Attention aux délais ! Les différentes étapes pour être en conformité avec le RGPD d'ici mai 2018

publié le **21/12/2017**, vu **2458 fois**, Auteur : Murielle Cahen

Le Règlement général sur la protection des données (« RGPD ») est le nouveau texte phare en matière de protection des données personnelles en Europe. Prévu pour entrer en application le 25 mai 2018, le délai de mise en conformité est court et pourtant trop peu d'entreprises sont au courant des dispositions en la matière.

Le droit européen vient ici instaurer un cadre juridique qui se veut « stable » pour l'ensemble de l'Union européenne, concernant le droit des personnes au regard du traitement de leurs données à caractère personnel, tout en responsabilisant les traitants et sous-traitants de ces données.

Me CAHEN Murielle, Avocat, peut être choisi par une société pour être Avocat agissant en tant que délégué à la protection des données .

L'avocat délégué à la protection des données a un rôle de conseil et de sensibilisation sur les nouvelles obligations du règlement (notamment en matière de conseil et, le cas échéant, de vérification de l'exécution des analyses d'impact).

Le souci, c'est que très peu d'entreprises semblent prêtes à respecter cette multitude de dispositions nouvelles d'ici le mois de mai. Il apparaît nécessaire, de fait, d'accompagner les entreprises dans ces différentes étapes : l'ensemble des dispositions du texte se devra d'être compris par les entreprises (I), pour pouvoir organiser de manière rapide et efficace leur mise en conformité (II).

1. ## Le cadre juridique instauré par le RGPD

Le texte européen prévoit de nouvelles obligations pour les entreprises et, plus largement, tous traitants ou sous-traitants de données à caractère personnel (a). Le non-respect de ces obligations entraîne désormais des sanctions plus lourdes que par le passé (b), dans une volonté non dissimulée d'atteindre un cadre harmonisé.

1. ### *Des obligations nouvelles pour les entreprises*

L’entrée en vigueur du texte en mai 2018 renouvelle le cadre de la protection des données et des relations entre ceux qui les fournissent et ceux qui les traitent.

Pour commencer, le texte amène la « consécration » du **droit à l’oubli**, déjà soutenu par la Cour de justice de l’Union européenne dans **l’arrêt Google Spain** qui précisait qu’un traitement de données pouvait devenir « *avec le temps incompatible avec la directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées* ».

Les données devront être conservées aussi longtemps que nécessaire et leur accès, leur modification, leur restitution jusqu’à leur effacement sur la demande des individus concernés, devront être garantis.

De même, les entreprises devront veiller à ce que seules les données nécessaires à la finalité en cause soient collectées, et devront s’assurer du consentement éclairé et informé des individus quant à la collecte et au traitement de leurs données, consentement qu’elles devront recueillir et prouver.

Enfin, le texte prévoit également des mesures concernant le respect du droit à la portabilité des données, la mise en place d’un cadre strict pour un tel transfert en dehors de l’Union ainsi que l’obligation pour les entreprises d’informer le propriétaire des données ainsi que la CNIL d’une violation grave des données ou d’un **piratage**, dans les 72 heures.

2.

Des risques accrus pour les entreprises en cas de non-conformité

La tâche revient également aux entreprises de veiller à ce que les données soient à tout moment sécurisées contre les risques de perte, de vol, de divulgation ou contre toute autre compromission.

Pour toute violation de ces dispositions, le texte prévoit notamment des amendes administratives, pouvant s’élever jusqu’à 20 millions d’euros « ou, dans le cas d’une entreprise, jusqu’à 4 % du chiffre d’affaires annuel mondial total de l’exercice précédent ».

C’est également l’entreprise qui devra indemniser toute personne lésée matériellement ou moralement par un traitement non conforme de ses données, cette fois-ci sans plafonnement.

Une mise en conformité rapide des entreprises s’impose donc. Le RGPD veut aussi obliger les plus réticents à « jouer le jeu », dans la lignée de la décision de la CNIL espagnole du 11 septembre dernier, qui a infligé à l’entreprise Facebook une amende administrative d’un montant de 1,2 million d’euros la collecte et le traitement (notamment à des fins publicitaires) de données sensibles sans le consentement des utilisateurs.

Mais il s’avère que les entreprises n’ont pas forcément conscience de la façon dont elles traitent leurs données, ni même plus généralement de l’intégralité des donnés qu’elles traitent et qui peuvent se trouver sur leurs **bases de données**.

Cette transition se doit donc d’être structurée, et plusieurs étapes méthodiques apparaissent efficaces dans le suivi de cet objectif.

2.

Les étapes de la mise en conformité des entreprises aux nouvelles dispositions

Dans l'attente d'une entrée en vigueur imminente de cette nouvelle réglementation, il convient pour les entreprises de prendre de l'avance et d'entamer dès aujourd'hui un processus de mise en conformité. À cet égard, le délégué à la protection des données (a) jouera le rôle de celui en charge d'accompagner l'entreprise dans les différentes étapes (b) de cette transition.

1. ***Le délégué à la protection des données, « chef d'orchestre » de cette mise en conformité***

La désignation d'un pilote paraît essentielle au regard de la mise en conformité des entreprises avec le RGPD. Le délégué à la protection des données (« DPO ») sera dès lors en charge de l'organisation des différentes missions à mener dans l'accomplissement d'un tel objectif.

La désignation de celui-ci est obligatoire pour les organismes publics et entreprises responsables du traitement de données sensibles ou de traitement à grande échelle.

Néanmoins, la CNIL rappelle que si cette obligation n'incombe pas à certaines entreprises, il est « fortement recommandé » d'effectuer une telle désignation, « *le délégué (constituant) un atout majeur pour comprendre et respecter les obligations du règlement* ».

Le DPO n'a pas nécessairement à être membre de l'entreprise, puisqu'elle peut être liée avec lui sur la base d'un contrat de service. Il est soumis au secret professionnel ou à une obligation de confidentialité.

Le DPO devra jouer le rôle d'un coordinateur, à savoir comprendre et cerner les nouvelles obligations prévues par le texte, et guider le responsable du traitement en fonction. Ceci étant, il n'endosse pas la responsabilité d'une éventuelle non-conformité du traitant ou sous-traitant des données aux dispositions du Règlement.

2. ***Les détails du processus de transition pour les entreprises***

Une fois le DPO désigné, l'entreprise devra alors engager un processus de transition en trois étapes.

La première consiste à lister de manière précise et concise l'intégralité des données traitées, ainsi que les acteurs de ce traitement.

Pour ce faire, la tenue d'un registre des traitements peut être une solution : l'entreprise y consignera toutes les informations relatives aux traitements et aux traitants, à savoir la nature des données, leur provenance ou encore la manière dont elles sont traitées.

Par la suite, il faudra s’assurer que ces traitements s’appuient sur des bases légales toujours en vigueur, qu’ils respectent les droits des utilisateurs, qu’ils sont suffisamment sécurisés et qu’ils respectent les principes liés à la transparence prévus par le texte.

Enfin, la dernière étape consistera pour l’entreprise en une consignation par écrit d’une documentation prouvant la conformité de l’entreprise à la nouvelle réglementation, au fur et à mesure de l’exécution des précédentes consignes.