Fiche pratique n° 1- LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le délégué à la protection des données ("Data Protection Officer" ou "DPO" en anglais) occupe une place importante au sein du cadre juridique créé par le RGPD. Les articles 37 à 39 du RGPD posent les règles applicables à la désignation, à la fonction et aux missions du DPO.

Le DPO est principalement chargé:

- ✓ d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- ✓ de contrôler le respect du règlement et du droit national en matière de protection des données ;
- ✓ de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- ✓ de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Red Flag Nommer un DPO ne dégage pas le gérant de ses responsabilités en matière de gestion des données.

Les DPO doivent être nommés pour toute organisation qui traite de manière systématique ou stocke de grandes quantités de données à caractère personnel, qu'il s'agisse d'employés, de personnes extérieures à l'organisation ou des deux.

La désignation d'un DPO est obligatoire dans trois hypothèses :

- ✓ le traitement est effectué par une **autorité publique ou un organisme public** ;
- ✓ les **activités de base** de l'entreprise consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle** des personnes concernées ;
- ✓ les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données.

Red Flag Pour les cas où un DPO n'est pas obligatoire, une personne de contact en matière de protection des données est fortement recommandée afin de centraliser pour l'entreprise les mesures qu'impliquent la gestion de données.

Il est important que le DPO ou la personne de contact dédiée ait les connaissances, les ressources et la compétence pour exercer ses fonctions en matière de protection des données.

Exemple d'activité de base : Les activités de base d'une banque impliquent des traitements de données financières de ses clients. La banque doit aussi traiter des données RH de ses employés, mais c'est une activité accessoire.

Exemple de traitement à grande échelle : Le traitement de données de patients par un hôpital, contrairement au traitement de données de patients effectués par un médecin exerçant à titre individuel.
Exemple de suivi régulier et systématique: Une banque qui doit régulièrement et systématiquement suivre l'évolution des comptes et des transactions de ses clients notamment dans le cadre de ses obligations liées à la prévention de la fraude, du blanchiment d'argent ou du financement du terrorisme.