GUIDE DE BONNES PRATIQUES

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (R.G.P.D.)

Par les présentes fiches, l'Ordre des barreaux francophones et germanophone (AVOCATS.BE) formule des recommandations de bonnes pratiques destinées à aider les avocats à se conformer au règlement (U.E.) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

FICHE 6 : SOUS-TRAITANCE

Ce qu'il faut savoir

L'avocat peut faire appel à des personnes qui traitent les données pour son compte. Il s'agit de « sous-traitants », au sens de l'article 4.8 du R.G.P.D.

Par exemple **un prestataire informatique** qui stocke les données du cabinet (un prestataire de service de stockage en cloud par exemple),

Ce qu'il faut faire

Conditions à respecter:

- **Sous-traitants présentant des garanties suffisantes** (notamment en termes de connaissances spécialisées, de fiabilité et de ressources),
- **Communication par le prestataire de sa politique de sécurité** des systèmes d'information. Il devra prendre et documenter les moyens (audits de sécurité, visite des installations, etc.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données. Ces garanties incluent notamment :
    - le chiffrement des données selon leur sensibilité ou, à défaut, l'existence de procédures garantissant que le prestataire n'a pas accès aux données qui lui sont confiées ;
    - le chiffrement des transmissions de données (ex : connexion de type HTTPS, VPN, etc.) ;
    - des garanties en matière de protection du réseau, de traçabilité (journaux, audits), de gestion des habilitations, d'authentification, etc.
- **Contrat avec le sous-traitants**, qui définit notamment l'objet, la durée, la finalité du traitement et les obligations des parties. Ce contrat doit correspondre aux exigences de l'article 28 du R.G.P.D. et reprendre notamment :

    - leurs obligations de confidentialité des données personnelles confiées ;
    - des contraintes minimales d'authentification des utilisateurs ;

- les conditions de restitution et/ou de destruction des données en fin du contrat ;
- la possibilité d'audit de sécurité, de visite des installations ;
- les règles de gestion et de notification des incidents au responsable de traitement.