Comment mettre sa startup en conformité avec le RGPD ?

Le RGPD entre en vigueur le 25 mai prochain. Comment s'en sortir (sans paniquer) ?

Temps de lecture : minute

12 avril 2018

Texte initialement publié sur Medium

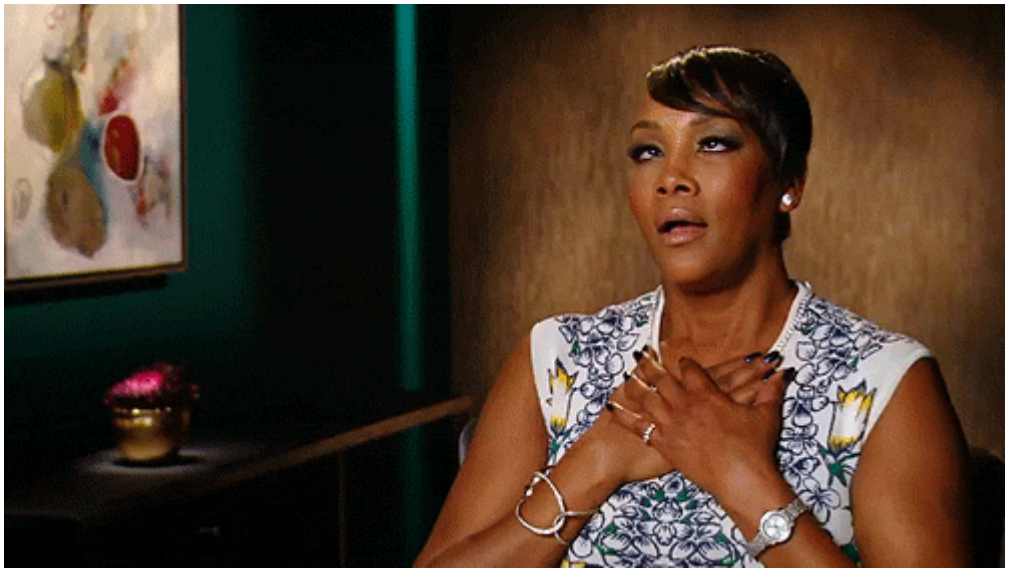
Le RGPD a été voté le 27 Avril 2016. C’est un nouveau règlement qui touche toutes les boites qui gèrent des données de gens comme vous et moi (des particuliers du coup). Ce règlement remet l’utilisateur au centre des préoccupations. Fini les fuites de données masquées et place à de nouveaux droits : droit à l’oubli / droit au déréférencement (Art 17 du RGPD), un droit à la portabilité (Art 20 RGPD) et un droit au consentement renforcé (Considérant 32 du RGPD).

Ça fait deux ans que tout le monde sait qu'il va devoir se mettre en conformité mais tout le monde s’affole au dernier moment. C’est toute l’ironie de la situation. Et comme tout le monde stresse, plein de gens sont prêts à vous faire payer cher pour vous mettre aux normes. Alors comment faire pour s'y retrouver ? Voici les quelques conseils prodigués par la CNIL elle-même.

À lire aussi
5 points essentiels à connaître avant le 25 mai 2018

Prenez le temps

Il faut savoir que la deadline du 25 mai 2018 (date d’entrée en vigueur du RGPD) impose uniquement que nous puissions prouver que nous avons commencé à effectuer les démarches pour se mettre aux normes... cela laisse un peu de marge !



Relativisez l'ampleur de la tâche

Le RGPD a pour objectif d’empêcher les géants de faire n’importe quoi de nos données personnelles. Les petites boîtes ne sont finalement que des dommages collatéraux (à cause de ce que l’on appelle la chaîne de responsabilité).

Cas particulier néanmoins : les boîtes dans le big (vraiment big) data devront s’embêter un peu plus. Mais ce ne sera pas non plus la mer à boire. En fait, la taille de votre boîte n’est pas importante (hé oui : ce n'est définitivement pas la taille qui compte). On s’intéresse ici à la taille de votre base de données (ou de votre fichier Excel).

Il est important de comprendre que seules les données personnelles sont concernées. L’email pro, par exemple, est considéré comme une donnée personnelle. Par contre, les emails génériques (contact@abc.com) ne sont pas concernés.

Sinon, côté pro, le consentement n’est pas obligatoire (l’opt-in) et vous devez toujours respecter les mêmes contraintes (informer l’utilisateur de l’objet du traitement, conserver les données moins de 3 ans sans

échange…). Peu de changements en terre de prospection B2B donc.

Faites-vous accompagner

Déjà, on choisit des gens en qui on a confiance pour nous accompagner dans ces démarches. Le monde du droit fait souvent très peur parce qu'il sert à vous vendre tout un tas de contrats. Certains sont absolument nécessaires, d’autres feront office de décoration dans vos nouveaux locaux. Trouvez des gens qui vont prendre le temps de vous expliquer la portée de ce nouveau règlement. En demandant un petit coup de main à un expert, on peut vite s’en sortir tout en dépensant des sommes très raisonnables.

À lire aussi
Comment le RGPD va vous empêcher de growth hacker tranquilles

Désignez un pilote

Prenez le CEO ou l'un des associés, ça fera bien l'affaire. Le vrai DPO (Data Protection Officer ou Délégué à la Protection des Données) n'est pas obligatoire lorsque l'on ne traite pas des données à grande échelle ou des données sensibles.

Cartographiez vos données

Allez voir votre dev et faites un énorme brainstorming qui doit répondre à ces questions : quelles données (1 colonne) ? où sont-elles stockées (1 colonne) ? pour quelle finalité (1 colonne) ?

Si vous demandez à vos utilisateurs le code de leur immeuble mais que vous ne l'utilisez pas, la CNIL ne va pas être contente. On dit qu'il faut appliquer le principe de minimisation de la collecte des données sur nos utilisateurs.

Priorisez les actions à mener

Si vous vous rendez compte qu'un truc cloche, ça doit être votre top priorité. Et priorisez les tâches en sachant qu'il est plus grave de collecter 100 millions de données en trop que d'avoir oublié une virgule dans vos mentions légales.

Gérez les risques

Si votre boîte ne gère pas des millions de données et surtout aucune donnée sensible, ce n'est pas obligatoire (pour l'instant).

Après, il est toujours intéressant de jeter un coup d'œil au parcours de vos données pour identifier des failles potentielles à l'avance. D'autant que la CNIL a créé un logiciel pour vous faciliter la tâche : le logiciel PIA (Privacy Impact Assessment).

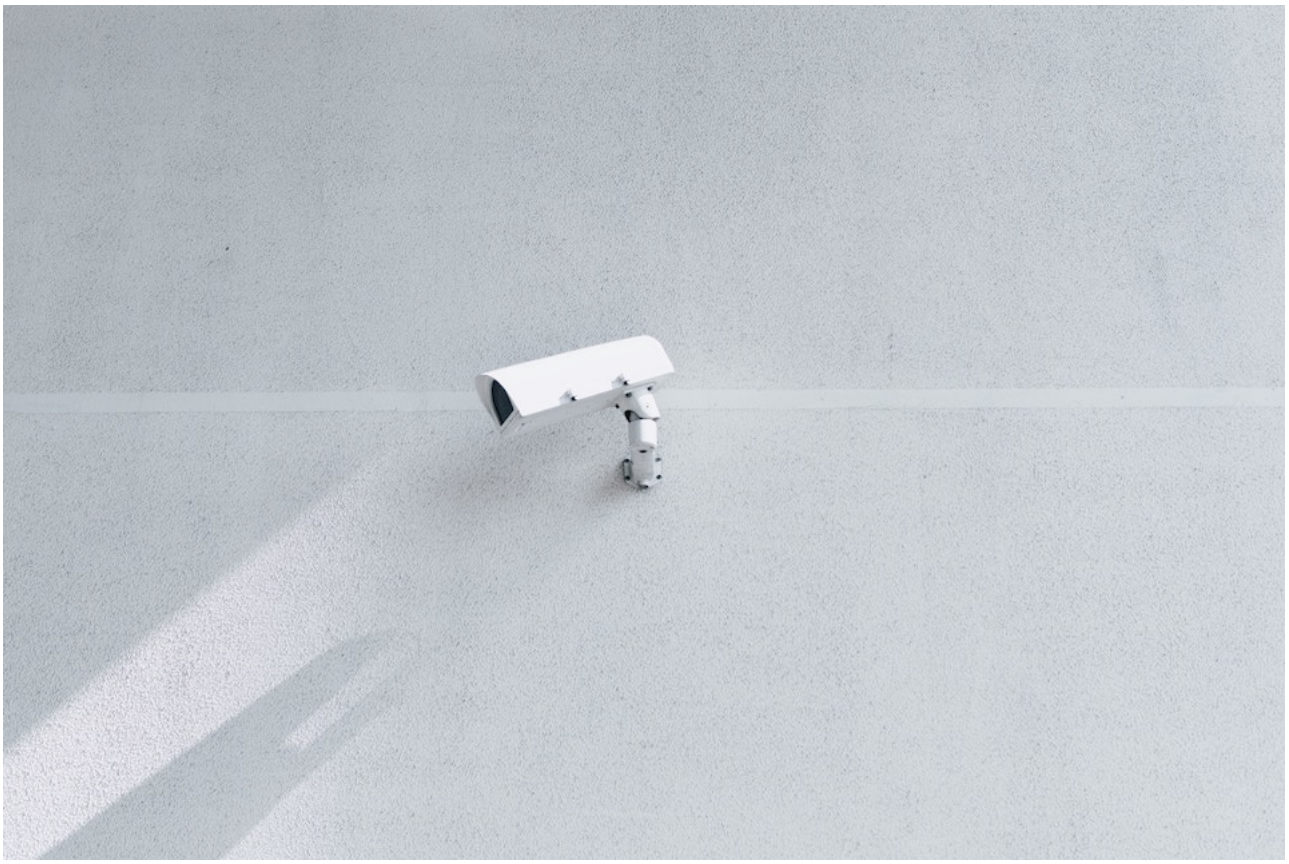
Organisez les processus internes

Il faut que tout le monde soit au courant de quoi faire et quand. Surtout, il faut apprendre à tout le monde à penser RGPD. L'un des principes du RGPD est le "Privacy by design" qui stipule que la démarche RGPD doit être intégrée au plus tôt dès la conception d'un produit/service.

Documentez votre démarche

Faites à la fin un gros document Word où vous expliquez tout ce que vous

devez faire, comment agir dans telle ou telle situation, etc…



À lire aussi
Comment céder mon entreprise en respectant le RGPD ?

Article écrit par Geraldine Russell