USERADGENTS

GUIDE PRATIQUE

RGPD & Apps mobiles

LES RECOMMANDATIONS DE LA CNIL POUR UNE APP RESPECTUEUSE DE LA VIE PRIVÉE

Introduction

Six ans après l'entrée en vigueur du RGPD, si les principes et obligations en matière de protection des données personnelles sont désormais bien connus des éditeurs de sites web, force est de constater que côté applications mobiles, bon nombre d'acteurs n'ont pas encore fait du sujet une priorité. Face à ces lacunes, la CNIL a publié en septembre 2024 une nouvelle recommandation pour mieux guider les acteurs du secteur. Ce document intervient à un moment clé, à l'aube d'une campagne de contrôle prévue pour mars 2025, qui pourrait intensifier la pression sur les éditeurs pour une mise en conformité stricte.

Le mobile, par définition privé et intime, offre aujourd'hui l'un des principaux moyens d'accéder à des contenus et services en ligne, à travers les apps notamment. Celles-ci accèdent à des données parfois sensibles grâce aux capteurs du téléphone (caméra, contacts, GPS, accéléromètre,...), qui nécessitent que l'utilisateur ait préalablement fait un choix éclairé sur leur collecte et leur traitement.

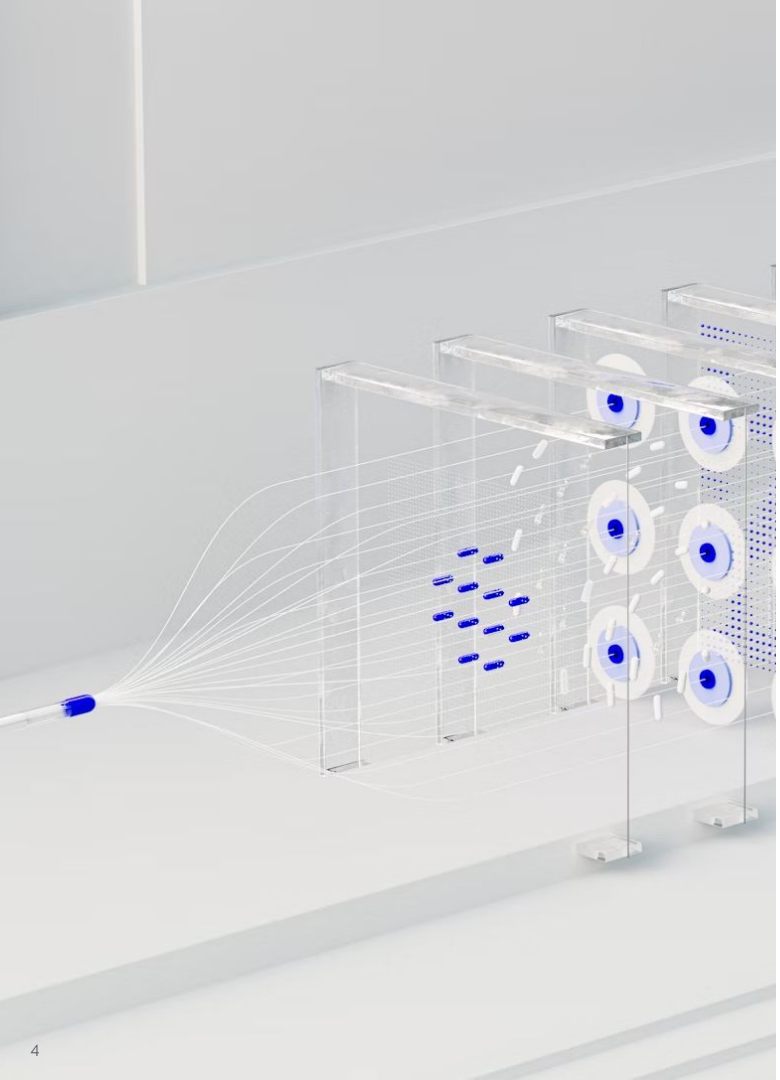
Ce guide a pour objectif d'accompagner les acteurs de l'app economy (développeurs, éditeurs, SDK, etc), plus spécialement les équipes projet, dans une démarche de "privacy by design" pour concevoir des applications mobiles respectueuses de la vie privée tout en restant performantes.

Ce document n'a pas valeur juridique. Il s'appuie sur l'analyse métier de USERADGENTS, la lecture des documents & recommandations de la CNIL. Il appartient à chaque entreprise & notamment au responsable du traitement des données, de s'assurer, avec l'appui d'experts juridiques, que ses applications mobiles soient conformes à la réglementation en vigueur.

Donnée personnelle

Définition

Toute information se rapportant à une personne physique identifiée ou identifiable. Par exemple, dans le cas d'une application mobile, cela peut être le nom et prénom de l'usager, mais aussi son alias, sa position géographique, ses données d'activité dans l'application ou même les identifiants techniques du terminal qu'il utilise.



Les différents types de données personnelles

Données fournies directement par l'utilisateur

Informations personnelles (nom, prénom, date de naissance, adresse postale / e-mail, N° tel, N° de carte de réduction ou fidélité)
Identifiants et mots de passe (biométrie)
Informations de profil (photo de profil, biographie)
Contenu généré par l'utilisateur (posts, commentaires, photos partagées)

Données collectées automatiquement par l'application

Données de l'appareil (modèle, OS, identifiants)
Données des capteurs (GPS, accéléromètre, gyroscope, etc.)
Historique de navigation dans l'app
Métadonnées (horodatage, langue, réseau utilisé)
Données d'utilisation (temps passé sur l'app, fonctionnalités utilisées)

Données dérivées ou inférées (créées à partir de l'analyse des deux premières)

Profils d'utilisateurs
Préférences et centres d'intérêt
Prédictions de comportement
Scores (crédit, risque, etc.)
Catégorisation des utilisateurs

Différents identifiants sur mobile

Dans l'écosystème des applications mobiles, des identifiants permettent de suivre chaque utilisateur de manière unique à des fins publicitaires ou de personnalisation des contenus. Ils peuvent être lus par l'éditeur et par des tiers (SDK & autres).

→ L'identifiant du compte de l'utilisateur n'est pas propre au mobile, c'est le même que sur le web. C'est l'identifiant métier du compte connecté, un même compte peut se connecter à plusieurs devices et un même device peut avoir hébergé plusieurs comptes différents. C'est grâce à cet identifiant qu'il est possible de personnaliser les suggestions au sein du magasin d'applications, de suivre son activité au sein d'une app et en améliorer les fonctionnalités.

→ L'identifiant publicitaire est un "fingerprint" technique du device, il est unique, afin de permettre le suivi du comportement de l'utilisateur dans l'app par des tiers publicitaires (IDFA sur iOS et AAID sur Android).

A chaque acteur ses responsabilités

malgré leur interdépendance

Le fournisseur d'OS*

met à dispo le système

Identifiants, compte utilisateur propre à l'OS, seuls ou combinés à d'autres données, données issues des capteurs (caméra, micro, GPS, accéléromètre, etc) et stockées sur le terminal (contact, photos, apps installées, etc).

Traitement de données pour ses propres finalités : bon fonctionnement du terminal, et pour des tiers : traçage pub,...

*système d'exploitation

Le magasin d'applications

met à dispo la plateforme de distribution des apps

Compte utilisateur pour les mises à jour des apps.

Traitement de données pour des propres finalités.

L'éditeur d'applications

publie l'app dans un magasin ou sur sa propre plateforme

Données techniques de connexion, données de navigation, données fournies par l'utilisateur ou par l'OS, (contact, paiement, localisation, etc.).

Traitement de données pour ses propres finalités : bon fonctionnement de l'app (vérification de la compatibilité de la version de l'OS) et des services proposés. Transmission à des tiers à des fins de monétisation de l'audience (traceurs, identifiant mobile de l'utilisateur,...)

Le développeur d'applications

produit le code d'une app

Configuration des traitements de données personnelles Maintenance (test de pré production, analytics, remontée de bugs...)

Le développeur peut endosser une forme de responsabilité au titre du RGPD.

Le fournisseur de SDK

met à dispo un kit de développement logiciel

Données issues du terminal (identifiant, adresse IP, identifiant publicitaire unique, localisation,...)

Traitement de données pour les finalités de l'app et son éditeur : bon fonctionnement des fonctionnalités (lecture de QR code, réalité augmentée, notifications,...), traçage des utilisateurs à des fins d'analytics (fournies par l'éditeur et à son seul bénéfice). Traitement réalisés par le SDK en tant qu'intermédiaire pub, pour tracer les utilisateurs, établir des profils, monétiser l'audience, au profit de tiers ou d'annonceurs.

A chaque acteur ses responsabilités

malgré leur interdépendance

Le fournisseur d'OS*

POTENTIELLEMENT CO-RESPONSABLE DU TRAITEMENT

Offre des outils de gestion des permissions aux utilisateurs

Facilite la mise en conformité des applications sur leur plateforme

*système d'exploitation

Le magasin d'applications

PAS DE RESPONSABILITÉ DANS LE TRAITEMENT

Affiche des infos sur la confidentialité des données sur les fiches store

Contrôle les infos fournies par l'éditeur / développeur de l'app

Facilite le processus de révocation des consentements

A le pouvoir de retirer les applications non conformes

L'éditeur d'applications

GÉNÉRALEMENT RESPONSABLE DU TRAITEMENT

Détermine les finalités et les moyens du traitement

Assure la conformité globale au RGPD

Garantit la transparence envers les utilisateurs

Met en place les mécanismes de consentement

Le développeur d'applications

GÉNÉRALEMENT SOUS-TRAITANT ou RESPONSABLE DU TRAITEMENT (selon le cas)

Traite des données personnelles pour le compte, sur instruction et sous l'autorité du responsable de traitement.

Implémente les principes de "privacy by design"

Assure la sécurité technique de l'app

Le fournisseur de SDK

GÉNÉRALEMENT SOUS-TRAITANT OU CO-RESPONSABLE DU TRAITEMENT

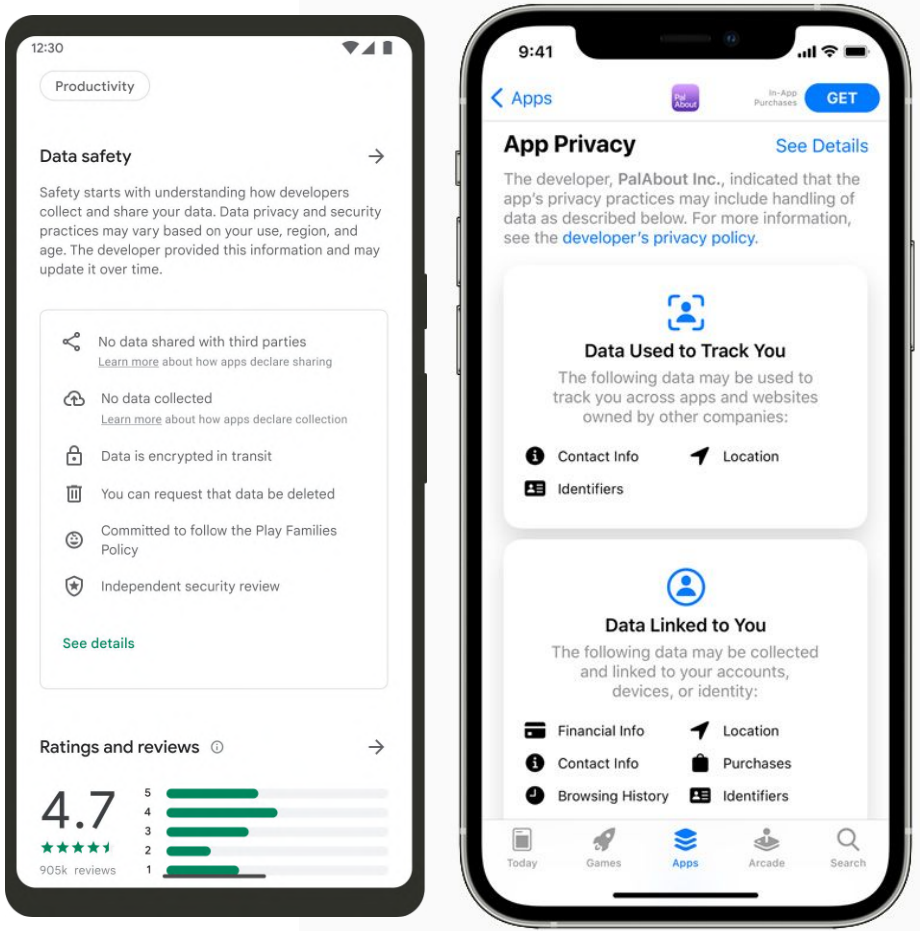
Fournit une documentation claire sur l'utilisation des données

Respecte les principes du RGPD dans ses outils

Collabore avec les éditeurs pour la conformité

Le rôle des magasins d'applications

Pour améliorer la transparence sur la collecte des données, les magasins d'applications ont introduit une section dédiée à la confidentialité des données sur les pages produits des apps. Cette section fournit des informations détaillées sur les types de données collectées par chaque application et leurs modalités d'utilisation. Les développeurs doivent déclarer toutes les modalités de collecte des données, y compris les différences entre les versions gratuites et payantes, ou selon la région et leur partage avec des tiers. Malheureusement, certaines déclarations peuvent être trompeuses.



17% | 19%

17% des applications Android et 19% des applications iOS déclarent faussement ne pas collecter de données personnelles

Source : Pradeo, 2024

Les principaux risques liés à la collecte de données par les apps

→ Collecte excessive de données qui ne sont pas nécessaires au fonctionnement de l'app.

→ Partage (et revente) de données avec des tiers à l'insu des utilisateurs. L'utilisation de SDK tiers dans les applications peut entraîner des transferts de données non maîtrisés.

→ Manque de transparence et de clarté des informations sur la collecte de données et leurs objectifs.

→ Accès intrusif aux capteurs (GPS, caméra, accéléromètres, etc.) dont certains révèlent des informations très précises sur les utilisateurs (géolocalisation notamment).

→ Sécurité insuffisante contre les fuites ou les piratages.

→ Difficulté d'exercer ses droits, car les utilisateurs peinent souvent à comprendre et contrôler l'utilisation de leurs données par les applications.

Source : Libération, 2024

20%

des applications envoient les photos, vidéos et fichiers audio des utilisateurs hors de leur appareil

14%

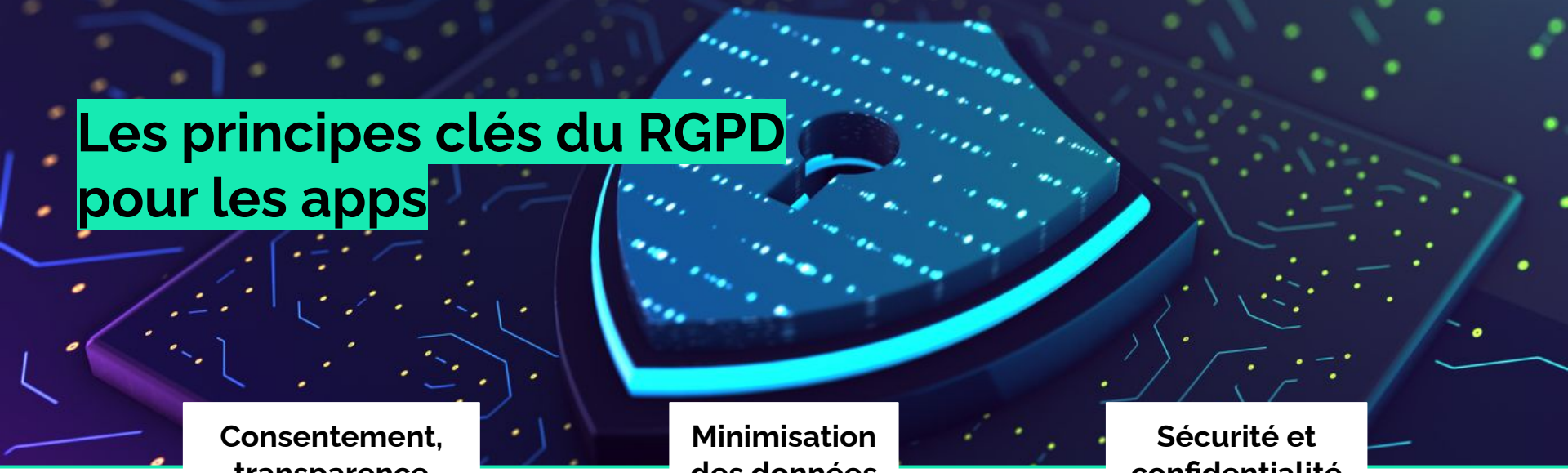
des applications transmettent les contacts des utilisateurs à des tiers

Source : Pradeo, 2024

RGPD

Obligations, recommandations & bonnes pratiques

pour les éditeurs & développeurs d'apps



Les principes clés du RGPD pour les apps

Consentement, transparence et contrôle

Obtenir le consentement explicite des utilisateurs avant de collecter des données non essentielles au fonctionnement de l'app.

Fournir une information claire et concise sur l'utilisation des données personnelles dès le premier lancement de l'application.

Permettre aux utilisateurs de supprimer et rectifier facilement leurs données, mais aussi de désactiver certaines fonctionnalités de collecte de données non essentielles.

Minimisation des données

Limiter la collecte aux données strictement nécessaires pour chaque fonctionnalité.

Privilégier les permissions minimales (ex : localisation approximative plutôt que précise).

Utiliser des techniques de pseudonymisation et d'anonymisation pour protéger les données collectées.

Sécurité et confidentialité

Mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des données dès la conception (sauvegarde, récupération en cas d'incident, chiffrement des données personnelles).

Détailler toutes les mesures de protection des données dans votre registre des traitements.

Privilégier le traitement local des données sur l'appareil plutôt que sur des serveurs distants quand c'est possible.

“Nous sommes confrontés à un paradoxe à l’ère de la data et de l’IA sur mobile : essayer de personnaliser et contextualiser une expérience tout en minifiant les données collectées. Il n’y a pas toujours de bonne réponse, mais des bonnes pratiques qui passent notamment par la clarté et la temporalité des consentements.”

Fabienne Latxague
Head of UX Design
USERADGENTS

Identifier l'existence de traitements de données personnelles

→ Une app ne traitant pas de données personnelles n'entre pas dans le champ du RGPD

→ Dans certains cas, le traitement peut relever de l'exemption domestique

- Traitement décidé et mis en œuvre pour le seul compte de la personne, effectué sous son contrôle, en parfaite autonomie, dans un environnement cloisonné
- Traitement dont la configuration répond aux critères de l'exemption domestique : calculs locaux vs APIs, bases de ressources in-app vs requêtes réseau, …

Assurer la conformité des traitements de données personnelles

→ **Définir les finalités de chaque traitement**

→ **Identifier une base légale pour chaque finalité**

- consentement (correctement recueilli)
- contrat (pouvoir démontrer en quoi l'objet principal du contrat ne peut être atteint en l'absence du traitement)
- intérêt légitime (formaliser une analyse de l'équilibre des intérêts entre l'utilisateur dont les données sont traitées et le responsable de traitement).

→ **Identifier les opérations de lecture / écriture**

= l'accès aux identifiants mobiles et/ou identifiants uniques (hardware), aux capteurs du mobile, aux données stockées dans le mobile, le fingerprinting (opérations d'identification des caractéristiques). Autant d'opérations qui nécessitent par défaut le consentement (exemption dans le cas d'opérations dont la finalité exclusive est de permettre la communication numérique).

Assurer la conformité des traitements de données personnelles

→ **Assurer que les données traitées sont limitées à ce qui est nécessaire pour les finalités poursuivies** (par exemple, ne pas collecter une date de naissance complète si seuls le jour et le mois sont nécessaires).

→ **Privilégier les données fournies manuellement par l'utilisateur** (afin de lui laisser la maîtrise et la précision de la donnée fournie voire même lui laisser le choix entre entrer manuellement la donnée ou permettre la transmission automatique si celle-ci est stockée dans le terminal).

→ **Fixer une durée de conservation des données strictement nécessaire à l'objectif de leur traitement**

→ **Porter une attention très particulière aux données sensibles (politiques, religieuses, santé,...)** dont le traitement est interdit sauf s'il repose sur le consentement libre, spécifique, éclairé et univoque. Interdiction de catégorisation / création de segments de ces données à des fins de profilage publicitaire.

Appliquer les principes de protection des données dès la conception & par défaut

→ **Ne collecter que les données personnelles essentielles à la fourniture du service** (par exemple, la géolocalisation peut simplifier une recherche de point de vente à proximité mais peut être remplacée par la saisie manuelle d'une adresse).

→ **Offrir le choix à l'utilisateur d'utiliser ou non les fonctionnalités non strictement nécessaires au bon fonctionnement de l'app**

→ **S'assurer que les paramètres par défaut de l'app sont les moins intrusifs possibles** (déterminer les paramètres minimaux notamment au regard des différentes catégories d'usagers s'il y a : abonnés payant vs gratuit par exemple).

→ **Vérifier que des technologies améliorant la confidentialité (Privacy Enhancing Technologies) peuvent s'appliquer aux traitements.**

→ **Minimiser les données transmises à ses partenaires** (éviter la transmission de données identifiantes, utiliser des mécaniques de chiffrement de bout en bout pour renforcer la sécurité).

Documenter son analyse

→ **Tenir à jour un registre des traitements** :
recenser, analyser les traitements de données,
justifier les finalités,
identifier et hiérarchiser les risques,
lister qui peut y accéder,
combien de temps elles sont conservées,
si des transferts vers des pays tiers sont prévus,
comment ces informations sont sécurisées.

→ **Mener une analyse d'impact relative à la protection des données dans le cadre de collecte présentant d'importants risques**

→ **Nommer un délégué à la protection des données lorsque c'est obligatoire**

Cartographier ses partenaires

En qualité de responsable du traitement, l'éditeur de l'app doit avoir une vision complète de l'écosystème intervenant dans le traitement de données et un contrôle des rôles et de la conformité des mesures mises en œuvre par ses partenaires.

→ **Clarifier la qualification du développeur : sous-traitant et encadrer la prestation via un contrat (data processing agreement - DPA)**
Fournir des instructions claires et documentées au développeur concernant les traitements à mettre en œuvre, notamment en matière de sécurité et de processus de conformité (contenues dans le registre des traitements).

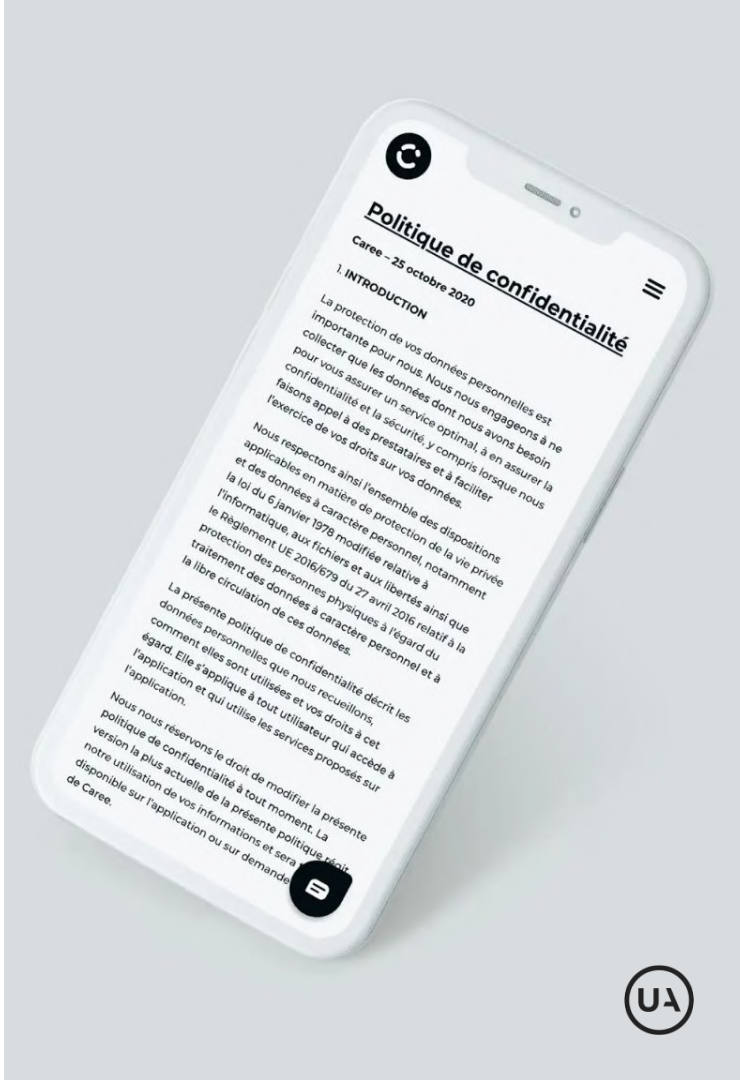
→ **Identifier les éventuelles relations avec d'autres tiers :** traitements liés aux SDK tiers, aux appels aux API des OS, aux analyses relatives à la performance, à l'usage de la batterie, etc. La CNIL recommande que le développeur mette en œuvre des mécanismes de sélection des SDK respectant certains critères.

Une politique de confidentialité accessible

→ **Informer à travers la politique de confidentialité**
Incluant les éléments obligatoires au titre de l'article 13 du RGPD*, la liste des permissions d'accès aux données demandées, leur nature obligatoire ou facultative (et en quoi le refus impacte l'usage de l'app) et les finalités poursuivies via ces permissions.

→ Celle-ci doit être **facilement accessible** avant le téléchargement de l'app ou son lancement, via la fiche store et sur son site, mais aussi in-app, par le biais d'un onboarding, d'une entrée dans le menu ou au niveau de la page du compte client par exemple.

→ La politique doit par ailleurs être **claire et concise**, compréhensible grâce à un langage simple et illustré.



*identité et coordonnées du responsable du traitement, du délégué à la protection des données, les finalités du traitement, la base juridique (voir plus)

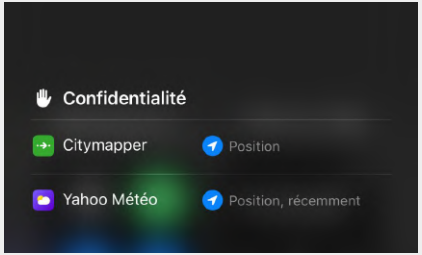
Un consentement contextualisé, clair & valide

→ **Contextualiser** les demandes d'accès à des données personnelles et utiliser des mécaniques de présentation simplifiées.

→ **Obtenir un consentement valide** si la base légale est celle du consentement ou lorsqu'une opération de lecture et/ou d'écriture est mise en œuvre (non soumise à exemption).

→ **Réinformer les utilisateurs** sur l'accès ou le partage de certaines **données** particulièrement **intrusives** (géolocalisation, carnet de contacts, microphone, etc.), par exemple via l'usage d'**indicateurs persistants** dans les interfaces quand ces fonctionnalités sont activées. Des précautions également prises par l'OS par le biais d'un capteur lumineux au niveau de la caméra ou encore d'une flèche alertant d'une géolocalisation active.

→ **Permettre l'exercice des droits :** droit d'accès, droit à l'effacement, droit d'opposition, droit à la portabilité, droit à la rectification et droit à la limitation du traitement. En fonction de la base légale retenue, certains de ces droits ne sont pas applicables. Cela peut se faire en mettant à disposition un centre de gestion des droits au sein de l'app.

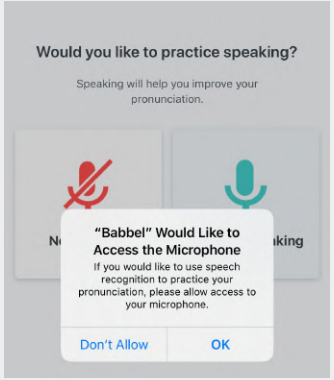


Faire bon usage des permissions

Les permissions constituent une mesure technique indépendante qui permet à l'utilisateur de donner ou bloquer l'accès aux ressources du terminal, indépendamment des finalités poursuivies par l'éditeur de l'app. Le fournisseur d'OS conseille d'informer au sein de la permission pour quelle raison celle-ci est demandée. Ces permissions « techniques » ne sont pas conçues pour collecter le consentement des utilisateurs, au sens du RGPD et de la loi Informatique et Libertés.

→ Choisir la permission impliquant **le moins de collecte supplémentaire** de données pour chaque donnée dont la collecte est nécessaire, et garder en optionnel la collecte des données non obligatoires au fonctionnement de l'app. Si possible, proposer des **alternatives** à l'usage des permissions (saisie manuelle d'adresse, de numéro de téléphone) et assurer les **traitements** des données **localement**.

→ Certaines permissions relèvent de **l'exemption domestique** et ne sont donc pas obligatoires au sens du RGPD. L'accès à une ressource (caméra, contacts, micro,...) via une demande de permission, si cette ressource est ensuite traitée de manière purement locale, peut relever de l'exemption domestique et ainsi ne pas exiger de consentement préalable.

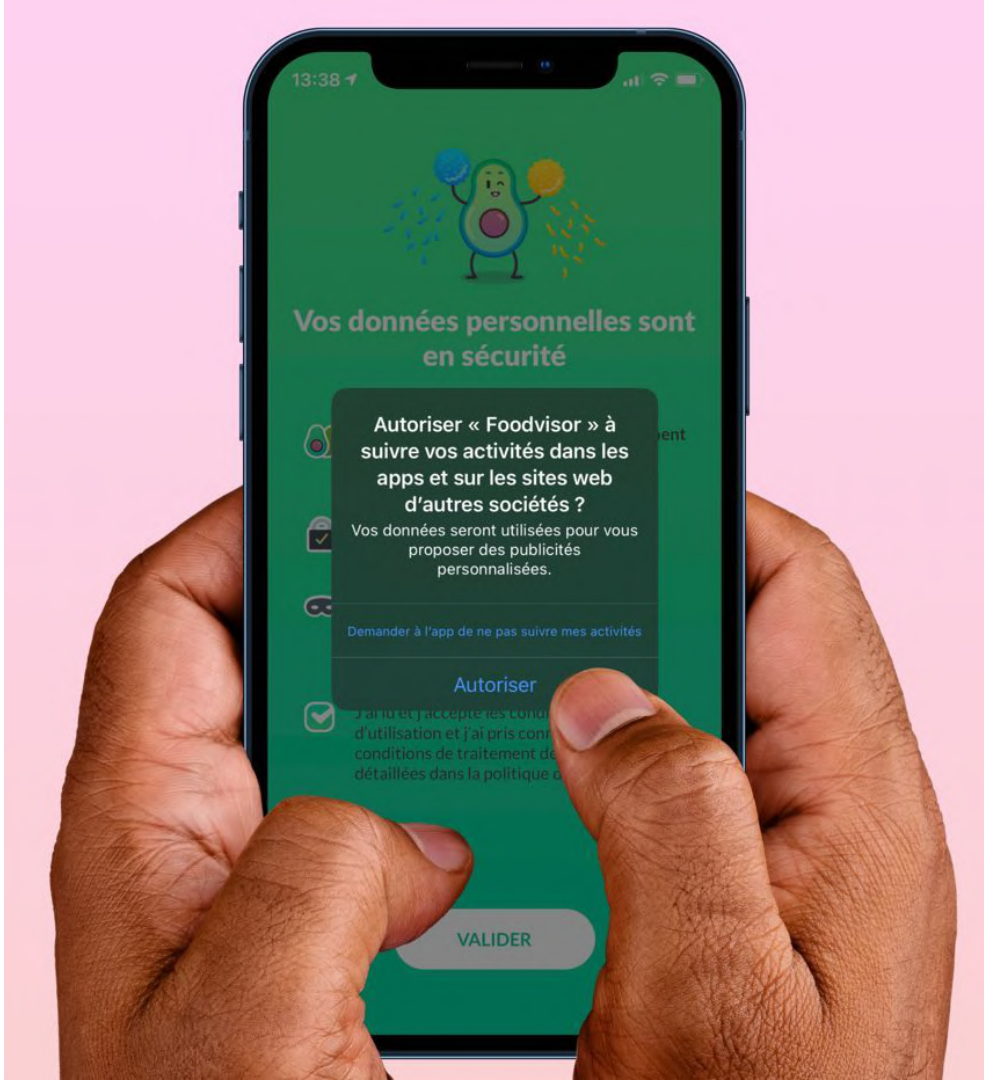


L'impact de l'App Tracking Transparency

Introduit par Apple avec iOS 14.5 en 2021, l'ATT permet aux utilisateurs de refuser la collecte de leurs données personnelles et leur transfert à des sociétés tierces (notamment des apps tierces), à des fins de ciblage publicitaire. L'utilisateur peut gérer son autorisation de façon générale, ou au cas par cas, par application.

Les applications sont donc contraintes d'obtenir le consentement explicite des utilisateurs par le biais d'une popup, indépendante de la CMP « Consent Management Platform ». Apple refuse les apps qui affichent la CMP avant la demande d'ATT, ou qui affichent la CMP après avoir refusé l'ATT.

Ce mécanisme contribue à une plus grande transparence en informant clairement les utilisateurs sur l'utilisation de leurs données même s'il tend également à réduire le taux de consentement des utilisateurs.



Une demande de consentement en plus d'une permission

→ **Un consentement est nécessaire en plus de la permission** si la ressource collectée n'est pas traitée en local, le plus souvent via une **CMP** « Consent Management Platform ».

Indiquer de manière claire et intelligible si la fonctionnalité liée à la permission recherchée est :

→ nécessaire pour le fonctionnement de l'application,

→ relative à une fonction accessoire pour le bénéfice de l'utilisateur (faciliter sa navigation, permettre de scanner un code QR, enregistrer un mémo vocal)

→ relative à des traitements effectués pour le bénéfice de l'éditeur ou d'un tiers

“Il est important de prendre en compte qu’une application peut être multi-utilisateurs. S’il est possible de se connecter avec des comptes différents, il est alors nécessaire de demander son consentement à chaque utilisateur, et de conserver les choix à chaque changement de compte afin que chacun puisse avoir un profil de consentement distinct.”

Stéphanie Spenlé-Landais
Cheffe de Projet Technique
USERADGENTS

La bonne articulation entre consentement et permissions

→ Il peut être difficile pour l'utilisateur de s'y retrouver entre les fenêtres de permissions et celles de consentement. Si un utilisateur refuse une permission mais donne ensuite son consentement via la CMP pour des traitements incluant cette permission (comme la géolocalisation), ce consentement ne sera pas valide au regard du RGPD, car il n'est pas considéré comme clair et explicite.

→ Détails des finalités disponibles via un bouton de déroulement ou un lien hypertexte.

→ Possibilité de consentir de manière granulaire sur un second niveau d'info.

“Sur mobile, il est essentiel d’adapter les demandes de consentement aux petits écrans. Évitez les CMP encombrées qui poussent à tout accepter d’un coup et peuvent s’apparenter à du dark pattern. Au contraire, privilégiez une interface claire, lisible, découpée en plusieurs rubriques, pour permettre de faire des choix éclairés.”

Cyrille Legrand
Lead Développeur iOS
USERADGENTS

L'accès à la géolocalisation : spécificités

→ Demander l'accès à la localisation approximative plutôt que précise et uniquement active quand l'appli est en premier plan.

→ Limiter la permission à une seule fois plutôt qu'une permission permanente et si permanence, demander à intervalles réguliers confirmation de son accord à ce que la localisation soit collectée.

→ Eviter la transmission d'information à des tiers si possible (par exemple une permission fondée sur le seul GPS et non l'analyse de l'environnement réseau).

→ Avant tout envoi des données de localisation vers les serveurs de l'app, identifier le niveau de précision minimal qui est nécessaire pour atteindre ses finalités et tronquer localement les coordonnées.

L'accès aux données de contacts stockées au sein du terminal

Certaines apps nécessitent l'accès aux contacts pour identifier les utilisateurs également usagers de l'app et faciliter les connexions.

→ Chaque utilisateur doit consentir à l'utilisation future de ses coordonnées par d'autres. Ce consentement ne peut pas être implicite via une autorisation d'accès au carnet d'adresses. Par défaut, la visibilité des coordonnées doit être configurée au niveau le plus restreint, avec des options ajustables par l'utilisateur.

→ Utiliser des méthodes limitant l'intrusion (comme le "Private Set Intersection") et supprimer les données des contacts après analyse.

→ Fixer une durée limitée pour l'autorisation d'accès aux contacts, nécessitant un renouvellement pour tout nouvel usage.

L'accès au microphone : spécificités

→ Si le besoin est ponctuel, l'éditeur devrait révoquer la permission après la captation du son.

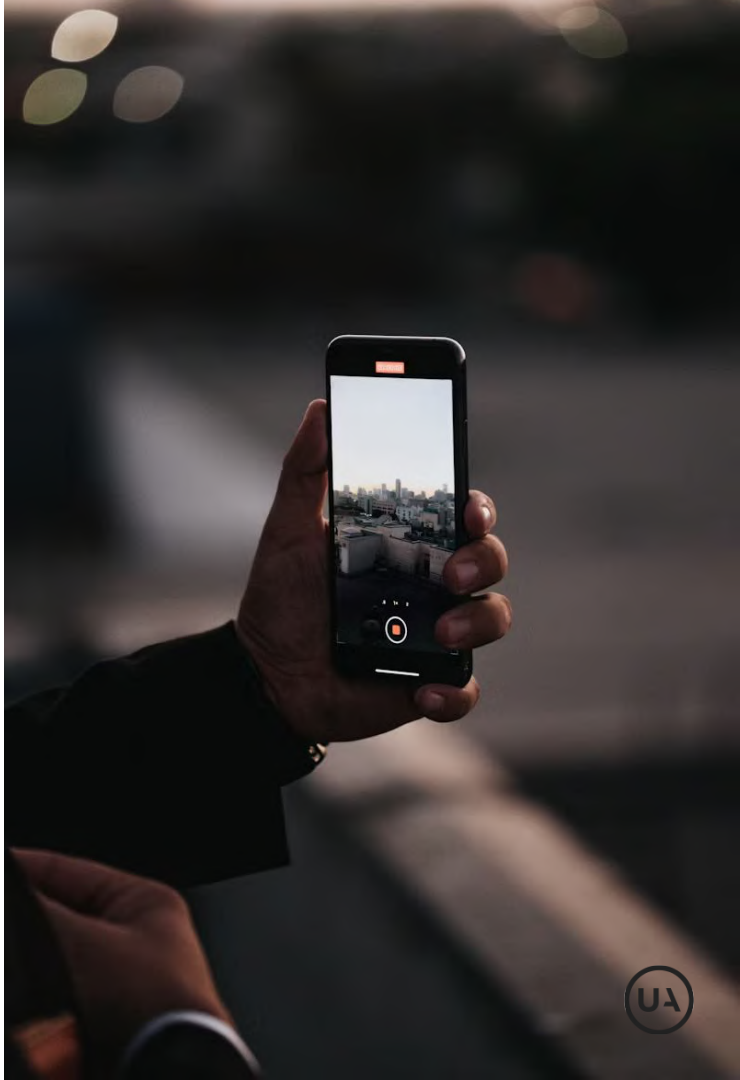
→ Avant tout envoi des contenus audio vers les serveurs de l'application, l' éditeur devrait proposer à ses utilisateurs de tronquer ou de réécouter les contenus partagés

L'accès à l'appareil photo : spécificités

→ Bien faire la distinction entre l'accès à l'appareil photo ou l'accès aux photos stockées dans le mobile.

→ Exclure l'usage de permissions demandant l'accès à l'ensemble des contenus multimédia de l'utilisateur si le traitement n'exige pas cet accès complet au regard des finalités qu'il poursuit. Au contraire, s'appuyer sur des permissions permettant la sélection de photos.
- dans le cas où une prise de photo ou de vidéo en direct est nécessaire, privilégier les solutions déléguant cette captation aux applications système ;
- si cela n'est pas possible (par exemple, pour des usages interactifs du flux vidéo), s'assurer de ne requérir que le strict minimum en termes d'autorisation matérielles (par exemple, ne pas activer l'enregistrement audio si ce n'est pas une nécessité).

→ Supprimer les métadonnées associées à l'image (géolocalisation, horodatage, données EXIF) si elles ne sont pas nécessaires.
→ Avant tout envoi des images vers les serveurs de l'app, l'éditeur devrait analyser la nécessité de l'obtention de l'ensemble de l'image. À défaut, il devrait proposer des outils de sélection ou de floutage à l'utilisateur. Ne pas conserver les images collectées sur un serveur distant sauf en cas d'usage précis et justifié, ou la rendre optionnelle.



Usage de fonctionnalités mises à dispo par l'OS

→ Analyser si l'usage d'outils fournis par l'OS implique le traitement de données personnelles.

→ Analyser l'ensemble des API fournies par les OS (notification, paiement, authentification unique « single sign-on », suivi de santé du système, sécurité, gestion des pannes, etc.), pour s'assurer qu'il ne met pas en œuvre un traitement sans instruction de son responsable de traitement.

→ Suivre les évolutions des OS et de leurs fonctionnalités, notamment en termes de minimisation des données traitées.

Intégration de SDK

→ Analyser si l'intégration de SDK implique le traitement de données personnelles (collecte d'un identifiant unique, adresses IP, identifiants Wi-Fi environnants,...) et auquel cas choisir avec l'éditeur la bonne qualification (sous-traitant généralement) en recueillant la liste des données personnelles collectées et l'objet, la nature et la finalité des traitements (ou renoncer à l'usage du SDK).

→ Choisir une bonne configuration de SDK et suspendre toute lecture ou écriture au lancement de l'app avant réception d'un signal de consentement.

→ La transmission d'identifiants inter-applications à des fournisseurs de SDK devrait être évitée. Si cette transmission est nécessaire, un hachage des identifiants devrait préalablement être opéré.

→ S'assurer que le SDK :
- présente des moyens de bloquer tout traitement ou accès à des données stockées sur le terminal
- permette la mise en œuvre d'une permission,
- permette de répondre aux demandes d'exercice des droits.

16

On compte en moyenne 16 SDK par app

Source : Cnil, 2024

“La protection des données personnelles est un enjeu crucial. C’est pourquoi, parmi les nouvelles recommandations, la gestion des vulnérabilités potentielles dans les librairies externes soumises au consentement doit être anticipée : l’éditeur de la librairie, ou à défaut le développeur, doit prévoir un système de désactivation de la librairie à distance, et s’assurer que dans ce cas, aucune donnée utilisateur ne sera transmise.”

Stéphanie Spenlé-Landais
Cheffe de Projet Technique
USERADGENTS

Assurer la sécurité de l'app

→ Sécurisation des communications avec les serveurs en les encapsulant systématiquement dans un canal TLS, dont les suites cryptographiques sont fixées explicitement, en respect du guide TLS de l'ANSSI.

→ Stockage des secrets cryptographiques par empaquetage au moyen des API permettant l'utilisation des suites cryptographiques incluses dans le téléphone, en privilégiant les protections matérielles telles que le « Hardware Keystore » d'Android ou la « Secure Enclave » d'Apple.

→ Prise en compte de la possibilité de sauvegarde automatique d'une donnée par l'OS : désactivation des sauvegardes non souhaitées ou chiffrement des données.

“Les données sensibles (santé, informations sur des utilisateurs mineurs,...) doivent être chiffrées selon des standards éprouvés (RSA,...), et ce, même si stockées on-device, pour éviter toute extraction des fichiers d’une app suite à une sauvegarde locale.”

Cyrille Legrand
Lead Développeur iOS
USERADGENTS

Maintenir la conformité durant le cycle de vie de l'app

→ **Mettre en œuvre des audits de sécurité :** en utilisant des outils d'analyse statique permettant de vérifier les SDK ou le OWASP MASTG (Mobile Application Security Testing Guide) proposé par l'ONG Open Web Application Security Project comme base pour analyser la sécurité de son app. La CNIL considère le niveau L1 comme le strict minimum à respecter.
La mise en place d'un banc de test pour vérifier le bon fonctionnement des outils de recueil de consentement mis en œuvre est également conseillée.

→ **Mettre en place des processus robustes en termes de conformité :** processus de validation afin que toute évolution impactant les conditions de mise en œuvre du traitement (choix de sous-traitant ultérieur, SDK, fonctionnalités, recueil de consentement) soit approuvée. Actualiser le registre des traitements afin de prendre en compte les évolutions des traitements de données mis en œuvre, ainsi que la politique de confidentialité des données. mettre en œuvre des contrôles d'accès journalisés pour éviter les détournements internes (personnels ou structurels), superviser et vérifier la suppression des données dont la durée de conservation est échue.

RGPD

Encadrer la relation entre l'éditeur et le développeur

La checklist ✔

Côté éditeur :

→ Identifier les permissions les plus protectrices
→ Pour les permissions les plus intrusives, signaler à l'utilisateur lorsqu'elles sont actives
→ Rendre l'usage de la permission optionnelle et prévoir des alternatives dans la mesure du possible
→ Traiter les données obtenues en local
→ Obtenir un consentement
→ Assurer la conformité juridique des traitements (base légale, identification des opérations de lecture / écriture, minimisation de la collecte, durée de conservation,...)
→ Maintenir la sécurité dans le temps

La checklist ✔

Côté développeur :

→ Formaliser sa relation avec l'éditeur (registre, interlocuteur côté éditeur pour la validation des choix impactant les traitements de données personnelles,...)
→ Assumer son rôle de conseil envers l'éditeur
→ Garder une cohérence dans l'information et éviter les dark patterns
→ Faire bon usage des SDK (granularité et retrait du consentement, configuration sans lecture / écriture, validation de l'éditeur,...)
→ Assurer la sécurité de l'app (niveau L1 de l'OWASP MAS, sauvegardes chiffrées avec une clé sauvegardée en local,...)

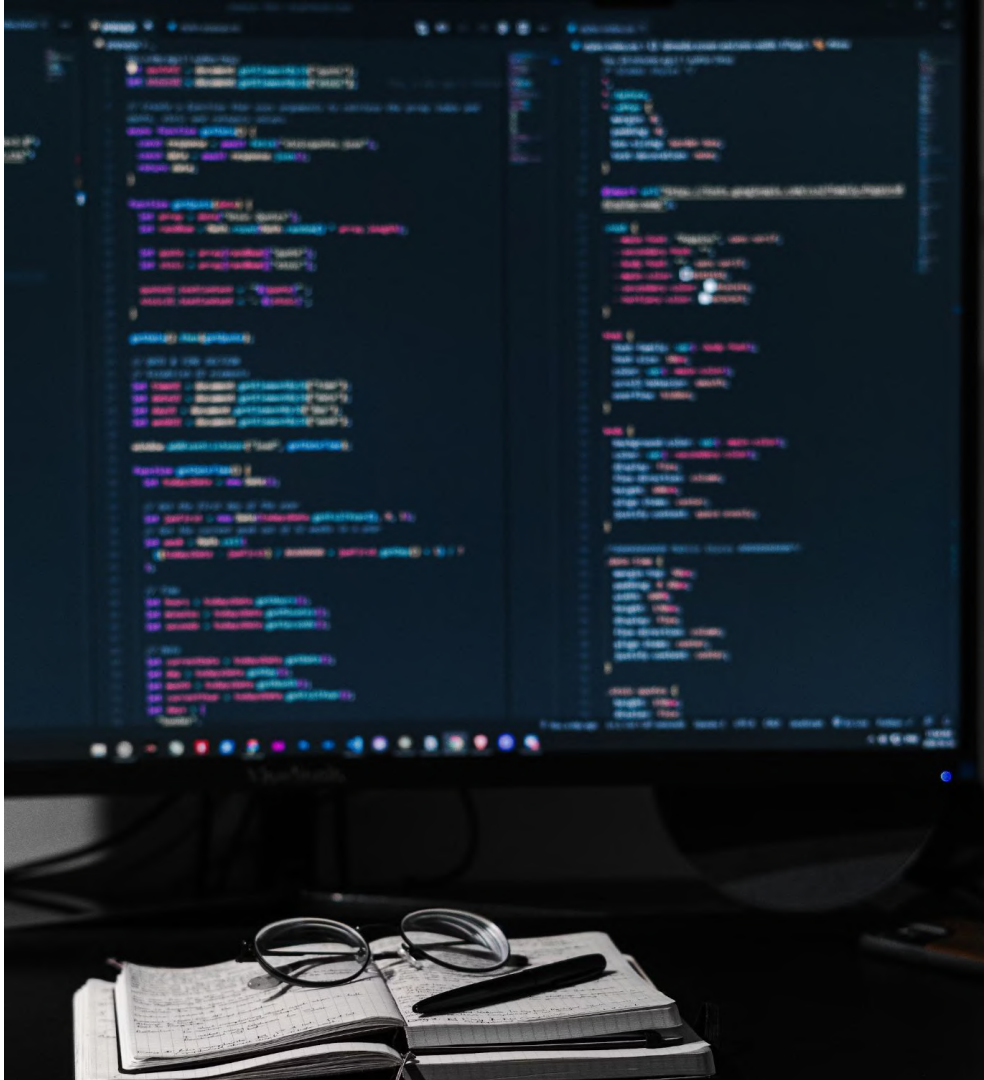
La relation agence / annonceur

Partage des rôles

Dans le cadre d'une application conçue et développée par une agence pour le compte d'un client annonceur, le rôle du développeur est central pour garantir que l'application respecte les principes du RGPD. Le développeur de l'application est défini comme l'entité morale ou l'entreprise individuelle qui procède aux opérations techniques de développement de l'application, pour le compte et sur instruction de l'éditeur.

Bien que la responsabilité juridique de réaliser l'analyse d'impact sur la protection des données incombe au **responsable de traitement** (l'annonceur), la sécurité de l'app dépend largement des choix techniques effectués par le **sous-traitant** (l'agence), tout comme l'implémentation des processus de recueil du consentement (l'articulation consentement / permissions), la mise en œuvre de l'infrastructure de traitement et de stockage des données ou la réalisation d'opérations sur des données hébergées sur le serveur de l'app à des fins de maintenance ou d'infogérance.

Elle préconise également que l'éditeur soit impliqué dans les décisions structurantes, notamment en matière de sécurité, tout au long du processus de conception et que le développeur mette en œuvre une démarche pour assurer l'information et l'approbation de l'éditeur concernant les choix techniques opérés ainsi que leurs implications et respecte ainsi son devoir de conseil.



La relation agence / annonceur

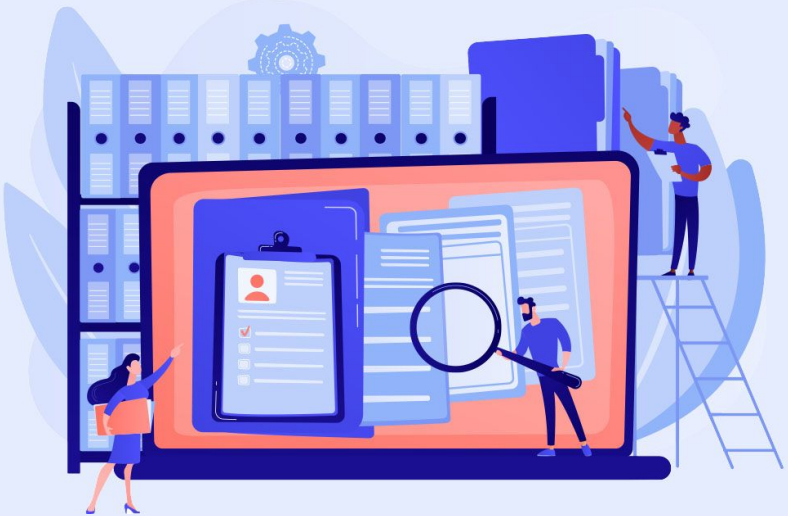
RGPD-compliant, stipulé dans le contrat

Dans ce contexte, la CNIL recommande que le contrat liant le développeur à l'éditeur stipule clairement l'obligation de concevoir une application qui traite les données en conformité avec le RGPD et en intégrant le respect de la vie privée dès la conception (privacy by design).

Enfin, il est rappelé dans la recommandation de la CNIL qu'un fonctionnement de l'application non conforme au RGPD pourrait engager la responsabilité civile du développeur vis-à-vis de l'éditeur.

“Le périmètre du projet n’étant pas toujours totalement défini au début d’une relation contractuelle, il est crucial de réévaluer et de mettre à jour le DPA (Data Processing Agreement) lorsque de nouvelles informations sur les traitements de données deviennent disponibles ou que les processus évoluent, afin qu’il reflète fidèlement la réalité des pratiques de traitement des données entre les parties (responsable de traitement et sous-traitant).”

Renaud Ménérat
Co-fondateur et COO
USERADGENTS



La relation agence / annonceur

Les bases du contrat

⟶ L'éditeur fournit au développeur, dans le cadre du cahier des charges, le **registre des traitements** concernant l'app. S'il n'existe pas encore, un cahier des charges suffisamment exhaustif et clair qui permette de définir les données qui seront utilisées.

⟶ L'éditeur doit clairement expliciter ses attentes et exigences au développeur, en matière de consentement, permissions et sécurité.

⟶ Une qualification claire du rôle du développeur pour chacun des traitements concernés.

⟶ Stipuler les conditions de mise en œuvre de chaque traitement.

⟶ Prévoir un point de contact pour valider les choix ayant un impact en matière de traitement de données personnelles (en général le DPD de l' éditeur).

La relation agence / annonceur

Les obligations de l'agence

→ Obligation de transparence et de traçabilité
→ Obligation de prendre en compte, au titre de son devoir de conseil, les principes de protection des données dès la conception et par défaut
→ Obligation d'assister son client dans le respect de ses obligations au titre du RGPD
→ Obligation de garantir la sécurité des données traitées
→ Obligation de rendre compte à l'éditeur (principe d'accountability) en tenant un registre des activités de traitements mis en œuvre pour le compte de l' éditeur et qui devra lui être mis à disposition
→ Alerter l'éditeur si les données personnelles collectées et traitées nécessitent une mise à jour du registre des traitements ou du cahier des charges détaillé.
→ Faire valider le recours à des sous-traitants ultérieurs et s'ils procèdent à des opérations de lecture / écriture, ils pourront être responsables ou responsables conjoints du traitement avec l'éditeur.

Les obligations de l'agence

→ Distinguer, d'une part, **l'environnement de test et de développement** du développeur, dans lequel le développeur peut être amené à mettre en œuvre des tests de traitements de données ou d'intégration de SDK, à la demande de l'éditeur ou de sa propre initiative et, d'autre part, **l'environnement de recette** dans lequel il est proposé à l'éditeur une version de l'application conforme à ses instructions, comportant uniquement les traitements prévus.

Tableau récapitulatif des obligations des éditeurs dans la conception de leurs apps [CNIL]

Identifier l'existence de traitements de données personnelles	1.1.1	L'ensemble des données personnelles et les traitements qui s'y rapportent sont identifiés.	L'éditeur doit identifier les traitements de données personnelles.
Assurer la conformité juridique des traitements	1.2.1	Chaque traitement mis en œuvre a une base légale identifiée.	L'éditeur doit s'assurer que chacun de ces traitements de données personnelles respecte le RGPD et la loi Informatique et Libertés.
	1.2.2	Les opérations de lecture et/ou d'écriture sur les terminaux des personnes mis en œuvre au sein des applications sont identifiés.	L'éditeur doit identifier les opérations de lecture et/ou d'écriture sur les terminaux.
	1.2.3	Aucune collecte de données non nécessaire n'est opérée. Celles nécessaires sont minimisées.	L'éditeur doit s'assurer que les données collectées pour chaque finalité sont limitées à ce qui est nécessaire pour la finalité recherchée/
	1.2.4	Une durée de conservation des données est associée à chaque traitement.	Les données traitées doivent être conservées pour une durée strictement nécessaire à l'objectif poursuivi par le traitement.
	1.2.5	Les données sensibles traitées sont identifiées.	
	1.2.6	Des mesures additionnelles sont appliquées sur les données des personnes mineures.	

Tableau récapitulatif des obligations des éditeurs dans la conception de leurs apps [CNIL]

Appliquer les principes de protection des données dès la conception et par défaut (article 25 du RGPD)	1.3.1	La liste des paramètres minimaux pour fournir le service demandé est déterminée et sont proposés par défaut.	L'éditeur doit mettre en œuvre des mesures techniques et organisationnelles permettant de protéger les données personnelles dès la conception.
	1.3.2	Ces paramètres sont analysés au regard des différentes catégories d'usagers.	
	1.3.3	La possibilité d'intégrer des mécanismes de protection de la vie privée est étudiée dès la conception.	L'éditeur doit analyser si des technologies améliorant la confidentialité (Privacy Enhancing Technologies) peuvent s'appliquer aux traitements mis en œuvre.
Documenter son analyse (articles 5.2 et 24 du RGPD)	1.4.1	Un registre des traitements est réalisé.	L'éditeur doit adopter des outils et procédures pour assurer la conformité de leurs traitements de manière continue.
	1.4.2	Les durées de conservation sont justifiées et documentées.	
	1.4.3	Une AIPD est réalisée si le traitement en remplit les critères.	
	1.4.4	Un délégué à la protection des données est nommé au sein de l'éditeur.	

Tableau récapitulatif des obligations des éditeurs dans la cartographie de leurs partenaires [CNIL]

Encadrer les relations avec les développeurs	2.1.1	La qualification du développeur est convenue entre celui-ci et l'éditeur.	L'éditeur doit encadrer les relations avec les partenaires techniques auxquels il a recours pour le développement de l'application.
	2.1.2	L'ensemble des mentions de l'article 28 du RGPD figurent dans le contrat avec le développeur.	
	2.1.3	Les instructions données au développeur sur les traitements à mettre en œuvre sont claires et documentées, et un point de contact dédié aux problématiques de vie privée est mis à sa disposition.	L'éditeur doit fournir des instructions claires concernant les traitements à mettre en œuvre, par exemple via le contrat de sous-traitance.
Identifier les éventuelles relations avec d'autres tiers	2.2.1	L'ensemble des tiers impliqués dans l'application sont analysés pour identifier s'ils procèdent à des traitements de données personnelles.	L'éditeur doit encadrer les relations avec les partenaires techniques auxquels il a recours pour le développement de l'application.
	2.2.2	Tout SDK mis en œuvre est analysé avec l'aide potentielle du développeur pour identifier s'il procède à des traitements de données personnelles.	

Tableau récapitulatif des obligations des éditeurs dans la gestion du consentement et du droit des personnes [CNIL]

Informer correctement les utilisateurs (articles 12 à 14 du RGPD)	3.1.1	Les obligations en termes de recueil de consentement telles qu'explicitées par la CNIL dans ses lignes directrices et recommandations sur les cookies et autres traceurs sont mises en œuvre.	L'éditeur doit s'assurer du respect des droits des personnes que ce soit en termes d'information, de consentement ou d'exercice des autres droits même quand leur mise en œuvre pratique dépend d'un tiers.
	3.1.2	La politique de confidentialité est accessible avant tout téléchargement de l'application, par exemple sur la page de téléchargement de celle-ci. La politique de confidentialité est également accessible au sein de l'application.	L'éditeur doit correctement informer les utilisateurs, par exemple dans une « politique de confidentialité ».
Obtenir un consentement valide des utilisateurs (article 4 et 7 du RGPD)	3.2.1	La politique de confidentialité est accessible avant tout téléchargement de l'application, par exemple sur la page de téléchargement de celle-ci. La politique de confidentialité est également accessible au sein de l'application.	L'éditeur doit s'assurer que la politique de confidentialité est facilement accessible avant que tout traitement soit mis en œuvre, directement depuis l'application.
Faciliter l'exercice des droits (articles 15 à 22 du RGPD)	3.3.1	Une analyse sur les droits applicables aux personnes est effectuée (droit d'accès, droit à la portabilité, droit à la limitation, etc.).	L'éditeur, doit faciliter l'exercice, par les utilisateurs, de leurs droits et en assurer le respect.
	3.3.2	Un centre de gestion des droits est mis en place directement au sein de l'application.	L'éditeur, doit faciliter l'exercice, par les utilisateurs, de leurs droits et en assurer le respect.

Tableau récapitulatif des obligations des éditeurs dans la maintenance de la conformité durant le cycle de vie de l'app [CNIL]

Assurer le maintien de la sécurité au cours du temps (article 32 à 34 du RGPD)	4.1.1	Les exigences en termes de mesures techniques attendues sont formalisées auprès des sous- traitants.	L'éditeur doit s'assurer de la mise en œuvre de mesure pour assurer la sécurité des données notamment via le contrat de sous-traitance-
	4.1.2	Les obligations en termes d'alerte de sécurité afin de permettre la notification de violations de données personnelles sont rappelées aux sous- traitants.	
	4.1.3	Le processus de mise à jour en cas de vulnérabilité est contractualisé avec les tiers.	
Auditer le respect des engagements des partenaires	4.2.1	Si les risques le justifient, des audits sont mis en œuvre auprès des sous-traitants pour contrôler le respect des instruction données.	
Mettre en place des processus robustes en termes de conformité	4.3.1	Les mises à jour sont reflétées dans le registre des traitements, dans l'AIPD et dans la politique de confidentialité.	L'éditeur doit actualiser le registre des traitements.
	4.3.2	Des instructions sont données aux sous-traitants pour que toute évolution impactant les problématiques de vie privée soit approuvée avant mise en œuvre.	L'éditeur doit encadrer l'accès aux données personnelles par les sous-traitants.
	4.3.3	Les données personnelles sont protégées et leur accès est journalisé pour éviter tout détournement.	L'éditeur doit encadrer l'accès aux données personnelles par les sous-traitants.
	4.3.4	La suppression des données dont la durée est échue est organisée.	L'éditeur doit encadrer l'accès aux données personnelles par les sous-traitants.

Tableau récapitulatif des obligations des éditeurs dans l'utilisation des permissions [CNIL]

Utiliser les permissions	5.1.1	Pour chaque donnée dont la collecte est nécessaire, la permission impliquant le moins de collecte supplémentaire de données est choisie.
	5.1.2	Des alternatives à l'usage des permissions sont proposées aux personnes lorsque cela est possible.
	5.1.3	Les données collectées sont traitées localement lorsque cela est possible.
	5.1.4	Le consentement est valablement recueilli lorsqu'il est nécessaire.
	5.1.5	Avant toute collecte distante, la précision de la donnée est diminuée au minimum nécessaire.

Un peu de lecture

Ressources et textes de références de la CNIL

→ La recommandation de la CNIL relative aux applications

→ Les webinaires de la CNIL

→ Les règles et conseils pour les professionnels

→ Les conseils pour les utilisateurs finaux

→ Les recommandations concernant les permissions

Un guide pratique réalisé par :

Marie Billon
Directrice de la Communication & des Etudes
m.billon@useradgents.com

USERADGENTS

8 rue de la Rochefoucauld - 75009 Paris
📩 uainfo@useradgents.com
☎️ 01 77 75 65 90
www.useradgents.com