

La mise en conformité au RGPD au sein des entreprises : défis et opportunités

Face à l'utilisation croissante des données personnelles des personnes physiques par les entreprises, l'Union européenne a fait le pari de protéger leur utilisation en la sanctuarisant de façon assez inédite.

Ainsi, le Règlement général sur la protection des données qui entrera en vigueur le 25 mai prochain, crée de nouvelles obligations pour toute entreprise manipulant des données personnelles, ainsi que ses sous-traitants. La mise en conformité à cette réglementation représente pour les entreprises un véritable défi nécessitant de procéder à un changement de culture en matière de gouvernance des données personnelles.

Le RGPD tend à responsabiliser les acteurs économiques, incités à entrer dans l'ère de la compliance en matière de données personnelles. Les entreprises devront s'autoréguler à travers la mise en oeuvre de mesures techniques et opérationnelles garantissant un traitement des données respectant la vie privée et les nouveaux droits garantis par le RGPD aux citoyens européens : droit à l'oubli, droit à la rectification et droit à la portabilité des données.

Concrètement, les entreprises auront à identifier elles-mêmes les potentiels risques que représentent leurs modes de traitement et prendre les mesures appropriées pour assurer la sécurité des données personnelles. Ces mesures seront contrôlées a posteriori par la CNIL qui verra, par là même, son pouvoir de contrôle renforcé et pourra infliger une amende administrative de 20 millions d'euros ou bien équivalent à 4% du chiffre d'affaires annuel mondial de l'entreprise.

A moins de 10 jours de l'entrée en vigueur de cette réglementation historique, quels chantiers les entreprises doivent-elles mettre en oeuvre ?

Chantier n°1 : la tenue d'un registre des données

Les entreprises devront répertorier toutes les données à caractère personnel collectées au sein d'un registre des traitements. Ce dernier devra indiquer les finalités pour lesquelles ces dernières sont utilisées, l'emplacement de ces données, et préciser la liste des personnes autorisées à y accéder, ainsi que les mesures garantissant leur sécurité. Toutes les données qui ne seront plus nécessaires au regard des finalités initiales devront être supprimées. Dans ce cadre, un nouveau rôle voit le jour, celui du Data Protection Officer ou responsable de la protection des données, garant du respect du RGPD au sein de l'entreprise.

Chantier n°2 : le respect du consentement libre et éclairé en matière de recueil des données personnelles

Le consentement tel que défini par la RGPD devra être libre, éclairé et univoque. Autrement dit, il ne pourra pas être « noyé » parmi des conditions générales de vente, ou donné « en cochant une case lors de la consultation d'un site internet ». Les entreprises devront donc informer les utilisateurs de ces nouvelles modalités et mettre en place de nouveaux procédés pour recueillir leur consentement.

Chantier n°3 : la mise en place d'étude d'impact pour certains types de traitements de données

Le RGPD impose la réalisation d'une étude d'impact pour tous les modes de traitement présentant « un risque élevé pour les droits et libertés des personnes physiques ». Cette étude devra évaluer les risques que représente le traitement des données, notamment au regard de la vie privée, et ainsi permettre la mise en place des mesures de sécurité adéquates. L'étude d'impact s'impose notamment quand le traitement des données produit des effets juridiques ou affecte particulièrement une personne physique.

Chantier n°4 : la mise à niveau des mesures garantissant la sécurité des données

Les entreprises restent libres de choisir les mesures appropriées pour garantir la sécurité des données. Le règlement offre néanmoins quelques pistes en énumérant des mesures parmi lesquelles la pseudonymisation (opération visant à remplacer une donnée personnelle par un pseudonyme), ou le chiffrement.

Quel bénéfice tirer du RGPD ?

Le défi est de taille, mais revêt de nombreuses opportunités. A l'heure où l'utilisation des données personnelles est source de nombreuses inquiétudes au sein de la société, fort est à parier qu'à l'avenir les clients accorderont davantage leur confiance aux entreprises respectant cette réglementation. En ce sens, la conformité au RGPD constituera peut-être à terme un véritable avantage concurrentiel. Il ne s'agit donc pas uniquement d'un enjeu réglementaire, mais bel et bien d'un point stratégique en matière d'image et de développement, dont les entreprises doivent se saisir au plus vite !