Comment une start-up se conforme au RGPD ?

Vous avez tous entendu parler du Règlement Général pour la Protection des Données (RGPD). Si ce n'est pas le cas, il serait peut-être temps de vérifier votre boîte mail… Pour ceux qui ne sont pas tout à fait à jour sur le sujet, voici un bref récapitulatif (les autres peuvent directement passer au paragraphe suivant). Depuis le 25 mai 2018, tous les organismes, quelle que soit leur taille, ont dû revoir leur façon de travailler. Le RGPD s'applique à toutes les entreprises établies sur le territoire de l'UE ou qui traitent des données personnelles de résidents Européens. Il vise une plus grande transparence de la part des responsables de traitement de données personnelles. Il a également pour objectif de donner aux utilisateurs plus de contrôle sur leurs données personnelles. Le règlement s'applique dans tous les pays de l'Union européenne. Le RGPD concerne donc énormément d'entreprises. Mais en pratique, comment une start-up se conforme-t-elle à la nouvelle réglementation ?

Dans cet article en 2 parties, nous nous penchons sur le cas de Lawbox, une start-up bruxelloise qui a su s'entourer des bonnes personnes pour se mettre en ordre. Thibaut Roberti (CEO de Lawbox) et Nathan Vanhelleputte (avocat chez Lex4u) nous expliquent les étapes nécessaires pour ce processus qui n'est, vous allez le voir, jamais fini.

Combien de temps dure le processus de mise en conformité ?

T.R : Le processus de mise en conformité est un travail constant. Si aujourd'hui on ne fait plus attention pour notre prochain contrat, si je ne mets pas les bonnes clauses ; si dans la prochaine newsletter, il n'y a pas d'opt-out, ça ne

marche pas ! Il y a une certaine rigueur à avoir pour rester conforme. On a commencé à s'y intéresser quand on s'est mis à en parler dans la presse, début 2017. Ça tombait assez bien pour nous, parce que c'était un moment où on devait décider si on allait redévelopper notre plateforme en partant d'une feuille blanche. C'est ce qu'on a fait. Donc c'est tombé au bon moment.

N.V. : Le fait de respecter les principes du RGPD et de protection des données de manière plus générale, c'est un changement de mentalité. Dès lors qu'une entreprise va mettre en place une documentation et des systèmes répondant aux prescrits du RGPD, elle devra vérifier que la documentation est bien appliquée et vérifier que tout le monde l'utilise. En outre, il conviendra de vérifier que les systèmes permettent de bien appréhender toutes les facettes du RGPD. (application de droits, cartographie des données…)

Dans un premier temps, le RGPD semblait être une préoccupation pour les grosses entreprises. Pourquoi en avez-vous fait une priorité avant même l'entrée en vigueur du règlement ?

T.R. : Comme on a pour objectif de travailler avec des grandes entreprises, c'est tout simplement obligatoire. Ces clients, par exemple dans le secteur bancaire, ne vont pas travailler avec une société qui n'est pas conforme aux règles. En plus on vend des documents juridiques donc pour notre image, c'était très important de pouvoir montrer patte blanche par rapport à cela.

Avant mai 2018, la loi qui était d'application était la loi de 1992, mais celle-ci n'avait pas du tout les mêmes obligations. Mais nous étions conformes par rapport aux nouvelles règles, pour une grande partie, pour le lancement de notre nouvelle

plateforme. C’était en avril 2018, donc 1 mois avant l’entrée en vigueur du RGPD.

Qui a aidé Lawbox pour sa mise en conformité ?

Pour sa mise en conformité, Lawbox a pu compter sur l’aide du cabinet d’avocats Lex4u, dont Frédéric Dechamps, qui est le fondateur de Lawbox. Ils ont principalement travaillé avec les avocats ou ex-avocats de Lex4u (Caroline Lambilot, Chloé de Clercq et Nathan Vanhelleputte) pour être prêts avant le 25 mai 2018.

N.V. : Depuis début 2018, on a commencé à se positionner comme un cabinet de niche sur la question de la protection des données afin de nous permettre de fournir des conseils toujours plus précis et spécialisés. C’est une matière qui a énormément évolué récemment et qui continue de s’affiner avec toutes les décisions jurisprudentielles qui sont prises, on pense notamment aux décisions qui concernent Facebook et Google. Aujourd’hui, les clients demandent des conseils de plus en plus fins, avec des questions de plus en plus précises et pour faire face à ceci, il faut donc, je le pense, se spécialiser dans une matière et certainement plus encore dans celle de la protection des données.

T.R. : Au début on a plus travaillé sur le côté IT, puis il y a eu la revue des documents, qui est un processus interne. Et troisièmement, c’était des réunions avec Nathan Vanhelleputte qui ont permis de faire des audits pour savoir ce qu’on récoltait comme données. Un cas concret : sur l’identity server (l’endroit où se connectent les clients) les libellés des cases à cocher n’étaient pas clairs. Nous avons donc dû reformuler les opt-ins pour être plus transparent envers nos utilisateurs.

Quels changements ont été apportés au sein de l'entreprise ?

T.R. : On a revu notre privacy policy. Au début, notre privacy et cookie policy n'étaient qu'un seul document. On en a fait 2, on a donc une privacy policy et une cookie policy qui sont tout à fait à jour et qui se veulent être très clairs pour les utilisateurs. Il y a une grande transparence à ce niveau-là sur quelles données on récolte et ce qu'on en fait. En interne, on a fait des avenants aux contrats de travail. On a refait notre contrat de sous-traitant par rapport à notre provider IT.

Mais une autre étape importante du processus qu'il ne faut pas sous-estimer est celle du changement de mentalité. Il a fallu conscientiser les employés de Lawbox aux nouvelles règles, expliquer qu'on ne peut plus faire n'importe quoi avec les données des personnes physiques. On a fait ça à travers des formations par des avocats spécialisés dans la protection des données privées.

N.V. : Du point de vue juridique, il y a 2 catégories principales de changements à effectuer.

Tout d'abord, ce que j'appelle les changements de conformité externe. C'est toute la documentation qui doit être mise en place pour informer les clients, pour encadrer les transferts de données vers les sous-traitants ou les co-responsables de traitement. Cette conformité externe concerne avant tout la formalisation des obligations du texte par rapport aux tiers.

Ensuite, au point de vue de la conformité interne, c'est toute la documentation liée aux employés, cela passe des avenants au contrat de travail, aux documents de sensibilisation mais aussi une révision des clauses de confidentialité afin d'y intégrer les points relatifs à la protection des données.

Qu’est ce qui a changé dans votre façon de travailler avec vos sous-traitants ?

Le RGPD s’applique aussi à tous les sous-traitants des entreprises, c’est-à-dire, les hébergeurs, fournisseurs etc.

T.R. : Nos sous-traitants, aujourd’hui, c’est essentiellement notre provider IT, Vox Teneo. On a la chance qu’ils soient aussi actionnaires de notre société. Chez eux, c’est Denis Muyldermans qui a suivi la formation DPO (Data Protection Officer). Évidemment, tout Vox Teneo s’est très vite mis en conformité. Donc ce n’était pas un gros travail de notre part à ce niveau-là, ils l’ont fait par eux-mêmes.

NV : La plupart des entreprises ne mettent à jour que leur documentation juridique et c’est une énorme erreur car s’il y a un grand pan juridique dans le RGPD, le côté technique et plus précisément la mise en conformité des systèmes d’un point de vue sécurité et gestion est également essentielle. Évidemment, ces modifications seront proportionnées à la taille de l’entreprise, la nature des données traitées et la sécurité déjà en place.

Dans la deuxième partie de cet article, nous nous arrêterons plus en détails sur les phases du processus de mise en conformité.