Focus sur les tenants et aboutissants du RGPD (2)

Tout ce que vous devez savoir sur le RGPD (seconde partie).

Par Paul Salaun.

La première partie de l'article est ici

L'enjeu de la nomination d'un délégué à la protection des données : le DPO

L'entrée en vigueur du RGPD le 25 mai 2018 rend obligatoire la désignation d'un délégué à la protection des données à caractère personnel dans deux cas. Le premier est celui des organismes publics. Le second est celui des entreprises dont l'activité de base consiste à réaliser un suivi régulier et systématique de l'activité de personnes physiques ou morales intéressant l'activité de l'entreprise.

Pour que cette obligation se manifeste dans ce second cas il faut que le traitement des données concernées se déroule à une grande échelle ou que lesdites données soient « sensibles » ou relatives à des condamnations pénales ou à des enquêtes et instructions sur des infractions.

1. *Une faculté de nommer ce délégué dans tous les cas de figures :*

Seules les deux situations précédemment évoquées rendent obligatoires la nomination d'un délégué à la protection des données à caractère personnel. Néanmoins, dans les cas où cette désignation n'est pas obligatoire, il est toujours très intéressant pour un organisme privé ou public de procéder à ce choix. Le délégué à la protection des données personnelles acquiert rapidement une très bonne connaissance des relais internes liés aux enjeux de sa fonction dans l'entreprise. Il a en charge de s'assurer de la correcte mise en conformité au RGPD au fonctionnement de l'organisme privé ou public pour lequel il intervient. Il est enfin demandé au délégué de dialoguer avec l'ensemble des autorités de protection des données à caractère personnel, ce qui lui permettra théoriquement de réduire de manière efficace les risques de contentieux quant à la mise en œuvre du RGPD. Pour le bon exercice de ses fonctions ce délégué devra recevoir une formation appropriée lui permettant de bien comprendre et de respecter l'ensemble des obligations découlant du RGPD.

1. *Les qualités attendues chez un DPO :*

Le délégué à la protection des données personnelles devra être doté de connaissances juridiques et techniques sur les enjeux de la mise en œuvre du RGPD. Il pourra ainsi mener les expertises juridiques et techniques inhérentes à sa mission. À cette fin le DPO devra faire preuve d'une réelle et effective maîtrise des opérations informatiques liées au traitement des données à caractère personnel, ainsi que des besoins concrets en termes de protection et de sécurité desdites données.

Il est par ailleurs impératif que ce délégué dispose de tous les moyens nécessaires (matériels et humains) pour pouvoir au mieux accomplir sa mission. À cette fin, ce délégué devra également pouvoir accéder à toutes les informations utiles à l'exercice de sa mission et être associé à l'ensemble des formations ou projets portant sur la protection des données à caractère personnel.

Enfin, ce délégué devra impérativement être joignable par toute personne ayant besoin d'une information ou portant une réclamation sur la protection des données à caractère personnel.

Le succès des missions confiées à ce délégué dépendra enfin de l'indépendance qui lui sera accordée. La première garantie de cette indépendance sera l'absence de conflit d'intérêt en cas de cumul de fonctions au sein de la structure pour laquelle il intervient. Ainsi, il est fortement recommandé pour les organismes de taille importante que la fonction de DPO soit une profession à part entière.

Cette indépendance implique enfin que le délégué à la protection des données à caractère personnel puisse dès que le besoin s'en fait ressentir, rendre compte de ses missions au plus haut niveau de sa direction, sans être victime de pressions ou de menaces de sanctions. Seules ces garanties d'indépendance protégeront le libre arbitre du délégué à la protection des données à caractère personnel dans l'exercice de ses missions.

Le RGPD : Un outil de lutte contre la souveraineté des GAFAMs :

1. *Le RGPD, un outil théoriquement pertinent pour lutter contre les intrusions des GAFAMs dans la vie privée des internautes :*

On nomme usuellement GAFAMs l'acronyme des géants du Web, à savoir l'association Google, Apple, Facebook, Amazon et Microsoft. Ces cinq firmes américaines dominent le marché du numérique et sont régulièrement accusées d'orienter la politique des différents pays au monde du fait de la masse de données à caractère personnel détenue et utilisée par lesdites firmes.

Ces GAFAMs sont donc particulièrement concernés par l'application territoriale et extraterritoriale du RGPD, laquelle vient frapper théoriquement durement leur possibilités d'intrusions dans la vie privée des internautes et donc leur souveraineté. L'exigence du consentement explicite des personnes physiques et morales au traitement et à la conservation de leurs données personnelles devrait théoriquement impacter l'activité des GAFAMs.

Ainsi ont été instaurées des amendes suffisamment fortes pour frapper les finances des GAFAMs en cas d'irrespect des exigences du RGPD. Le Règlement du 27 avril 2016 prévoit désormais des amendes pouvant atteindre jusqu'à 4 % du chiffre d'affaires mondial de la firme concernée ou 20 millions d'euros. Ce montant des 4% du chiffre d'affaires permettra théoriquement de prononcer des amendes particulièrement lourdes. Si l'on prend l'exemple du chiffre d'affaires de Google, l'amende pourrait ainsi être établie à hauteur de 3,7 Md€. Dans le cas de Facebook l'amende maximale atteindrait ainsi d'1,3 Md€. Il faut noter ici toutefois que le montant des amendes prononcées sera graduel. Plus un organisme sera sanctionné, plus les amendes prononcées à son encontre seront élevées.

1. *Un RGPD susceptible de rater ses objectifs du fait d'apparences de mise en conformité :*

L' ONG « NOYB[1] » dans un communiqué paru dès le 25 mai 2018 a souligné que

le RGPD est censé permettre aux utilisateurs de choisir librement s'ils souhaitent autoriser ou non l'utilisation de leurs données. Or, c'est bien le contraire qui s'est produit ces derniers jours sur les écrans de nombreux utilisateurs : une multitude de « cases à cocher » est apparue en ligne et sur les applications avec pour seule mention « J'accepte », souvent assortie d'une menace. Celle que le service ne pourrait plus être utilisé si l'utilisateur ne donnait pas son accord. Le RGPD interdit un tel consentement forcé et toute forme de conditionnement de la mise à disposition d'un service à l'obligation de donner son consentement pour pouvoir l'utiliser. Par conséquent, l'accès aux services ne peut plus dépendre du simple fait que l'utilisateur accepte l'utilisation qui est faite de ses données[2].

L'attitude de la CNIL, laquelle aborde le RGPD comme une formalité de mise en conformité avec le droit européen pourrait ainsi porter préjudice à la bonne mise en œuvre du Règlement.

Il ne faudrait pas évaluer comme un succès la seule mise en conformité avec le RGPD des procédures des organismes privés ou publics. Une telle évaluation simpliste ne permettrait pas de faire le lien entre conformité aux exigences du RGPD et réalité opérationnelle du succès de sa mise en œuvre.

Le contrôle de la mise en conformité au RGPD n'est ainsi pas la seule clef de perception de sa réussite ou de son échec. Premièrement, ce contrôle n'est pas à même de vérifier que l'organisme public ou privé concerné a acquis une véritable culture numérique.

Pour autant les entreprises ou les administrations n'ont plus le choix de développer ou non une culture data. Le Big-Data et le Fast-Data ne sont plus une simple ressource intéressante de développement mais une condition sine qua non de celui-ci. L'absence de mise en œuvre de stratégie de valorisation du traitement de données à caractère personnel par une structure privée ou publique va fortement impacter son développement, lequel demeurera alors des plus fragiles.

Il en ira de même si cette structure n'a pas développé de culture numérique auprès de ses collaborateurs. Ainsi il est impératif aujourd'hui que les administrations et les entreprises développent de véritables règles de gouvernances garantissant la disponibilité, la traçabilité, la sécurité et la qualité de ses données concernées.

Remarquons enfin que de nombreux porteurs de solutions essaient aujourd'hui de profiter d'un marché du RGPD auprès des organismes publics et privés dans l'obligation de se mettre en conformité.

Ces sociétés proposent à juste titre la vente et l'apprentissage de logiciels permettant la mise en conformité des procédures des structures concernées avec le RGPD. Ces logiciels et ses formations sont le plus souvent présentés comme apportant des solutions de gestion de référentiels de données à caractère personnel ainsi que de communication ou de restitution de celles-ci. Si certaines de ces publicités sont tout à fait pertinentes, d'autres sont abusives et les logiciels vendus n'apportent pas de réelles solutions.

Les structures privées et publiques faisant l'acquisition desdits logiciels et des formations correspondantes ne seront efficaces qu'à la condition que l'organisme concerné ait embrassé l'ensemble de enjeux inhérents au traitement et à la conservation de ses données à caractère personnel. Ainsi, un organisme public ou privé investira durablement dans son avenir s'il mène ces démarches…

1. NOYB, *None Of Your Business* est une association établie à Vienne depuis 2017 par Max Schrems. Cette ONG a pour vocation de faire respecter la protection des données personnelles des citoyens. Son fondateur Max Schrems a principalement mené un combat en ce sens contre Facebook.
2. NOYB, « RGPD : noyb.eu dépose quatre plaintes pour consentement forcé contre Google, Instagram, WhatsAap et Facebook », Vienne le 25 mai 2018, pris sur www.noyb.eu,