Série GDPR, partie 1 : le GDPR s'applique-t-il à votre entreprise ?

Le Règlement général sur la protection des données (GDPR) de l'Union européenne, le successeur de la Directive sur la protection des données (95/46/CE), suscite beaucoup d'intérêt (et d'inquiétude) à travers le monde. Son application est prévue pour mai 2018, et les entreprises non conformes peuvent s'attendre à des sanctions financières très sévères. D'ici là, il est important que les entreprises réévaluent leurs stratégies de sécurité et de conformité afin de s'assurer qu'elles sont prêtes à satisfaire les exigences du GDPR.
La présente publication est la première d'une série de quatre articles de blog examinant le GDPR, et plus particulièrement :

- Les entreprises auxquelles le GDPR s'applique
- Les exigences clés du GDPR en matière de sécurité des données
- Les implications du GDPR pour les entreprises
- Les sanctions en cas de non-conformité

Pour commencer, passons en revue certaines des définitions fondamentales du GDPR.

Termes clés

Données à caractère personnel et personnes concernées

On entend par ces termes « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou par référence à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »[1]

Exemple : vous travaillez pour une société Fortune 500 et, comme cette société est votre employeur, elle détient vos données à caractère personnel. Vous êtes la personne concernée.

Responsable du traitement

Il s'agit de « la personne, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. »[2]

Exemple : une entreprise de fabrication qui recueille des informations personnelles auprès de ses employés est le responsable du traitement.

Sous-traitant

Il s'agit de « la personne physique, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. »[3]

Exemple : une société de traitement de la paie qui gère les salaires des employés pour le compte de la société de fabrication est le sous-traitant.

À qui le GDPR s'applique-t-il ?

Les entreprises et entités établies en dehors de l'Union européenne peuvent penser que le GDPR ne les concerne pas. Mais ce n'est pas toujours vrai.

Les exigences du GDPR s'appliquent à toute entreprise qui développe son activité au sein de l'Union européenne ou qui traite des données à caractère personnel provenant de l'Union européenne, qu'il s'agisse de données de résidents ou de visiteurs.

Le GDPR s'applique donc aux entreprises de toutes tailles qui traitent les données de quiconque, à condition que ces données proviennent de l'Union européenne.

Les exigences du GDPR restent liées aux données

Comme Internet ne connaît pas de frontières, les responsables du traitement et les sous-traitants n'ayant pas l'intention de traiter des données provenant de l'Union européenne peuvent être quand même tenus de respecter les exigences du GDPR.

Imaginez les deux scénarios suivants :

Vous travaillez pour un cabinet d'analyse financière chargé de prévoir le chiffre d'affaires d'une entreprise européenne pour les trois prochaines années. Vous travaillez dans un bureau aux États-Unis, mais vous utilisez des données à caractère personnel qui vous ont été fournies par votre client et qui ont été recueillies au sein de l'Union européenne. Étant donné que ces données ont été recueillies dans l'Union européenne, elles sont soumises aux exigences du GDPR, même si vous êtes basé aux États-Unis et que vous ne vous êtes pas chargé vous-même de la collecte des données.

Un site Web mobile et en ligne permet aux clients de rechercher, d'acheter et d'évaluer de produits. La société basée aux États-Unis qui est propriétaire du site Web recueille des données à caractère personnel sur les personnes qui le visitent et y font des achats. Ces informations sont ensuite utilisées dans le cadre de campagnes publicitaires et de rapports de vente. Si une personne visite le site Web alors qu'elle est physiquement présente sur le territoire de l'Union européenne, les exigences du GDPR suivent les données à caractère personnel recueillies pendant sa visite. Pour faire simple, cela signifie que tout site Web ou application mobile accessible par une personne qui se trouve dans l'Union européenne devra se conformer aux exigences du GDPR.

Il y a bien sûr des exceptions pour les petites entreprises ainsi que des limites pratiques en ce qui concerne la mise en application par l'Union européenne. Mais les entités basées en dehors de l'Union européenne qui commercialisent leurs produits ou qui développent leur activité avec des clients au sein de l'Union européenne devront envisager les conséquences du non-respect du GDPR.

Cadre de planification

La présente publication n'est que la première partie de notre série de quatre articles sur le GDPR. La partie 2 examinera plus en détail les exigences en matière de sécurité des données. Si vous êtes prêt à approfondir la question de la préparation aux exigences du GDPR, lisez notre article de blog et découvrez notre cadre de préparation au GDPR, qui comprend des jalons pour chaque étape.

Autres articles de la série

Série GDPR, partie 2 : quelles sont les règles qui requièrent une technologie de protection des données ?

Série GDPR, partie 3 : comment préparer votre entreprise au GDPR ?

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016