Startup: comment faire sa mise en conformité RGPD

Souvent perçu comme une contrainte, la mise en conformité au RGPD et l'intégration de la protection de la vie privée dans votre startup peut s'imposer comme un avantage concurrentiel pour votre activité, afin de gagner la confiance de vos clients professionnels comme des consommateurs.

Dans quels cas ?

Les startups, sont soumises au RGPD dès lors qu'elles traitent des données personnelles, c'est à dire des données permettant d'identifier directement ou indirectement des personnes physiques.

Exemple : tenue d'un fichier clients, collecte de coordonnées de prospects, de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles!
https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

Dois-je désigner un DPO dans ma startup ?

La désignation d'un délégué à la protection des données est obligatoire si vos activités de base font apparaître :

- un suivi régulier et systématique des personnes à grande échelle ou
- si vous traitez à grande échelle des données dites « sensibles » (telles que les données de santé ou les données biométriques aux fins d'identifier une personne de manière unique).

Dans les autres cas, la désignation d'un DPO n'est pas obligatoire mais la CNIL encourage sa désignation.
https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

Quelles actions mettre en place?

Cartographier ses données et construire son registre

Le Registre est un document de recensement et d'analyse qui reflète la réalité de vos traitements.
Utiliser le modèle de la CNIL :
https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Définir la/les finalité(s) d'utilisation de vos données et vérifier leur pertinence

La finalité doit être déterminée, explicite et légitime :
https://www.cnil.fr/fr/definir-une-finalite

Clarifier le rôle de chaque intervenant et encadrer la relation avec vos sous-traitants par un contrat.

Si vous faites appel à des sous-traitants qui vont traiter vos données sur vos instructions, il faut encadrer cette relation par un contrat permettant de s'assurer que les données personnelles que vous confiez à vos sous-traitants sont protégées.
En cas de transfert des données hors UE, utilisez les outils juridiques : https://www.cnil.fr/fr/transferts-de-donnees-hors-ue-le-cadre-general-prevu-par-le-rgpd

Informer les personnes concernées de leurs droits, et recueillir dans certains cas leur consentement

Les personnes concernées doivent :

- connaître la raison de la collecte des différentes données les concernant ;
- pouvoir exercer leurs droits.

https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

Organiser la sécurité des données, et dans certains cas anonymiser ou pseudonymiser les données

la sécurité est une obligation essentielle du RGPD mais c'est aussi une nécessité pour offrir un service ou produit de confiance. https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Pour en discuter : Coralline MANIER-GALAS, WOOG & Associés, Avocat au Barreau de Paris
cmanier@woogassocies.com