les principes de minimisation et de proportionnalité introduits par le GDPR imposent également de définir **les durées de conservation des données** (quel que soit le support : papier ou numérique). Ces "politiques de conservation des données" doivent être fiables et fondées sur des critères clairs, tels que les finalités pour lesquelles les données sont utilisées (je ne dois pas conserver des données dont je n'ai pas besoin), les obligations légales ou les délais de prescription applicables.

Le GDPR insiste aussi fortement sur la mise en œuvre des **mesures nécessaires, qu'elles soient techniques ou organisationnelles, pour assurer un niveau de sécurité suffisant des données traitées**. Il prévoit également l'obligation de notifier à l'autorité de contrôle nationale les pertes et violations graves de données à caractère personnel dans les 72 heures suivant la découverte de la violation, ce qui est généralisé à toutes les organisations. En outre, lorsque la violation est susceptible d'affecter la vie privée des personnes concernées, celles-ci devront également être notifiées.

Le GDPR a modifié les attentes des entreprises et organisations qui traitent des données : alors qu'auparavant, comme en France, il suffisait de faire de simples déclarations à la Commission Nationale Informatique et Libertés, il est désormais exigé d'avoir une connaissance approfondie des traitements mis en œuvre et de documenter la manière dont les exigences réglementaires sont respectées.

3. Protection accrue des droits des personnes concernées

Le caractère protecteur du GDPR se traduit par un renforcement des droits des personnes concernées. Ainsi, aux droits existants tels que le droit d'accès ou le droit de rectification ont été ajoutés de nouveaux droits que les personnes concernées peuvent exercer auprès des entreprises :

Droit à l'information étendu (articles 13 et 14 du GDPR) : En plus des informations déjà prévues dans le règlement précédent, l'information des personnes doit notamment porter également sur "la durée de conservation" et "toute autre information nécessaire pour assurer un traitement loyal des données", ce qui est très large.

Consentement (articles 4 et 7 du GDPR) : Lorsqu'il est requis, le consentement doit être explicite et distinct. En d'autres termes, les personnes doivent donner leur consentement pour chaque utilisation de leurs données pour laquelle il est requis. En outre, le GDPR introduit des exigences de consentement spécifiques pour les enfants de moins de 16 ans pour la fourniture de certains services.

Le droit à l'**effacement** ou "droit à l'oubli" (article 17 du GDPR) : Les personnes concernées peuvent demander l'effacement de leurs données dans de nombreux cas, notamment lorsque les données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou traitées, ou lorsqu'elles souhaitent retirer leur consentement ou s'opposer au traitement.

Le droit à la **portabilité** (article 20 du GDPR) : Les responsables du traitement doivent permettre que les données d'une personne concernée soient fournies à un autre responsable du traitement dans un format "structuré, couramment utilisé et lisible".

La gestion des demandes d'exercice des droits par les personnes concernées doit être anticipée afin de pouvoir y répondre de manière complète et dans les délais imposés par le GDPR. Cela inclut, par exemple, pour le droit à l'information, la révision des notices d'information ou de la politique de confidentialité sur son site web ou tout autre support par lequel des données sont collectées. De même, afin de pouvoir répondre à une demande de droit d'accès, il est recommandé d'anticiper une procédure visant à identifier quelles données doivent ou peuvent être transmises et comment extraire de ses systèmes d'information des volumes de données qui peuvent être significatifs.

Pour assurer le respect de ces obligations et donner aux autorités de protection un véritable levier contre les entreprises qu'elles contrôlent, le GDPR a ajouté des **sanctions administratives dont le** montant a été fortement augmenté. Selon le type de violation, l'amende peut atteindre 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. L'arsenal des sanctions contient également la possibilité pour les autorités de contrôle de rendre leurs décisions publiques, ce qui est très impactant et donc dissuasif pour les entreprises sanctionnées.

<u>Les principales mesures de mise en conformité</u>

Quelles sont les principales étapes ?

1. **Définir la gouvernance** : pour aborder la conformité de manière appropriée et rationnelle, il est recommandé de :

- Déterminer s'il est obligatoire ou pertinent de désigner un DPD et identifier les acteurs stratégiques internes et/ou externes chargés d'assurer la conformité ;
- Mener des campagnes de sensibilisation internes pour diffuser les bonnes pratiques et garantir l'efficacité de l'approche.

2. **Inventaire des traitements** : cette étape est essentielle pour adapter les mesures de conformité et assurer la création d'un registre complet. Pour ce faire, il est souvent utile de commencer par rassembler et analyser la documentation existante (registre, anciennes déclarations CNIL, etc.) avant de procéder à l'inventaire des principales catégories de traitements par projet et/ou par finalité (clients, ressources humaines, prestataires de services informatiques, etc.)

3. **Prioriser les actions à mener** : il est nécessaire d'**établir un calendrier en tenant compte des éléments suivants**
    - Les activités, la taille et la structure des équipes impliquées
    - Facteurs externes éventuels susceptibles d'avoir une incidence sur les actions prioritaires à entreprendre (par exemple, nouveau projet en cours ou à venir)

4. **Garantir la conformité** :

Toutes ces actions peuvent être mises en œuvre au fur et à mesure des besoins, en fonction des priorités spécifiques de chaque activité.