

POUR LES DÉVELOPPEURS D'APPLICATIONS

Certains assistants – et notamment les plus répandus auprès du grand public – se basent sur des approches de type plateforme pour héberger des applications tierces. En pratique, il est généralement nécessaire de respecter les contraintes de développement imposées par le concepteur de l'assistant. Toutefois, de bonnes pratiques de développement peuvent également être observées.

Mettre en œuvre les principes de *Privacy by design* et de responsabilité

Les développeurs d'applications se voient souvent proposer des kits de développement (*Software Development Kit* ou SDK). Dès lors, il leur faut penser le cycle de vie

des données dans un cadre spécifique : Comment circulent-elles ? Où se situent les responsabilités ? Quelles sont les bonnes pratiques à mettre en œuvre ? Le chapitre « Maîtriser vos bibliothèques et vos SDK » du Guide du développeur de la CNIL permet de couvrir les points techniques à vérifier (voir l'encadré ci-contre).

Nos conseils

- Être transparent et expliquer les différentes étapes du traitement depuis la phase de collecte par le concepteur de l'assistant jusqu'à la réponse de l'application, en précisant quelles sont les données accédées par chacun des acteurs, pourquoi et pour combien de temps.
- Ne collecter que les seules données nécessaires à la réalisation de l'application.
- Vérifier que la collecte de données pour l'application ne déclenche pas d'autres collectes de données par le concepteur ou des tiers associés.
- Vérifier régulièrement les fonctionnements des SDK et API ainsi que les données collectées par ces canaux.
- Contrôler et sécuriser les données personnelles transmises de l'application à l'utilisateur par le biais de son assistant vocal en prenant des précautions particulières pour les données personnelles très révélatrices de la vie privée des utilisateurs (données de consommation énergétiques, soldes bancaires, données de santé etc.).
- Définir clairement les termes de contrat et engagements relatifs aux questions de vie privée concernant l'utilisation de ressources mises à disposition par le concepteur de l'assistant et ne pas conclure de contrats génériques ne prenant pas en compte les spécificités des besoins de l'application.
- Préciser de façon claire la chaîne de responsabilité impliquant le concepteur de l'assistant et le développeur de l'application. Sur le périmètre qui relève de la responsabilité de l'entreprise développant son application, mettre en place les obligations du RGPD, notamment l'information des personnes, l'exercice de leurs droits et la sécurité des données.
- Utiliser au mieux les possibilités laissées par le concepteur du SDK pour délivrer une information claire et proposer des mécanismes d'authentification appropriés lors des premiers paramétrages.

ZOOM SUR...

Le Guide RGPD du développeur

> GUIDE RGPD
> DU DÉVELOPPEUR



Afin d'accompagner les développeurs dans la mise en conformité de projet web ou applicatif, la CNIL a élaboré un guide de bonnes pratiques des développements en open source^{149 150}. Il propose des conseils et des bonnes pratiques, et offre ainsi des clés de compréhension du RGPD utiles pour tous les acteurs, quelle que soit la taille de leur structure.

Ce guide est découpé en 16 fiches thématiques qui couvrent la plupart des besoins des développeurs pour les accompagner à chaque étape de leur projet, de la préparation du développement à la mesure de l'audience. Ces bonnes pratiques, qui n'ont donc pas vocation à couvrir l'ensemble des exigences des réglementations ni à être à prescriptives, apportent un premier niveau de mesures permettant de prendre en compte les problématiques de protection de la vie privée dans les développements informatiques qui ont vocation à être appliquées à tous les projets traitant des données personnelles.

¹⁴⁹ - CNIL, Notifier une violation de données personnelles, <https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles>

¹⁵⁰ - <https://github.com/LINCNIL/Guide-RGPD-du-developpeur>