Que vous impose le RGPD ?

Dans les grandes lignes le RGPD impose 4 obligations pour tous :

- **Obligation 1** – Une information transparente des personnes dont vous conservez et utilisez les données. Renforce votre obligation générale d'information et de transparence des personnes concernées par le traitement. Il vous sera nécessaire de vous doter de politiques de données à caractère personnel, tant à destination de vos salariés que de vos utilisateurs, ainsi que de mentions d'informations devant être portées à la connaissance des personnes qui voient leurs données à caractère personnel collectées ;

- **Obligation 2** – Protéger et sécuriser vos données, c'est-à-dire, selon le RGPD, prendre les mesures nécessaires pour empêcher que les données ne soient détruites, endommagées ou qu'un tiers non autorisé y ait accès. En cas de violation de données, vous devez prévenir immédiatement la Cnil ;

- **Obligation 3** – Ne pas faire traiter les données à caractère personnel par des entreprises situées hors du territoire de l'Union Européenne sans vous assurer que les prestataires en questions respectent bien les règles fixées par le RGPD ;

- **Obligation 4** – Identifier avec précision les prestataires à qui vous transmettez des données (fichier paie, agence de communication, solutions SaaS, etc.) et avoir avec eux un contrat qui fixe les règles précises imposées par le RGPD.

Le RGPD fixe également des obligations spécifiques selon le type de traitement mis en œuvre ou la taille de l'entreprise :

- **Obligation 1** - Tenir un registre des activités de traitement c'est-à-dire un listing de vos traitements si vous avez plus de 250 employés, sauf dans certains cas spécifiques (ex : lorsque le traitement présente un risque majeur pour les données à caractère personnel ou lorsqu'il s'agit d'un traitement de catégories de données dites « sensibles ») ;

- **Obligation 2** - Désigner un délégué à la protection des données dans 3 cas : les acteurs publics (État, collectivités locales et leurs établissements), les traitements des données à grande échelle (big data, profiling, …) ou encore un traitement de données sensibles ;

- **Obligation 3** - Réaliser une analyse d'impact dans le cas particulier où, compte tenu de la nature, de la portée, du contexte et des finalités du traitement, il est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Que faire en pratique ? La mise en œuvre du RGPD implique 4 phases :

- **Phase 1** – la cartographie des traitements qui doit vous permettre d'identifier avec précision les traitements que vous utilisez dans votre entreprise ;

- **Phase 2** – l'analyse d'écart entre vos pratiques et le RGPD ;

- **Phase 3** – la mise en œuvre du RGPD sur les aspects non traités ;

- **Phase 4** – sensibiliser vos collaborateurs.

Cas particulier de l'obligation de sécurité. Le RGPD renforce de manière très significative vos obligations en termes de sécurité. Après avoir procédé à une analyse de risque, il vous faudra en effet selon les termes mêmes du RGPD « mettre en œuvre les mesures techniques et organisationnelles appropriées » pour protéger vos traitements et fichiers. Le RGPD impose un certain nombre de règles :

- **Règle 1** - Protéger les données elles-mêmes par des solutions de chiffrement par exemple ;

- **Règle 2** - Limiter et contrôler les accès aux données ;

- **Règle 3** - Mettre en place des mesures de reprise ou de continuité d'activité sur les traitements (PCA/ PRA).

Sur la partie sécurité, le RGPD impose par ailleurs que vous mettiez en place une procédure d'audit et de vérification et que les mesures de sécurité elles-mêmes soient toujours pertinentes.

Que risquez-vous à ne pas appliquer le RGPD ? Les entreprises ou les acteurs publics qui ne respecteraient pas le RGPD au 25 mai 2018 s'exposent à une sanction financière sous forme d'amende administrative de la Cnil. Cette amende peut atteindre 10 à 20 millions d'euros ou 2 à 4% du chiffre d'affaires annuel mondial de l'entreprise.