ESSN – TP Privacy #1

Antoine Boutet, Victor Morel

Etude de cas « Eventoo »

Vous arrivez dans l'entreprise Eventoo qui fournit un service innovant pour proposer des sorties aux utilisateurs. Afin de respecter la réglementation en terme de données personnelles, on vous demande de faire le PIA lié à l'application (faites vos propres suppositions si la description de l'application ci dessous n'est pas suffisamment explicite). 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 législation.

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"

Application Eventoo
(alimenter cette description pour vos besoins)

L'application Eventoo permet de rester informer des actualités des offres sociaux culturelles autour de soit. Eventoo analyse les habitudes de sortie de l'utilisateur afin de mieux l'orienter dans ses choix.

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

L'application mobile capture les contacts twitter et facebook de l'utilisateur, et a accès à la localisation, au microphone, au stockage, à l'appareil photo, à la galerie photo et vidéo, agenda, appareils à proximité, capteur corporels, activité physique, message texte, musique et audio, fichier, et journaux d'appels.

Au lancement de l'application, on demande à l'utilisateur de se prendre en photo afin de créer un avatar. L'application demande aussi l'adresse mail, le numéro de téléphone, la date de naissance, le genre, le poids, la taille et le login twitter et facebook.

L'application va calculer nos préférences de sorties et celles de nos amis afin de nous émettre des propositions (en avance ou en temps réel).

Lors de soirée, afin de capter l'ambiance, l'application peut enregistrer l'ambiance sonore, accéder aux photos, aux capteurs vitaux et activité physique afin de pouvoir émettre des recommandations à vos amis à proximité.

L'application mobile collecte des données sur la base du consentement et de la nécessité pour l'exécution du contrat.

L'utilisateur peut refuser de donner accès à certains permissions telles que le microphone et la caméra, au détriment de la qualité du service.

L'unique moyen de s'informer est de cliquer sur un lien dans l'application qui pointe vers une politique de confidentialité (privacy policy), rédigée 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.

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

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

Les serveurs (principaux et de sauvegarde) sont louées des entreprises sous-traitantes.

Tout les employés n'ont pas accès à toutes les données, comme les stagiaires et le personnel non-technique par exemple.

Par contre, la politique de contrôle d'accès fait que pouvoir accéder back-end donne accès à tout le backend en lecture seule.

Les administrateurs systèmes et les cadres dirigeants peuvent aussi modifier les données.

Notez qu'Eventoo 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).

Schéma de l'application

- Le serveur est hébergé aux US
- Les données sont partagés avec des partenaires et peuvent être postées sur les réseaux sociaux
- Des cookies sont utilisés sur le site web
- Un cookie wall est utilisé sur le site web
- Possibilité d’acheter avec sa carte bancaire directement des entrées dans l’application