RGPD - RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

CONTEXTE

Dans un jugement rendu il y a peu, la justice belge a demandé à l'entreprise Facebook de cesser le pistage des internautes sans leur consentement, et souhaite que la société américaine détruise toutes les données personnelles obtenues illégalement. Au nom du respect de la vie privée, le premier réseau social mondial devra ainsi payer une astreinte de 250 000 euros par jour de retard.

Avec cette décision inédite, les juges belges viennent d'envoyer un signal fort aux grandes entreprises du Web : il n'est dorénavant plus possible d'utiliser les données des internautes sans leur autorisation. Problématique actuelle et générale, tant les données* récoltées par les entreprises sont aujourd'hui aussi nombreuses que diverses, l'Union Européenne s'est dotée d'une nouvelle réglementation sur le sujet : le Règlement Général sur la Protection des Données.

Livre blanc AFTM 2017

Le 25 mai 2018 entrera en vigueur l'application de cette loi, le RGPD, ou Règlement Général sur la Protection des Données (*GDPR** en anglais) qui s'appliquera à l'ensemble de l'Union Européenne. Cette réglementation constitue le nouveau texte de référence européen en matière de protection des données personnelles et vient remplacer la loi informatique et libertés de 1978 en France.

LA NOTION DE DONNÉE

La donnée a permis de développer un modèle économique, un mode de fonctionnement et de consommation de la société. A l'heure actuelle, la donnée influence le rôle du modèle numérique. La CNIL* permet l'utilisation de la donnée dans cet univers. Il faut l'accompagner et la protéger afin de montrer aux citoyens qu'ils maîtrisent leurs informations.

La donnée est aujourd'hui un élément clé dans l'économie mondiale, en devenant un produit marchand. Son contrôle a pour but de protéger les citoyens et de vérifier la conformité des entreprises.

PRINCIPALES FINALITÉS

Le RGPD répond aux nouvelles attentes que demandent les citoyens européens depuis les révélations de l'affaire Snowden en 2011. Ils sont demandeurs de garanties nouvelles en matière de données personnelles. En imposant une régulation de celles-ci, que ce soit sur leur utilisation propre ou l'échange, monétaire ou non, l'Union Européenne pose un cadre à ces problématiques nouvelles. Elle offre ainsi un environnement technologique plus fiable, aujourd'hui au coeur des stratégies des entreprises, des différentes industries, et de toute notre société.

Le RGPD n'est pas une nouvelle loi mais un renforcement fort des textes existants. Ainsi, il intègre les principes de base de responsabilité et de protection des données, qui sont protégées par les responsables de traitement, garants sous le cadre légal. **La sécurité de ces données doit être assurée de bout en bout, au sein de chaque entité en ayant l'accès**. Il faut ajouter à cette veille règlementaire l'évolution technologique des outils intégrant ces données, afin d'en assurer la protection lors des mises à jour et nouvelles versions.

Le RGPD définit le responsable de la donnée comme "la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement".

LIMITES - SANCTIONS

En cas de contrôle de la CNIL, si l'entreprise ne respecte pas le RGPD, les sanctions peuvent être lourdes. **Le chef d'entreprise ou le dirigeant est tenu responsable. Sa responsabilité personnelle est alors d'ordre pénal.**

Il existe aussi une responsabilité vis-à-vis de ses sous-traitants. Si la collecte ou le traitement de données est externalisée, le sous-traitant peut aussi être tenu pour responsable. Dorénavant si on utilise des données sans respecter le RGPD, nous pouvons être impliqué lors d'une procédure. Il s'agit d'engager ses partenaires, afin de prouver une démarche de bonne foi en cas de contrôle, mais aussi d'impacter positivement l'alignement à cette régulation de toute l'industrie.

Outre les sanctions pénales, le non-respect du RGPD implique de lourdes indemnités financières. L'autorité de protection du règlement, (la CNIL pour la France) peut sanctionner l'entreprise à hauteur de 2% à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Chaque entreprise doit ainsi faire les efforts nécessaires pour se mettre en conformité dans les prochains mois, car de telles sommes peuvent mener tout droit à la liquidation judiciaire.

Selon Armand Heslot, ingénieur au service de l'expertise technologique à la CNIL : "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. Aujourd'hui, avec le développement des services digitaux, cette data (donnée) est récoltée partout, lorsque vous communiquez votre adresse mail ou postale, votre géolocalisation, votre empreinte digitale, votre numéro de téléphone"

PRINCIPAUX ENSEIGNEMENTS

Notre industrie ne fait pas abstraction à la règle.

Avec des informations nombreuses, et souvent sensibles (numéro de passeport, carte de crédit, préférences alimentaires, etc), les acteurs du *business travel* doivent impérativement s'aligner à cette nouvelle réglementation.

Les agences de voyages doivent notamment soumettre une déclaration à la CNIL pour la collecte et le traitement des profils voyageurs, les équipes implémentation doivent s'assurer de l'application des principes répondant à la législation RGPD lors de la migration de certaines procédures ou données sur de nouveaux logiciels.

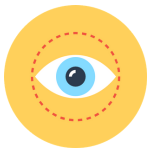
On estime à 35% le nombre d'entreprises qui seront prêtes au démarrage de la loi. Il faut définir une donnée personnelle et son parcours pour identifier les services qui vont être impactés.

Toute transmission de données doit faire l'objet d'une déclaration auprès de la CNIL, la règle peut prévaloir sur le RGPD pour les factures par exemple. L'entreprise doit être en mesure de justifier le cryptage des données collectées et d'établir des droits d'accès à la base.

1 - Qu'est-ce qu'une donnée ?
2 - Qui voit passer la donnée ?
3 - Parcours de la donnée : d'où vient-elle et où va-t-elle ?
4 - Quelle est son utilité ?
5 - Suis-je en mesure de supprimer / modifier la donnée dans les systèmes ?

Il est nécessaire de cartographie des données et de définir des flux pour chaque service, si l'entreprise perd ses données, elle doit informer immédiatement la CNIL.

Afin d'assurer une protection efficace, il faut impliquer l'ensemble de l'entreprise : le service juridique sera sollicité afin d'assurer une compréhension complète des termes de cette nouvelle réglementation, et l'application aux activités de chaque entité. Il pourra aussi gérer la collecte des données et le traitement des consentements des salariés. L'entreprise a l'obligation de communiquer auprès de ses collaborateurs et de leur expliquer le nouveau mode de fonctionnement. Le service communication sera impliqué pour informer les salariés de cette nouvelle réglementation. Certaines entreprises disposent d'un chargé de projet spécifique au RGPD.



Le RGPD challenge l'avancée de la technologie de la *blockchain : nouvel enjeu dans l'environnement technologique d'aujourd'hui, elle promet une transparence et un suivi sur l'échange des données entre acteurs, mais également une plus grande sécurité. Le protocole d'une *blockchain* est, par définition, contraire à cette nouvelle réglementation Européenne. Pour autant, encore à ses prémices, la *blockchain* n'est pour l'instant pas réglementée par les instances internationales, et certains acteurs développent des solutions de cryptage afin de protéger ces données de manière à répondre au cadre légal. Affaire à suivre.**

**Data : donnée | *Donnée : information relative au voyageur | *CNIL : Commission Nationale de l'Informatique et des Libertés | *Blockchain : technologie de stockage et transmission d'information sans organe central de contrôle | GDPR : General Data Protection Regulation*

AFTM
Réalisation :
© CBT Conseil