Post-Brexit : les nouveaux défis de protection des données pour les entreprises

Depuis des mois, le Brexit est au cœur des préoccupations des entreprises qui doivent se conformer à cette nouvelle configuration politique. Sont-elles vraiment préparées aux nouvelles réglementations en matière de données et de protection ?

Fin 2020, la signature de l'accord sur les futures relations commerciales entre le Royaume-Uni et l'Union européenne, promettant plus de transparence et de confiance pour le secteur numérique, a rassuré de nombreux dirigeants. Mais en réalité, de nombreuses incertitudes demeurent.

Si elle a été accueillie avec soulagement, la décision de l'UE d'autoriser les flux de données vers le Royaume-Uni n'est pas synonyme de relâchement en matière de protection et de gestion des données. Bien qu'actuellement le Royaume-Uni continue d'appliquer les principes du RGPD, rien ne dit que le pays ne décidera pas de les remplacer par une réglementation totalement différente dans les prochaines années.

Les responsables de la sécurité et de la protection des données doivent par conséquent rester informés et vigilants aux potentiels changements de législation ainsi qu'aux futurs enjeux auxquels ils devront faire face.

Eduquer pour mieux appréhender cette nouvelle réglementation

Pour comprendre et réussir ce défi, l'éducation est la clé. Le positionnement du Royaume-Uni est désormais similaire à celui des pays hors UE, ce qui a un impact significatif.
A titre d'exemple, bien que l'application du RGPD soit toujours d'actualité, l'interaction entre les entreprises britanniques et les autorités européennes spécialisées dans la protection des données a changé. En pratique, les politiques de protection en matière de transfert de données ont dû être repensées en France mais aussi outre-Manche.

La décision du Royaume-Uni de quitter l'UE a complexifié cet environnement, incluant de nouvelles difficultés en matière d'infrastructures. Le défi principal à relever se situe donc dans l'harmonisation de trois ensembles de connaissances essentielles, à savoir la sécurité, les données et le droit.

Miser sur l'agilité pour éviter toute confusion

L'incertitude et les nombreux éléments qui restent encore à éclaircir représentent sans doute le défi le plus difficile à relever dans ces préparatifs. Malgré la décision de Bruxelles de maintenir le respect du RGPD, rien n'indique que le Royaume-Uni ne remplace pas ces principes par tout autre

chose dans les mois ou années à venir. Cela nécessiterait des changements beaucoup plus radicaux de la part des entreprises et des régulateurs européens.

Dans la juridiction des données, il est probable que le Royaume-Uni crée de nouveaux organes directeurs, de nouvelles politiques et de nouveaux règlements au fil du temps. Ce nouveau positionnement étant déjà en cours de discussion, les entreprises des deux côtés de la Manche doivent d'ores et déjà surveiller tout changement en temps réel. D'un point de vue relationnel et communicationnel, il se peut qu'il faille repenser un bon nombre d'activités, comme le reporting par exemple.

Construire une infrastructure numérique « future proof », capable de respecter les règlementations actuelles mais d'être également assez agile pour s'adapter aux règlementations futures, tel est le véritable défi auquel les CISO doivent faire face. Pourtant, les besoins des clients doivent rester le leitmotiv principal dans le choix de technologies adaptées plutôt que l'adaptation à de potentielles lois futures.

A titre d'exemple, la mise en place de contrôles nécessaires à l'identification, au suivi et à l'anonymisation des données est un impératif, non pas uniquement pour respecter la loi et éviter une amende mais également pour respecter le client. Assurer une expérience client réussie en respectant la vie privée de ce dernier est un levier fondamental et complémentaire au respect de la loi.

Pour ce faire, les marques vont sans aucun doute sur-indexer sur les technologies, dont font partie le cloud et l'automatisation assistée par machine learning. En plus d'offrir une observabilité accrue en matière de données, bases de données et applications, ces technologies permettent également de gérer le contrôle et le consentement. Le traitement de données structurées et non structurées, tant historiques qu'en temps réel, assuré par ces technologies permet ainsi aux marques d'anticiper les attaques et d'y répondre de manière rapide et efficace.

Collaborer pour mieux s'adapter

A l'image de la mise en place du RGPD, le Brexit peut en fin de compte être considéré comme une opportunité à saisir. En effet, en rassemblant les parties prenantes des différentes entreprises pour assurer une collaboration optimale, le Brexit peut participer à créer des entreprises plus dynamiques et axées sur les données. L'approche collaborative et multidimensionnelle permettra de couvrir les entreprises sous tous les angles.

Face aux législations en constante évolution, la collaboration avec des acteurs juridiques semble être devenue incontournable pour prendre les décisions adéquates.

Les entreprises souhaitent dorénavant garder une visibilité accrue sur l'utilisation de leurs données par leurs partenaires car ils en sont avant tout propriétaires et responsables. Ainsi, la sécurité, la chaîne d'approvisionnement et la gestion des risques sont autant de secteurs désormais concernés. Pour éviter tout faux pas et rester dans les clous, il devient essentiel d'accorder plus de temps aux spécialistes de la protection de la vie privée. Comme le dit le dicton, un problème partagé est un problème à moitié résolu.

Dans les faits il n’est pas possible d’éliminer toutes les menaces, ni d’opter pour l’infrastructure numérique idéale tout en maintenant l’activité de l’entreprise. L’enjeu se situe plutôt dans l’anticipation des menaces et dans la capacité de s’adapter constamment.

Être en mesure de protéger les entreprises, les employés et les citoyens dans cette nouvelle ère post Brexit signifie s’organiser aussi bien au niveau des entreprises, qu’au niveau national ou encore régional. Pour les entreprises, le meilleur moyen de trouver l’origine d’un incident ou d’une attaque est d’adopter une gestion efficace des complexités.

Plus que jamais, la rapidité et l’agilité sont devenues les clés d’une bonne préparation à cette nouvelle ère dans la gestion et la protection des données.