Check-list RGPD

Mise en conformité avec
le Règlement (UE) 2016/679

1. Nommer un Délégué à la Protection des Données (*DPD*)

Cette disposition est fortement recommandée, même si elle n'est pas strictement obligatoire pour une majorité de PME. Le DPD sera un relais essentiel auprès du chef d'entreprise ou des responsables de traitement des données pour informer sur les obligations du RGPD et réduire les risques de non-conformité et de sanctions.

2. Évaluer objectivement votre niveau d'exposition au risque de non-conformité en procédant à une *Analyse d'Impact* (*AIPD*)

Si vous estimez qu'un traitement ou un ensemble de traitements est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées, le RGPD préconise de procéder à une *Analyse d'Impact relative à la Protection des Données*. Les autorités européennes ont publié des *lignes directrices* visant à distinguer les cas de figure où un traitement des données requiert ou non une Analyse d'Impact. En cas de contrôle la Cnil exigera la production d'une AIPD.

3. Tenir un Registre des traitements

Format papier ou numérique. Vous devez y consigner toutes les informations explicitant la nature, la finalité et la sécurisation du traitement des données. Il n'est pas obligatoire pour les entreprises de moins de 250 employés, mais il est recommandé, même pour de très petites entreprises, de tenir un Registre dès lors que vous réalisez des traitements de données personnelles.

4. Mettre à jour de conformité l'ensemble des contrats avec les Prestataires et Sous-traitants

Le RGPD stipule que désormais, le ou les sous-traitants participant avec leur client à un traitement de données personnelles sont automatiquement considérés comme coresponsables. Pour chacun des traitements, veillez donc à ce qu'un contrat écrit précise les obligations de chaque partie.

5. Sensibiliser et former le personnel de l'entreprise

La formation de l'ensemble des collaborateurs de l'entreprise sur les nouveaux enjeux et obligations du RGPD fait partie de la démarche globale de mise en conformité de l'entreprise.

6. Prévoir une procédure de crise

En cas de violation de données à caractère personnel, vous devrez prévenir la Cnil dans les 72h.

----- Fin check-list ------