

Le Règlement général sur la protection des données (« *RGPD* ») est entré en vigueur le 25 mai dernier.

Afin de vous mettre rapidement en conformité avec les dispositions du RGPD les principales mesures à prendre sont les suivantes :

- **Réaliser un audit interne :**
Identifier l'ensemble des traitements de données à caractère personnel, les personnes concernées, les données collectées et les mesures de sécurité d'ores et déjà en place.
- **Mettre en place un registre des traitements de données à caractère personnel :**
Mettre en place et tenir à jour un registre recensant l'intégralité des traitements de données à caractère personnel effectués.
- **Vérifier la conformité au RGPD de ses sous-traitants :**
S'assurer que vos sous-traitants agissent en conformité avec le RGPD et que les contrats vous liant en tant que responsable de traitement avec vos sous-traitants prévoient des obligations en ce sens à la charge de ces derniers.
- **Informez les personnes concernées :**
Informez les personnes concernées de leurs droits relatifs à la collecte et au traitement de leurs données à caractère personnel et, lorsque cela est matériellement possible, obtenir leur consentement exprès lors de la collecte de ces données.
- **Sécuriser l'environnement informatique des données :**
Instaurer toutes les mesures organisationnelles et techniques qui s'imposent pour assurer la sécurité des données à caractère personnel.
- **Veiller à la protection des données transférées en dehors de l'Union européenne :**
En cas de transfert de données à caractère personnel en dehors de l'Union européenne, s'assurer que le destinataire de ces données présente un niveau de protection suffisant.
- **Nommer un Délégué à la protection des données (« DPO ») :**
La désignation d'un DPO est notamment obligatoire lorsque les traitements de données sont effectués par une autorité publique ou un organisme public.
- **Réaliser une analyse d'impact :**
L'analyse d'impact s'impose dès lors que le traitement de données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées.

A noter que les montants des sanctions financières pouvant être prononcées par la CNIL en cas de non-conformité aux dispositions du RGPD ont été considérablement augmentés (les sanctions financières pourront désormais atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial).

Les éléments listés ci-avant ne sont pas exhaustifs ; ils constituent uniquement des indications essentielles pour une mise en conformité avec le RGPD. Pour toute information complémentaire, vous pouvez vous rapprocher de nos avocats, le cabinet Lafarge Associés (Me Stéphane Colombet et Me Pauline Buche – 41 rue des Acacias 75017 Paris – tél. 01 44 29 32 00 – s.colombet@lafargeassocies.com).