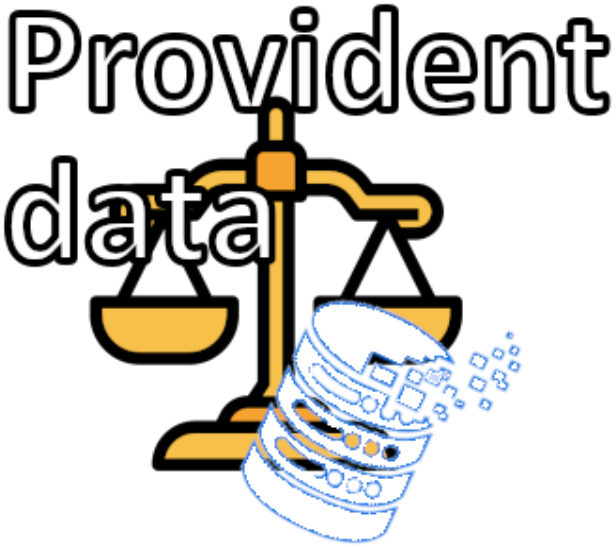
LE JOSSEC Lukas
MICHELANGELI Louis
MINGOUOLO Noah



Introduction

La société Provident Data a été créée afin d'aider des entreprises à mettre en conformité les données qu'elles stockent. Que ce soit des données de leurs clients, des données sur leurs employés, nous n'avons pas de limite dans le traitement de ces données.
Ce rapport est destiné à l'entreprise Stid-Fit. Voulant adapter leurs données stockées sur des serveurs de stockage, nous sommes là afin de les aider à mieux respecter la conformité des du RGPD au sein de leur entreprise (Stid Fit).

Ce rapport sera constitué de plusieurs parties, indiquant chacune d'entre elles, les questions essentielles à se poser afin d'être en conformité avec les RGPD.

I] - *Quelles données personnelles peuvent être collectées par Stid-Fit ?*

En effet, une entreprise, peu importe sa nature (TPE, PME…) doit absolument être en conformité avec les RGPD. Et cela commence par s'interroger sur les données personnelles que Stid-Fit collecte directement depuis leurs clients.
Avant toute chose, il faut garder en tête que les données doivent être récoltées afin de répondre à un objectif défini initialement.
Dans votre cas, vous souhaitez faire remplir un questionnaire à vos clients. Il faut garder en tête que les questions ne doivent pas être détournées de l'objectif d'utilisation initial **(Principe de finalité)**.
Chaque donnée doit absolument être utilisée pour l'objectif et en aucun cas, être archivées pour des utilisations ultérieures.
Dans votre questionnaire, vous souhaitez récolter des informations de santé sur vos clients.
Étant des données jugées sensibles, vous devez impérativement faire une demande à la CNIL afin d'avoir une ''autorisation''. En effet, les données en rapport avec la santé des clients sont des données médicales. Et ces données n'ont pas le droit d'être demandés, sauf exception. Vous devez également vous assurer de la sécurité de vos serveurs de stockage (Mots de passe, administrateurs…). Vous pourrez donc récolter ces données, mais vous devez impérativement supprimer ces données de santé une fois que le programme a été validé par le client. Et ce, pour chaque client.

II] - *Qu'est-ce que Stid-Fit doit faire afin d'être en conformité ?*

Comme dit précédemment, vous devez vous assurer que les données récoltées doivent être protégées le temps de leurs traitements. Et une fois vos programmes terminés, vous pourrez donc supprimer ces données qui sont par la suite inutiles.
Pour rentrer dans les détails, dans les RGPD, vous avez 5 grands principes à respecter. Les voici :
→Les données traitées doivent être proportionnelles et pertinentes.
→Les données traitées doivent être conservées de façon limitée.
→Les données traitées doivent être sécurisées et confidentielles.
→Les données traitées doivent être conformes avec les données autorisées à être traitées.
→Les données traitées doivent respecter les personnes concernées.
Vous souhaitez traiter des données médicales. Ce traitement est entouré de plusieurs nuances et est très strict. Vous devez en faire la demande à la CNIL, car vous souhaitez obtenir plusieurs informations médicales, certaines peuvent être acceptées et d'autres, totalement interdites.

III] - *Quels risques encourez-vous en cas de litige ?*

Les seules situations où nous pourrions encourir des risques, serait le cas où nous ne tiendrons pas nos engagements auprès des clients. C'est-à-dire si nous vous donnions des conseils qui nuiraient à la RGPD de l'entreprise. La sanction dépendra de la situation.

IV] - *Pouvez-vous garantir à vos pratiquants la sécurité des données lors des webinaires ?*

Aucun des différents médias utilisé par STID-FIT pendant la période de covid-19, pour faire des Webinaires, ne respectaient les règles des RGPD. Tout d'abord, Facebook, c'est le réseau social qui recueille le plus de données personnelles en termes de quantité, et c'est aussi l'un de ceux qui utilise le plus ces données. Ils collectent nos discussions personnelles et nos appels fait sur l'application. Ces données leur servent à faire de la publicité ciblée ou alors à les revendre, c'est ce qui a entraîné sur les dernières années, une fuite conséquente des données personnelles de nombreux utilisateurs Facebook.

Zoom lui, collecte toutes les données concernant les discussions (même les appels de groupe) et il a été révélé récemment que Zoom avait vendu certaines de leurs données concernant leurs utilisateurs à Facebook. Suite à cela, Zoom a annoncé qu'ils ne vendraient plus les données de ses utilisateurs mais ils n'ont pas arrêté de collecter les données pour autant.

Et enfin, Discord, même si l'application reste plus discrète que les autres, ils prélèvent tout de même une énorme quantité de données, même les appels entre utilisateur et discussion de groupe sont enregistrés et gardés par l'application. Ils admettent eux-mêmes recueillir les données des utilisateurs. Ils nous laissent peut-être l'opportunité de bloquer « les informations sur nous », mais le réglage n'est pas précis et ne garantit absolument pas l'arrêt total de la récolte de nos données.

S'il y avait eu des problèmes de fuite de données suite à ces séances à distance, STID-FIT aurait pu être tenu comme responsable. C'est pour cela que l'entreprise ne pourra pas faire ses futures séances de Webinaires sur les mêmes médias.

V] - Auriez-vous des possibilités de recours en cas de litige ?

La possibilité de recours en cas de litiges n'est pas propre qu'à notre entreprise, il y en aura forcément un en cas de litige entre 2 entreprises. Toutefois, par le fait que nous ne soyons pas responsables lors d'un litige entre vous et Discord, on ne le fera évidemment pas pour vous, mais vous auriez la possibilité de le faire. Cela relèverait plus du domaine juridique ensuite.

VI] - *Seriez vous responsable en cas de litige ?*

N'étant juste une société de conseils en RGPD, nous ne serons évidemment pas responsables en cas de litiges entre votre entreprise et Discord (Ex: Certaines données des clients de STID-Fit fuitent vers Discord). En cas de problèmes, il faudra se tourner vers le ST (Sous-traitant) et celui qui est responsable de lui : le RT (Responsable de traitement), qui eux seront les responsables dans cette situation, dans ce cas précis ils seront responsables du manque de protection des données.
Nous vous rappelons que notre but est de vous rendre le plus autonome possible sur la RGPD et de vous sensibiliser aux sanctions existantes en cas de manque à la RGPD.

VII] - *Que pourriez-vous faire des données récupérées, relatives aux coachs de l'entreprise ?*

Pour répondre à cette question, tout dépend de la nature des données que vous détenez sur les coachs. En effet, si les données concernant les coachs sont relatives au secret médical, alors les données doivent être supprimées. Cependant, si les données concernant les coachs de Stid-Fit se limite aux lives des réseaux sociaux ainsi qu'à leurs détails tels que leurs noms, prénoms, âges et d'autres informations que vous jugerez utiles, dans ce cas, il vous ait tout à fait possible d'utiliser ces données afin d'en tirer des statistiques sur les performances de vos coachs par exemple. Mais vous devez justifier, en cas de contrôle de la CNIL, pourquoi est-ce que vous gardez telles ou telles données. C'est pour cela qu'avant de conserver des données, même temporairement, vous devez initier un objectif pour lequel elles serviront. La présence de CHAQUE donnée dans la base doit être justifiée.