EDITIONS LEGISLATIVES
actuEL Direction Juridique
Le quotidien du directeur juridique

RGPD : trois DPO racontent leur travail de mise en conformité

25/05/2018

Le RGPD est - enfin - entré en application ! Création du registre des traitements, formation des collaborateurs, réussites, difficultés... Les DPO de l'ESSEC, d'OVH et de Mailjet reviennent sur les derniers mois employés à devenir « RGPD compliant ».

« Nous sommes complétement prêts ! ». Darine Fayed, responsable juridique et DPO (*data protection officer*) chez Mailjet (société française et leader européen de l'*emailing*), se dit très fière du chemin parcouru et de ses équipes.

« Les premiers mois ont été consacrés à la mise en conformité interne. En mai 2017, nous avons réalisé une analyse de toutes les obligations à mettre en place. Nous avons établi une *roadmap* et organisé des réunions mensuelles entre les différents services : principalement le juridique et le marketing. La certification ISO 27001 (management de la sécurité de l'information) a facilité le processus. Nous l'avons obtenue en octobre 2017. Cela nous a permis d'élaborer de nouvelles procédures spécifiques au RGPD ».

La certification a facilité le processus »,

Darine Fayed

Florent Gastaud, DPO d'OVH (société spécialisée dans le *cloud*), a préféré l'élaboration d'un code de conduite à la certification. « Les dispositions du RGPD ne sont pas forcément adaptées aux spécificités de notre secteur d'activité. Le code de conduite est un outil, prévu par le RGPD, qui

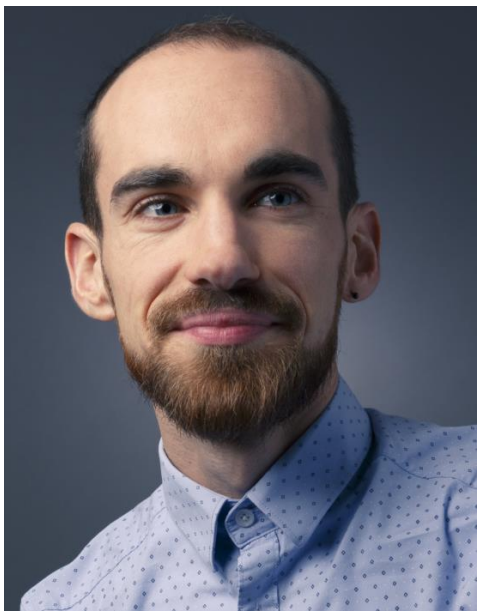
permet d'y remédier. Nous avons fondé l'association CISPE avec d'autres *cloud providers* afin de concevoir un code de conduite commun ». Le projet va prochainement être soumis à une autorité de protection des données personnelles en Europe. Il sera ensuite transmis au comité européen des données personnelles, qui remplace le G29. « Les règles pourront ensuite être applicables à tous les acteurs du secteur sur décision de la Commission européenne » (art. 40 du RGPD).

Des formations présentielles pour les cibles critiques

En interne, le DPO a insufflé une « culture de la *privacy* ». « Nous avons mis en place des formations de *e-learning* pour l'ensemble des salariés et notamment ceux à l'étranger, pour parer à la barrière de la langue ». Des formations présentielles ont été réservées aux « cibles les plus critiques » : les directions marketing, directions en charge du *Big data*, directions supports au contact de la clientèle, direction des ressources humaines.

Chaque salarié est une maille de la donnée »,

Florent Gastaud



« Chaque salarié est une maille de la donnée », justifie Florent Gastaud. Chez Mailjet, tous les employés ont également été sensibilisés. « Nous avons organisé des *sandwich lunches* avec les équipes de Paris et mis en place des visioconférences pour l'étranger », explique Darine Fayed. Les nouveaux entrants ont droit à un « chapitre Données personnelles », intégré à la formation de base, dès leur arrivée. « Nous envoyons des *newsletters* via notre propre plateforme pour diffuser des rappels aux employés. Par exemple, sur les mots de passe ». La charte informatique et sécurité de Mailjet a été complétée d'un point sur les données personnelles. « Elle est affichée dans les bureaux ».

A l'ESSEC, le travail de sensibilisation a commencé il y a plus de 2 ans. Patrick Blum, DPO de l'école de commerce, a « pris son bâton de pèlerin » dès qu'il a eu connaissance du projet de réglement. Du Comex aux directeurs de services, il « distille les bonnes paroles aux collaborateurs » via plusieurs canaux de communication : lettres d'informations hebdomadaires, mais également des « échanges informels à la cafétéria ».
Comme chez Mailjet, un volet « Données personnelles » a été ajouté à la charte informatique. Le DPO a fait le choix de ne pas organiser de réunions de formation. « Une démarche trop structurée et rigoureuse n'aurait pas fonctionné. J'ai préféré travailler individuellement avec les responsables métiers ».

Certains services moins coopérants que d'autres

Je découvre des traitements presque tous les jours », Patrick Blum

Le plus difficile, concède Patrick Blum, a été de créer le registre des traitements. « Je découvre des traitements de données presque tous les jours ». Et certains services sont moins coopérants que d'autres. « Avec les offres de services externalisées, ils peuvent mettre en oeuvre des solutions sans la DSI (direction des services informatiques). Ils ont une grande autonomie. Je dois souvent aller à la pêche aux informations ». Il se félicite en revanche lorsqu'un collaborateur vient le voir spontanément pour mettre en place un nouveau traitement. « J'essaye de leur expliquer que la confidentialité des données a un intérêt pour le *business* ».

Chez Mailjet, le registre des traitements a été créé « main dans la main » avec les équipes IT, et plus particulièrement avec l'*IT quality manager*. « Nous nous sommes réunis chaque semaine. C'était une vraie collaboration entre les différentes équipes ».

Mais l'ancienne avocate a, elle aussi, rencontré certaines difficultés dans sa mission de sensibilisation. « Nous avons, notamment, eu des points de divergences avec les équipes UX (*user experience*). Par exemple, concernant les mentions obligatoires pour recueillir le consentement des personnes qui souscrivent à une *newsletter*. Ils voulaient limiter au maximum la phrase obligatoire alors que nous souhaitions l'élargir ». Dernière étape ? Décrocher la Certification AFAQ Protection des données personnelles délivrée par l'Afnor. La procédure est en cours. L'audit aura lieu le 28 mai prochain. « J'espère que nous l'obtiendrons », confie Darine Fayed, sur un ton optimiste.

Leslie Brassac