ESSN – Analyse d'impact relative à la protection des données (AIPD)

Margo Bernelin, Antoine Boutet

Etude de cas « Coach2me »

Vous arrivez dans l'entreprise Coach2me qui fournit un service innovant pour le coaching personnel aux utilisateurs. Afin de respecter la réglementation en terme de données personnelles, le responsable vous demande de faire le PIA lié à l'application.

Utilisez l'outil de la Cnil afin de réaliser ce PIA et le cas échéant émettez des recommandations à l'entreprise afin d'être conforme à la réglementation.

Ressources :
- Outil PIA : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- Analyse d'impact relative à la protection des données (AIPD) 1 : la méthode
- Analyse d'impact relative à la protection des données (AIPD) : étude de cas "Captoo"

Description de l'application Coache2me :

Important : faites vos propres hypothèses si la description de l'application ci dessous n'est pas suffisamment explicite.

L'application Coach2me fournit un service de coaching orienté santé et bien-être aux utilisateurs. Le service est global avec :

- l'aide au maquillage : prise de photographies du visage afin que l'application propose des conseils de maquillage en fonction de la couleur des yeux, de la peau et des cheveux. L'application pourra proposer aux utilisateur. l'achat de certains produits en fonction de partenariats commerciaux .
- l'aide à la préparation de repas : recommandations de repas en prenant en compte les allergies et préférences alimentaires des membres de la familles.
- l'aide à la prise de traînements et à la vaccination avec la fourniture d'un calendrier des prises médicamenteux / vaccins avec une option de rappels
- reporting sur les activités physique : nombre de pas + masse corporelle et taille pour proposer un coaching de remise en forme personnalisé.

Coach2me se matérialise en un site web et une application mobile.

A l'installation l'application mobile demande à l'utilisateur l'accès à la caméra, au microphone, la localisation, au stockage, à la galerie photo et vidéo, agenda, capteur corporels, activité physique, message texte, musique et audio, et fichier.

L'application mobile collecte des données sur la base du consentement (pour la collecte des données à des fins de coaching) , de la nécessité pour l'exécution du contrat (pour les données permettant la création d'un compte utilisateur : adresse mails, identifiants, date de naissance) et l'intérêt légitime (pour le partage des données avec des partenaires commerciaux) . L'utilisateur peut refuser de donner accès au microphone et à la caméra, au détriment de la qualité du service mais ne peut s'opposer au traitement des autres données collectées et de leurs transferts.

Les données partagées avec les annonceurs sont uniquement pseudonymisées. L'entreprise partage mes données collectées avec des partenaires commerciaux afin de proposer de la publicité ciblées, des offres personnalisées (par exemple pour le maquillage) et avec des assureur lesquels souhaitent mener des études sur l'état de santé des assurer et leurs habitudes de vie.

L'unique moyen de s'informer est de cliquer sur un lien dans l'application qui pointe vers les conditions générales d'utilisation (CGU), rédigées principalement en jargon juridique. Cependant, il y est précisé qu'un Data Protection Officer (DPO) peut répondre aux questions et accompagner dans l'exercice des droits RGPD. Aucune mention sur le partage des données avec des assureurs n'est présente.

Les données sont conservées pour une durée non déterminée, archivées sur un serveur de sauvegarde dont le système de fichier n'est pas chiffré.

La communication avec le serveur principal est chiffrée via SSL/TLS.

Les serveurs (principaux et de sauvegarde) sont louées des entreprises sous-traitantes hébergés aux US. Il n'y a aucune politique de contrôle d'accès, tous les employés ont accès à toutes les données. L'hébergeur n'est pas certifié pour l'hébergement de données de santé.

Le développement et la maintenance de l'application mobile est effectuée par un sous-traitant lequel a accès à l'intégralité des données afin des en mesure de résoudre toute difficulté technique. Cette sous-traitant est organisée par un contrat dédié.

Notez qu'Coach2me est une jeune pousse (start-up), qui en plus d'avoir une politique libérale sur le télé-travail ne formule pas de recommandations sur la sécurité des machines professionnelles (la plupart des employés se servent aussi de leurs PCs portables à des fins privées).

Réaliser le schéma de l'application en fonction de vos hypothèses.