Mathias | Avocats

Le 8 avril 2025, la CNIL a publié de nouvelles recommandations relatives aux applications mobiles. En outre, les données collectées via les applications mobiles figurent également parmi ses thématiques prioritaires annuelles.

Retrouvez nos fiches pratiques sur les bons réflexes à adopter :

I - Concernant les éditeurs d'applications
II - Concernant les développeurs d'applications
III - Concernant les fournisseurs d'applications
IV - Perspectives complémentaires : enjeux et obligations

I- FICHE PRATIQUE POUR L'ÉDITEUR D'APPLICATIONS

"L'éditeur de l'application est défini comme l'entité personne morale (ou l'entreprise individuelle d'une personne physique) qui met à disposition l'application aux utilisateurs"

Source : CNIL, recommandations mobiles.

1.Identifier les traitements de données personnelles

S'agit-il d'un traitement de **données à caractère personnel** au sens de l'art. 4 du RGPD (toute information se rapportant à une personne physique identifiée ou identifiable y compris les identifiants techniques du terminal utilisé) ?

Vérifier l'applicabilité de l'**exemption domestique** (art. 2.2.c RGPD) :
Le traitement doit être initié à la discrétion de la personne, opéré sous son contrôle et pour son seul compte ET réalisé dans un environnement cloisonné (sans intervention possible d'un acteur tiers)

L'importance d'une démarche globale de conformité

Dans son Webinaire explicatif du 12 novembre 2024, la CNIL a mis en avant l'importance du principe d'*accountability* (responsabilisation). Commanditaire de l'application, l'éditeur joue un rôle clef, souvent en tant que responsable de traitement (RT). Sa démarche de conformité doit être proactive et documentée. Il est notamment attendu qu'il soit en mesure de prouver que les choix de conception de l'application ont été effectués, le cas échéant avec l'aide de ses partenaires, en tenant compte des exigences de protection des données à caractère personnel (limitation des finalités et de la conservation, minimisation des données, obtention d'un consentement spécifique à chaque finalité, etc.)
Le déploiement de SDK doit par ailleurs être encadré par un consentement spécifique et un contrat de sous-traitance.

Rappel : les conditions de validité du contrat de sous-traitance

Dans la délibération SAN-2024-002 du 31 janvier 2024, la CNIL a sanctionné l'encadrement insuffisant des traitements effectués pour le compte du responsable de traitement. En raison de l'article 28.3 du RGPD, le contrat ou autre acte juridique contenant l'instruction de traitement doit contenir :
-l'objet clairement défini du traitement
-la durée du traitement
-la nature et la finalité du traitement
-le type de données à caractère personnel
-les catégories de personnes concernées
-les obligations et les droits du responsable de traitement
-les conditions dans lesquelles le sous-traitant s'engage à effectuer les opérations de traitement.

La CNIL a ainsi relevé que les documents contractuels fournis au moment du contrôle du responsable de traitement ne comprenaient pas l'ensemble des mentions requises, ce qui constitue le manquement. La rédaction à posteriori d'un avenant pleinement conforme ne suffit pas à libérer le responsable de traitement de sa responsabilité : elle ne fait que réduire la durée du manquement retenu (confirmation du raisonnement de la délibération SAN-2023-015 du 12 octobre 2023).

2. Assurer la conformité des traitements identifiés

Pour chaque traitement, les finalités de traitements sont elles correctement définies ? Une base légale est - elle identifiée pour chaque finalité ?

Autres principes du RGPD : les données personnelles traitées sont elles limitées à ce qui est nécessaire pour les finalités poursuivies ? La conservation des données est-elle limitée dans le temps ? Comment sont protégés les mineurs ?

3. Appliquer la "privacy" dés la conception et par défaut

En vertu des principes dits de "*data protection by design and by default*" (art. 25 RGPD), il est recommandé que l'éditeur détermine, pour chaques traitements, les paramètres minimaux permettant de fournir le service demandé.

Minimiser les risques : privilégier le chiffrement de bout en bout et la pseudonymisation, compartimenter les différents services proposés "en silos", permettre un consentement granulaire.

4. Documenter son analyse et sa démarche de conformité

Tenir à jour un registre des traitements, justifier et documenter les durées de conservation définies en fonction des finalités (art.5.2 et 24 RGPD)

Cartographier ses partenaires : en amont, identifier l'ensemble des sous-traitants, leurs responsabilités, Vérifier que les contrats de traitements de données correspondent à l'ensemble des conditions de validité.

Focus : la sélection de permissions

L'accès à une ressource du terminal à distance doit être indispensable au service demandé ; sinon, un consentement explicite est requis (art. 82 LIL).

La localisation

Niveaux de données (localisation, durée, usage en arrière-plan) doivent être justifiés.
Responsabilités : éditeur = RT, fournisseur SDK = ST..

Le microphone

Traiter les données localement par défaut ; tout envoi externe n'est possible que pour un usage justifié, optionnel et soumis à un consentement.

L'appareil photographique

Distinguer l'accès à l'appareil photo et l'accès aux photographies stockées du terminal.
Si l'usage n'est pas strictement nécessaire, il faut obtenir un consentement.

5. Maintenir la conformité avec l'évolution de l'application

Formaliser les mesures techniques attendues en terme de sécurité des données avec le développeur (art.32 RGPD).

Auditer le respect des engagements des partenaires (dans le contrat de sous-traitance).

Actualiser régulièrement le registre des traitements et la politique de confidentialité.

Vérifier la suppression effective des données dont la durée de conservation est arrivée à terme.

II- FICHE PRATIQUE POUR LE DÉVELOPPEUR D'APPLICATIONS

"Le développeur de l'application est l'entité morale ou l'entreprise qui procède aux opérations techniques de développement de l'application, pour le compte et sur instruction de l'éditeur"

Source : CNIL, recommandations mobiles.

1. Identifier les responsabilités et les obligations de chacun

Lors de la contractualisation avec l'éditeur : qualifier les rôles des parties pour chacun des traitements concernés.

Obligations du sous-traitant : art.28 RGPD :

- Transparence et traçabilité
- Assistance de l'éditeur dans l'exercice des droits des utilisateurs
- Alerter l'éditeur en cas d'instructions non-conformes au RGPD, etc

2. Suivre les processus de maîtrise d'œuvre agréés

Ne pas prendre de décision impactant la vie privée des utilisateurs (choix technique, design d'interface...) sans impliquer l'éditeur dans la décision.

Désigner un point de contact avec l'éditeur afin d'obtenir et actualiser des instructions claires (partenaires, permissions, consentement, droits des utilisateurs, etc.).

3. Identifier l'ensemble des traitements de données pers.

Le développeur doit informer l'éditeur de l'existence de traitements de données personnelles identifiés, notamment en raison des outils fournis par les OS.

L'usage de SDK nécessite d'analyser les traitements de données, de qualifier les tiers au regard du RGPD, d'informer l'éditeur et de s'assurer de la conformité des traitements.

4. Aider au bon respect des droits des utilisateurs

S'assurer que l'exercice des droits par les utilisateurs est possible, facile et effectif : l'ensemble des données concernées doivent être transmises à la personne.

L'interface doit garantir l'accessibilité : page dédiée aux droits, politique de confidentialité disponible, et écran d'information au premier lancement..

Le recueil du consentement et l'articulation des fenêtres de sollicitation (ATT...)

Les interfaces doivent être adaptées pour rester lisibles sur mobile. La CNIL recommande :

- D'afficher le détail des finalités via un lien ou un bouton déroulant dès le premier niveau d'information.
- De proposer un consentement granulaire grâce à un bouton "personnaliser mes choix", au même niveau que "tout accepter" ou "tout refuser".

Concernant les permissions, le consentement n'est requis que si l'accès n'est pas indispensable à la communication ou au service demandé.

Dans ce cas, deux demandes distinctes doivent être présentées à l'utilisateur : l'une pour le consentement RGPD, l'autre pour la permission d'accès. Les deux doivent être acceptées pour que le traitement soit valide ; un refus entraîne l'absence de base légale ou le blocage technique de l'accès.

En cas de refus de la première requête, la CNIL recommande de ne pas afficher la seconde.

Les fenêtres présentées par les fournisseurs d'OS visant à recueillir l'approbation de l'utilisateur pour une finalité spécifique peuvent constituer un recueil valide de consentement. Cependant, il faut rester vigilant dans deux scénarios :

1- Acceptation par l'utilisateur de la fenêtre "OS" mais refus dans l'application : le consentement n'est plus valide (il n'est plus univoque).

2- La fenêtre "OS" ne couvre pas l'ensemble des finalités du traitement : une autre fenêtre est alors requise dans l'application.

Les mesures de sécurité

- Le développeur doit respecter les obligations du RGPD (art. 28, 32) : communication via TLS, stockage sécurisé des secrets (API), désactivation par défaut des sauvegardes tierces, authentification adaptée au niveau de sécurité, et conformité aux recommandations OWASP (niveau L1).

Sauf exceptions (bancaires...), éviter de faire reposer son modèle de sécurité sur l'intégrité du terminal. Réaliser des contrôles réguliers.

Focus : les SDK (Software Development Kits)

Sélectionner le SDK selon les bons critères : s'assurer de la mise à disposition, par le SDK, de documents permettant de déterminer l'ensemble des traitements de données qu'implique son intégration. S'assurer qu'il permet de répondre aux demandes d'exercice des droits.

Attention à l'effet "poupées russes"

L'intégration d'un SDK peut impliquer celle d'autres SDK : s'assurer que le SDK initial apporte un niveau de garantie suffisant

5. Proposer des solutions qui respectent la vie privée

Vérifier que les traitements respectent les instructions de l'éditeur, notamment la minimisation des données. Privilégier les traitements locaux plutôt que via API. Ne traiter les données sensibles que sur instruction explicite de l'éditeur (art. 28.3 RGPD).

III - FICHE PRATIQUE POUR LE FOURNISSEUR DE SDK

"L'entité, personne physique ou morale, qui met à disposition un ou plusieurs SDK destinés à être intégrés dans des applications mobiles"

SDK : *Software Development Kits* :

Source : CNIL, recommandations mobiles.

1.Identifier et analyser ses obligations

Identifier les traitements pour lesquels le fournisseur est sous-traitant ou responsable de traitement.

Points d'attention spécifiques :

- l'information des personnes concernées par les traitements,
- l'identification de données sensibles,
- l'encadrement contractuel et technique adéquat en cas de transferts de données hors UE.

2. Appliquer les principes de protection des données dès la conception et par défaut

Principe de **minimisation** : limiter les données envoyées vers des serveurs au strict nécessaire. En particulier, la collecte d'identifiants de terminaux ou d'individus doit être dûment justifiée.

Cloisonner les services, afin de permettre à l'éditeur de n'utiliser que le SDK souhaité.

Distinguer, parmi les permissions, celles qui sont souhaitées de celles strictement **nécessaires**.

3.Identifier les informations à fournir

Analyser les traitements entraînés par l'utilisation du SDK et rendre cette documentation accessible. Indiquer la présence de traceurs lus sur le terminal de l'utilisateur, en explicitant les finalités, durées de vie, etc.

Points de vigilance :

- Pour chaque traitement, le fournisseur de SDK doit identifier sa qualification au sens du RGPD.
- En cas de sous-traitance ultérieure, s'assurer de l'autorisation du responsable de traitement.

4. Présenter ces informations dans un format accessible

Informer les parties lorsque des mises à jour du SDK font évoluer les traitements mis en oeuvre.

Mettre à disposition un registre dynamique en fonction des possibilités de paramétrage du SDK.

Le registre doit permettre d'identifier facilement chaque donnée collectée, les éléments juridiques (base légale, finalité, obligations) et techniques (lectures, écritures) associés

Gérer le consentement et les droits des personnes : aider au bon exercice des droits des utilisateurs

La CNIL a précisé plusieurs exigences concernant les fournisseurs de SDK et l'exercide des droits des utilisateurs :

- L'exercice des droits doit être pensé dès la conception, notamment en termes de structuration des bases de données. A titre d'illustration, le droit de suppression doit pouvoir être respecté indépendamment des contraintes techniques.
- Pour qu'on consentement soit valide, il doit être donné de manière spécifique (distincte notamment de l'acceptation des conditions d'utilisation de l'application) et libre (ce qui implique en principe de pouvoir choisir d'accorder ou de refuser un consentement en fonction des différents types de finalités)
- Pour faciliter la mise en œuvre pratique de l'exercice des droits, la CNIL recommande d'envisager son automatisation, notamment au moyen d'API intégrables au sein des applications ou au niveau du serveur des clients.

Le fournisseur de SDK est invité à utiliser le moins d'identifiants additionnels possible pour traiter l'exercice de ces droits

Sur quels principes est-il recommandé de faire reposer son modèle de sécurité ?

La CNIL recommande notamment de :

- Ne pas faire reposer son modèle de sécurité sur l'intégrité du terminal, sauf dans certains cas justifiés. Éviter de faire reposer son modèle de sécurité sur des mesures d'épinglage de certificat (« *certificate pinning* ») ou d'obfuscation de code.
- Concevoir son service de manière à maintenir le niveau de sécurité même avec des terminaux corrompus. Les recommandations de la CNIL en termes d'API44 sont recommandées pour sécuriser les serveurs utilisés par l'application.
- Protéger les données personnelles contre les éventuels accès non autorisés de la part de sous-traitants ultérieurs et mettre en œuvre des contrôles d'accès journalisés pour éviter les détournement internes.
- Privilégier la méthodologie de déploiement d'intégration continue pour les mises à jour.

Focus : la conformité en matière d'usage des traceurs

Lorsque l'accès à une ressource du terminal par le SDK nécessite le consentement de l'utilisateur, il est impératif que le responsable du traitement s'assure qu'un consentement valable a été obtenu pour chaque finalité poursuivie. Si l'accès par le SDK à une ressource du terminal et le traitement qui en résulte nécessitent le consentement de l'utilisateur, celui-ci ne peut être considéré comme obtenu sur la seule base d'une permission accordée à l'application.

Bonnes pratiques

Limiter l'usage de permissions en bloc à l'installation, préférer l'usage de permissions déclenchables durant le fonctionnement de l'application

Pour chaque consentement recherché, documenter les impacts fonctionnels d'une absence de consentement de l'utilisateur sur le fonctionnement du SDK, minimiser les blocages non-nécessaires

! La mise en place d'une **permission en bloc à l'installation dont l'utilisation future est improbable** est susceptible d'être contraire à l'obligation de configuer les traitements de données dans le sens le plus protecteur de la vie privée !

S'assurer que la révocation du consentement n'entraîne pas d'instabilité d'exécution de l'application ou une demande constante de permission.

5. Participer au maintien de la conformité dans le temps

Des rapports d'audits du SDK sont réalisés régulièrement et tenus à disposition des éditeurs partenaires.

Le SDK peut être mis en pause par l'éditeur en cas d'incertitude juridique ou un dysfonctionnement technique.

Un processus technique et organisationnel relatif aux violations de données est établi : il prévoit la transmission d'informations aux responsables de traitement et le formalisme des notifications de violation aux autorités de protection des données.

Mathias | Avocats

IV- POUR ALLER PLUS LOIN

ÉDITEURS D'APPLICATION, DÉVELOPPEURS, FOURNISSEURS DE SDK, QUELS ENJEUX ? QUELLES OBLIGATIONS ?

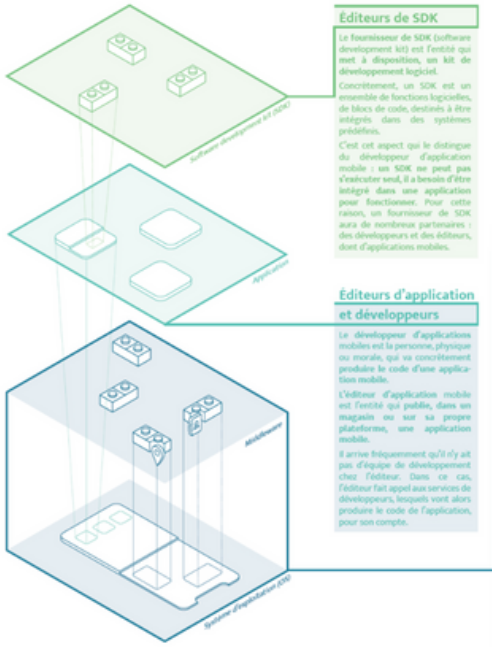
Consentement et autorisations/permissions : quelle articulation ?

- Choisir la permission d'accès impliquant le moins de collecte de données.
- Identifier les traitements soumis au consentement RGPD (art. 82 de la loi LIL* et art. 4 et 7 RGPD) : ceux-ci doivent correspondre à des « finalités déterminées, explicites et légitimes » (art. 5 du RGPD).
- Le consentement peut être obtenu indifféremment avant ou après la demande de permission.

→ **Points de vigilance :**

- La collecte de données personnelles doit se faire de manière **proportionnée** entre les données traitées et la finalité poursuivie.
- Une permission donne un accès technique à la ressource visée. A l'exception de cas limités (partie 8.3.2 de la recommandation), les permissions ne permettent pas de recueillir un consentement valide au titre du RGPD ou de l'art. 82 de la LIL.

**Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*



Source : CNIL, recommandations relatives aux applications mobiles, 24 septembre 2024.

Les SDK, une zone de vulnérabilité ?

Les SDK (*Software Developpement Kit*) sont les logiciels de traitement tiers ajoutés aux applications pour différentes finalités (marketing, fonctionnalités, etc.).

Leur contenu peut être opaque, même pour les développeurs de l'application initiale. Ainsi, les SDK peuvent réaliser des traitements de données personnelles à l'insu des éditeurs d'application.

Dans ce contexte, l'atteinte à la vie privée peut être intentionnelle (collecte de données dissimulée cf. X-Mode) et malveillante (cf. malware SpinOK) ou résulter d'une mauvaise configuration logicielle (cf. AppsFlyer).

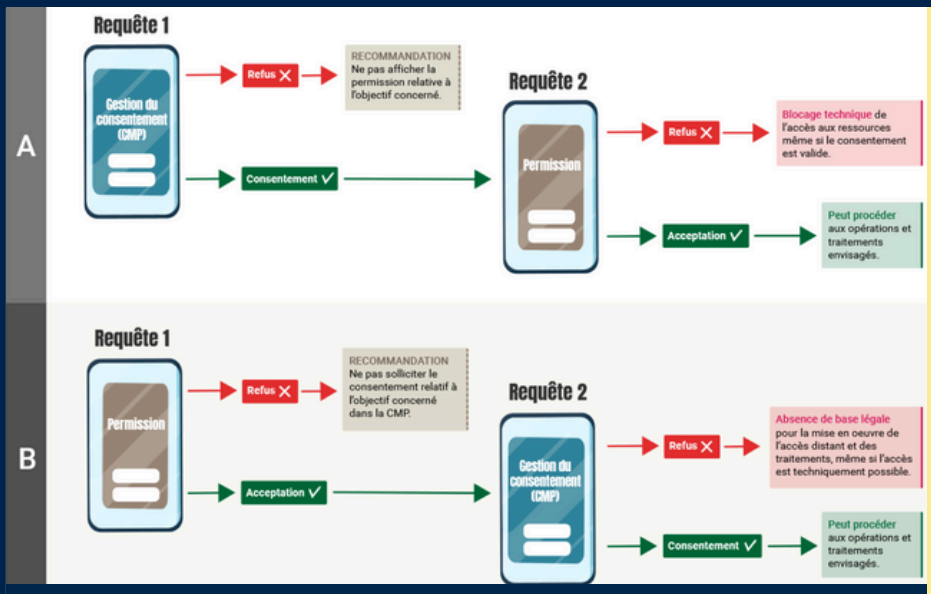
Les recommandations de la CNIL ont pour objectif de faciliter le travail de diligence des éditeurs d'application et des développeurs en rendant obligatoire pour les fournisseurs de SDK la transmission des informations détaillées sur les traitements de données personnelles réalisées (voir le point 7.2 des recommandations, en complément de l'art. 30 RGPD).

→ **Rappel RGPD** : est sous-traitant celui qui « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement » (art. 28.3.a) . Le simple partenariat n'est donc pas suffisant.

- La qualification que retient la CNIL du point de vue des responsables de traitement ne dépend pas exclusivement de la volonté des parties : c'est le fait de réaliser des traitements de données personnelles sur instruction d'un responsable de traitement qui détermine la qualification retenue.
- La zone de conformité concerne l'ensemble des droits reconnus aux utilisateurs finaux par le RGPD, qui doivent figurer dans la politique de confidentialité : il subsiste également un point de vigilance en ce qui concerne les transferts de données hors UE réalisés.
- Présenter à l'utilisateur une fenêtre de consentement à l'activation des SDK est possible, mais elle ne saurait être équivalente à une fenêtre globale de consentement aux cookies.

19 RUE VERNIER 75017 PARIS
+33 (0)1 43 80 02 01
CONTACT@AVOCATS-MATHIAS.COM

Mathias | Avocats



Source : CNIL, "Articuler la permission technique et le recueil du consentement" recommandations relatives aux applications mobiles, 24 septembre 2024.

Articuler SDK et recueil du consentement aux cookies

Il convient en particulier d'éviter tout design incitatif et ***dark patterns*** :(interfaces trompeuses) : cases pré-cochées, consentement conditionnant l'accès au service, boutons d'acceptation et de refus à des niveaux différents. Le refus ou retrait de consentement ne doit pas affecter les fonctionnalités de l'application.

Pour plus de détails, se référer aux figures du point 6.2.3 des recommandations. Les lignes directrices de la CNIL de 2020 concernant les cookies restent également applicables.

Quelles sont les suites et bonnes pratiques ?

La CNIL a annoncé que le paramétrage des SDK et les accès aux données du téléphone via la gestion des permissions seront ses priorités lors des contrôles des acteurs du mobile.

Il convient de noter que l'**activation des SDK** doit dépendre du **consentement** de l'utilisateur, et que ce dernier doit pouvoir dynamiquement activer ou désactiver ceux-ci. Le consentement accordé doit également être granulaire, permettant à l'utilisateur d'accepter ou de refuser des SDK **selon leur finalité**.

L'exercice de ce consentement doit être rendu effectif : l'accès aux données doit pouvoir être accordé, empêché ou retiré par l'utilisateur.

Pour minimiser les démarches de conformité à entreprendre, il est essentiel de favoriser *ex ante* la ***privacy by design*** – autrement dit, de favoriser la protection des données personnelles dès la conception de l'application. Cela peut notamment se concrétiser par l'**implication du DPO** dès le processus de développement de l'application pour minimiser les données collectées et favoriser une documentation claire des les finalités de traitement.

Avoir une bonne organisation initiale permet de diminuer l'ampleur du travail de conformité « en continu » à réaliser tout au long du cycle de vie de l'application.

Enfin, il convient de rappeler que la conformité aux recommandations mobiles de la CNIL est sans préjudice des principes fondamentaux de la protection des données, comme la limitation des durées de conservation des données, l'information des utilisateurs ou la sécurité des données (voir la délibération n°SAN-2023-023 du 29 décembre 2023).

Bonnes pratiques pour l'éditeur ou le développeur d'application :

- **Définir des processus** distincts pour l'obtention de permissions et le recueil du consentement.
- Pour les **systèmes Apple** : la lecture et l'exploitation de l'IDFV nécessite un consentement spécifique, (cf. délibération SAN-2022-026 du 29 décembre 2022).
- **Documenter** l'ensemble des diligences pour s'assurer de la conformité d'un sous-traitant.
- S'assurer que les **clauses contractuelles** délimitent efficacement les responsabilités et que le contrat d'instruction contienne bien l'ensemble des **mentions obligatoires** prévues à l'art. 28 RGPD.

Points de vigilance :

- Apple sanctionné par **l'Autorité de la concurrence** (Adlc) pour avoir abusé de sa position dominante en raison de la mise en oeuvre du dispositif App Tracking Transparency (**ATT**)
- Dans sa décision du 28 mars 2025, l'Adlc a considéré notamment que la mise en œuvre concrète d'un dispositif de protection de la vie privée des utilisateurs doit être **nécessaire** et **proportionnée** à l'objectif poursuivi, en particulier au regard des contraintes imposées aux éditeurs et utilisateurs.
- Cette sanction a tenu compte de deux avis rendus par la CNIL pour l'éclairer sur les questions de protection des données personnelles.

19 RUE VERNIER 75017 PARIS
+33 (0)1 43 80 02 01
CONTACT@AVOCATS-MATHIAS.COM