FICHE SAVOIR JURIDIQUE La collecte de l'information

La collecte d'adresses de clients et de création de fichiers est encadrée par la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et depuis le 25 mai 2018 par le **RGPD** (Règlement Général Européen sur la protection des données (en anglais GDPR *(General Data Protection Regulation)*). Ainsi donc, de nombreuses formalités auprès de la CNIL vont disparaître et en contrepartie, la responsabilité des organismes sera renforcée, ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer. Les règles du GDPR s'appliqueront à toutes les entreprises privées ou publiques des 28 États membres de l'Union européenne. Plus précisément, aux entreprises proposant des biens et services sur le marché de l'UE et/ou collectant et traitant des données à caractère personnel sur les résidents de l'UE.

Les principes du **RGPD** : le consentement, la transparence, le droit des personnes et la responsabilité (accountability).

1 > Le consentement

Le GDPR renforce la notion de consentement des individus quant à la collecte et au traitement des données à caractère personnel. Leur consentement devra être explicite et « positif ». La personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Le GDPR comporte aussi des conséquences dans le mode de gestion des cookies. La nouvelle réglementation impose la mention des informations suivantes : la finalité du cookie, le droit d'opposition de l'utilisateur et l'acceptation implicite de l'utilisateur si celui-ci décide de poursuivre sa navigation. Le consentement peut être retiré à tout moment par les personnes le demandant. Pour les entreprises à caractère B to B, la collecte du consentement n'est pas obligatoire si la finalité de la collecte est bien respectée (les cases pré-cochées sont autorisées).

2 > La transparence

Comme il est précisé dans l'article 12 du RGPD, les organisations doivent fournir aux individus des informations claires et sans ambiguïté sur la façon dont sont traitées leurs données. Celles-ci doivent être accessibles par tous, via des documents contractuels, des formulaires de collecte ou les pages « privacy » des sites web.

3 > Le droit des personnes

Le RGPD renforce les droits des personnes physiques. Les résidents européens se voient attribuer de nouveaux droits : un droit d'accès facilité pour tous les utilisateurs, un droit à l'oubli pour tous les utilisateurs, un droit à la limitation du traitement, applicable dans quelques cas précis et un droit à la portabilité des données (un nouveau droit qui permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers).

4 > Le principe de responsabilité (accountability)

Il regroupe toutes les mesures qui visent à responsabiliser davantage les entreprises dans le traitement des données à caractère personnel. Les organismes doivent par exemple mettre en place des mesures adéquates pour garantir la sécurité des données. Elles doivent également appliquer le « privacy by design », un concept qui impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. Elles doivent aussi choisir des sous-traitants qui soient conformes au RGPD ou encore désigner un data protection officer (DPO), chargé de contrôler la conformité de l'organisme avec le RGPD.

Le DPO, Délégué à la protection des données

La désignation d'un délégué à la protection des données (DPO) est obligatoire pour les organismes publics et pour les entreprises dont l'activité de base amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles ».