Applications mobiles : comment intégrer des SDK et respecter la vie privée des utilisateurs ?

21 janvier 2025

Les fournisseurs de SDK (« Software Development Kit » ou kit de développement logiciel) jouent un rôle central dans le fonctionnement des applications mobiles. La CNIL rappelle ses recommandations sur la manière d'intégrer des SDK et qu'elle conduira des contrôles pour garantir leur conformité au RGPD.

Le terme de SDK désigne un ensemble d'outils utilisés pour faciliter ou accélérer le développement d'une application. Par exemple, un développeur pourrait décider de coder lui-même un système d'affichage et d'interaction avec une carte au sein de son application, mais il lui est beaucoup plus facile d'intégrer dans son code un SDK d'affichage de carte qu'il pourra configurer selon ses besoins.

Les SDK les plus populaires proposent notamment des outils de gestion des erreurs logicielles, de mesure d'audience, de monétisation publicitaire, de rendu 3D, de gestion des notifications, etc.

Une application Android embarque en moyenne

plus de 15 SDK

(Source [en anglais] : Shoavi, Orly. « The All-Star Winners of Mobile App Tools (SDKs) ». SafeDK ; Lishi, He. « All iOS and Android 3rd Platform SDKs ». Fork.ai)

SDK : quels sont les risques pour la vie privée des personnes ?

Le code du SDK intégré au sein de l'application a le même niveau d'accès logiciel que le reste du code écrit par le développeur de l'application. Si une permission est accordée à l'application, tous les SDK intégrés ont, par défaut, la capacité technique d'accéder aux données. Ces accès par le SDK peuvent alors échapper au contrôle du développeur et porter atteinte au respect de la vie privée des utilisateurs de l'application.

Différents types de risques peuvent être rencontrés :

- **Le fournisseur de SDK commet une atteinte à la vie privée de manière intentionnelle, voire malveillante**

  Le malware SpinOK, qui a affecté plus de 100 applications différentes pour un total de 400 millions de

téléchargements à travers le monde, a été distribué sous la forme d'un SDK publicitaire à première vue légitime. Une fois activé, il collectait des documents, des photos et les mots de passe des utilisateurs, à l'insu des développeurs l'ayant intégré. Après son identification, les applications l'utilisant ont été retirées des magasins d'applications.

- **Le SDK collecte plus de données que ne le pensent le développeur et les utilisateurs de l'application.**

  En 2020, l'application « Muslim Pro », une application de prière et de suivi de comportements religieux, a été accusée de vendre les données de localisation de ses utilisateurs à des courtiers en données, qui les auraient ensuite revendues à des militaires américains. Les données incluaient des informations sensibles sur la localisation des utilisateurs. La société a indiqué par la suite avoir rompu ses relations contractuelles avec les SDK à l'origine de la collecte, en soutenant ne pas avoir été informée de leur activité.

- **L'atteinte à la vie privée peut découler d'un mauvais usage ou d'une mauvaise configuration du SDK par le développeur lui-même**.

  C'est notamment le cas de l'application de suivi des menstruations « MIA », identifié en 2020 par l'ONG Privacy International comme partageant des données de santé (comprenant des informations sur les cycles menstruels des utilisatrices ou leurs rapports sexuels) avec les SDK de AppsFlyer et Facebook. La société AppsFlyer répond en indiquant avoir pris contact avec les développeurs de l'application pour les aider à configurer le SDK afin que ces données ne soient pas partagées avec cette société.

Afin de permettre une utilisation des SDK qui soit respectueuse de la vie privée des personnes, l'ensemble des acteurs doivent s'assurer de respecter leurs obligations :

- d'une part, les éditeurs et développeurs doivent faire preuve de vigilance lors de l'utilisation de SDK ;
- d'autre part, les fournisseurs de SDK doivent respecter les instructions et apporter des garanties fortes à leurs clients. **La CNIL développe, dans ses recommandations, les éléments permettant de cadrer cette responsabilité.**

Les recommandations de la CNIL à l'attention des acteurs du secteur

Identifier les responsabilités relatives à l'intégration de SDK

Les éditeurs, les développeurs et les fournisseurs de SDK doivent qualifier leur rôle, au sens du RGPD, vis-à-vis des traitements effectués par le SDK. Cette qualification de leur rôle et la répartition des responsabilités qui en résulte doit figurer dans le contrat qui les lie ou tout autre acte juridique.

Dans le cadre de la fourniture de SDK, différentes qualifications sont possibles en fonction des spécificités du traitement de données personnelles :

- le fournisseur de SDK peut être responsable des traitements mis en œuvre via son SDK, seul ou conjointement avec d'autres (par exemple, l'éditeur) s'il utilise tout ou partie des données pour son compte ;
- il peut également agir en tant que sous-traitant s'il se limite à traiter des données pour le compte et sur les instructions de l'éditeur ou du développeur ;

- dans certains cas, le fournisseur de SDK peut n'avoir aucune responsabilité au sens du RGPD, s'il ne met en œuvre aucun traitement de données personnelles (c'est-à-dire, s'il ne traite aucune donnée ou identifiant relative à une personne susceptible d'être identifiée, directement ou indirectement).

Cette qualification doit être réalisée par les acteurs au cas par cas, en fonction de l'utilisation concrète qui est faite des données et en s'appuyant sur le principe de responsabilité posé par le RGPD.

Attention

Dans de nombreux cas, les fournisseurs de SDK se qualifient de sous-traitant dans leur documentation juridique (politique relative à la vie privée et conditions générales d'utilisation) pour l'ensemble des traitements qu'ils réalisent. Cette qualification imposée pré-contractuellement n'est pas toujours conforme aux critères prévus par le RGPD. La CNIL invite donc ces fournisseurs à analyser précisément leur situation au regard des critères du RGPD.

La CNIL rappelle qu'elle ne suit pas nécessairement les qualifications définies par les parties : elle analyse les responsabilités des acteurs au regard des justifications fournies et de l'influence de chacun sur le traitement de données.

Par ailleurs, **même lorsqu'il n'agit qu'en tant que sous-traitant (par exemple, de l'éditeur), des obligations juridiques s'imposent au fournisseur de SDK.** Ainsi :

- Il ne peut agir que sur instruction documentée de son client et doit mettre à sa disposition toutes les informations nécessaires pour démontrer le respect de ses obligations et permette la réalisation d'audits). Toute modification relative aux finalités ou aux moyens du traitement ne peut résulter que d'une instruction écrite de la part du responsable de traitement ;
- Il doit offrir, à ses clients, les garanties nécessaires afin que le traitement mis en œuvre pour leur compte respecte le RGPD.

Dans certains cas, les fournisseurs de SDK souhaitent collecter, par le biais de l'application, des données pour leurs propres objectifs et mettre en œuvre des traitements de données sous leur responsabilité : ils pourront le faire uniquement si l'éditeur, responsable du traitement initial, a été correctement informé et intègre le SDK en ayant connaissance de l'existence de ces traitements (notamment via les éléments contractuels). **Dans ce cas, le fournisseur de SDK est responsable de son traitement.**

Éditeurs et développeurs : être vigilant lors de la sélection des SDK

L'éditeur et le développeur doivent faire preuve de la plus grande vigilance lors de la sélection et de la configuration des SDK intégrés à l'application.

L'éditeur, responsable du traitement, doit s'assurer de la conformité de l'ensemble des traitements mis en œuvre par ses sous-traitants. Cependant, dans la pratique, il est fréquent que le développeur soit amené à décider de l'usage ou non de certains SDK pour des raisons principalement techniques. Il est donc important que l'éditeur donne des instructions claires au développeur quant au processus à mettre en œuvre pour la sélection et la configuration des SDK intégrés dans l'application.

Les recommandations de la CNIL accompagnent les professionnels dans la mise en œuvre des mécanismes de sélection des SDK (voir la recommandation, partie 6.3.1).

En particulier, elle rappelle l'importance :

- d'obtenir, du fournisseur de SDK, une documentation précise afin de **pouvoir identifier les traitements qui vont effectivement être mise en œuvre suite à l'intégration du SDK ;**
- de s'assurer que le SDK respecte, lorsqu'il est nécessaire, **le consentement des utilisateurs**, par exemple en suspendant toute opération jusqu'à l'obtention d'un signal de l'application lui indiquant que celui-ci a été recueilli de manière conforme ;
- de s'assurer que le SDK permet de **répondre aux demandes d'exercice de droits** concernant les traitements qu'il met en œuvre.

Les développeurs et les éditeurs sont tenus de choisir leurs partenaires de manière à être en mesure de respecter leurs obligations. Ils peuvent auditer leurs sous-traitants pour s'assurer du respect de leurs instructions, ceux-ci étant tenu de permettre et contribuer à ces audits.

Le fournisseur de SDK : permettre la conformité de l'application

Afin de répondre aux demandes légitimes des éditeurs et développeurs, le fournisseur de SDK doit porter la plus grande attention à la documentation des traitements mis en œuvre par leur intégration dans une application. La CNIL formule un ensemble de recommandations sur le contenu de ces informations et la forme sous laquelle elles devraient être mises à disposition (voir la recommandation, partie 7.2).

Dans tous les cas, **le fournisseur du SDK doit s'assurer que son fonctionnement ne fait pas obstacle à la conformité** de l'application à laquelle il s'intègre, notamment :

- en assurant le blocage de tout traitement ou accès à des données stockées sur le terminal nécessitant le consentement, jusqu'à ce qu'un consentement valable soit recueilli. En particulier, l'obtention d'une permission par l'application ne devrait généralement pas être confondue avec le recueil d'un consentement, au sens du RGPD, pour collecter et/ou traiter la donnée en cause (voir la recommandation, partie 7.3.2) ;
- en facilitant la réponse aux demandes d'exercice des droits notamment au moyen d'API intégrables au sein des applications ou au niveau du serveur des clients (voir la recommandation, partie 7.3.1).
- en mettant en œuvre les mesures de sécurité adéquates et en permettant le maintien de cette sécurité au cours du temps par des processus robustes de mise à jour (voir la recommandation, partie 7.4).

Une vigilance particulière de la CNIL

Dans les mois à venir, la CNIL va porter **une attention particulière à la conformité des fournisseurs de SDK**, tout d'abord dans le cadre de ses missions d'accompagnement du secteur, pour faciliter leur appropriation de la recommandation.

Par ailleurs, comme annoncé lors de la publication de la recommandation, cette question du respect des règles applicables par les fournisseurs de SDK **fera également l'objet de contrôles** à partir du printemps 2025, y compris dans le cadre de l'instruction de plaintes. Il s'agit d'une étape indispensable, car la conformité des traitements mis en œuvre par les éditeurs et développeurs est étroitement liée à la conformité des traitements mis en œuvre par les fournisseurs de SDK.

Pour approfondir

- Applications mobiles : la CNIL publie ses recommandations pour mieux protéger la vie privée
- Smartphones et applications : règles et conseils pour les professionnels