Quelles sont les sanctions prévues par le RGPD ?

Les plafonds des sanctions sont élevés.

En cas d'infraction, des amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent sont prévues pour l'organisme fautif, sachant que c'est le montant le plus élevé qui est retenu entre les deux cas de figure.

Pour certains géants du Net, l'amende pourrait atteindre des dizaines ou des centaines de millions de dollars, voir davantage. Il convient aussi de noter qu'une société doit veiller à ce que son sous-traitant reste bien dans les clous de la loi, sous peine d'en subir les conséquences, du fait de sa qualité de responsable du traitement.

Le règlement général sur la protection des données

Extraits de l'article Numerama de Julien Lausson du 21 juin 2018

Source :

https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-etes-un-

Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données (RGPD ou GDPR, pour *General data protection regulation* en anglais) est le nouveau cadre européen concernant le traitement et la circulation des données à caractère personnel, ces informations sur lesquelles les entreprises s'appuient pour proposer des services et des produits. Ce texte couvre l' ensemble des résidents de l'Union européenne.

Avant le RGPD — dont le nom plus solennel est le règlement du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données — existait une directive sur la protection des données personnelles qui date de 1995. Ce texte est abrogé par le RGPD.

Quel est l'objectif du RGPD ?

L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles, en remplaçant une directive datant de 1995. Une réforme de la législation européenne apparaissait nécessaire au regard de sa relative vétusté, accentuée par l'explosion du numérique et l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques.

Il s'agit aussi d'harmoniser le panorama juridique européen en matière de protection des données personnelles, afin qu'il n'y ait qu'un seul et même cadre qui s'applique parmi l'ensemble des États membres, que ce soit en France, en Allemagne, en Italie ou en Espagne ainsi que dans la vingtaine d'autres pays de l'Union. De cette façon, la fragmentation juridique sur le Vieux Continent s'en trouve atténuée.

Comment le RGPD se traduit en France ?

En France, le cadre du RGPD est transposé dans la législation via une loi relative à la protection des données personnelles. Le projet a été présenté le 13 décembre 2017 par Nicole Belloubet, la ministre de la justice. La procédure accélérée a été enclenchée par l'exécutif, pour aller vite, avec un seule lecture du texte devant chaque chambre parlementaire. Mais dans les faits, les choses se sont complexifiées et plusieurs va-et-vient ont eu lieu entre les différentes chambres du gouvernement.

Les Sages du Conseil constitutionnel ont rendu leur décision le 12 juin. On notera que la loi adaptant le droit français au RGPD a été validé pour l'essentiel, le Conseil ne censurant qu'un point relatif aux fichiers pénaux, lorsque les traitements sont « *sous le contrôle de l'autorité publique* ». Aucune réserve d'interprétation n'a été éditée par ailleurs.

Il a également précisé les prérogatives de la CNIL à travers ce texte et approuvé l'usage par une administration d'un algorithme, sans intervention humaine, pour établir des décisions individuelle, au motif que les garanties prévues dans la loi étaient assez nombreuses pour échapper aux abus et et garantir « *la sauvegarde des droits et libertés des personnes* ».

Le texte a été publié au Journal officiel le jeudi 21 juin 2018.

On m'a contacté pour me mettre en conformité, est-ce légal ?

Dans un peu plus de trois mois, le RGPD sera appliqué.

Les entrepreneurs vont devoir se mettre en conformité avec la gestion des données personnelles de leurs employés. Toutefois, il sera nécessaire de faire attention et de ne pas prendre n'importe qui en gestionnaire.

La Commission nationale de l'informatique et des libertés a ainsi mis en garde sur les risques d'arnaques autour du RGPD : si les grands groupes sont immunisés, parce que leur département juridique peut prendre en charge cette mise en conformité, les start-ups, les TPE et les PME sont plus exposés.

La Cnil peut conseiller par téléphone via une ligne dédiée : 01 53 73 22 22.

D'où vient le RGPD ?

L'idée initiale vient du constat fait par la Commission européenne que la législation d'alors, entrée en vigueur en 1995, avait besoin d'être actualisée pour tenir compte des évolutions technologiques. En 2012, Bruxelles a donc proposé un nouveau règlement, dont la carrière législative au niveau européen s'est étalée jusqu'en 2016, avec notamment le 15 décembre 2015, un accord entre le Conseil, le Parlement et la Commission.

Le parcours du texte au niveau européen s'est fait dans un contexte particulier : le 13 mai 2014, la Cour de justice de l'Union européenne rendait son fameux arrêt qui oblige essentiellement Google à donner satisfaction aux internautes du Vieux Continent qui demandent le retrait de résultats qui les concernent, consacrant ainsi l'existence d'un droit au déréférencement (sorte de droit à l'oubli *light*) sur le net.

Un an plus tard, le 1er octobre 2015, la même Cour de justice a invalidé le régime juridique dit du « Safe Harbor » qui permettait aux entreprises américaines d'importer aux USA des données personnelles de citoyens européens. Celui-ci a été jugé invalide en raison des révélations d'Edward Snowden sur le programme PRISM, par lequel la NSA accèderait aux données stockées aux USA.

Quand le RGPD entre-t-il en vigueur ?

Le déploiement du RGPD dans l'espace européen se fait en deux temps : il y a d'abord eu, le 14 avril 2016, l'adoption définitive du texte par le Parlement, suivi quelques jours plus tard, le 27, de sa promulgation au Journal Officiel. Cependant, son application ne s'est pas déroulée au même moment : il a été décidé de la décaler de deux ans, au 25 mai 2018. Dans à peine plus de trois mois.

Ce laps de temps permet à la fois aux législations nationales et aux entités procédant à la collecte et au traitement des données personnelles de s'y préparer, en transposant dans le droit des États membres les dispositions du RGPD et en adaptant les traitements déjà mis en œuvre pour qu'ils soient en conformité avec le texte. Après le 25 mai, tout traitement en infraction avec le RGPD pourra déboucher sur des sanctions.

C'est quoi une donnée personnelle ?

Une donnée personnelle (ou donnée à caractère personnel) est une information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'un mail, etc.

Certaines données sont sensibles, car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés :

Une opinion politique, une sensibilité religieuse, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des idées philosophiques sont des données sensibles. Elles ont un cadre particulier, qui interdit toute collecte préalable sans consentement écrit, clair et explicite, et pour des cas précis, validés par la Cnil et dont l'intérêt public est avéré.

Qu'est-ce que le RGPD change pour l'internaute ?

Du point de vue de l'internaute, le RGPD met en place ou conforte un certain nombre de protections. Il faut par exemple que les entreprises récoltent au préalable un consentement écrit, clair et explicite de l'internaute avant tout traitement de données personnelles, ou qu'ils s'assurent que les enfants en-dessous d'un certain âge aient bien reçu l'aval de leurs parents avant de s'inscrire sur un réseau social.

Le RGPD inclut aussi une reconnaissance d'un droit à l'oubli pour obtenir le retrait ou l'effacement de données personnelles en cas d'atteinte à la vie privée, le droit à la portabilité des données, pour pouvoir passer d'un réseau social à l'autre, d'un FAI à l'autre ou d'un site de streaming à l'autre sans perdre ses informations, le droit d'être informé en cas de piratage des données.

Les internautes pourront aussi être défendus par les associations dans le cadre d'une action de groupe en vue de faire cesser la partie illicite d'un traitement de données.

Qui doit se conformer au RGPD ?

Toute entité manipulant des données personnelles concernant des Européens doit se conformer, qu'il s'agisse d'une entreprise, d'un sous-traitant ou même d'une association. Attention : le texte ne s'applique pas qu'aux organisations établies sur le territoire du Vieux Continent. Un groupe américain, japonais ou chinois qui collecte et mouline des données personnelles européennes doit aussi s'y conformer.

Des géants comme Google, Facebook, Amazon ou encore Uber doivent donc tenir compte des modalités du RGPD s'ils veulent continuer sans risque à fournir des biens et des services à la population européenne. La taille de l'entreprise, son secteur d'activité ou son caractère public ou privé n'entre pas en ligne de compte. Même une petite startup qui se lance dans de l'e-santé doit aussi être dans les clous.