RGPD : 1 an après, trois DPO font le bilan

27/05/2019

Il y a tout juste un an, le RGPD entrait en application. Demandes de droits, violation de données, difficultés… Après avoir témoigné sur leurs débuts de mise en conformité l'an dernier, trois DPO ont accepté de faire le point sur les 12 mois qui viennent de s'écouler.

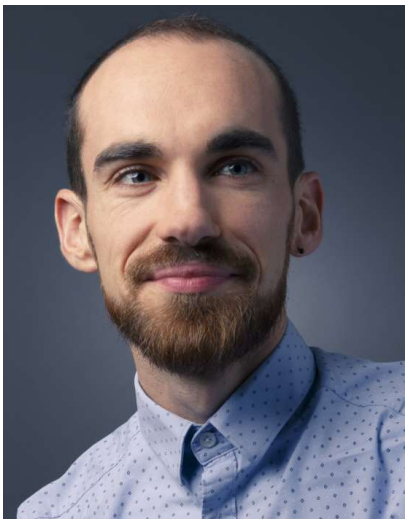
« Avant le 25 mai 2018, une partie des grandes entreprises se préoccupaient très peu de la protection des données. C'était un sujet vaguement géré par la direction juridique », se souvient Florent Gastaud, ex-DPO d'OVH. Entre temps, il a sauté le pas pour créer sa propre structure, « après avoir constaté les besoins croissants des entreprises en termes d'accompagnement sur le marché ». « J'accompagne les DPO de plusieurs sociétés du CAC 40 dans leur mise en conformité avec le RGPD en tant que consultant. J'ai par ailleurs été nommé DPO externe d'une dizaine de filiales de grands groupes ».

Alors, aujourd'hui où en est-on ? « Depuis 12 mois, on assiste à un mouvement général de mise en œuvre. La majorité des entreprises ont nommé un DPO. La protection des données est devenue un sujet à part entière et géré en tant que tel. La plupart des entreprises - des grands groupes aux PME -, ont désormais compris les enjeux. Le poids des sanctions, très élevées, s'est fait ressentir », analyse Florent Gastaud.

Stade de mise en conformité : 3 types d'entreprises

Toutes les entreprises en sont-elles au même stade de leur mise en conformité ? « Non, il y a plusieurs catégories. Certaines entités débutent seulement. Elles ont pris du retard sur le sujet. Au contraire, d'autres ont déjà commencé leur mise en œuvre, nommé un DPO interne ou externe et échelonnent leur mise en conformité sur une ou plusieurs années. Dans ces structures, un véritable plan d'actions est défini. La troisième catégorie vise les entreprises qui étaient déjà familières avec la protection des données. Elles poursuivent leur démarche. Par exemple, dans certains secteurs historiques comme la banque ou l'assurance, elles avaient déjà des directions de l'audit, du contrôle interne et de la conformité. Pour celles-ci, le choc au 25 mai a été un peu moins brutal ».

Les grands groupes peuvent dépenser une fortune pour se mettre en conformité mais cela ne sera pas efficace si l'entité manque d'organisation
Florent Gastaud



« En fonction de l'organisation de la société, les projets de mise en conformité du RGPD peuvent être plus ou moins efficaces », constate Florent Gastaud. « Des grands groupes peuvent dépenser une fortune pour se mettre en conformité mais cela ne sera pas efficace si l'entité manque d'organisation, de communication et de responsabilisation des salariés ». Il conseille de « mettre l'accent sur la méthode, le processus de mise en œuvre et l'interaction entre les différents acteurs ». Et de donner de véritables moyens au DPO. « Si vous prenez parti pour que le DPO soit le chef d'orchestre, il doit avoir les moyens de piloter ».

Violations de données : quels *process* ?

Sur les difficultés rencontrées au cours de l'année, le DPO évoque « avoir connu des violations de données personnelles ». A ce moment-là, « plusieurs questions se sont posées ». Quels *process* mettre en place ? Comment gérer cette situation de crise ? « Il a fallu déterminer si nous devions notifier à la CNIL », raconte Florent Gastaud. En interne, l'incident a été géré par le DPO, en collaboration avec la direction informatique, la direction juridique et la communication.

Le DPO a par ailleurs déjà dû faire face à des demandes d'exercice de droits des personnes concernées par des traitements de données. « Cela nécessite de nouvelles procédures, des développements informatiques. Beaucoup d'entreprises n'étaient pas prêtes. Il a fallu les accompagner ».

Sur ce point, Patrick Blum, DPO de l'ESSEC, estime avoir « eu de la chance ». « Nous avons eu jusqu'à présent assez peu de demandes. Cela se compte sur les doigts d'une main ». Comment cela se justifie-t-il ? « Nos métiers ont compris l'intérêt de mieux cibler les campagnes. Les fichiers sont mieux qualifiés ». L'intérêt également « d'avoir mis en place un mécanisme d'opposition et de désinscription en ligne ».

Au niveau des violations de données, un seul cas s'est présenté. « Un collaborateur s'est fait voler son ordinateur dans lequel figuraient quelques fichiers, tels que des listes d'étudiants ». Cela a amené le DPO à faire une notification à la CNIL. Mais « après analyse, l'impact étant considéré comme mineur », il n'y a pas eu lieu d'informer les personnes concernées.

De plus en plus de demandes après le 25 mai 2018

Chez Mailjet (société française et leader européen de l'emailing) en revanche, la DPO a reçu « de plus en plus de demandes après le 25 mai 2018 », relate Darine Fayed, responsable juridique et DPO de la société. Depuis quelques mois, l'entité a donc « mis en place plus d'*automation* dans

ses *process* ». « Cela nous a sauvé la vie ». Désormais, le « traitement des demandes est automatisé et plus fluide ». La mise en conformité précoce de la société avec le RGPD, fin 2017, a aidé. Cela a permis aux équipes d' « améliorer encore les process IT » notamment.

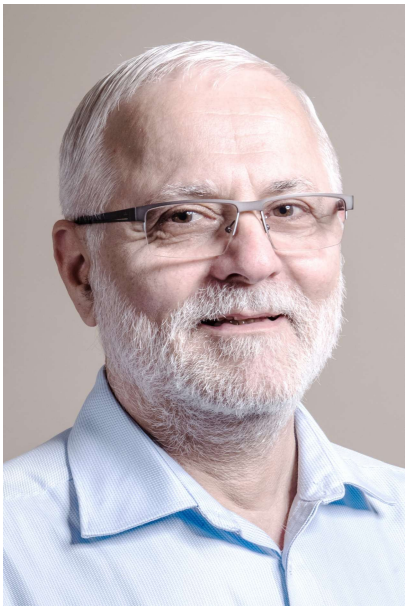
Mailjet a mis en place plus d'*automation* dans ses *process* » Darine Fayed

En un an, grâce aux formations des équipessur la protection des données personnelles, la DPO a également constaté « un changement de culture en interne ». Le principe de *privacy by design* est totalement acquis par l'équipe Produit. « Pour la création de chaque fonctionnalité, figure désormais un chapitre sur les données personnelles ». Les collaborateurs posent les questions adéquates : « Est-ce nécessaire de collecter les données ? Pour quelle durée ? », évoque la DPO. Le travail de sensibilisation et d'information, qui se poursuit encore par le biais de « newsletters, de groupes dédiés sur la messagerie interne des salariés ou encore de fausses tentatives de *phishing* » montre de bons résultats.

Et la certification, délivrée par l'Afnor, « rassure les prospects sur la mise en conformité de Mailjet avec le RGPD ». L'entreprise est même « exonérée de répondre à certaines questions figurant dans les questionnaires envoyés par les grands groupes ». « Certains prospects sont venus spécifiquement vers nous en raison de notre certification. C'est solide et concret », affirme Darine Fayed.

Rencontre des différents métiers

Nous avons commencé à développer un réseau de contacts relais » Patrick Blum



A l'ESSEC, Patrick Blum persévère également dans sa mission de sensibilisation des équipes en place. Il est désormais accompagné de sa successeuse, nommée en interne « car elle avait les qualités requises, tandis que par ailleurs, le marché des DPO est très tendu ». Ils rencontrent régulièrement ensemble les différents métiers.

« Nous avons commencé à développer un réseau de contacts relais, qui sont désormais formellement en charge de ces problématiques. Certains métiers ont éprouvé ce besoin ».

L'objectif ? « Diffuser la bonne parole, faire remonter en temps utile toutes les problématiques et signaler les nouveaux traitements de données ». Ces relais « sont des évangélistes ». Désormais, le DPO n'est « plus tout seul à ramer ». Et il « rame dans le bon sens ».

Attente de la finalisation du cadre juridique

Enfin, les DPO attendent la finalisation du cadre juridique entourant le RGPD. Patrick Blum attend l'adaptation du décret de 2005, pour l'application de la Loi Informatique et Libertés, qui devrait être publié avant le 1er juin. Ce décret « est un texte de référence opérationnel » qui précise notamment les missions et l'organisation de la CNIL, ainsi que certaines formalités et obligations incombant aux responsables de traitement.
Florent Gastaud évoque de son côté l'ordonnance du 12 décembre 2018, qui doit encore faire l'objet d'une loi de ratification d'ici mi-juin. « Une difficulté importante pour les entreprises. Nous n'avons toujours pas de loi nationale parfaitement adaptée au RGPD », s'inquiète le DPO.

Leslie Brassac

Ecrit par

Leslie Brassac

Mots-clés

donnée personnelle

A lire également

- DPO : affirmer la valeur de ce métier nouveau
- Un an après, les entreprises sont-elles 100% «RGPD compliant» ?
- Le numéro de sécurité sociale : une donnée qui bénéficie d'une protection particulière
- La CNIL intensifie sa politique répressive en 2019

Autres articles de l'édition

- [Infographie] LIL 4 : les changements apportés au RGPD
- Gun Jumping : les entreprises face au risque
- L'ANSSI fête ses 10 ans
- Un an après, les entreprises sont-elles 100% «RGPD compliant» ?
- 1 an de RGPD : le bilan chiffré de la CNIL
- RGPD : la Commission européenne fait le bilan