GDPR : Une législation peu connue qui va changer la gestion et la protection des données au niveau européen

Le nouveau règlement européen en matière de protection des données a changé. Peu de personnes le savent, mais il va considérablement changer notre rapport à la sécurité informatique.

Qu'est-ce que le GDPR ?

Il s'agit de l'acronyme anglais d'un nouveau règlement européen modifiant le cadre juridique relatif à la protection des données personnelles au sein de l'union européenne, effectif début 2015. Il impactera toutes les entreprises collectant, gérant, ou stockant des données et aura pour but principal de simplifier et harmoniser la protection des données dans les 28 pays de l'union européenne. En cas de non respect du règlement par les entreprises, des amendes allant jusqu'à 100 millions d'euros ou 5% du chiffre d'affaire mondial seront applicables. L'objectif du GDPR est de faire face aux nouvelles réalités du marché, notamment en matière de protection des données liée aux réseaux sociaux ou encore au cloud computing, Les notions de transferts de fichiers sécurisés et de droit à l'oubli font également parti du GDPR. Le développement des clouds privés, publics, ou encore de solutions hybrides a compliqué le stockage et le traitement des données au cours de ces dernières années. Le GDPR clarifiera les responsabilités de chaque entreprise en contact avec les données, facilitant ainsi la mise en conformité.

Actuellement, comment les organisations gèrent-elles les impératifs de protection des données ?

Existe-t-il des différences en fonction des pays ? Chaque pays détient sa propre autorité de protection des données pour le moment. Puisque le GDPR est un règlement et non une directive, il s'appliquera directement à tous les pays de l'UE sans avoir besoin de changer les législations nationales. Le GDPR aura un impact significatif sur les compagnies non-européennes opérant sur le sol européen, puisqu'il s'appliquera aussi bien aux compagnies européennes qu'aux non-européennes commerçant dans l'UE, reflétant ainsi la réalité actuelle : le business est sans frontière.

Quel sera l'impact sur les entreprises ?

Les entreprises devront repenser la manière dont elles collectent, traitent et stockent les données. Il sera obligatoire de tenir à disposition des internautes dont les données sont stockées un texte clair expliquant la politique de sécurisation des données. Les entreprises devront également pouvoir leur fournir toutes leurs données personnelles dans un format simple et transférable via internet. Bien sur le droit à l'oubli devra également rendre possible la suppression rapide de toutes les données. Cette partie du règlement influence déjà certaines sociétés, comme Facebook et Google qui se préparent peu à peu au GDPR.

Les entreprises sont elles prêtes pour la mise en place de ce règlement ?

Il semble que peu d'entreprises soient prêtes. Selon un sondage Ipswitch réalisé fin 2014 sur 316 entreprises européennes, 52% des sondés ont répondu ne pas être prêts. Plus grave encore 56% ne savaient pas exactement à quoi correspond le sigle GDPR. Par ailleurs, 64 % des personnes interrogées ont reconnu n'avoir aucune idée de la date d'entrée en vigueur supposée de ce règlement. Seules 14 % des personnes interrogées ont pu indiquer clairement que le GDPR est censé entrer en vigueur début 2015. Autre point préoccupant : 79% des sondés font appel à un fournisseur cloud, mais seulement 6% ont pensé à demander à leur prestataire s'il était en règle avec le règlement européen.

Que peuvent faire les entreprises pour s'assurer qu'elles sont en conformité avec le GDPR ?

Plusieurs mesures peuvent être prises pour s'assurer de la conformité de sa structure informatique. Les contrats avec tous les prestataires informatiques, notamment les fournisseurs de services cloud, doivent être passer en revue. Il faut s'assurer que, pour chaque information collectée, une demande de consentement soit effectuée et enfin il est nécessaire de savoir précisément où les données sont stockées. Une fois les processus en règle, l'entreprise pourra demander un certificat européen, valable 5 ans, attestant sa conformité au GDPR.