Pourquoi et comment nous avons obtenu la certification RGPD / AFNOR

En vigueur depuis plus d'un an, le RGPD renforce les droits des internautes et contraint les entreprises à de nombreux efforts. Comment une entreprise qui fait l'effort pour respecter les règles du RGPD peut-elle valoriser le travail réalisé ? L'exemple de Tilkee.

Temps de lecture : minute

16 juillet 2019

Dès qu'on évoque le terme de "tracking", la 1ère question posée par nos prospects concerne souvent la légalité de notre offre : "mais c'est bien légal ?". Pourtant nous nous sommes toujours conformé aux règles de la CNIL. Mais avant le RGPD, le règlement était peu connu chez nos clients. Nous avions beau expliquer - courrier d'avocats à l'appui - que notre solution était conforme aux règles de la CNIL en matière de respect de la vie privée, le doute subsistait.

Avec l'arrivée du RGPD, les prospects ont musclé leur savoir sur le sujet (le risque d'amende à hauteur de 4% du chiffre d'affaires a bien aidé). Nous avons alors choisi d'en faire un avantage concurrentiel et de maîtriser parfaitement le sujet.

À quoi sert cette certification ?

Il n'existe pas encore de certification officielle de la CNIL concernant le RGPD. De nombreux opportunistes se sont alors lancé dans ce marché juteux de la certification RGPD… Pas simple de s'y retrouver dans la jungle des prestataires plus ou moins sérieux sur le sujet !

Néanmoins, l'enjeu était fort pour Tilkee car cette certification devait permettre de :

- construire une relation saine avec des services juridiques qui ne maîtrisent pas pleinement le sujet et à qui Tilkee faisait peur,
- raccourcir le cycle de vente (souvent ralenti par les services support qui ne sont pas directement concernés par l'usage de Tilkee),
- renforcer notre avantage concurrentiel et notre savoir-faire face à une concurrence américaine qui commence à pointer son nez en France (Showpad, GetAccept…).

En l'absence de certification "officielle", nous nous sommes tournés vers l'organisme leader de la certification en France, l'AFNOR. Lors de nos échanges commerciaux, ils nous ont prévenu : "*la certification n'est pas garantie, attention, le processus est assez lourd !*". Cela nous a rassurés… On ne voulait pas d'une certification "*facile à obtenir*" mais bien d'un audit complet et sérieux.

Par ailleurs, en Allemagne, notre plaquette comprend 18 pages d'annexes sur notre traitement des données, le respect de la vie privée… C'est un enjeu très fort sur le marché allemand. Il était primordial de travailler avec un organisme international pour pouvoir utiliser cette certification dans les pays que nous visons (Angleterre, Allemagne, Espagne, Bénélux).

Comment obtenir cette certification ?

Concrètement, comment ça se passe ? Le consultant AFNOR nous a fourni un référentiel sans trop d'explications. Ce référentiel reprend des articles du RGPD et la première mission consiste à montrer que l'entreprise respecte ces différents articles.

Toutefois, ne sachant pas précisément jusqu'où le besoin de preuves

pouvait aller, il nous a fallu opérer un audit assez complet, identifier les procédures existantes et rédiger celles qui n'étaient pas documentées : nous avions par exemple prévu de faire évoluer les produits pour mieux intégrer la notion de consentement, ainsi que de crypter l'ensemble des données personnelles.

Ce que nous n'avions prévu

Pour déterminer le niveau de connaissances au sein de l'entreprise sur le sujet du RGPD, le consultant AFNOR choisit au hasard au moins un collaborateurs dans de chaque service. A la manière d'un interrogatoire, le consultant posait des questions sur la façon de travailler, sur les logiciels utilisés, sur la configuration des ordinateurs, sur le discours tenu face aux clients, etc.

En tant que DPO, c'était très perturbant pour moi : j'étais présent dans la même salle, mais contraint à n'être que spectateur, sans pouvoir rien dire. Par exemple, quand un collègue explique qu'il ne manipule pas de données personnelles des clients alors qu'il gère les newsletters/mailings, il faut prendre sur soi et attendre la fin de l'interview pour ré-expliquer avec pédagogie ce qu'est une donnée personnelle.

Une fois l'audit terminé, étant donné les évaluations très hétérogènes, il a été décidé de mettre en place des séances de sensibilisation pour que l'ensemble des collaborateurs comprennent l'essentiel des impacts du RGPD. Pour les commerciaux, une deuxième étape de formation a aussi été mise en place.

Lors de la première rencontre avec le consultant RGPD de l'AFNOR, nous étions un peu stressés. On se demandait à quelle sauce nous allions être mangés mais surtout on se demandait si celui-ci allait être dépité par ce qu'il allait découvrir… Nous avions tort de nous inquiéter : il a été très à l'écoute, pédagogue, et nous a plusieurs fois félicités pour les mesures

déjà en place. Son approche ressemblait plus à un accompagnement qu'à un audit "sanction".

En quelques chiffres :

Depuis début 2018, notre responsable DPO a passé plus de 400 heures sur le sujet RGPD, soit environ ⅓ de son temps de travail. L'audit n'était que l'aboutissement quand un certain niveau d'exigence pour être conforme au RGPD avait été atteint. L'audit en tant que tel n'a d'ailleurs duré que 2-3 jours.

Si le DPO est le principal collaborateur impliqué, il n'est que le chef d'orchestre du projet. Toute l'entreprise est sensibilisée, à commencer par le directeur technique. Des correctifs techniques ont dû être créés. Il a fallu expliquer à chaque collaborateur les enjeux éthiques, techniques et marketing du RGPD.

Au final, nous avons estimé le temps passé à une centaine de jours de travail pour notre entreprise qui compte aujourd'hui 35 personnes. Enfin sur un plan financier, la certification coûte environ 15 000 euros, auxquels il faut ajouter une centaine de jours de process/R&D.

Les bénéfices retirés du processus de certification

Il sont de 3 ordres

- Interne

Les questions permanente sur la légalité de Tilkee peuvent devenir pesantes. Le fait d'avoir formé toute l'équipe a permis de monter en compétence, de gagner en connaissance et de savoir répondre à toutes les objections ! Désormais, nous sommes même considérés comme des

experts du sujet. Et les questions ne font plus peur à nos équipes.

- Auprès des clients

Le sujet RGPD est désormais rapidement évacué. Dès que nous annonçons que nous sommes “certifiés par l’AFNOR sur notre conformité au RGPD depuis avril 2019”, on passe à un autre sujet. Cela n’empêche pas d’avoir des discussions animées avec les services juridiques de nos clients… Mais notre interlocuteur (directeur marketing ou commercial généralement) est généralement suffisamment rassuré par le certificat et n’ose pas s’aventurer plus longuement sur le sujet.

Certains de nos interlocuteurs nous ont même demandé de venir “sensibiliser” leurs équipes commerciales à la prospection compatible avec le RGPD : c’est une occasion en or pour nous de rencontrer les équipes commerciales et de leur présenter Tilkee !

- A l’international ?

En Allemagne, la sécurité des données et l’utilisation des données personnelles sont des enjeux majeurs au niveau business et bloquants pour qui n’est pas assez convaincant sur le sujet. Depuis l’obtention de notre certificat, nous avons vu la différence. L’AFNOR est une marque suffisamment puissante pour rassurer nos interlocuteurs germaniques ! Et nous pouvons enfin parler business avec eux.

Sylvain Tillon est le CEO et cofondateur de Tilkee

Article écrit par Sylvain Tillon