Les Echos

Données nominatives : **anticiper les mesures à prendre pour respecter le RGPD au 28 mai 2018**

FRÉDÉRIC RAIMBAULT (HTTPS://WWW.LESECHOS.FR/IDEES-DEBATS/CERCLE/AUTEURS/INDEX.PHP?ID=65391) / Avocat associé Steering Legal | Le 28/02 à 13:50

Pour respecter le règlement général sur la protection des données (RGPD), qui s'applique à compter du 28 mai prochain, les entreprises et les administrations doivent mettre en place un certain nombre de mesures si elles veulent se mettre à l'abri des lourdes sanctions financières prévues.

Ce nouveau cadre, commun à tous les États membres de l'Union européenne, vise à protéger les données se rapportant, directement ou indirectement, à une personne physique identifiable (notamment par référence à un identifiant, un numéro ou à des éléments spécifiques propres à son identité physique, physiologique, économique, sociale...). Il concerne donc largement tous les traitements de données, du simple fichier Excel à la base de données hébergée dans un serveur.

Aussi, un véritable bouleversement en France

Même si la France est précurseur en ce domaine et si entreprises et administrations françaises ne partent pas de zéro, il ne leur suffit plus désormais de déclarer leurs fichiers à la CNIL.

La nouvelle logique de responsabilisation (accountability) leur impose de pouvoir justifier, à tout moment, respecter le nouveau cadre. Pour cela, responsables de traitement ou sous-traitants doivent mettre en place sur le terrain certaines mesures concrètes, au-delà de celles déjà pratiquées en France depuis 1978.

10 mesures pour respecter le RGPD :

1. Recueillir le consentement des personnes physiques dont les données figurent dans leurs fichiers, les modalités variant selon la finalité des fichiers

2. Leur accorder un droit de rectification et un droit à l'oubli pour faire effacer les données les concernant

3. Prendre en compte - pour les fabricants de produits, prestataires de services et producteurs d'applications - le droit de la protection des données lors de l'élaboration et la conception des produits pour observer le principe de protection des données dès la conception (protection by design)

4. Pseudonymiser les données à caractère personnel pour respecter le principe de protection des données par défaut (protection by default)

5. Réaliser une étude d'impact identifiant et cartographiant les risques induits par les traitements de données à caractère personnel sur la vie privée des personnes physiques concernées pour respecter ces deux nouveaux principes

6. Tenir un registre pour les activités de traitement afin de démontrer que les prescriptions sont respectées et coopérer avec la CNIL

7. Désigner obligatoirement un délégué à la protection des données (data protection officer ou DPO) dans les administrations et les entreprises de plus de 250 employés

8. Le choisir pour ses qualités professionnelles, sa connaissance du droit et des pratiques en matière de protection des données et sa capacité à accomplir ses missions particulières (informer, conseiller le responsable du traitement ou ses sous-traitants, contrôler le respect des règles de protection des données, dispenser des conseils, coopérer avec la CNIL), pour lesquelles il ne pourra être ni relevé de ses fonctions ni pénalisé

9. Avec son aide, mettre en place des changements techniques et organisationnels

10. Revoir ses contrats.

Même si sa prévention représente un coût économique certain, il en vaut la peine compte tenu du "risque RGPD", très lourd. Les sanctions peuvent, en effet, désormais atteindre 20 millions d'euros ou, dans le cas d'une entreprise, 4 % du CA annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.