Lire cet article en ligne

RGPD : comment se mettre en conformité d'ici le 25 mai 2018 ?

Le règlement européen sur la protection des données personnelles (RGPD) s'appliquera à partir du 25 mai 2018 sur tout le territoire de l'Union européenne. Les entreprises vont devoir assurer une protection renforcée des données à caractère personnel sous peine de sanctions pouvant atteindre 4% de leur chiffre d'affaires annuel. Le règlement, qui comporte 99 articles et 173 considérants, mêle le juridique et le technique dans une démarche d'*accountability*. Que faut-il en retenir concrètement ?

Quelles entreprises ?

Toutes les entreprises, quelle que soit leur taille (start-up, TPE, PME, ETI et grandes entreprises), établies dans l'Union européenne, mais également celles établies en dehors de l'Union européenne qui ciblent les résidents de l'Union européenne par une offre de biens ou de services ou le profilage.

Quels changements ?

Le RGPD implique un changement profond de culture. Les entreprises vont devoir intégrer un nouveau principe de protection des données dès la conception du traitement (*Privacy by design*) et par défaut (*Privacy by default*). Elles devront ainsi tenir compte des règles d'or de la protection des données dès la phase de conception du produit, du service ou du traitement. Il s'agira en particulier de minimiser à tout point de vue le traitement effectué. Ces principes s'intègrent dans le principe plus général d'*accountability* qui consiste pour les entreprises à mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Les entreprises seront ainsi appelées à formaliser des politiques de confidentialité des données, des procédures relatives à la gestion des consentements, des demandes d'exercice des droits et des failles de sécurité et à adapter leurs contrats. Dans certains cas, elles devront même tenir un registre de leurs activités de traitement, effectuer des analyses d'impact sur la vie privée ou désigner un délégué à la protection des données.

Comment procéder ?

Les entreprises doivent structurer leur démarche et il est utile pour cela de se faire accompagner à la fois par des avocats et des consultants en SI (systèmes d'information) expérimentés. Commencer par réaliser un audit pour analyser l'existant (Comment sont collectées les données et les consentements ? Pour quelles finalités ? Quelles sont ces données ? Le principe de minimalisation est-il respecté ? Où sont-elles stockées ? Quels sont les transferts de ces données ? Quel est le niveau de sécurité des bases de stockage et des flux (cryptage, anonymisation, etc.) ? Quelles sont les procédures en vigueur en cas de failles ?). L'audit doit permettre d'identifier les écarts de conformité et les travaux de mise en conformité à mener. Une troisième étape consiste à construire un plan d'action dans lequel devront être listés et programmés les différentes actions et chantiers à entreprendre. L'équipe du projet doit être pluridisciplinaire et réunir les ressources internes et/ou externes permettant de prendre en compte tous les enjeux du projet : juridiques, organisationnels, technologiques, commerciaux et marketing.

Notre Cabinet vous accompagne dans toutes les étapes de cette mise en conformité.