# Recommandation

## relative aux applications mobiles

Publiée le 8 avril 2025 (*Délibération n° 2025-024 du 27 mars 2025 portant modification de la recommandation relative aux applications mobiles et abrogeant la délibération n° 2024-061 du 18 juillet 2024 portant adoption de la recommandation relative aux applications mobiles*)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

# Table des matières

# 1. Introduction

Les applications mobiles sont l'un **des principaux moyens d'accès à des contenus et des services numériques**.

Pour ses utilisateurs, le téléphone mobile multifonctions (ou ordiphone, « *smartphone* » en anglais), terminal personnel par définition, **relève de la sphère privée et intime**. Il est essentiel pour chacun de pouvoir contrôler les données auxquelles les applications mobiles ont accès. Pour autant, les traitements de données mis en œuvre au sein des applications peuvent être ou apparaître opaques. En particulier, les informations sur l'existence de collectes de données et sur leurs objectifs sont souvent peu claires. L'utilisateur peut avoir des difficultés à comprendre la nature des autorisations qui lui sont demandées, ce qui complique l'expression de ses choix. Enfin, les mobiles multifonctions embarquent de nombreux capteurs plus ou moins connus des utilisateurs (caméra, GPS, base de contacts, accéléromètres, etc.) et qui peuvent permettre aux applications d'accéder à des données dont la collecte peut se révéler très intrusive.

**Les acteurs qui participent à la mise à disposition d'applications mobiles doivent s'assurer du respect de leurs obligations en matière de protection des données et des droits des utilisateurs. Ces acteurs sont nombreux :** les développeurs d'applications (dont certaines peuvent s'échanger des données), les fournisseurs de systèmes d'exploitation, les gestionnaires de magasins d'applications, les éditeurs de kits de développement logiciel (« *software development kits* » ou SDK en anglais) liés à des réseaux sociaux ou à des fonctionnalités techniques, etc.

En pratique, des échanges de données ont souvent lieu entre ces différentes entités, avec des partages de responsabilité parfois mal définis. En particulier, le recours à des SDK traitant des données à caractère personnel (ou « données personnelles » dans la suite de ce document) de manière non conforme et l'usage non conforme d'identifiants du mobile ont déjà pu faire l'objet de mises en demeure ou de sanctions de la part de la CNIL[1].

**Si les principes et obligations en matière de protection des données sont désormais bien connus des opérateurs de sites web et font l'objet de recommandations de la part de la CNIL[2], leur mise en œuvre dans le contexte des applications mobiles nécessite d'être précisée.**

Cette recommandation vise à clarifier ces règles afin que les acteurs de l'écosystème mobile aient une bonne compréhension de leurs obligations et propose des recommandations concrètes pour s'y conformer ainsi que des bonnes pratiques.

**Ces recommandations sont sans préjudice des règles applicables sur d'autres fondements juridiques que la protection des données personnelles, notamment le droit de la concurrence et le règlement 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (dit règlement sur les marchés numériques, « *Digital Markets Act* » ou DMA).**

[1] Déc. n° MED 2018-022, 25 juin 2018, Déc. n° MED 2018-023, 25 juin 2018, Déc. n° MED 2018-043, 8 oct. 2018 , Déc. n° MED-2018-042, 30 oct. 2018, Déc. n° SAN-2022-025, 29 déc. 2022 (cette décision fait l'objet d'un recours devant le Conseil d'Etat à la date de l'adoption de cette recommandation), Déc. n° SAN-2022-026, 29 déc. 2022.

[2] CNIL, délibérations n° 2020-091 et n° 2020-092 du 17 septembre 2020 portant respectivement adoption de lignes directrices et d'une recommandation en matière de « *cookies* et autres traceurs ». Voir également « Évolution des pratiques du web en matière de *cookies* : la CNIL évalue l'impact de son plan d'action », cnil.fr.

# 2. Périmètre de la recommandation

## 2.1. À qui s'adresse cette recommandation ?

Cette recommandation vise à rappeler et expliciter le droit applicable aux traitements de données personnelles des utilisateurs d'applications mobiles. Elle doit guider les professionnels de l'environnement des applications mobiles dans leur conformité à la réglementation relative à la protection des données.

Elle s'adresse aux professionnels évoluant dans le secteur des applications mobiles, à savoir :

- les éditeurs d'application ;
- les développeurs d'application ;
- les fournisseurs de kits de développement logiciel ;
- les fournisseurs de systèmes d'exploitation ;
- les fournisseurs de magasins d'applications.

Cette recommandation s'adresse particulièrement aux professionnels ayant un impact en termes de protection des données personnelles, par exemple les délégués à la protection des données. Elle est également à l'usage de tous les conseils en matière de protection des données personnelles.

Elle doit aider chaque professionnel à déterminer sa qualification juridique au sens du RGPD (responsable ou responsable conjoint du traitement ou sous-traitant), afin de mieux comprendre ses obligations.

Les obligations, recommandations et bonnes pratiques découlant de ces qualifications sont détaillées dans les parties dédiées à chaque acteur. Toutefois, chaque acteur est invité à se référer non seulement aux recommandations qui le concernent mais également à celles s'adressant à ses partenaires afin de mieux comprendre les obligations de chacun.

## 2.2. Que désigne-t-on par « application mobile » ?

La notion d'application mobile désigne les logiciels applicatifs distribués dans l'environnement des téléphones mobiles multifonctions (ou *smartphones*) et tablettes, c'est-à-dire des terminaux individuels et portatifs, permettant un accès au réseau Internet ainsi que, le plus souvent, au réseau téléphonique, et pouvant permettre l'installation et l'exécution d'applications tierces en leur sein. Cette notion inclut l'ensemble des typologies d'applications, qu'elles soient utilisées dans un contexte privé ou professionnel.

- Ces applications sont le plus souvent distribuées via des plateformes de diffusion intégrées au terminal par les constructeurs et sont exécutées sur celui-ci de manière isolée entre elles (modèle de « bac à sable », ou « *sandbox* » en anglais). Les applications peuvent accéder à un certain nombre de fonctionnalités et de données du système via des interfaces de programmation applicatives (« *application programming interface* » ou *API* en anglais) mises à disposition à cet effet par le fournisseur du système d'exploitation ((« *operating system* », ou OS)).

- La présente recommandation couvre l'ensemble des typologies d'applications, qui peuvent être :

  - « natives », au sens où elles sont développées dans le langage de programmation propre au système d'exploitation dans lequel elles sont exécutées (en pratique, Kotlin ou Java pour Android et Swift ou Objective-C pour iOS) ;

  - « hybrides », c'est-à-dire développées avec des langages et technologies issus de la programmation web, puis transformées en application au moyen d'outils spécifiques (tels que React-Native ou Flutter), afin de conserver dans le temps une base de code uniforme sur l'ensemble des versions de l'application ;

  - « web progressives » (« *PWA* », pour « *Progressive Web App* »), c'est-à-dire des pages web dynamiques qui sont présentées à l'utilisateur sous forme d'applications.

**Comment la présente recommandation s'applique-t-elle aux environnements logiciels similaires à ceux des mobiles multifonctions ?**

Dans ces contextes, si toutes les recommandations ne sont pas applicables, les acteurs sont invités à prendre connaissance de celles-ci pour transposer les éléments applicables à leur situation.

**Quels sont ces environnements ?**

Il s'agit des environnements permettant la distribution d'applications sur un système d'exploitation mobile adapté à un usage spécifique, par exemple :

- les montres connectées, des enceintes connectées (« *smart speakers* ») ;
- les tableaux de bord automobiles connectés ;
- les dispositifs médicaux personnels connectés ;
- les capteurs et objets connectés à Internet (« *Internet of Things* » ou « IoT ») de façon générale ;
- l'informatique individuelle (sous Windows, MacOS, Linux, etc.) ;
- certains environnements dédiés (p. ex. : jeux vidéo sur Steam).

## 2.3. Quels sont les acteurs du secteur des applications mobiles[3] ?

De multiples acteurs interviennent dans l'écosystème des applications mobiles et traitent des données personnelles de différentes manières. Il s'agit principalement du fournisseur du système d'exploitation, du fournisseur du magasin d'application, de l'éditeur de l'application, du développeur et de l'éditeur des kits de développements logiciels. Le plus souvent, ces acteurs sont interdépendants.

### Le fournisseur du système d'exploitation

*Quel est le rôle du fournisseur du système d'exploitation ?*

Le fournisseur du système d'exploitation (« OS ») met à disposition le système d'exploitation spécialement configuré et installé sur le terminal mobile de l'utilisateur, environnement dans lequel l'application sera par la suite exécutée.

*Qu'est-ce que l'OS ?*

L'OS est la brique logicielle qui définit et assiste l'ensemble des interactions autorisées entre l'utilisateur et le terminal, mais également entre les applications mobiles tierces (celles qui seront installées ensuite) et le terminal.

Plusieurs acteurs peuvent participer à la construction d'un OS tel qu'il sera utilisé par l'utilisateur final.

Ainsi, un fournisseur d'OS tiers peut faire le choix d'utiliser la base de code d'un autre OS pour ensuite y intégrer des surcouches logicielles dans son propre OS. Ces surcouches logicielles sont des composants logiciels tiers inclus dans la version finale d'un système d'exploitation, tel qu'il sera proposé aux utilisateurs, ajoutant des fonctionnalités qui pourront être utilisées par les applications à l'OS (p. ex. : applications de clavier virtuel, assistant vocal, etc.). De plus, le constructeur d'appareil mobile peut choisir d'intégrer des applications mobiles qu'il n'aura pas développées lui-même et qu'il aura choisi d'intégrer à son propre système (p. ex. : suites bureautiques, applications des opérateurs de téléphonie mobile).

C'est par exemple le cas pour des constructeurs de mobiles multifonctions qui utilisent un socle technique *open source* et y intègrent des composants logiciels tiers[4] ainsi que leurs propres applications. C'est également le cas pour les opérateurs de téléphones mobiles proposant à la vente des mobiles multifonctions incluant un lot de services préinstallés.

Les recommandations s'appliquent à l'ensemble des acteurs qui participent à la fourniture de cette brique fonctionnelle.

---

[3] Cette partie vise à présenter les acteurs évoluant dans le secteur des applications mobiles. Se référer à la partie 4 des présentes recommandations s'agissant des rôles de chaque acteur dans le cadre de l'utilisation de l'application.

[4] En 2023, certains constructeurs (ex. : Samsung, Oppo, Xiaomi) utilisent ainsi le socle technique AOSP mis à disposition par Google (Android Open Source Project : base de code du système d'exploitation Android en *open source*) et intègrent les Google Play Services et/ou Google Mobile Services (services d'arrière-plan, d'applications propriétaires et de services d'interfaces de programmation applicatives produits par Google pour les appareils Android) ainsi que leurs propres applications.

*Quels sont les traitements de données personnelles impliqués ?*

L'OS génère des identifiants propres à chaque terminal ou compte utilisateur propre à l'OS, qui, seuls ou combinés à d'autres données, permettent l'identification de l'utilisateur à différentes fins : finalités techniques pour le fonctionnement du terminal, traçage publicitaire, etc. Ils peuvent être utilisés pour le compte propre du fournisseur d'OS ou être transmis à des tiers, notamment les éditeurs d'applications.

C'est également à travers les possibilités logicielles proposées par le fournisseur du système d'exploitation que l'éditeur d'une application peut avoir accès aux différents capteurs du terminal mobile (appareil photo, microphone, localisation du terminal, accéléromètres, etc.) ainsi qu'aux données stockées sur ce dernier (carnet de contacts, galerie photographique, liste des applications installées, etc.).

## Le magasin d'applications

*Quel est le rôle du fournisseur de magasin d'applications ?*

Le fournisseur de magasin d'applications met à disposition la plateforme de distribution en ligne des applications.

Cette plateforme est accessible sur le terminal de l'utilisateur depuis un système d'exploitation compatible (par exemple l'App Store pour un terminal doté du système d'exploitation iOS, ou le Play Store pour un terminal doté du système d'exploitation Android).

*Quel lien entre le magasin d'applications et le système d'exploitation ?*

Le fournisseur du magasin d'applications est fréquemment, mais pas systématiquement, le fournisseur du système d'exploitation. Cependant, un magasin d'applications spécifique peut aussi être proposé par le constructeur du terminal (Samsung, Huawei, etc.). Enfin, concernant notamment le système d'exploitation Android, de nombreux magasins d'applications sont également disponibles, proposés par des tiers non-constructeurs, et peuvent le plus souvent être installés en tant qu'applications standards (F-Droid, Aurora Store, etc.). Le magasin d'applications peut fixer les règles applicables aux applications et conditionnant leur publication dans le magasin, par exemple en termes de mesures de sécurité ou d'information des utilisateurs.

*Quels sont les traitements de données personnelles impliqués ?*

La fixation des règles relatives à la procédure de vérification et de validation des applications n'implique pas en soi de traitements de données personnelles.

En revanche, le magasin d'applications peut être amené à traiter des données pour ses propres finalités, à l'instar des autres applications mobiles. En particulier, les magasins d'application sont généralement liés à un compte utilisateur, permettant au moins d'installer les mises à jour des applications.

## L'éditeur d'applications

*Quel est le rôle de l'éditeur ?*

L'éditeur met l'application à la disposition des utilisateurs (le plus souvent par l'intermédiaire d'un magasin d'applications) pour proposer ses produits ou services. Il en définit également le modèle économique.

*Quels sont les traitements de données personnelles impliqués ?*

L'éditeur traite, dans la majorité des cas, des données personnelles à l'occasion de l'utilisation de son application : données techniques de connexion, données fournies par l'utilisateur ou déjà présentes sur son terminal, données inférées de sa navigation, etc. Il peut ainsi s'agir de données nécessaires à la fourniture d'un bien ou service au travers de cette application (données de contact, de paiement, de localisation, etc.), comme de données liées au fonctionnement de l'application en elle-même (données techniques pour assurer le bon fonctionnement de l'application, vérification de la compatibilité de la version de l'OS, etc.). L'éditeur peut également transmettre les données collectées à des tiers, notamment à des fins de monétisation de son audience, via différents moyens propres à l'écosystème mobile (mise en place de traceurs spécifiques à l'environnement mobile, mise à disposition de l'identifiant mobile de l'utilisateur, etc.).

## Le développeur d'applications

*Qui est le développeur de l'application ?*

L'éditeur de l'application peut procéder au développement de son application en interne ou la faire développer par un développeur externe. Dans le premier cas, éditeur et développeur se confondent. Dans le second cas, éditeur et développeur sont deux entités distinctes liées contractuellement.

Le développeur contribue à définir l'architecture et effectue les choix afférents : choix d'éventuels SDK, modalités d'hébergement, etc.

*Quels sont les traitements de données personnelles impliqués ?*

En participant au développement, le développeur de l'application configure de futurs traitements de données personnelles. En participant à sa maintenance (tests de préproduction, analyse des données [*analytics,* en anglais], remontées d'erreurs, etc.), le développeur peut être impliqué dans l'ensemble des traitements de données personnelles réalisés par l'application et parfois endosser une forme de responsabilité au titre du RGPD.

## Les fournisseurs de SDK

*Quel est le rôle du fournisseur de SDK ?*

Les SDK (« *Software Development Kits* », ou « kits de développement logiciel ») désignent un ensemble d'outils utilisés pour le développement, par exemple d'applications mobiles, en fonction du système d'exploitation utilisé. Cette pratique, extrêmement développée dans l'écosystème mobile, est notamment due au fait que les SDK permettent le plus souvent de faciliter ou d'accélérer le développement de fonctionnalités logicielles, en permettant d'éviter au développeur d'écrire l'intégralité du code de l'application.

*Qu'est-ce qu'un SDK concrètement ?*

Il s'agit d'une brique logicielle tierce implantée dans l'application. Si le SDK peut permettre de réaliser des opérations localement sur le terminal, dans de nombreux cas, les SDK permettent « d'appeler » des fonctionnalités offertes par des services en lignes tiers, le cas échéant en transmettant des informations personnelles issues du terminal (identifiant, adresse IP, configuration, etc.).

Le SDK peut ainsi permettre de mettre en œuvre certaines fonctionnalités dans l'application (p. ex. : paiement, partage sur les réseaux sociaux, etc.).

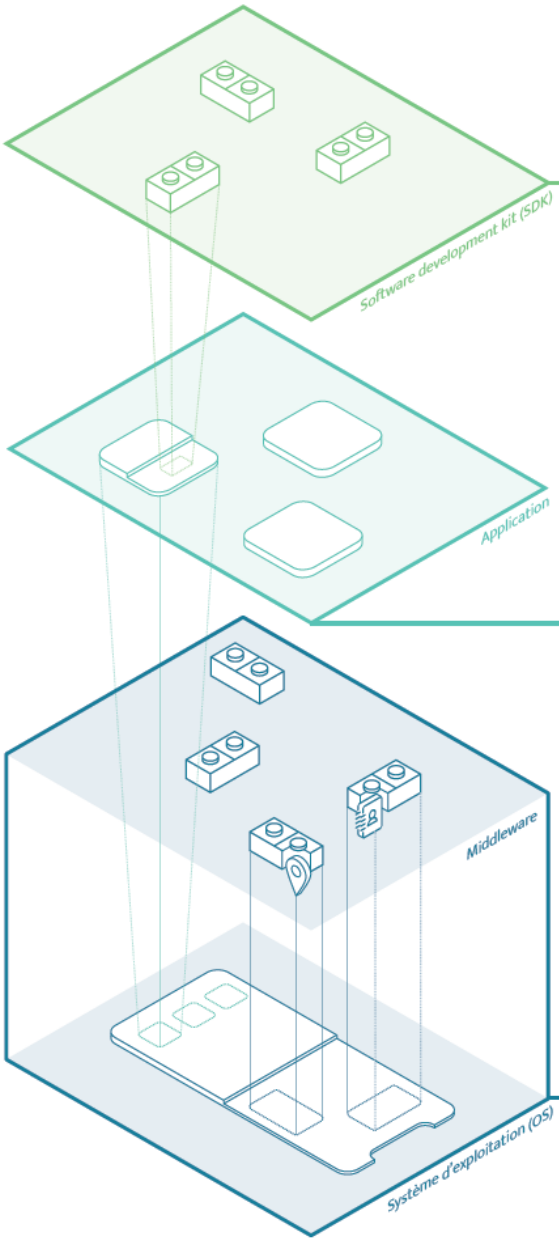
D'autres SDK permettent d'effectuer des demandes d'accès à l'OS, comme par exemple à l'identifiant publicitaire unique associé au terminal ou sa localisation et donc de tracer l'utilisateur de l'application à différentes fins par exemple pour des finalités publicitaires.

*Quels sont les traitements de données personnelles impliqués ?*

Les fournisseurs de SDK conçoivent des briques logicielles susceptibles de configurer de futurs traitements de données personnelles. Ils peuvent par ailleurs être impliqués dans différents traitements de données personnelles à travers ces briques logicielles, dépendant des caractéristiques et des finalités de chaque SDK, et parfois endosser une responsabilité au titre du RGPD.

Il peut s'agir par exemple :

- de traitements consistant à proposer certaines fonctionnalités à travers l'application, par exemple d'analyse ou de traitement d'image (lecture de code QR, réalité augmentée, etc.) ;
- de traitements consistant à tracer les utilisateurs à des fins d'analyse des données (*analytics*) sur la base de données fournies par l'éditeur de l'application, au seul bénéfice de ce dernier ;
- de traitements réalisés par le fournisseur de SDK en tant qu'intermédiaire en publicité, en permettant à l'éditeur de l'application de tracer ses utilisateurs et d'établir des profils au bénéfice de tiers publicitaires ou d'annonceurs, pour monétiser son audience.




## Éditeurs de SDK

Le **fournisseur de SDK** (software development kit) est l'entité qui **met à disposition, un kit de développement logiciel.**

Concrètement, un SDK est un ensemble de fonctions logicielles, de blocs de code, destinés à être intégrés dans des systèmes prédéfinis.

C'est cet aspect qui le distingue du développeur d'application mobile : **un SDK ne peut pas s'exécuter seul, il a besoin d'être intégré dans une application pour fonctionner.** Pour cette raison, un fournisseur de SDK aura de nombreux partenaires : des développeurs et des éditeurs, dont d'applications mobiles.

## Éditeurs d'application et développeurs

Le **développeur d'applications** mobiles est la personne, physique ou morale, qui va concrètement **produire le code d'une application mobile.**

**L'éditeur d'application** mobile est l'entité qui **publie, dans un magasin ou sur sa propre plateforme, une application mobile.**

Il arrive fréquemment qu'il n'y ait pas d'équipe de développement chez l'éditeur. Dans ce cas, l'éditeur fait appel aux services de développeurs, lesquels vont alors produire le code de l'application, pour son compte.

## Fournisseur d'OS

Le fournisseur d'OS (operating system, système d'exploitation en français), est **l'entité qui met à disposition ce système.**

En pratique, plusieurs acteurs peuvent intervenir dans le développement d'un système d'exploitation. Ainsi, un fournisseur d'OS tiers peut faire le choix d'utiliser la base de code d'un autre OS pour ensuite y intégrer des surcouches logicielles dans son propre OS.

Ces intergiciels, ou middlewares, sont les composants logiciels tiers inclus dans la version finale d'un système d'exploitation, tel qu'il sera proposé aux utilisateurs. En pratique, il s'agit le plus souvent d'applications mobiles que le constructeur d'appareil mobile n'aura pas développées lui-même et qu'il aura choisi d'ajouter à son propre système. Ces applications étant préinstallées, il n'est en principe pas possible pour l'utilisateur final de les désinstaller.

Le fournisseur d'OS est, lui, responsable de la version finale du système, tel qu'il sera utilisé par les personnes. En pratique, ce terme désigne le plus souvent le constructeur du terminal mobile.

# 3. L'application est-elle soumise à la réglementation relative à la protection des données personnelles ?

Les recommandations s'appliquent aux opérations mises en œuvre par l'intermédiaire d'une application :

- les opérations de lecture et d'écriture sur le terminal mobile telles que définies par l'article 82 de la loi Informatique et Libertés, en application de la directive 2002/58/CE du 12 juillet 2002 dite « vie privée et communications électroniques » (ci-après « directive ePrivacy »), qu'elles portent ou non sur des données personnelles.
- Les opérations constituant un traitement de données personnelles au sens de l'article 4 du RGPD.

## 3.1. Application de la directive relative à la vie privée et aux communications électroniques dite « ePrivacy »

### Comment savoir si la directive ePrivacy est applicable ?

L'article 5 de la **directive ePrivacy,** transposé à l'article 82 de la loi Informatique et Libertés, est applicable si une opération de lecture ou d'écriture est opérée sur le terminal de l'utilisateur à travers un réseau de communication électronique, à savoir « *toute action tendant à* ***accéder****, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à* ***inscrire*** *des informations dans cet équipement* » (article 82 de la loi Informatique et Libertés).

C'est en particulier le cas, lorsqu'ils sont transmis à travers un réseau, de :

- l'**usage des identifiants spécifiques à l'environnement mobile** (identifiant unique du terminal, adresse MAC, etc.)[5] ou d'autres techniques de traçage telles que le ***fingerprinting***[6] ;
- l'**accès à certaines informations contenues dans le terminal** (galerie photographique, contacts, etc.) ;
- l'**accès à certains capteurs du terminal** (appareil photo, microphone, localisation etc.) ;

**Focus : le rôle des identifiants du mobile**

- Dans l'écosystème des applications mobiles, des identifiants spécifiques à cet environnement permettent, seuls ou combinés avec d'autres informations, de suivre chaque utilisateur de manière unique.
- Ils peuvent être liés au terminal mobile sur lequel est installé le système d'exploitation (dont l'identifiant publicitaire unique)[7], ou au compte de l'utilisateur authentifié au sein de l'environnement

[5] Voir le point 13 des lignes directrices modificatives de la CNIL sur les *cookies* et autres traceurs. L'usage des identifiants du mobile a pu donner lieu à des sanctions aussi bien d'éditeurs d'application (voir déc. n° SAN-2022-026, 29 déc. 2022) que de magasins d'applications (voir déc. n° SAN-2022-025, 29 déc. 2022, cette décision fait l'objet d'un recours devant le Conseil d'Etat à la date de l'adoption de la recommandation).

[6] Traçage via un identifiant calculé à partir des informations techniques du terminal

[7] Par exemple, dans l'environnement Apple, il s'agit de l'identifiant publicitaire attaché à chaque terminal (« *Identifier for Advertisers* » ou « IDFA ») ou l'identifiant commun aux applications d'un même éditeur (« *Identifier for Vendors* » ou « *IDFV* »). Dans l'environnement Google, l'identifiant publicitaire Google (« *Advertising ID* » ou « AAID ») est généré sur les téléphones équipés du système d'exploitation Android. À l'inverse des *cookies*, dont la valeur est fixée indépendamment pour chaque tiers publicitaire, ces identifiants sont générés aléatoirement lors du premier démarrage du téléphone et sont les mêmes pour tous les tiers. Ils facilitent ainsi la mise en relation entre ces tiers des données collectées relatives à un individu. Couplé à un environnement authentifié, ils permettent également de relier ces données à une activité sur d'autres terminaux informatiques de l'utilisateur depuis lesquels celui-ci s'est également authentifié. Ceci peut permettre à des acteurs publicitaires de valoriser les données collectées sur un utilisateur dans le contexte d'une application en lui proposant des publicités ciblées dans d'autres applications. Cela augmente également l'intrusion potentielle de cette technologie dans la vie privée des utilisateurs de mobiles multifonctions.

du système d'exploitation[8], ou encore être associés à une installation de l'application. Ces identifiants permettent dans le premier cas aux acteurs publicitaires et aux éditeurs d'identifier le terminal de manière unique dans chaque application installée sur le système d'exploitation afin d'adapter le contenu éditorial et la personnalisation publicitaire en fonction des caractéristiques et des comportements de l'utilisateur. Dans le deuxième cas, ils permettent au fournisseur du système d'exploitation de suivre les utilisateurs pour son propre compte et ses propres finalités et ne peuvent pas en général être utilisés par des tiers.

- Ces identifiants peuvent ainsi être transmis à des tiers (notamment les éditeurs d'applications, mais également les intermédiaires publicitaires).
- Ces identifiants peuvent être uniques (c'est-à-dire que le même identifiant est fourni à chaque application y ayant accès, ce qui facilite le traçage inter-applications pour les tiers) ou bien spécifiques à chaque éditeur d'application.

### Quelles conséquences ?

Les internautes doivent être **informés** et donner leur **consentement** préalablement à ces opérations de lecture et/ou d'écriture, sauf si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique (voir article 82 de la loi Informatique et Libertés et CNIL, délibérations n° 2020-091 et n° 2020-092 du 17 septembre 2020[9]).

Les traitements de données mis en œuvre à partir des données récupérées via ces opérations (aussi appelés les « traitements subséquents ») doivent, par ailleurs, reposer sur une des bases légales prévues par le RGPD[10].

## 3.2. Application du RGPD

### Champ d'application matériel

Le RGPD s'applique à l'ensemble des traitements de données personnelles mis en œuvre par l'application.

### Champ d'application territorial

Le RGPD s'applique (article 3) :

- Aux traitements de données personnelles mis en œuvre dans le cadre des activités d'acteurs (responsables de traitement ou sous-traitant) établis sur le territoire de l'Union européenne (UE), que le traitement ait lieu ou non dans l'UE. Par exemple, le RGPD s'appliquera aux traitements de données personnelles effectués au sein d'une application éditée par une société ayant son unique établissement dans le territoire de l'Union européenne ;
- Aux traitements de données personnelles de personnes qui se trouvent sur le territoire de l'UE et mis en œuvre par des acteurs (responsable de traitement ou sous-traitant) qui ne sont pas établis dans l'UE, lorsque les activités de traitement sont liées i) à l'offre de biens ou de services à ces personnes dans l'UE ou ii) au suivi du comportement, au sein de l'UE, de ces personnes. Ainsi, le RGPD s'appliquera aux traitements réalisés par une application destinée à des personnes dans l'UE et qui traite les données de ces mêmes personnes, quand bien même les traitements seraient mis en œuvre par des acteurs situés en dehors du territoire de l'Union.

## 3.3. Traitements relevant de l'exemption domestique

### L'exemption domestique : qu'est-ce que c'est ?

Le RGPD ne s'applique pas aux traitements de données personnelles relevant de l'exemption domestique, c'est-à-dire des traitements réalisés par une personne physique dans le cadre d'activités « personnelles » (activités propres à l'activité d'un seul individu et effectuées en principe dans un cadre non professionnel) ou

[8] Par exemple l'UDID dans l'environnement iOS (Apple), pour « *Unique Device IDentifier* », qui permet d'identifier un terminal Apple (iPhone, iPad, etc.).
[9] « *Cookies* et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », cnil.fr
[10] Les bases légales, cnil.fr

« domestique » (activités communes à un nombre limité de personnes, dans un cadre familial ou amical) (article 2.2.c et considérant 18 du RGPD).

**L'exemption domestique dans les textes**

**Article 2.2.c du RGPD :**

« *Le* [RGPD] *ne s'applique pas au traitement de données à caractère personnel effectué* [...] *par une personne physique dans le cadre d'une* ***activité strictement personnelle ou domestique***. »

**Considérant 18 du RGPD :**

« *Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques*. »

## Quelles conséquences ?

Un traitement bénéficiant de l'exemption domestique n'est pas soumis aux dispositions du RGPD.

Les moyens du traitement fournis par les tiers peuvent également ne pas être soumis au RGPD, sous certaines conditions (considérant 18).

## Dans quels cas le RGPD ne s'applique-t-il pas aux moyens du traitement fournis par les tiers dans le cadre d'un traitement relevant de l'exemption domestique ?

**La CNIL recommande d'analyser les deux critères cumulatifs suivants afin de déterminer si les moyens de traitement fournis par un tiers ne sont pas soumis au RGPD** :

- le traitement est initié à la discrétion de la personne (ici l'utilisateur de l'application), opéré sous son contrôle et pour son seul compte, c'est-à-dire décidé et mis en œuvre par cette dernière ;
- le traitement est réalisé dans un environnement cloisonné, c'est-à-dire sans intervention possible d'un acteur tiers sur ces données : le tiers a fourni les moyens du traitement, mais il ne peut plus agir en aval sur les données.

La CNIL considère que, dans ces conditions, l'acteur ne fait que fournir un logiciel au service de l'utilisateur. Le RGPD n'est pas applicable au logiciel fourni.

**Dans les autres cas, le tiers qui traite les données à la demande de la personne est susceptible d'assumer une forme de responsabilité de traitement pour l'application du RGPD**, soit comme responsable de traitement, soit comme sous-traitant.

Il existe des **cas d'usage issus de l'environnement mobile respectant ces conditions cumulatives.**

Ainsi, la CNIL a considéré que le RGPD ne s'appliquait pas, dans certaines conditions, aux moyens du traitement fournis par les éditeurs d'applications dans les cas suivants :

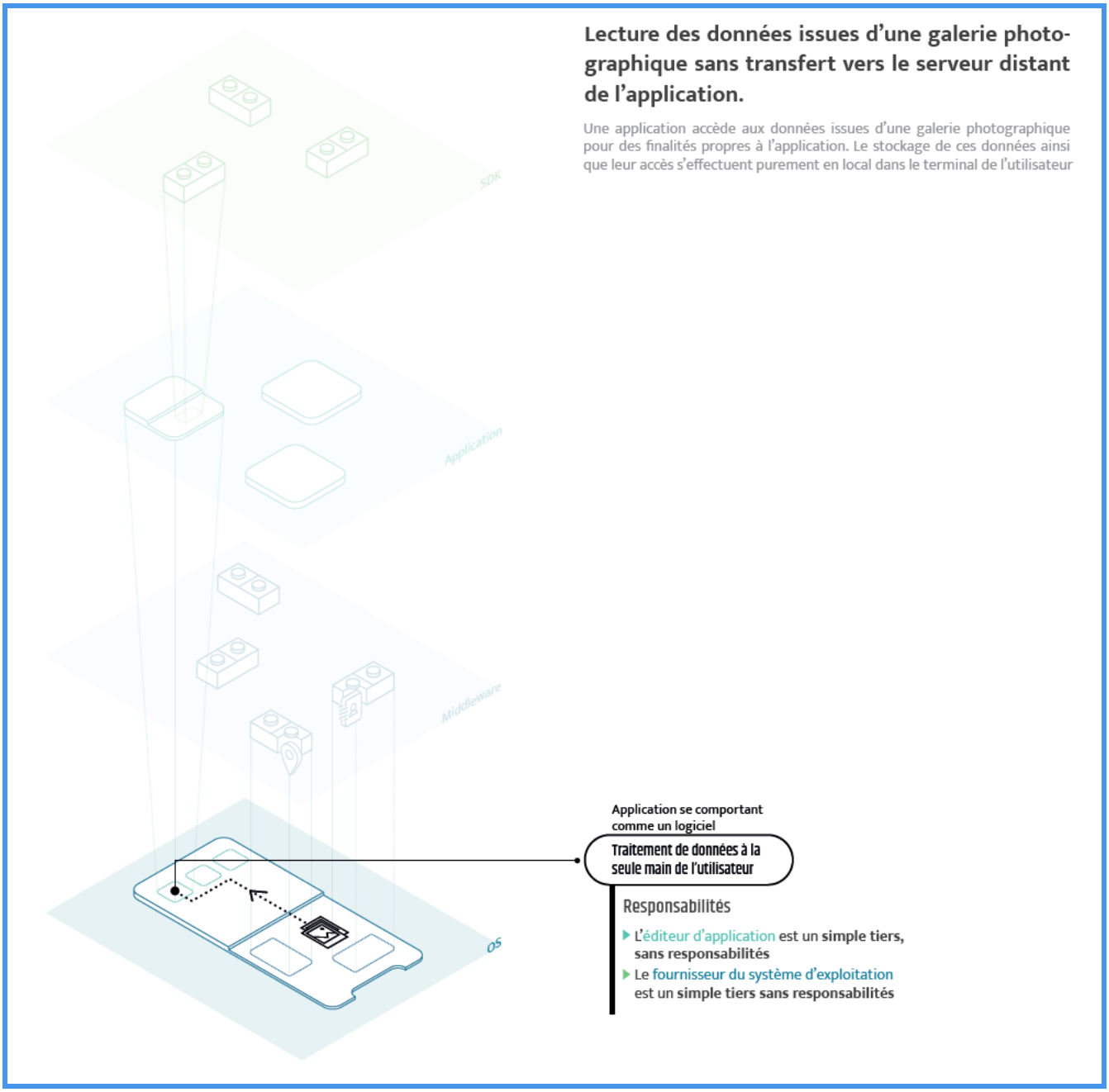
- Authentification biométrique dans les mobiles multifonctions : c'est le cas lorsque le traitement est effectué sur seule décision de l'utilisateur, avec un stockage uniquement local et chiffré de ses données biométriques. En effet, le traitement est bien réalisé à la discrétion de la personne, et les données restent entièrement sous son contrôle ;
- Application mobile en santé : c'est le cas lorsque l'application enregistre et conserve les données de manière uniquement locale, sans connexion extérieure et à des fins exclusivement personnelles, sans que l'application ne propose de fonctionnalités permettant d'assurer un service à distance à son utilisateur. Dans ce cas, les données sont entièrement sous le contrôle de l'utilisateur, sans intervention possible de tiers sur celles-ci. Le traitement est bien réalisé à la discrétion de la personne, qui n'a recours à l'application que dans le cadre d'une utilisation personnelle.

Le même raisonnement peut s'appliquer aux éditeurs d'applications fournissant les moyens du traitement dans les cas suivants :

- Partage des données en mode « pair à pair » (« *peer-to-peer* »), c'est-à-dire sans stockage ni transit via un serveur centralisé ;
- Applications fonctionnant comme un simple logiciel mis à disposition de l'utilisateur et fonctionnant sans échange de données avec un tiers, en dehors de mises à jour ponctuelles (p. ex. : clavier avec configuration évolutive [« apprentissage »] locale sans fédération, fonctionnalités n'impliquant que des données pré-enregistrées statiquement dans l'application).

**Exemple : lecture des données issues d'une galerie photographique sans transfert vers le serveur distant de l'application**

Une application accède aux photographies pour des finalités propres à l'application (par exemple, pour permettre de retoucher la photographie). Le stockage de ces données ainsi que leur accès s'effectuent uniquement au sein du terminal de l'utilisateur, sans qu'aucune information ne soit partagée avec les serveurs de l'éditeur de l'application ni avec ceux du fournisseur du système d'exploitation. Ni l'éditeur ni le fournisseur du système d'exploitation ne peuvent intervenir d'une quelconque manière sur ces données.
Dans cette hypothèse, l'application fonctionne comme un simple logiciel mis à disposition de l'utilisateur. L'éditeur et le fournisseur du système d'exploitation doivent alors être considérés comme de simples tiers, dans la mesure où ils ne déterminent ni les finalités ni les moyens du traitement des données.




**La CNIL considère comme une bonne pratique le fait de proposer des applications mobiles reposant sur des traitements effectués entièrement à l'initiative et sous le contrôle de la personne selon les conditions définies ci-dessus : ces applications et les traitements qui en découlent garantissent la protection des données dès la conception.**

La CNIL encourage les éditeurs et développeurs de ce type d'applications à respecter les bonnes pratiques suivantes :

- veiller à la sécurité de leurs applications, notamment en maintenant à jour les versions de leurs applications et en déréférençant les applications qui ne doivent plus être utilisées en raison de vulnérabilités logicielles ;
- concevoir leurs applications en ligne avec les principes de minimisation et de sécurisation des données du RGPD afin de limiter les risques que courent les utilisateurs en cas de violations de données.

## Quelle qualification de l'éditeur d'application fournissant les moyens du traitement domestique si le RGPD lui est applicable ?

**Le RGPD s'applique aux moyens du traitement fournis par l'éditeur de l'application, lorsque ce dernier ne respecte pas les conditions précisées ci-dessus. Auquel cas, l'éditeur est notamment susceptible d'être qualifié de responsable du traitement s'il définit les finalités et les moyens du traitement.**

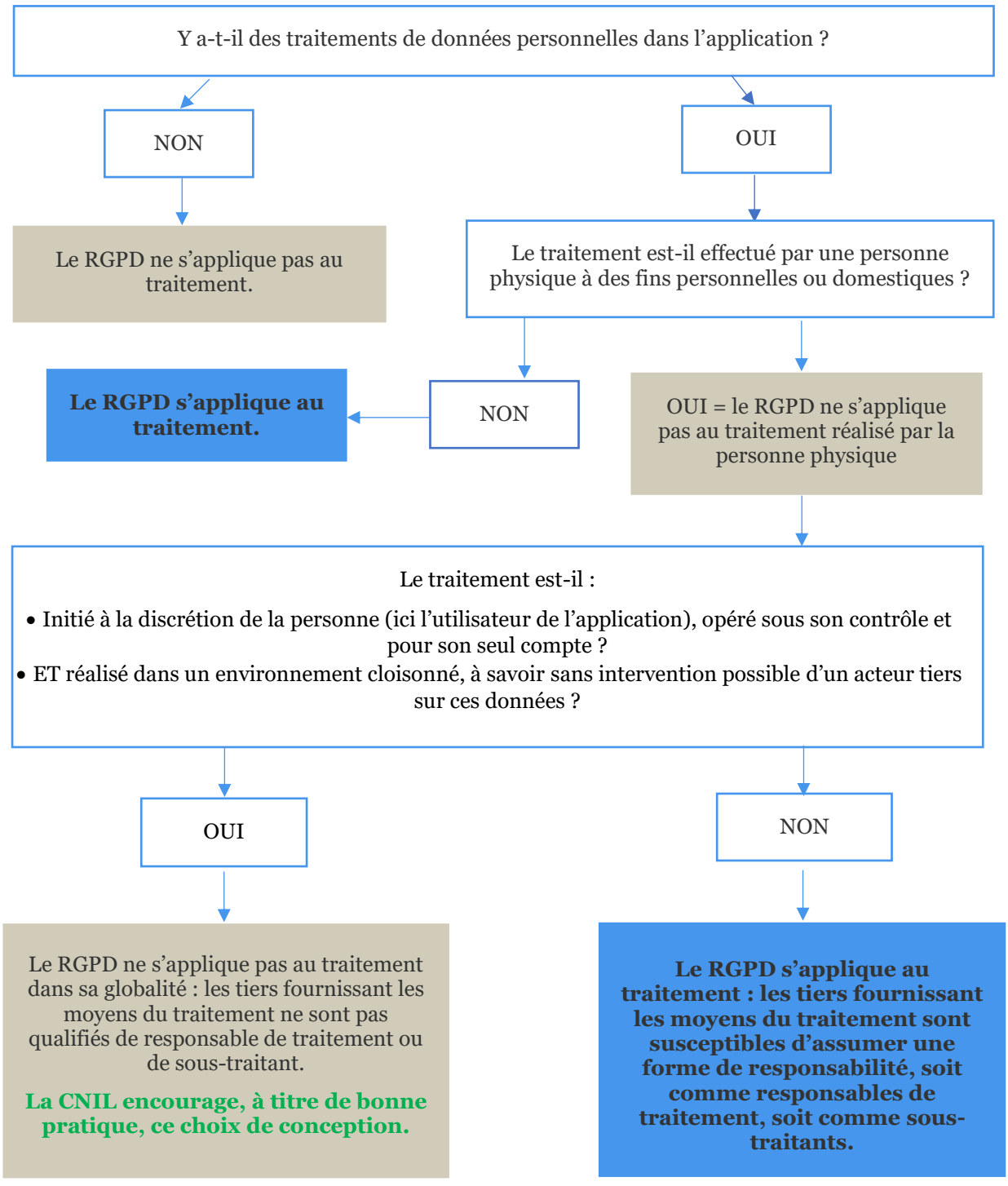
**Exemple : création d'un album partagé de photos de famille au sein d'une application de galerie photographique**

Une famille utilise une application pour créer des albums photos. Les albums sont partagés entre tous les membres de la famille utilisant cette application afin de mutualiser les photos entre les différents utilisateurs.

Dans cette hypothèse, le RGPD ne s'applique pas au traitement relatif à l'album photo car celui-ci est réalisé par une personne physique dans le cadre d'une activité strictement domestique, dans le but de partager des photos de famille avec des membres de sa famille.

En revanche, l'éditeur de l'application est susceptible d'assumer une responsabilité de traitement au sens du RGPD dès lors que l'album est stocké dans ses serveurs ou ceux de tiers. Son rôle au sens du RGPD (responsable de traitement ou sous-traitant) s'analyse au regard des circonstances d'espèce et notamment des finalités poursuivies.

## À retenir : les questions à se poser en tant que développeur, éditeur ou fournisseur de SDK pour déterminer si le RGPD s'applique aux traitements mis en œuvre dans l'application




## Références

- Article 2 du RGPD
- Article 4 du RGPD
- Article 82 de la loi Informatique et Libertés

# 4. Quels sont les rôles de chaque acteur dans le cadre de l'utilisation de l'application ?

## 4.1. Pourquoi est-il important de déterminer le rôle de chacun au sens du RGPD ?

Les acteurs qui interviennent dans l'environnement des applications mobiles n'ont pas tous le même rôle dans le traitement des données personnelles de leurs utilisateurs. Si le RGPD leur est applicable, ils peuvent revêtir l'une des trois catégories suivantes :

- Responsable du traitement[11] ;
- Responsable conjoint du traitement ;
- Sous-traitant[12].

**Responsable du traitement**

*Détermine les finalités et les moyens du traitement*

**Par exemple*, je suis responsable du traitement si :**

Je décide de la création du traitement

Je définis le « pourquoi » et le « comment » du traitement

Je dispose d'un pouvoir décisionnel

...

**Responsables conjoints du traitement**

*Déterminent conjointement les finalités et les moyens d'un même traitement*

**Par exemple*, je suis responsable conjoint du traitement si :**

Je décide de manière commune avec un autre les finalités et les moyens du traitement

Ces décisions sont convergentes, complémentaires et nécessaires

Le traitement n'est pas possible sans la participation des responsables conjoints identifiés du traitement

...

**Sous-traitant**

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

**Par exemple*, je suis sous-traitant si :**

Je fournis le service à la demande du responsable du traitement

Le responsable du traitement mentionne spécifiquement le traitement de données personnelles dans les éléments contractuels

Le traitement de ces données est un élément clé du service que je fournis

Le responsable du traitement contrôle la manière dont je fournis le service

...

[11] Personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (article 4.7 du RGPD).
[12] Personne physique ou morale,' autorité publique, service ou autre organisme qui traite des données personnelles pour le compte du responsable du traitement (article 4.8 du RGPD).

*Il s'agit d'exemples d'indices non exhaustifs allant dans le sens de la qualification.*

D'autres acteurs peuvent être impliqués contractuellement dans la conception, le développement, la distribution et le fonctionnement d'une application mobile, sans revêtir aucune de ces trois qualifications.

Conformément au principe de responsabilité (« *accountability* ») posé par le RGPD, chaque acteur doit déterminer sa qualification au regard de son rôle effectif pour chaque traitement de données personnelles, en suivant les critères définis par le CEPD[13]. Ils doivent être en mesure d'expliquer la qualification retenue, en précisant les raisons ayant conduit au choix de cette qualification, et notamment : qui a décidé de créer le traitement ? qui a défini sa finalité ? qui détermine les données personnelles collectées, leurs durées de conservation, les mesures de sécurité mises en place ?

Les acteurs doivent démontrer qu'une telle réflexion a été menée. Elle doit être formalisée dans l'analyse d'impact relative à la protection des données lorsque celle-ci est effectuée.

## 4.2. Déterminer les qualifications de chaque acteur

**Point d'attention**

La qualification des acteurs doit être réalisée au cas par cas. Les exemples ci-dessous ne préjugent pas des qualifications qui pourraient être retenues en pratique, compte tenu de chaque situation particulière.

Les autorités de contrôle ne sont pas liées par les qualifications choisies par les parties, notamment au sein des contrats ; il leur est possible de retenir une qualification différente en fonction du cas d'espèce.

### Qualifications de l'éditeur

*Dans quels cas l'éditeur de l'application peut-il être responsable de traitement ?*

Dès lors qu'il ne se contente pas de fournir le logiciel au public mais participe à son exploitation (par exemple, des transferts de données entre le terminal de l'utilisateur et ses serveurs), l'éditeur de l'application est responsable des traitements de données personnelles de l'utilisateur effectués dans l'application, car il en a déterminé les finalités et les moyens, c'est-à-dire l'objectif et la façon de les réaliser (nature des données collectées, durée de conservation, exigences de sécurité, etc.).

Il est en particulier **responsable** :

- **des traitements de données personnelles réalisés à l'occasion de l'utilisation de l'application, par exemple :**
  - les données du compte de l'utilisateur (nom, prénom, adresse courriel, numéro de téléphone, etc.) ;
  - les données nécessaires à l'utilisation des services proposés par l'application (adresse de livraison, données bancaires, numéro de carte de réduction, etc.).
- **des opérations de lecture et/ou d'écriture qu'il réalise pour son compte, ainsi que des traitements de données personnelles qui en découlent.** Il s'agit notamment de :
  - la lecture des identifiants mobiles pour diverses finalités, par exemple :
    - lecture de l'identifiant publicitaire unique du mobile afin de permettre le suivi du comportement de l'utilisateur dans l'application par des tiers publicitaires ;
    - lecture par le fournisseur d'un magasin d'applications[14] de l'identifiant du compte de l'utilisateur pour personnaliser les suggestions au sein du magasin d'applications ;
    - lecture par le fournisseur du système d'exploitation[15] de l'identifiant du compte de l'utilisateur pour suivre son activité pour améliorer les fonctionnalités des applications mobiles système qu'il met à disposition.
  - l'accès aux différents capteurs du terminal mobile (appareil photo, localisation, etc.) lorsque les données sont transmises à travers un réseau pour diverses finalités, par exemple :

[13] Lignes directrices 07/2020 du CEPD concernant les notions de responsable du traitement et de sous-traitant (PDF, 1,6 Mo), edpb.europa.eu

[14] Le fournisseur de magasin d'applications est compris ici comme éditeur de l'application mobile que constitue le magasin d'applications.

[15] Le fournisseur du système d'exploitation est compris ici comme éditeur des applications mobiles système qu'il met à disposition.

        - lecture de la localisation de l'utilisateur pour faciliter sa navigation au sein d'une application de calcul d'itinéraire ;
        - utilisation du capteur de l'appareil photo par une application pour scanner un code QR.
    - l'accès aux données stockées sur le terminal mobile (contacts, galerie photo, explorateur de fichiers, etc.) pour répondre à diverses finalités, par exemple :
        - accès aux fichiers stockés par l'utilisateur pour fournir des fonctionnalités de sauvegarde ;
        - accès à la galerie pour charger une photo de profil ;
        - accès à un carnet de contacts pour la découverte de contacts dans le cadre de l'utilisation d'une messagerie instantanée.
- **des opérations de lecture et/ou d'écriture réalisées par des tiers[16] (conjointement avec ces tiers dans l'hypothèse où ils définissent ensemble les finalités et les moyens du traitement)**. Par exemple :
    - lecture de l'identifiant publicitaire unique des utilisateurs par un SDK tiers à des fins de profilage publicitaire pour le compte de l'éditeur : l'éditeur de l'application est responsable du traitement s'agissant de l'opération (éventuellement conjointement avec le fournisseur de SDK) ;
    - lecture d'un identifiant technique par un SDK tiers à travers l'application pour le compte du tiers pour réaliser des statistiques à des fins d'amélioration de son service : l'éditeur est responsable conjoint du traitement.
- **des opérations de lecture et/ou d'écriture effectués par des tiers pour son compte ainsi que des traitements qui en sont issus et qui sont également effectués par ces tiers pour son compte.** Par exemple, l'éditeur de l'application est responsable de l'opération effectuée par le fournisseur de SDK tiers consistant à lire l'identifiant publicitaire unique ainsi que des traitements de profilage publicitaire des utilisateurs réalisés par le fournisseur du SDK pour le compte de l'éditeur sur la base de cette opération.

**En revanche, l'éditeur n'est pas responsable des traitements effectués par les tiers pour leur propre compte sur des données personnelles issues d'opérations de lecture et/ou écriture qu'ils réalisent à travers l'application.** Dès lors que le traitement utilise les données collectées via l'application, cette collecte doit être prévue contractuellement entre l'éditeur et le tiers. Par exemple :

- lecture d'un identifiant technique par le tiers pour réaliser des statistiques à des fins d'amélioration de son service : l'éditeur n'est pas responsable des traitements statistiques effectués par le tiers ;
- lecture de l'identifiant publicitaire unique par le tiers à des fins de croisement de données avec celles issues d'autres applications pour réaliser ses propres finalités publicitaires : l'éditeur n'est pas responsable des traitements de croisement de données effectués par le tiers.

## Qualification du développeur

**L'éditeur peut faire développer son application par un développeur externe**. Se pose alors la question de la qualification du développeur au regard du RGPD.

*Note : lorsque l'éditeur développe son application en interne, éditeur et développeur se confondent et ont les mêmes responsabilités.*

[16] Dans l'environnement web, la responsabilité de traitement de l'éditeur d'un site web a ainsi été retenue s'agissant des opérations de lecture/écriture réalisées par des tiers dans une décision « Éditions Croque Futur », n° 412589 du 6 juin 2018, dans laquelle le Conseil d'État estime que l'éditeur d'un site qui autorise le dépôt et l'utilisation de *cookies* tiers doit être considéré comme responsable de traitement. De même, dans une délibération n° SAN-2021-013 du 27 juillet 2021, la CNIL a considéré que l'éditeur du site avait une certaine responsabilité (une obligation de moyens) s'agissant du recueil du consentement sur les *cookies* tiers.
Ainsi, le fait que les *cookies* proviennent de partenaires n'affranchit pas l'éditeur du site de sa propre responsabilité dans la mesure où il a la maîtrise de son site et de ses serveurs.

*Dans quels cas le développeur de l'application n'endosse aucune forme de responsabilité au titre du RGPD ?*

Si le développeur ne fait que fournir à l'éditeur le code de l'application et n'a ensuite plus aucun rôle dans son fonctionnement, ni aucune maîtrise des données personnelles traitées par l'application, il n'est ni responsable de traitement ni sous-traitant au sens du RGPD.

Le rôle du développeur est cependant essentiel pour que l'application soit conçue d'une façon qui respecte les principes du RGPD. En outre, si la charge de réaliser l'analyse d'impact à la protection des données incombe au responsable de traitement, la sécurité de l'application repose en pratique sur les choix du prestataire de développement. La CNIL considère donc comme de bonnes pratiques, dans cette configuration :

- que le contrat liant le développeur à l'éditeur impose à celui-ci de concevoir une application permettant que les données puissent être traitées conformément au RGPD, dans une logique de protection des données dès la conception (*privacy by design*) ;
- que l'éditeur soit associé aux choix structurants, notamment de sécurité, tout au long de la conception de l'application.

Fournir une application dont le fonctionnement méconnaîtrait, par lui-même, le RGPD engage la responsabilité civile du développeur vis-à-vis de l'éditeur[17].

*Dans quels cas le développeur de l'application peut-il être sous-traitant ?*

Le développeur doit être qualifié de **sous-traitant** s'il traite des données personnelles pour le compte de l'éditeur, responsable du traitement. Cela peut être le cas par exemple lorsque :

- le développeur met en œuvre l'infrastructure de traitement et de stockage des données ;
- le développeur réalise des opérations sur des données hébergées sur le serveur de l'application à des fins de maintenance ou d'infogérance de l'application.

*Dans quels cas le développeur de l'application peut-il être responsable du traitement ?*

Par exception, le développeur doit être qualifié de **responsable du traitement** distinct de l'éditeur s'il traite des données pour son propre compte, pour des finalités qu'il définit.

Cela peut être le cas par exemple lorsque :

- le développeur traite des données personnelles issues de l'application à des fins d'amélioration de la sécurité d'autres applications qu'il développe ;
- le développeur traite des données personnelles issues de l'application pour réaliser des statistiques à des fins d'amélioration de ses services propres ;
- le développeur croise des données issues de différentes applications dans le but de proposer de nouveaux services.

Dès lors qu'il envisage de réutiliser les données qui lui sont confiées en sa qualité de sous-traitant pour des finalités qui lui sont propres, le développeur doit informer l'éditeur de l'application des finalités de cette réutilisation et obtenir son accord préalable. L'éditeur devra déterminer si ce traitement ultérieur est compatible avec la finalité pour laquelle les données ont été initialement collectées (article 6-4 du RGPD).

**Pour aller plus loin**

La CNIL a publié une fiche relative à la réutilisation, par le sous-traitant, des données confiées par le responsable du traitement[18].

## Qualification du fournisseur de SDK

L'éditeur peut recourir à des SDK lors du développement de son application (voir le paragraphe relatif aux fournisseurs de SDK ci-dessus).

Souvent, des échanges de données de données personnelles ont lieu entre ces acteurs, ce qui impose au fournisseur de SDK d'identifier et de documenter sa qualification, au sens du RGPD.

[17] Le contrat liant l'éditeur de l'application et son développeur peut en particulier être frappé de nullité si le non-respect des obligations du cocontractant au titre du RGPD constitue une erreur sur les qualités essentielles de l'objet du contrat (voir en ce sens CA Grenoble, 12 janv. 2023, n° 21/03701, dans le cas de la conception d'un site web).

[18] « Sous-traitants : la réutilisation de données confiées par un responsable de traitement », cnil.fr

*Dans quels cas le fournisseur de SDK peut-il être sous-traitant ?*

**Le fournisseur de SDK doit être qualifié de sous-traitant** lorsqu'il traite des données personnelles pour le compte de l'éditeur responsable du traitement.

C'est notamment le cas lorsque :

- le SDK réalise des opérations de lecture et/ou d'écriture **pour le seul compte de l'éditeur** ;
- le SDK permet l'utilisation d'un service de paiement au sein de l'application ;
- le SDK analyse le comportement d'un utilisateur sur l'application mobile dans le but de le profiler à des fins publicitaires pour le compte de l'éditeur, grâce à la lecture de l'identifiant publicitaire unique du terminal ;
- le SDK analyse la localisation de l'utilisateur dans le but de le profiler pour le compte de l'éditeur.

Lorsque le développeur de l'application – qui traite des données personnelles pour le compte de l'éditeur en tant que sous-traitant – recours à un fournisseur de SDK pour lui confier une partie des opérations de sous-traitance, ce dernier doit être considéré comme un sous-traitant ultérieur. Les sous-traitants ultérieurs doivent apporter le même niveau de garanties que celles offertes par le sous-traitant initial vis-à-vis du responsable du traitement.

*Dans quels cas le fournisseur de SDK peut-il être responsable du traitement ?*

**Le fournisseur de SDK est responsable des traitements de données personnelles effectués dans l'application dont il détermine les finalités et les moyens, c'est-à-dire l'objectif et la façon de les réaliser.**

**Il est en particulier responsable :**

- **des opérations de lecture et/ou d'écriture qu'il réalise (conjointement avec l'éditeur qui permet cette collecte) s'il récupère des données issues de ces opérations pour ses propres finalités.** Il peut s'agir par exemple :
  - de la lecture de l'identifiant publicitaire unique à des fins de profilage publicitaire des utilisateurs et à des fins d'amélioration du service de profilage ;
  - de la lecture d'un identifiant technique du terminal de l'utilisateur à des fins de diagnostic et/ou de télémétrie de l'application et pour réaliser des statistiques à des fins d'amélioration du SDK.
- **des traitements portant sur les données personnelles issues de ces opérations.** Le fournisseur de SDK est tenu de s'assurer de la bonne information de l'éditeur de l'application lors de la mise en œuvre de tels traitements pour son propre compte, notamment dans les éléments de contractualisation avec celui-ci. Il peut s'agir par exemple :
  - des traitements statistiques qu'il effectue sur l'utilisation de son service réalisés grâce au suivi des utilisateurs permis par la lecture de l'identifiant technique de leurs terminaux, à des fins d'amélioration de son service.

## Qualification du fournisseur du système d'exploitation

*Dans quels cas le fournisseur du système d'exploitation peut-il être responsable du traitement ?*

Dans de nombreux cas, le fournisseur du système d'exploitation n'est pas partie prenante des traitements de données personnelles opérés au sein des applications.

**Le fournisseur du système d'exploitation est néanmoins responsable** des traitements, qui sont susceptibles de constituer des traitements de données personnelles, pour certaines finalités de sécurisation ou d'opération de l'OS (p. ex. : recherche de mises à jour de l'OS, télémétrie, amélioration du service, détection de la fraude), dès lors qu'il en détermine les finalités et les moyens.

Ces traitements sont, pour une grande partie, indépendants des applications, mais certains sont en lien avec elles, notamment parce qu'ils leur fournissent des informations et identifiants dont certains sont des données personnelles concernant l'utilisateur.

**Les situations suivantes doivent faire l'objet d'une analyse pour déterminer la qualification du fournisseur du système d'exploitation** :

- l'opération de création en local d'un identifiant mobile ;
- la mise à disposition d'un identifiant mobile à un tiers, notamment un éditeur d'applications ;

- la mise à disposition des autres informations présentes sur le terminal de l'utilisateur à des tiers, notamment les éditeurs d'applications. C'est le cas notamment de la mise à disposition de la localisation, du carnet de contacts ou de la galerie de photos.

**Ces analyses doivent prendre en compte chaque environnement spécifique :**

- dans le cas d'iOS, l'ensemble des autres acteurs (éditeurs, développeurs, SDK) ne peuvent s'adresser qu'à une seule entité, Apple, concernant ces problématiques. De plus, il n'existe pas à ce jour d'autre fournisseur de magasin d'applications que l'App Store sur iOS et iPadOS.
- dans le cas d'Android en revanche, les tiers à l'OS (éditeurs, développeurs, SDK) peuvent s'adresser à différentes entités[19].
- ainsi, ces différentes entités sont susceptibles de partager des responsabilités en fonction des réutilisations de données qui sont faites, en particulier entre Google, qui peut ensuite être amené à **réutiliser des données pour son propre compte, et les constructeurs.**

Même lorsqu'ils se limitent à fournir des outils techniques sans procéder à des traitements eux-mêmes, les fournisseurs d'OS conditionnent dans une certaine mesure, par leurs choix techniques, la manière dont les traitements de données personnelles sont mis en œuvre par les éditeurs d'applications. **Les fournisseurs d'OS sont, à ce titre, visés par certaines bonnes pratiques** (voir la partie 8 des présentes recommandations : « Recommandations spécifiques au fournisseur d'OS »).

*Quel rôle pour le fournisseur d'OS agissant en tant qu'éditeur d'application mobile ?*

**Le fournisseur d'OS qui agit en tant qu'éditeur d'une application** (telles que les applications système préinstallées au sein de l'OS et développées par lui-même)**, se voit appliquer les mêmes qualifications et obligations que pour n'importe quel éditeur d'applications**. Ainsi, lorsque le fournisseur d'OS effectue des traitements de données personnelles pour ses propres finalités au sein des applications qu'il développe et met à disposition au sein de l'OS, il doit être qualifié de responsable du traitement.

*Quel rôle pour le fournisseur d'OS agissant en tant que fournisseur de SDK ?*

**De même, le fournisseur d'OS qui agit en tant que fournisseur d'un SDK se voit appliquer les mêmes qualifications et obligations que n'importe quel fournisseur de SDK**. Ainsi, lorsque le fournisseur d'OS effectue des traitements de données personnelles pour ses propres finalités au sein des applications qu'il développe et met à disposition au sein de l'OS, il doit être qualifié de responsable du traitement (le cas échéant conjointement avec l'éditeur).

## Qualification du fournisseur de magasin d'applications

*Quel rôle pour le fournisseur de magasin d'applications fixant les règles de publication des applications ?*

La fixation des règles relatives à la procédure de vérification et de validation des applications n'implique pas, en soi, de traitements de données personnelles. Les magasins d'applications n'ont donc pas, dans ce cadre, de responsabilité, **au sens du RGPD[20].** Cela n'exclut pas leur responsabilité à un autre titre, notamment si le fonctionnement du magasin le conduit à traiter les adresses IP des utilisateurs.

*Quel rôle pour le fournisseur du magasin d'applications agissant en tant qu'éditeur d'application mobile ?*

**L'éditeur du magasin qui agit en tant qu'éditeur d'application** (le magasin d'applications mobiles étant lui-même une application) **se voit appliquer les mêmes qualifications et obligations que n'importe quel autre éditeur d'applications**.

---

[19] Ainsi, à titre d'exemple, à la date d'adoption des présentes recommandations, un système d'exploitation sous Android sera composé de :

- AOSP (*Android Open Source Project* : mise à disposition par Google de la base de code du système d'exploitation Android en *open source)*, les Google Play Services et GMS (suite logicielle publiée par Google permettant l'accès à d'autres fonctionnalités, dont les services Google (Chrome, Youtube, Gmail, etc.)) pour les terminaux Google ; ou
- AOSP, les Google Play Services, GMS et une suite constructeur (certains constructeurs de mobiles multifonctions développent leurs propres suites d'applications destinées à intégrer le système d'exploitation de leurs terminaux) pour certains terminaux (Samsung, Oppo, Nokia, Blackberry, OnePlus, Motorola, Xiaomi, etc.) ; ou
- AOSP et une suite logicielle constructeur pour d'autres (Huawei, Amazon, Murena, Fairphone, etc.), sans le recours à Google Play Services ni à GMS.

[20] La mise en place par un co-contractant d'obligations contractuelles ayant une influence sur les traitements de données à caractère personnel réalisés par son co-contractant ne suffit pas à déterminer une responsabilité conjointe entre eux. Il convient en effet de déterminer si, par ces obligations contractuelles, le co-contractant influe, à des fins qui lui sont propres, sur les opérations de traitement de données à caractère personnel et détermine, de ce fait, les finalités de ces opérations et les moyens à l'origine de ces opérations (CJUE, aff. C-604/22, 7 mars 2024).

Ainsi, lorsque le fournisseur de magasin d'applications effectue des traitements de données personnelles pour ses propres finalités (p. ex. : traitement des données de développeurs dans le cadre des processus de revue des applications avant publication, traitement d'un éventuel identifiant unique pour ses propres finalités, traitement d'informations spécifiques telles que la liste des applications installées par l'utilisateur et leur état), il est qualifié de responsable du traitement.

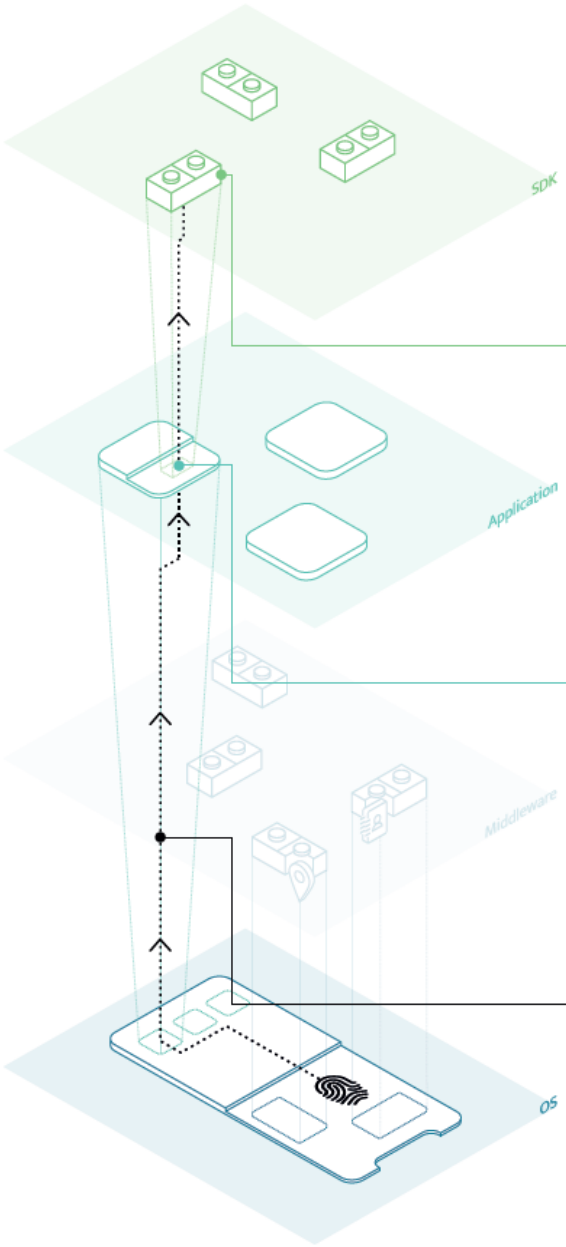
## Exemples

***Lecture et traitement d'un identifiant mobile par un SDK pour le compte de l'éditeur et pour son propre compte***

Un éditeur d'application fait appel aux services d'un fournisseur de SDK pour faciliter le développement de son application. Celui-ci introduit un SDK permettant d'accéder à l'identifiant publicitaire unique du mobile pour suivre le comportement de l'utilisateur. Si l'utilisateur a donné son consentement, le SDK interroge le système d'exploitation pour accéder à l'identifiant publicitaire du mobile. Le SDK mesure grâce au suivi permis par l'identifiant les interactions entre l'utilisateur et l'application et procède à des analyses pour le compte de l'éditeur afin de lui permettre de connaître son audience et ainsi de monétiser les espaces publicitaires présents dans l'application auprès d'annonceurs. Dans ce cas d'espèce, le fournisseur de SDK souhaite par ailleurs, avec l'accord contractuel de l'éditeur, utiliser les données collectées pour poursuivre des finalités qui lui sont propres, à savoir l'amélioration de son service de profilage des utilisateurs pour l'ensemble de ses clients.

**Dans cette hypothèse :**

- l'éditeur et le fournisseur de SDK sont responsables conjoints du traitement s'agissant de l'accès à l'identifiant publicitaire (qui constitue une opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés) par le fournisseur de SDK car ils participent de manière conjointe à la détermination des finalités et des moyens du traitement concernant cette opération ;
- s'agissant des traitements effectués par le fournisseur de SDK, pour le compte de l'éditeur (monétisation des espaces publicitaires dans l'application), sur les données personnelles collectées grâce à l'accès à cet identifiant publicitaire , l'éditeur est responsable du traitement et le fournisseur de SDK son sous-traitant.
- le fournisseur de SDK peut par ailleurs effectuer des traitements sur les données personnelles collectées grâce à l'accès à cet identifiant publicitaire pour des finalités qui lui sont propres, 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 (par exemple via les éléments contractuels). Dans ce cas, le fournisseur de SDK est responsable de son traitement.




## Lecture et traitement d'un identifiant mobile par un SDK pour le compte de l'éditeur et pour son propre compte.

Un éditeur d'application fait appel aux services d'un fournisseur de SDK pour faciliter le développement de son application. Celui-ci introduit un SDK dans l'application ayant pour fonctionnalité d'accéder à l'identifiant publicitaire unique du mobile afin de pouvoir suivre le comportement de l'utilisateur dans l'application.

Finalité SDK

Amélioration du service de profilage des utilisateurs

Responsabilités

- Le fournisseur de SDK est **responsable de traitement**
  Il ne peut effectuer ces traitements que si cela a été convenu contractuellement avec l'éditeur

Finalité éditeur

Monétisation des espaces publicitaires

Responsabilités

- L'éditeur d'application est **responsable de traitement**
- Le fournisseur de SDK est **sous-traitant**

Finalités déterminées conjointement

**Accès à l'identifiant publicitaire**

Responsabilités

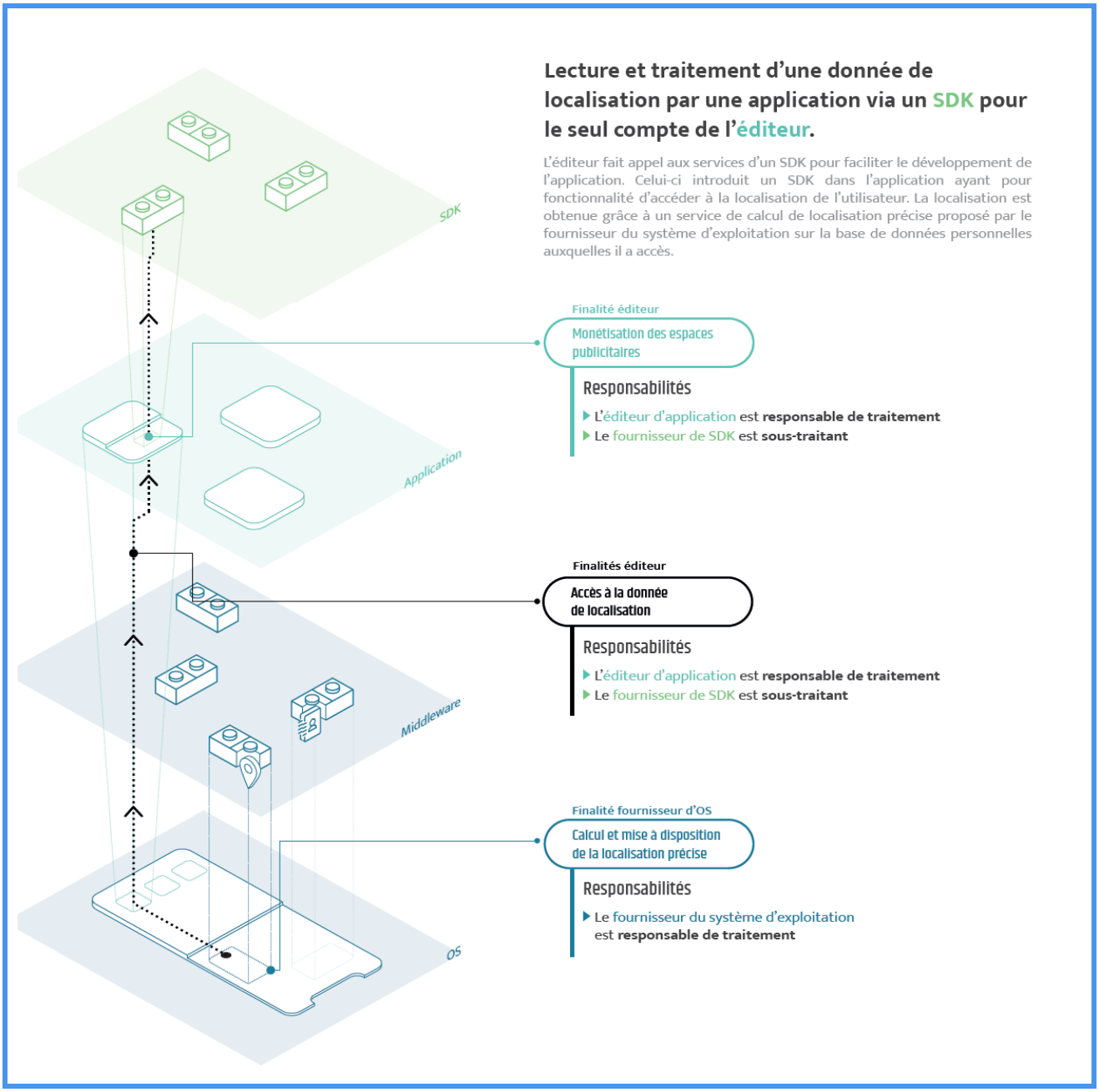
- L'éditeur d'application est **co-responsable de traitement**
- Le fournisseur de SDK est **co-responsable de traitement**

***Lecture et traitement d'une donnée de localisation par une application via un SDK pour le seul compte de l'éditeur***

L'éditeur fait appel aux services d'un fournisseur de SDK pour faciliter le développement de l'application. Ce SDK a pour fonctionnalité d'accéder à la localisation de l'utilisateur. Cette information est obtenue grâce à un service de calcul de localisation précise proposé par le fournisseur du système d'exploitation sur la base de données personnelles auxquelles il a accès (adresse IP, listes des points d'accès Wi-Fi et identifiants Bluetooth autour du terminal). L'accès à la localisation se fait à la fois au bénéfice de l'utilisateur et de l'éditeur. En effet, cela permet à l'utilisateur de bénéficier de certaines fonctionnalités de l'application (ex : aide à la navigation, recherche de points d'intérêts dans les environs). Cela bénéfice également à l'éditeur : ainsi, le fournisseur de SDK utilise cette information relative à la localisation pour procéder à des analyses pour le compte de l'éditeur de l'application afin de permettre à celui-ci de connaître son audience et ainsi de monétiser les espaces publicitaires présents dans l'application auprès d'annonceurs.

**Dans cette hypothèse :**

- l'éditeur est responsable du traitement s'agissant de l'inclusion au sein de l'application d'un SDK ayant pour fonction d'accéder à la donnée de localisation (ce qui constitue une opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés), et le fournisseur de SDK son sous-traitant car le fournisseur de SDK ne poursuit ici aucune finalité propre ;
- s'agissant des traitements effectués par le fournisseur de SDK sur la donnée de localisation qu'il a collectée pour le compte de l'éditeur (connaissance de l'audience et monétisation des espaces), l'éditeur est responsable du traitement et le fournisseur de SDK son sous-traitant car le fournisseur de SDK ne poursuit ici aucune finalité propre ;;
- le fournisseur du système d'exploitation est de son côté responsable des traitements qu'il effectue dans le but de proposer le service de calcul de localisation précise à des tiers, incluant notamment l'éditeur de l'application.

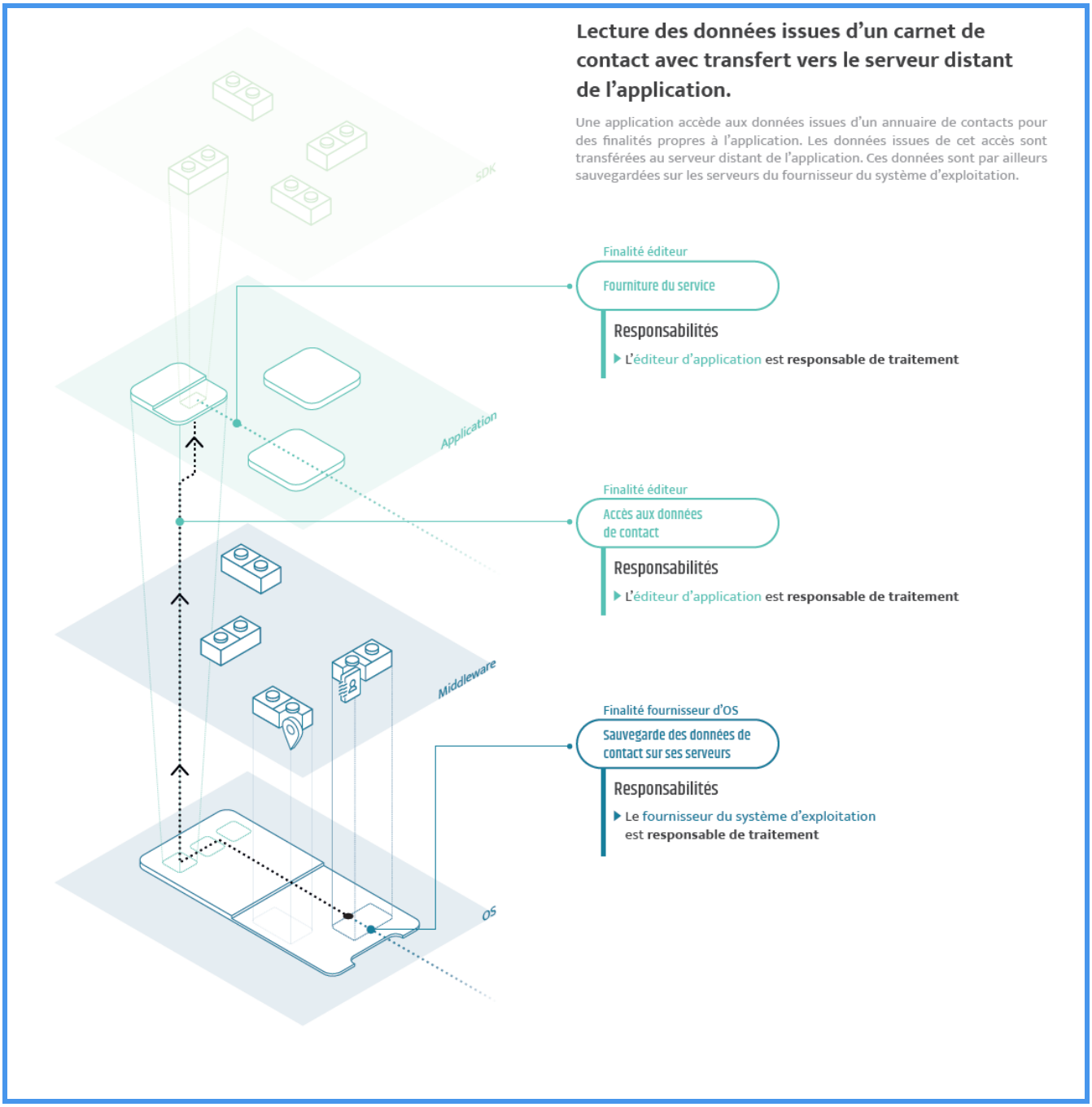



***Lecture des données issues d'un carnet de contacts avec transfert vers le serveur distant de l'application***

Une application accède aux données présentes dans un carnet de contacts, sauvegardées sur les serveurs du fournisseur du système d'exploitation, pour des finalités propres à l'application. Ces données sont ensuite transférées sur le serveur de l'éditeur de l'application.

**Dans cette hypothèse :**

- le fournisseur du système d'exploitation est responsable du traitement des données de l'utilisateur sauvegardées sur ses serveurs ;
- l'éditeur de l'application est responsable du traitement s'agissant de l'accès à ces données (qui constitue une opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés) et du traitement de données consécutif à cet accès car il en détermine les finalités et les moyens.




## Références

- Article 4 du RGPD
- Article 82 de la loi Informatique et Libertés

# 5. Recommandations spécifiques à l'éditeur

**Comment lire cette section ?**

Cette section rappelle les obligations posées par la règlementation (par exemple, « le responsable du traitement doit ») et formulent des recommandations pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer aux obligations, mais ils doivent alors pouvoir justifier leur choix et engagent leur responsabilité. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

## Notice

### À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **éditeurs 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** (le plus souvent au travers d'un magasin d'application) pour proposer ses produits ou services.
- Les obligations, recommandations et bonnes pratiques s'appliquent à l'ensemble des éditeurs, y compris lorsque ceux-ci endossent par ailleurs le rôle de fournisseurs d'OS ou de magasin d'application.
- Ces recommandations s'adressent plus spécialement au sein de l'éditeur :
  - au délégué à la protection des données (DPD ou *Data Protection Officer – DPO*) ;
  - aux membres de l'équipe chargés de l'édition d'applications, plus particulièrement ceux chargés des spécifications de celles-ci (tels que le directeur produit ou « *product owner* »).

### Quel est l'objet de ces recommandations ?

- Ces recommandations ont pour but d'aider les éditeurs à s'assurer du respect de leurs différentes obligations au titre de la réglementation en matière de protection des données et ainsi de la conformité des traitements de données personnelles qu'ils mettent en œuvre, tout au long de la durée de vie de l'application.

### Comment utiliser ces recommandations ?

- Chaque section correspond à une étape dans la mise à disposition d'une application.
- Chaque recommandation thématique expose les enjeux de la conception et du fonctionnement d'une application en termes de protection des données personnelles, rappelle les principales obligations issues du RGPD et de la loi Informatique et Libertés, et regroupe une série de recommandations et de bonnes pratiques à mettre en œuvre.
- Une **liste récapitulative des principales vérifications à réaliser** est proposée à la fin de cette partie. Les éditeurs sont invités à s'y référer, notamment lorsqu'ils documentent leur conformité.

**Voir aussi**

Les éditeurs sont invités à consulter également, dans ce document, les recommandations applicables aux autres acteurs, susceptibles de les concerner, et en particulier les :

- Recommandations spécifiques aux développeurs
- Recommandations spécifiques aux fournisseurs de SDK

## 5.1. Concevoir son application

En tant que responsable du traitement, l'éditeur doit, le cas échéant avec l'aide de ses partenaires, définir clairement les traitements de données personnelles mis en œuvre. Il doit prendre en compte la protection des données personnelles dès la phase de conception des applications.

### 1. Identifier l'existence de traitements de données personnelles

L'éditeur doit identifier si des traitements de données personnelles seront mis en œuvre par l'intermédiaire de son application pour que le RGPD s'applique.

- **S'agit-il bien d'un traitement de données personnelles** ?
  - Une donnée personnelle telle que définie dans le RGPD est toute information se rapportant à une personne physique identifiée ou identifiable. Par exemple : 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.
  - Dans certains cas, des applications peuvent offrir le service recherché sans traiter de données personnelles (p. ex. : applications lampe torche, niveau à bulle virtuel, boussole, calculatrice, chronomètre ou minuteur, métronome, accordeur, certains jeux, etc.)

- **Le traitement peut-il être exempté de l'application du RGPD ?**
  - À certaines conditions (rappelées à la partie 4 des présentes recommandations :« Quels sont les rôles de chaque acteur dans le cadre de l'utilisation de l'application ? »), le traitement relève de l'exemption domestique, sans entraîner de responsabilité de l'éditeur d'application au sens du RGPD.

**Point d'attention**

Il ne faut pas oublier d'inclure dans l'analyse les traitements potentiellement effectués par des tiers.

- Voir la partie 5.2 des présentes recommandations : « Cartographier ses partenaires »

### 2. Assurer la conformité des traitements de données personnelles

L'éditeur doit s'assurer que chacun de ces traitements de données personnelles respecte le RGPD et la loi Informatique et Libertés.

- **La ou les finalités des traitements de données sont-elles correctement définies ?**
- **Une base légale est-elle identifiée pour chaque finalité ?** L'éditeur doit identifier une base légale valable au sens de l'article 6.1 du RGPD pour chacune des finalités. Les traitements effectués dans le contexte des applications mobiles peuvent notamment se fonder sur le consentement, le contrat ou l'intérêt légitime :
  - Lorsque le traitement repose sur le consentement, l'éditeur doit s'assurer que celui-ci est correctement recueilli (voir la partie 5.3 des présentes recommandations : « Gérer le consentement et les droits des personnes ») .
  - Le traitement ne peut reposer sur la base légale du contrat que s'il est objectivement nécessaire au contrat souscrit par la personne concernée. Cela signifie qu'il doit il doit être objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à la personne concernée. Le responsable du traitement doit ainsi être en mesure de démontrer en quoi l'objet principal du contrat ne pourrait être atteint en l'absence du traitement en cause et, partant, qu'il n'existe pas d'autres solutions praticables et moins intrusives.
  - Pour se reposer sur la base légale de l'intérêt légitime, l'éditeur doit formaliser une analyse de la balance des intérêts entre l'utilisateur dont les données sont traitées et le responsable de traitement. Comme rappelé par le groupe de travail « Article 29 », *« [il] serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes comme base légale*

*pour des pratiques intrusives de profilage et de suivi à des fins de marketing ou de publicité* » [21].

- **Le terminal de l'utilisateur fait-il l'objet d'opérations de lecture et/ou d'écriture ?**

  - L'éditeur doit identifier les opérations de lecture et/ou d'écriture sur les terminaux des personnes au sens de l'article 82 de la loi Informatique et Libertés mises en œuvre au sein de ses applications. Cela inclut, par exemple, l'accès aux identifiants mobiles (qu'ils aient une nature publicitaire ou non), les résultats d'opérations d'identification des caractéristiques (« *fingerprinting* »), l'accès à des identifiants uniques, tels que les identifiants matériel (« *hardware* »), l'accès aux capteurs du téléphone ou encore aux données stockées dans le terminal (carnet de contacts, galerie photographique, etc.).
  - Le consentement est nécessaire pour ces opérations sauf si elles ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique ou si elles sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.
  - La CNIL recommande que cette analyse soit réalisée par l'éditeur en lien avec le développeur afin que des instructions précises lui sont fournies. Pour prendre connaissance des recommandations pratiques de la CNIL pour permettre le recueil du consentement dans les applications mobiles, referez-vous au la partie 6.2.3 des présentes recommandations (« Participer à la conformité en matière de recueil du consentement »).

[21] Avis du groupe de travail « Article 29 » sur le profilage et la prise de décision automatisée, WP 251, rév. 01 « *[il] serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes comme base légale pour des pratiques intrusives de profilage et de suivi à des fins de marketing ou de publicité, par exemple celles qui impliquent le suivi d'individus sur plusieurs sites web, emplacements, dispositifs, services ou courtage de données* ».

<table>
<tr><th colspan="4">Des opérations de lecture et/ou écriture sur le terminal de l'utilisateur sont mises en œuvre</th></tr>
<tr><td>Par défaut : Le consentement de la personne est nécessaire<br><br>Exemples :<br>• collecte de l'identifiant publicitaire à des fins publicitaires<br>• collecte des données de contact à des fins de découverte de contact<br>• collecte de la localisation à des fins de recommandation de contenus</td><td colspan="3">Par exemption : le consentement de la personne n'est pas nécessaire</td></tr>
<tr><td rowspan="2">L'opération de lecture et/ou d'écriture a pour finalité exclusive de permettre ou de faciliter la communication par voie électronique<br><br>Exemple :<br>• utilisation d'identifiants à des fins de répartition de charge (load balancing) ou de routage</td><td colspan="3">L'opération est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur</td></tr>
<tr><td>Fonctionnalité demandée expressément par l'utilisateur<br><br>Exemples :<br>• accès au GPS pour fournir une fonctionnalité de localisation demandée<br>• utilisation d'identifiants d'authentification (voir le cas d'usage 3.2 des lignes directrices à ce sujet[22])</td><td>Usage de sécurisation du service, centré sur la protection de l'utilisateur (voir le cas d'usage 3.3 des lignes directrices à ce sujet[23])<br><br>Exemples :<br>• utilisation de traceurs pour prévenir d'attaques en déni de service<br>• utilisation de traceurs pour prévenir de bourrages d'identifiants (credential stuffing)</td><td>Mesure d'audience limitée<br><br>Exemple : simple comptage du nombre d'utilisateurs journaliers à des fins de dimensionnement du service</td></tr>
</table>

- **Les données personnelles traitées sont-elles limitées à ce qui est nécessaire pour les finalités poursuivies (article 5.1.c du RGPD) ?**

L'éditeur doit s'assurer que les données collectées pour chaque finalité sont limitées à ce qui est nécessaire pour la finalité recherchée (p. ex. : il est exclu de collecter la date de naissance complète si le traitement n'a besoin que de l'année).

Pour un certain nombre de données à caractère personnel, l'éditeur doit en particulier choisir entre le traitement de données techniques remontées par l'application ou de données fournies manuellement par l'utilisateur.

[22] Avis 04/2012 du groupe de travail « Article 29 » sur l'exemption de l'obligation de consentement pour certains cookies, p. 7.
[23] Avis 04/2012 du groupe de travail « Article 29 » sur l'exemption de l'obligation de consentement pour certains cookies, p. 7.

Ainsi, une application de météorologie peut utiliser une donnée de localisation remplie manuellement par l'utilisateur ou une donnée de localisation remontée par le terminal.

La CNIL recommande, chaque fois que cela est possible, de privilégier des données fournies manuellement par l'utilisateur, qui a ainsi la maîtrise de la donnée fournie et de sa précision. Il est important que tous les acteurs recevant cette donnée pour traitement (notamment d'éventuels destinataires tiers de cette donnée) aient alors conscience de ce qu'il s'agit d'une donnée remplie manuellement par l'utilisateur (cette donnée a alors le même statut qu'une donnée remplie sur un formulaire d'un site web).

Il est également recommandé, lorsque cela est pertinent, de donner à l'utilisateur le choix entre fournir manuellement la donnée pertinente ou permettre la transmission automatique d'une donnée contenue dans son terminal.

- **La conservation des données est-elle limitée dans le temps (article 5.1.e du RGPD) ?**

Les données traitées doivent être conservées pour une durée strictement nécessaire à l'objectif poursuivi par le traitement.

- **Des données sensibles (données politiques, religieuses, de santé etc.) sont-elles traitées (article 9 du RGPD) ?**
  - Ces traitements de données sensibles sont interdits sauf s'ils reposent sur l'une des exceptions prévues à l'article 9.2 du RGPD, telle que le consentement libre, spécifique, éclairé et univoque de la personne concernée.
  - De plus, toute catégorisation ou création de segments sur la base de telles données à des fins de profilage publicitaire est interdite (article 26 du Règlement n° 2022/2065 sur les services numériques, dit « *Digital Services Act* » ou DSA).
  - Si ces traitements sont fondés sur le consentement, celui-ci doit être donné préalablement au traitement de données et de manière libre, spécifique et éclairée. Ainsi, l'utilisateur doit pouvoir décider librement et sans contrainte de la mise en œuvre du traitement. Ce choix doit s'exprimer de manière spécifique. La CNIL recommande à cette fin d'afficher un avertissement ou une information spécifique avant le recueil du consentement ou d'ajouter une case pour recueillir un consentement distinct[24].

- **Comment protéger les données des mineurs ?**
  - Ces recommandations ne traitent pas spécifiquement des mesures à mettre en œuvre à ce titre ; se référer aux travaux publiés par la CNIL sur le sujet[25].
  - Les mineurs bénéficient de protections particulières au titre de la réglementation, il faut mettre en œuvre des mesures additionnelles pour protéger leurs données personnelles et respecter leur vie privée.
  - De manière additionnelle, la diffusion de publicité basée sur du profilage utilisant des données personnelles est interdite lorsque le destinataire du service est un mineur (article 28 du règlement sur les services numériques, dit « *Digital Services Act* » ou DSA).

## 3. Appliquer les principes de protection des données dès la conception et par défaut (article 25 du RGPD)

L'éditeur doit mettre en œuvre des mesures techniques et organisationnelles permettant de protéger les données personnelles dès la conception et par défaut (principes dits de « *data protection by design* and *by default* »).

- **Les paramètres par défaut de l'application sont-ils les moins intrusifs possibles ?**
  - Il est recommandé que l'éditeur détermine, pour chacun des traitements, les paramètres minimaux permettant de fournir le service demandé (p. ex. : il ne devrait pas collecter par

[24] Paragraphe 56 de la Délibération n° SAN-2023-006 du 11 mai 2023 : « *Lorsque le service demandé par l'utilisateur implique nécessairement le traitement de données de santé, il est cependant nécessaire que l'utilisateur ait pleinement conscience de ce que ses données de santé seront traitées et parfois conservés par le responsable de traitement, ce qui implique en principe une information explicite sur ce point lors du recueil du consentement* ».
[25] « Les droits numériques des mineurs », cnil.fr

défaut les données de localisation de la personne si celles-ci ne servent qu'à faciliter l'usage d'un outil de recherche qui peut être fonctionnel sans elles).
    - Pour ce faire, l'éditeur devrait analyser ces paramètres au regard de chacune des catégories d'usagers (p. ex. : l'adresse électronique des personnes ne devrait pas être systématiquement collectée si celle-ci n'est utile que pour les utilisateurs payants dans le cadre de la facturation).
    - Si l'éditeur fournit de nombreux services, il est recommandé de permettre à l'utilisateur d'utiliser indépendamment chacun des services proposés.

- **La conception du système permet-elle de protéger la vie privée des utilisateurs ?**
    - L'éditeur doit analyser si des technologies améliorant la confidentialité (*Privacy Enhancing Technologies*) peuvent s'appliquer aux traitements mis en œuvre.
    - Pour une revue de certaines de ces techniques et des exemples d'usage, l'éditeur peut se référer aux guides produits par l'OCDE[26] et par l'autorité britannique de protection des données (ICO)[27].

- **Cette conception permet-elle de minimiser les risques pour les utilisateurs ?**
    - L'éditeur doit minimiser les données transmises à ses partenaires.
    - Il est recommandé de ne pas transmettre de données identifiantes (nom, alias, numéro d'identifiant unique, etc.) si celles-ci ne sont pas nécessaires pour les finalités poursuivies.
    - Il est recommandé que l'éditeur utilise des mécanismes de chiffrement de bout en bout afin de renforcer la sécurité des données.

### 4. Documenter son analyse (articles 5.2 et 24 du RGPD)

Le principe de responsabilité des acteurs oblige les éditeurs à adopter des outils et procédures pour assurer la conformité de leurs traitements de manière continue. Ils doivent, en particulier :

- **Tenir et garder à jour un registre des traitements (qui est une obligation si l'éditeur n'en est pas exempté au titre de l'article 30.5 du RGPD, et une recommandation sinon).**
- **Justifier et documenter les durées de conservation définies** en fonction des finalités poursuivies.
- **Mener une analyse d'impact relative à la protection des données (AIPD)** lorsque le traitement est susceptible d'entraîner des risques importants pour les personnes concernées.
- **Nommer un délégué à la protection des données lorsque c'est obligatoire (dans certains cas précisés sur le site internet de la CNIL).** Dans les autres cas, la CNIL le recommande.

## 5.2. Cartographier ses partenaires

Il est fréquent que tout ou partie des traitements de données mis en œuvre impliquent des tiers. L'éditeur doit donc, en qualité de responsable du traitement, avoir une vision complète des acteurs intervenant dans le traitement de données et des mesures mises en œuvre par ses partenaires pour répondre à ses obligations au titre de l'article 24.1 du RGPD.

### 1. Encadrer les relations avec les développeurs

L'éditeur doit encadrer les relations avec les partenaires techniques auxquels il a recours pour le développement de l'application.

- **La qualification du développeur est-elle claire pour les deux parties ?**
    - L'éditeur doit identifier précisément et en amont les traitements de données personnelles qui seront mis en œuvre par le développeur pour son compte dans le cadre du développement et du fonctionnement de l'application. Le développeur agit alors en qualité de sous-traitant de l'éditeur (voir la partie 4 des présentes recommandations).
    - Il doit encadrer la prestation de sous-traitance, par exemple via un contrat (*data processing agreement – DPA* – en anglais) cette qualification et les obligations qui y sont liées.

---

[26] *« Emerging privacy-enhancing technologies »* (en anglais), oecd-library.org
[27] Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 ko), sept. 2022, ico.org.uk

- Attention : si le développeur met en œuvre des traitements pour son propre compte, il pourra être qualifié de responsable de traitement pour ceux-ci (voir la partie 4 des présentes recommandations, en particulier : « Qualification du développeur »). Toutefois, en sa qualité de commanditaire de l'application, l'éditeur doit être informé de ces traitements et les avoir acceptés, par exemple via les éléments contractuels.
- L'éditeur reste potentiellement responsable de traitement même s'il ne va pas jusqu'au bout du développement de l'application. C'est le cas s'il charge une entreprise de développer une application et participe à la détermination des finalités et des moyens du traitement, même s'il ne procède pas lui-même aux opérations de traitement, ne donne pas explicitement son accord pour la réalisation des opérations concrètes d'un tel traitement ou pour la mise à disposition du public de l'application et qu'il n'acquiert pas cette même application. Ainsi, si le processus de développement est interrompu en cours de route, il est nécessaire que l'éditeur s'oppose explicitement à la mise à disposition du public et au traitement de données à caractère personnel qui en résulterait. Dans le cas contraire, il serait considéré comme responsable de traitement[28].

- **Le développeur dispose-t-il des éléments nécessaires au respect de ses obligations ?**
  - L'éditeur doit fournir des instructions claires concernant les traitements à mettre en œuvre, par exemple via le contrat de sous-traitance (article 28.3.a du RGPD).
  - Il est recommandé que l'éditeur :
    - mette en place un point de contact clair concernant les problématiques de protection des données (par exemple le délégué à la protection des données) ;
    - donne des instructions claires et documentées en termes de mesure de sécurité et de processus de conformité (voir la partie 6.4 des présentes recommandations, en particulier : « Assurer la sécurité de l'application ») ;
    - prévoie dans le contrat un test d'acceptation (« recette ») concernant le respect de ces points.

### 2. Identifier les éventuelles relations avec d'autres tiers

Si le développeur est le principal interlocuteur de l'éditeur dans la réalisation d'une application, il est fréquent que celle-ci implique d'autres tiers dans les traitements mis en œuvre.

- **Si l'éditeur doit pouvoir assurer la conformité de l'ensemble des traitements mis en œuvre par ses sous-traitants,** ceci peut être complexe dans le contexte des applications mobiles, notamment s'agissant des traitements liés aux SDK tiers, aux appels aux API des OS, aux analyses relatives à la performance, à l'usage de la batterie ou à la télémétrie effectuées par les OS.
- **La CNIL recommande de se référer à la partie 4 des présentes recommandations pour identifier l'ensemble des traitements mis en œuvre par des tiers dans le cadre de la conception et du fonctionnement de l'application.**
- L'éditeur peut, en tant que responsable de traitement, exiger de l'ensemble de ses sous-traitant, y compris le cas échéant le développeur, la garantie que les seuls traitements mis en œuvre sont ceux qui découlent de ses instructions documentées, au titre de l'article 28.3.1 du RGPD.
- **La CNIL recommande à l'éditeur de demander à son développeur de mettre en œuvre les mécanismes de sélection des SDK décrits dans la partie 6.3.1 des présentes recommandations (« Sélectionner le SDK selon les bons critères »)**, dès lors qu'en tant que responsable de traitement, l'éditeur assumera à minima une co-responsabilité pour l'usage de traceurs par un SDK inclus dans son application.

## 5.3. Gérer le consentement et les droits des personnes

Pour les traitements qui relèvent de sa responsabilité, 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.

[28] CJUE, aff. C-683/21, 5 déc. 2023

## 1. Informer correctement les utilisateurs (articles 12 à 14 du RGPD)

Pour assurer la transparence, et indépendamment du caractère direct ou indirecte de la collecte de données, l'éditeur doit correctement informer les utilisateurs, par exemple dans une « politique de confidentialité ».

- **Quelles informations fournir aux utilisateurs de l'application dont les données sont traitées ?**
  - Cette information doit inclure :
    - les éléments obligatoires au titre des articles 13 ou 14 du RGPD[29] ;
    - le caractère obligatoire ou facultatif de chaque traitement (et le cas échéant en quoi le refus impacte l'usage de l'application).
  - La CNIL recommande, en outre, d'inclure la liste des permissions d'accès aux données demandées, leur nature obligatoire ou facultative et les finalités poursuivies via ces permissions.
  - La transmission de données personnelles des utilisateurs à des partenaires commerciaux, par exemple à des fins de monétisation de l'application, doit être explicitement portée à la connaissance des personnes. Si les traitements en question nécessitent le consentement, les informations données doivent être de nature à permettre aux personnes concernées d'apprécier les conséquences de leur choix en les informant de l'étendue de celle-ci. La CNIL recommande de mettre en évidence, auprès des personnes concernées, le nombre et le secteur d'activité des partenaires qui seraient rendus destinataires des données.

- **Comment mettre l'information à disposition des utilisateurs ?**
  - 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.
  - **La CNIL recommande également de la mettre à disposition avant tout téléchargement de l'application, par exemple sur son site ou,** lorsque cela est possible, d'utiliser la page dédiée à l'application dans le magasin d'applications pour :
    - fournir la politique de confidentialité de l'application ;
    - indiquer les éléments principaux, notamment l'identité de l'éditeur, les finalités des traitements et les modalités d'exercice des droits.
  - A titre de bonne pratique, la CNIL encourage à présenter les permissions de manière scindée en deux catégories, selon qu'elles ne servent uniquement le service rendu par l'application à l'utilisateur ou poursuivent aussi d'autres finalités.
  - L'éditeur doit s'assurer que la politique de confidentialité est concise, compréhensible par son public en utilisant un langage simple.
  - L'information peut être réalisée en plusieurs niveaux et accompagnée d'éléments visuels.
  - L'utilisation d'une seule politique de confidentialité n'est pas le seul moyen de répondre à cette obligation d'information, et peut souvent, dans le contexte des applications mobiles, ne pas atteindre les objectifs en termes de simplicité et de concision : la CNIL recommande de contextualiser l'information donnée lors de chaque collecte spécifique et d'utiliser dans ce cas des méthodologies de présentation simplifiées[30].
  - L'éditeur peut envisager, à titre de bonne pratique, d'inclure une information spécifique dans les interfaces des applications sur l'accès ou le partage de certaines données particulièrement intrusives (localisation, carnet de contacts, microphone, etc.), par exemple via l'affichage d'indicateurs persistants quand ces fonctionnalités sont activées.

## 2. Obtenir un consentement valide des utilisateurs (article 4 et 7 du RGPD)

Le consentement peut être nécessaire pour certaines opérations de lecture et/ou d'écriture (article 82 de la loi Informatique et Libertés) ou parce qu'il constitue la base juridique la plus appropriée pour le traitement de données (article 6.1.a du RGPD).

- **Comment recueillir un consentement dans le contexte des applications mobiles ?**

[29] « Fiche n°12 : Informer les personnes », guide de l'équipe de développement, lincnil.github.io
[30] « [Synthétiser] Résumé », design.cnil.fr

- Les lignes directrices et la recommandation sur les *cookies* et autres traceurs[31] de la CNIL demeurent applicables aux opérations de lecture et/ou d'écriture dans le contexte des applications mobiles.
- La CNIL recommande à l'éditeur de tenir compte des spécificités de l'interface du mobile, notamment les limitations en termes d'espace disponible.

**Point d'attention**

- L'éditeur étant responsable pour le recueil du consentement, il lui est recommandé de clairement expliciter ses attentes à son développeur et de mettre en œuvre des mesures pour s'assurer du respect de ses instructions. Pour prendre connaissance des recommandations pratiques de la CNIL pour permettre le recueil du consentement dans les applications mobiles, référez-vous à la partie 6.2.3 des présentes recommandations (« *Participer à la conformité en matière de recueil du consentement* »).

## 3. Faciliter l'exercice des droits (articles 15 à 22 du RGPD)

L'éditeur, responsable du traitement, doit faciliter l'exercice, par les utilisateurs, de leurs droits et en assurer le respect.

- **À quels droits l'éditeur doit-il donner suite ?**
  - Dans le cas général, les droits des personnes sont le droit d'accès, le droit à l'effacement, le droit d'opposition, le droit à la portabilité, le droit à la rectification et le droit à la limitation du traitement[32].
  - En fonction de la base légale retenue, certains de ces droits ne sont pas applicables[33].
- **Quels moyens mettre à la disposition des utilisateurs et comment y donner suite ?**
  - Les textes n'imposent pas de modalités spécifiques pour permettre aux personnes d'exercer leurs droits.
  - La CNIL recommande de mettre à disposition des utilisateurs un centre de gestion des droits au sein de l'application où l'ensemble des droits peuvent être exercés. L'éditeur peut demander à son développeur de le conseiller dans cette démarche.
  - L'éditeur responsable de traitement doit s'assurer que les réponses fournies aux demandes d'exercices des droits sont complètes, y compris concernant les traitements effectués par les sous-traitants. Les sous-traitants doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour aider l'éditeur à répondre aux demandes d'exercice des droits.
  - A titre de bonne pratique, il peut s'assurer qu'une réponse automatique soit apportée aux utilisateurs (par exemple via des API de réponse aux demandes d'expressions des droits).

[31] « Sites web, *cookies* et autres traceurs », cnil.fr
[32] « Fiche n° 13 : Préparer l'exercice des droits des personnes », guide de l'équipe de développement, lincnil.fr.github.io
[33] « Fiche n° 15 : Prendre en compte les bases légales dans l'implémentation technique. Les exercices des droits et les modalités d'information à prévoir suivant la base légale », guide de l'équipe de développement, lincnil.fr.github.io

## 5.4. Maintenir la conformité durant le cycle de vie de l'application

L'éditeur, en tant que responsable du traitement, doit mettre en place un ensemble de processus pour assurer cette conformité tout au long du cycle de vie de l'application.

### 1. Assurer le maintien de la sécurité au cours du temps (article 32 à 34 du RGPD)

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 (article 28.3.c du RGPD).

L'éditeur doit prévoir que les sous-traitants effectuent la transmission des alertes de sécurité pouvant les mener à formaliser une notification de violation de données (article 33 du RGPD) dans le respect du délai légal de première notification (72h) à l'autorité de protection des données (en France, la CNIL).

Par ailleurs, la CNIL recommande :

- de formaliser les mesures techniques attendues en termes de sécurité des données avec le développeur (article 32 du RGPD), en précisant que ces exigences sont applicables aux sous-traitants ultérieurs. L'éditeur peut, par exemple, demander le respect des recommandations formalisées par la CNIL dans la partie 6 des présentes recommandations (« Recommandations spécifiques au développeur ») ;
- de s'assurer que le contrat avec le développeur prévoie la mise à jour de l'application en cas de vulnérabilité d'un tiers ou dans le code ;
- de découpler les mises à jour de sécurité importantes (par exemple la correction de vulnérabilités critiques), pour les mettre à disposition des utilisateurs dans les meilleurs délais, des mises à jour fonctionnelles classiques (ajout de nouvelles fonctionnalités).

### 2. Auditer le respect des engagements des partenaires

L'éditeur doit mettre en œuvre des moyens suffisants et adaptés pour contrôler le respect de ses instructions par son sous-traitant (article 28.1 du RGPD).

- **Comment mettre en œuvre des audits ?**
  - L'éditeur doit prévoir, dans le contrat de sous-traitance, que le développeur permet la réalisation d'audits.
  - En raison de la complexité de certaines briques applicatives, les mesures techniques mises en œuvre ne suffisent pas à elles-seules à assurer le respect des obligations et doivent être complétées par des mesures organisationnelles (voir la partie 5.2 des présentes recommandations : « Cartographier ses partenaires »).
- A titre de bonnes pratiques :
  - L'éditeur peut utiliser le *OWASP Mobile Application Security Testing Guide* (MASTG)[34] proposée par l'ONG Open Web Application Security Project comme base pour analyser la sécurité de son application.
  - L'éditeur peut utiliser un outil d'analyse statique. Ces outils permettent de vérifier que les SDK inclus et les permissions demandées correspondent à ses instructions. En cas de doute, l'éditeur peut demander à son développeur de justifier les éléments observés (SDK inclus, permissions demandées, etc.). Certains outils proposent des analyses plus poussées, en incluant notamment des problématiques de sécurité.
  - L'éditeur peut mettre en place (ou engager un prestataire tiers à cette fin) un banc de tests pour vérifier le bon fonctionnement des outils de recueil de consentement mis en œuvre. À cette fin il peut :
    - équiper un téléphone de test ou un émulateur pour l'interception des communications réseaux ;
    - tester son application, et s'assurer qu'aucune requête symptomatique de l'usage de traceurs n'est émise avant qu'un consentement soit effectivement obtenu.

[34] « OWASP MASTG » (en anglais), mas.owasp.org

### 3. Mettre en place des processus robustes en termes de conformité

Des décisions pouvant impacter la conformité d'une application peuvent être prises après le développement initial de celle-ci. Afin d'assurer le maintien de la conformité, la CNIL recommande de concevoir en amont puis de mettre en œuvre des processus appropriés (sur une base régulière ou lorsqu'un développement significatif est entrepris).

- **Est-ce que le contrôle des éventuelles évolutions des traitements de données est bien réalisé ?**
  - L'éditeur doit actualiser le registre des traitements afin de prendre en compte les évolutions des traitements de données mis en œuvre, ainsi que l'AIPD et la politique de confidentialité des données.
  - La CNIL recommande que l'éditeur mette en place un processus de validation afin d'approuver tout évolution des conditions de mise en œuvre du traitement (choix d'un sous-traitant ultérieur, SDK, fonctionnalités, modalités de recueil du consentement) y compris lorsque celle-ci intervient dans le cadre d'une opération de maintenance.

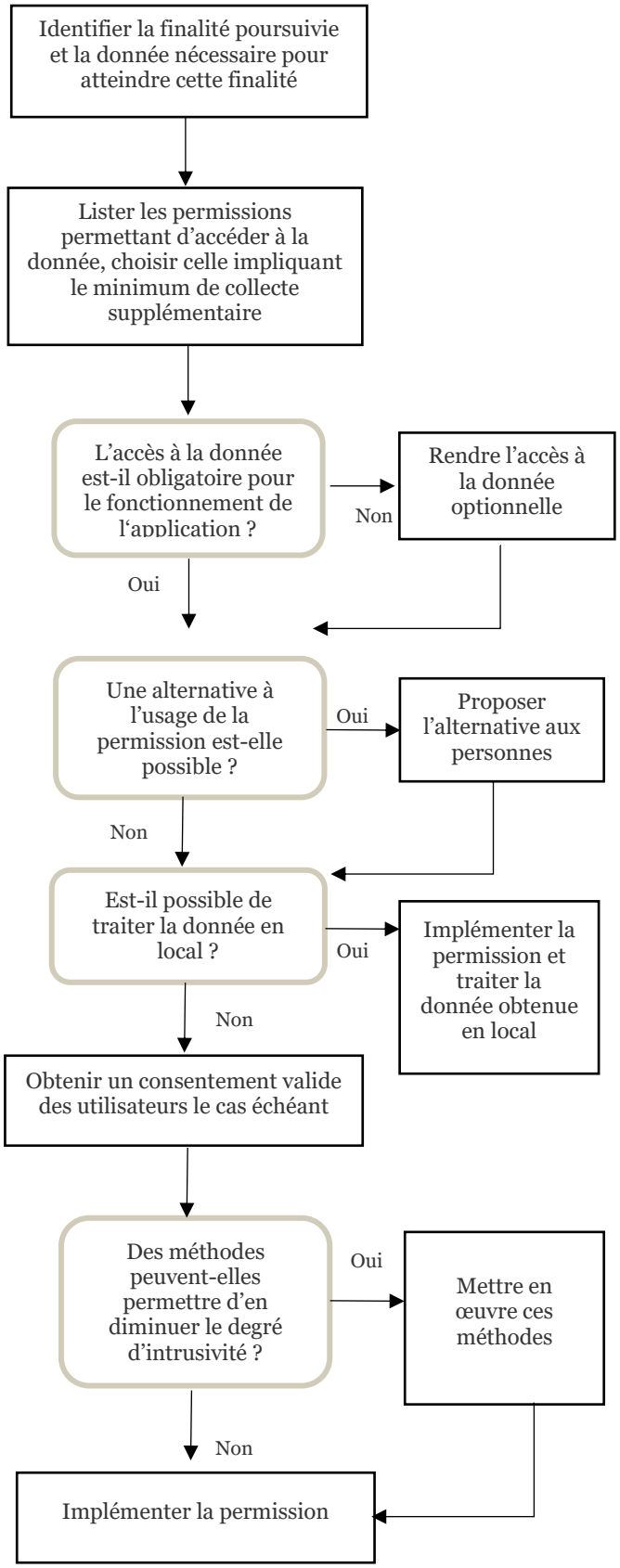
- **Est-ce que des processus qui permettent d'assurer la confidentialité des données sont mis en place ?**
  - L'éditeur doit encadrer l'accès aux données personnelles par les sous-traitants.
  - La CNIL recommande de mettre en œuvre des contrôles d'accès journalisés pour éviter les détournements internes (personnels ou structurels), tel que mentionné par la CNIL dans sa recommandation sur la journalisation[35]. L'usage de données fictives ou synthétiques par les sous-traitants est une solution alternative.
  - La CNIL recommande que l'éditeur supervise et vérifie la suppression des données dont la durée de conservation est arrivée à terme.

## 5.5. Permissions et protection des données dès la conception

L'accès aux ressources du téléphone est souvent soumis par les OS à un système de permission : l'utilisateur du terminal doit autoriser son système d'exploitation à donner accès à l'édition à un certain type de données. La CNIL considère que la mise en œuvre de systèmes de permissions pour donner l'accès à certaines ressources stockées sur le terminal (localisation, carnet de contact, appareils photographiques et photographies/films, etc.) en fonction du choix de l'utilisateur constitue une bonne pratique, indépendamment des obligations légales.

Lors du développement d'une application, le choix des permissions d'accès (ci-après, « permissions ») à utiliser et à mettre en œuvre des traitements de données qui peuvent y être associés est une étape cruciale pour la protection de la vie privée des personnes.

[35] Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation et « La CNIL publie une recommandation relative aux mesures de journalisation », cnil.fr.




## 1. Utiliser les permissions

- **Comment analyser les permissions au vu des textes applicables ?**

Les permissions en elles-mêmes n'ont pas pour objet de répondre à des obligations légales et constituent une mesure technique indépendante. Cependant, l'accès distant à une ressource du terminal suite à une demande de permission peut être soumis :

- au respect de l'article 82 de la loi Informatique et Libertés et au RGPD. L'article 82 de la loi l'obtention impose un consentement préalable, sauf lorsque les opérations de lecture et/ou écriture sont nécessaire soit au fonctionnement du protocole de communication électronique, soit à la fourniture du service expressément demandé par l'utilisateur. Voir la partie 5.3 des présentes recommandations « Gérer le consentement et les droits des personnes ».
- au recueil d'un consentement au titre du RGPD.
- Des difficultés pratiques peuvent survenir dans l'articulation entre ces deux types de consentement (qui peuvent être fusionnés) et la permission (voir la partie 6.2.3 des présentes recommandations : « Participer à la conformité en matière d'usage de traceurs et de recueil du consentement »)
- Lorsque la permission porte sur l'accès à des données à caractère personnel, ce qui est la plupart du temps le cas, l'éditeur doit :
- s'assurer que la personne octroie la permission en toute connaissance de cause et donc dispose de toute l'information nécessaire pour qu'elle comprenne pour quelles raisons l'accès aux données est demandé. Il est recommandé d'indiquer de manière claire et intelligible si la fonctionnalité liée à la permission recherchée est i) nécessaire pour le fonctionnement de l'application, ii) relative à l'activation d'une fonction accessoire pour le bénéfice de l'utilisateur (faciliter sa navigation, permettre de scanner un code QR, enregistrer un mémo vocal) ou iii) relative à des traitements effectués pour le bénéfice de l'éditeur ou d'un tiers distinct de la fourniture du service rendu par l'application (valorisation publicitaire).
- permettre à l'utilisateur de consentir de manière distincte lorsque les finalités poursuivies sont différentes (granularité du consentement).

L'appréciation de la conformité à ces principes se fait globalement (sur le fait que les éditeurs doivent pouvoir fournir l'information nécessaire au moment du recueil des permissions, et sur l'articulation des différentes interfaces, voir la partie 6.2.3 des présentes recommandations : « Participer à la conformité en matière d'usage de traceurs et de recueil du consentement ») en tenant compte des principes de transparence et de loyauté qui pourraient, dans certaines conditions, rendre

illicite le recueil d'une permission dans des termes particulièrement vagues afin d'orienter le recueil postérieur d'un consentement davantage éclairé.

- **Comment mettre en œuvre une démarche de sélection des permissions ?**

Dans la logique de protection des données dès la conception, la CNIL recommande de mettre en œuvre une procédure de sélection des permissions suivant les étapes décrites dans le schéma ci-contre.

## 2. Cas d'usages pratiques pour la sélection de permissions

- **Comment gérer l'usage de la localisation ?**
  - L'éditeur doit identifier au cas par cas, parmi les permissions mises à disposition par l'OS, celle permettant de remplir les objectifs poursuivis dans le respect du principe de minimisation :
    - une localisation approximative plutôt que précise,
    - une permission limitée à une seule fois plutôt qu'une permission permanente,
    - une permission uniquement active quand l'application est en premier plan plutôt qu'en permanence,
    - une permission qui ne transmet pas d'information à des tiers lorsque cela est possible (par exemple une permission fondée sur le seul GPS et non l'analyse de l'environnement réseau).
  - A titre de bonne pratique, l'éditeur peut proposer une alternative à l'usage de cette permission, par exemple l'entrée manuelle d'un code postal ou d'une adresse au lieu du traitement de la donnée de localisation. Il est recommandé de clairement indiquer le fait qu'il s'agit d'une donnée remplie manuellement par l'utilisateur et non issue du fonctionnement du système aux organismes conduits à la traiter.
  - La CNIL recommande à l'éditeur de traiter la donnée de localisation sur le terminal. Par exemple, pour trouver le lieu le plus proche de son utilisateur parmi une liste de lieux, la CNIL recommande d'intégrer la liste en question dans le contenu de l'application et calculer sur le terminal le lieu le plus proche en fonction de la localisation de la personne.
  - A moins que cette collecte ne soit nécessaire pour fournir un service expressément demandé par l'utilisateur, l'éditeur doit obtenir un consentement valide pour la collecte distante de la donnée de localisation de la personne.
  - Avant tout envoi des données de localisation vers les serveurs de l'application, l'éditeur doit identifier le niveau de précision minimal nécessaire pour atteindre ses finalités et tronquer localement les coordonnées en fonction de celui-ci, en vertu du principe de minimisation.
  - La CNIL recommande à l'éditeur de ne pas conserver la donnée de localisation qu'il a utilisée sur un serveur distant mais de privilégier sa conservation dans l'application, sur le terminal, pour la proposer à nouveau à l'utilisateur (via un item : « ma dernière localisation »).
  - La CNIL recommande de ne pas collecter la localisation quand l'application n'est pas activement utilisée par l'utilisateur.
  - A titre de bonne pratique, dans le cas où la permission donnée par l'utilisateur est permanente, l'éditeur peut lui rappeler l'existence de la permission de manière visible dans l'interface de l'application et lui demander à intervalles réguliers confirmation de son accord à ce que la localisation soit collectée.

- **Comment gérer l'accès aux données de contacts stockées au sein du terminal de l'utilisateur ?**
  - Il est nécessaire de déterminer avec précision le besoin et les raisons d'accès à ces données de contact, et notamment si cet accès est nécessaire au fonctionnement de l'application.
  - L'éditeur doit alors identifier la permission associée permettant de poursuivre la finalité tout en respectant le principe de minimisation. Par exemple, si une consultation des données est suffisant compte tenu de l'objectif poursuivi, l'éditeur ne doit pas demander de droits en écriture.
  - Pour toute permission d'accès impliquant la sélection d'un contact, il est recommandé de faire cette sélection directement sur le terminal de l'utilisateur.
  - Si certaines permissions d'accès entraînent la mise en commun de données de contacts entre plusieurs utilisateurs de l'application (par exemple, la découverte de contacts inscrits à une

messagerie, mécanisme qui permet aux personnes d'identifier si certaines des personnes dans leur répertoire utilisent la messagerie qu'ils souhaitent utiliser), l'éditeur doit collecter un consentement (article 82 de loi Informatique et Libertés). Il doit informer l'ensemble des personnes susceptibles d'être concernées par le traitement[36]. L'éditeur doit s'assurer de la bonne information de l'utilisateur quant à la nature de la collecte. A titre de bonne pratique il peut proposer des méthodes alternatives (p. ex. : entrée manuelle de numéro par la personne pour vérification ponctuelle de présence) en s'assurant qu'il ne peut être fait un usage malveillant de ces outils, par exemple en plafonnant le nombre ou la fréquence de requête possibles pour éviter de multiples requêtes automatisées à des fins de moissonnage de données (« *scraping* »).

- Dans un cas où l'éditeur souhaite afficher à l'utilisateur les contacts qui utilisent déjà l'application afin de lui proposer de le connecter :
  - La CNIL recommande d'obtenir le consentement de chaque utilisateur de l'application à ce que ses propres coordonnées soient utilisées à l'avenir pour être identifié sur des terminaux tiers ou être retrouvé par les comptes d'utilisateurs tiers qui disposent de ses coordonnées ;
    - La permission pour accéder aux « contacts » du téléphone ne doit pas être considérée comme consentement à l'utilisation de ses propres coordonnées de contact par des tiers ;
    - Si l'utilisateur consent, la CNIL recommande que le paramètre relatif à la capacité à être identifié ou recherché soit configuré **par défaut** à un niveau le plus restreint possible. L'utilisateur aurait alors le choix entre plusieurs options de paramétrage (« Seulement moi », « Amis », « Amis d'amis », « Tous les inscrits », « Tout le monde, y compris les non-inscrits », etc.).
  - La CNIL recommande d'utiliser les méthodes les plus adaptées pour limiter l'intrusivité de l'accès et l'analyse des contacts partagés (par exemple via des techniques de « *Private Set Intersection* »).
  - La CNIL recommande de supprimer, dès la fin de l'analyse, les données de contacts qui auraient été stockées. Il est recommandé de fixer une durée limitée du consentement à l'accès aux contacts du terminal pour cette finalité de comparaison avec les carnets de contacts d'autres utilisateurs.

- **Comment gérer l'usage du microphone ?**
  - Il est nécessaire de déterminer avec précision le besoin et les raisons justifiant un accès au microphone, et notamment si celui-ci est obligatoire pour le fonctionnement de l'application.
  - L'éditeur doit identifier la permission associée permettant de poursuivre la finalité tout en respectant le principe de minimisation (notamment en termes de possibilité de captation concurrente de flux audio, qui peut présenter un risque important pour la personne).
  - La CNIL recommande de traiter les contenus audios en local : par exemple si un accordeur est proposé, l'utilisation des capacités locales de calcul du téléphone devrait être privilégiée plutôt que le traitement distant des contenus.
  - Sauf si l'usage du microphone est nécessaire pour fournir un service expressément demandé par l'utilisateur, l'éditeur doit obtenir un consentement valide pour la collecte distante des contenus audio, en s'assurant de la bonne compréhension par la personne du fait que ces contenus seront envoyés vers ses serveurs.
  - D'une manière générale, la CNIL recommande de ne pas conserver les sons enregistrés sur un serveur distant sauf en cas d'usage précis et justifié. Plus particulièrement, elle recommande de rendre optionnelle la mise en œuvre de sauvegardes sur un serveur distant, et d'obtenir à cette fin le consentement libre, spécifique et éclairé des utilisateurs.
  - A titre de bonnes pratiques :

[36] Ainsi, dans sa décision 1/2021 adoptée le 28 juillet 2021, concernant le litige relatif au projet de décision de l'autorité de contrôle irlandaise concernant WhatsApp Ireland en application de l'article 65, paragraphe 1, point a), du RGPD, le CEPD a constaté non seulement une violation de l'article 14 concernant la collecte des données des non-utilisateurs, mais également qu'en raison de la non-validité du processus d'anonymisation utilisé, cette violation persiste pour le traitement des données des non-utilisateurs sous la forme de listes des non-utilisateurs après application de la procédure de hachage avec perte.

- si le besoin est ponctuel, l'éditeur peut révoquer la permission après la captation du son ;
- si l'usage du microphone n'est utile que pour certaines actions dans l'application (par exemple enregistrer un message), l'éditeur peut alerter l'utilisateur quand le microphone est activé, par exemple par le biais d'une icône clairement identifiée et dédiée ;
- l'éditeur peut proposer à ses utilisateurs de tronquer ou de réécouter les contenus partagés avant tout envoi des contenus audio vers les serveurs de l'application.

- **Comment gérer l'usage de l'appareil photographique ?**
  - Il est nécessaire de déterminer avec précision le besoin et les raisons justifiant un accès à l'appareil photo, et notamment si celui-ci est obligatoire pour le fonctionnement de l'application.
  - L'éditeur doit identifier la permission associée permettant de poursuivre la finalité tout en respectant le principe de minimisation. La CNIL recommande notamment :
    - De faire la distinction entre l'accès à l'appareil photo en lui-même et l'accès aux photographies prises par la personne et stockées au sein de son terminal si uniquement l'un des deux est nécessaire.
    - d'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, il doit s'appuyer sur des permissions qui mettent l'utilisateur en capacité de sélectionner spécifiquement les contenus qu'il souhaite partager avec l'application ;
    - si cela n'est pas possible (par exemple, pour des usages interactifs du flux vidéo), de ne doit requérir que le strict minimum en termes d'autorisations matérielles (par exemple, ne pas activer l'enregistrement audio si ce n'est pas une nécessité).
    - dans le cas où une prise de photo ou de vidéo en direct est nécessaire, il est recommandé de privilégier les solutions déléguant cette captation aux applications système ;
  - A titre de bonne pratique, l'éditeur peut proposer une alternative évitant l'accès à la caméra de l'utilisateur.
  - La CNIL recommande de traiter la donnée sur le terminal : par exemple, si le terminal propose des outils de retouche, il est possible d'envisager l'utilisation des capacités de calcul locales du téléphone plutôt que le traitement distant des images. De même, elle recommande de supprimer les métadonnées associées à l'image (localisation, horodatage, données EXIF) si elles ne sont pas nécessaires.
  - Quand l'usage de l'appareil photo n'est pas nécessaire à la réalisation d'un service expressément demandé par l'utilisateur, l'éditeur doit en principe obtenir un consentement valide pour la collecte distante des images, au titre de l'article 82 de la loi Informatique et libertés.
  - Avant tout envoi des images vers ses serveurs, la CNIL recommande d'analyser la nécessité de l'obtention de l'ensemble de l'image. À défaut, elle recommandé de proposer des outils de sélection ou de floutage à l'utilisateur.
  - D'une manière générale, la CNIL recommande de ne pas conserver les images collectées sur un serveur distant sauf en cas d'usage précis et justifié. Plus particulièrement, elle recommande de rendre optionnelle la mise en œuvre de sauvegardes sur un serveur distant et que le paramétrage par défaut n'inclue pas cette sauvegarde.

## 5.6. Liste de vérifications

Ces vérifications ont pour objet de guider les éditeurs dans la mise en œuvre de ces recommandations et sont présentées à titre indicatif. Certaines des vérifications à effectuer peuvent correspondre à des bonnes pratiques ou recommandations et non à des obligations : en cas de doute, se référer au texte de la recommandation.

| Catégorie | Sous-Catégorie | Identifiant | Description |
|---|---|---|---|
| **Concevoir son application** | 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 |
| | Assurer la conformité juridique des traitements | 1.2.1 | Chaque traitement mis en œuvre a une base légale identifiée. |
| | | 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. |
| | | 1.2.3 | Aucune collecte de données non nécessaire n'est opérée. Celles nécessaires sont minimisées. |
| | | 1.2.4 | Une durée de conservation des données est associée à chaque traitement. |
| | | 1.2.5 | Les données sensibles traitées sont identifiées. |
| | | 1.2.6 | Des mesures additionnelles sont appliquées sur les données des personnes mineures. |
| | 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. |
| | | 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. |
| | Documenter son analyse (articles 5.2 et 24 du RGPD) | 1.4.1 | Un registre des traitements est réalisé. |
| | | 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. |
| **Cartographier ses partenaires** | Encadrer les relations avec les développeurs | 2.1.1 | La qualification du développeur est convenue entre celui-ci et l'éditeur. |
| | | 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. |

| | | | |
|---|---|---|---|
| | 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. |
| | | 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. |
| **Gérer le consentement et les droits des personnes** | Informer correctement les utilisateurs (articles 12 à 14 du RGPD) | 3.1.1 | Une politique de confidentialité complète, concise et compréhensible par son public est rédigée. |
| | | 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. |
| | Obtenir un consentement valide des utilisateurs (article 4 et 7 du RGPD) | 3.2.1 | 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. |
| | 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.). |
| | | 3.3.2 | Un centre de gestion des droits est mis en place directement au sein de l'application. |
| **Maintenir la conformité durant le cycle de vie de l'application** | 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. |
| | | 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. |
| | | 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. |
| | | 4.3.3 | Les données personnelles sont protégées et leur accès est journalisé pour éviter tout détournement. |
| | | 4.3.4 | La suppression des données dont la durée est échue est organisée. |

| | | | |
|---|---|---|---|
| **Permissions et protection des données dès la conception** | 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 (voir 3.2.1). |
| | | 5.1.5 | Avant toute collecte distante, la précision de la donnée est diminuée au minimum nécessaire. |

# 6. Recommandations spécifiques au développeur

**Comment lire cette section ?**

Cette section rappelle les obligations posées par la règlementation (par exemple, « le responsable du traitement doit ») et formulent des recommandations pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer aux obligations, mais ils doivent alors pouvoir justifier leur choix et engagent leur responsabilité. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

## Notice

### À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **développeurs d'applications**.
- 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**.
- Les obligations, recommandations et bonnes pratiques s'appliquent à l'ensemble des développeurs, y compris lorsque ceux-ci endossent par ailleurs le rôle d'éditeur, de fournisseur de SDK, d'OS ou de magasin d'application. En particulier, dans le cas où le développeur et l'éditeur sont une unique entité, il devra consulter à la fois les recommandations applicables à l'éditeur et au développeur.
- Ces recommandations s'adressent plus spécialement au sein du développeur :
  - au délégué à la protection des données (DPD ou *Data Protection Officer* – DPO) d'une agence de développement d'application ;
  - aux chefs de projets chargés du développement d'applications ;
  - aux membres de l'équipe chargés du développement d'applications.
- Ces recommandations peuvent également être consultées par tout partenaire du développeur ou tiers intéressé pour évaluer la conformité des démarches du développeur.

### Quel est l'objet de ces recommandations ?

- Le développeur effectue un certain nombre de choix techniques durant la conception et le développement de l'application susceptibles d'avoir de forts impacts sur les traitements de données personnelles qui seront mis en œuvre par l'éditeur.
- Il doit donc mettre en œuvre une démarche pour assurer l'information et la validation de l'éditeur concernant les choix techniques opérés ainsi que leurs implications et respecte ainsi son devoir de conseil. **Ces recommandations ont pour but d'aider le développeur dans cette démarche, tout au long de son activité de développement et de maintenance de l'application.**

### Comment utiliser ces recommandations ?

- Chaque section correspond à une étape dans l'activité de développement d'une application et expose les enjeux en matière de vie privée et regroupe une série de recommandations et de bonnes pratiques à mettre en œuvre par les développeurs.
- Une **liste récapitulative des principales vérifications à réaliser** est proposée à la fin de cette partie. Les développeurs sont invités à s'y référer, notamment lors de la rédaction de leur documentation afin d'évaluer le niveau de prise en compte des recommandations de la CNIL par leurs partenaires.

**Voir aussi**

Les fournisseurs de SDK sont invités à consulter également les recommandations applicables aux autres acteurs, susceptibles de les concerner de manière incidente, et en particulier les :

## 6.1. Formaliser sa relation avec l'éditeur

À noter que si ne sont traitées ici que les relations directes entre éditeurs et développeurs, le recours à des sous-traitants ultérieurs (par exemple des prestataires engagés par les développeurs), nécessitera la prise en compte en cascade de ces recommandations.

### 1. Identifier les responsabilités et obligations de chacun

Le contrat de sous-traitance entre le responsable de traitement (éditeur) et le sous-traitant[37] (développeur) doit définir les responsabilités de chacun.

- **Le développeur est-il un sous-traitant au sens du RGPD** ?
  - Le développeur doit être qualifié sous-traitant s'il intervient sur des traitements de données personnelles pour le compte et sur instruction du responsable de traitement.
  - Pour rappel, le fait que le développeur procède à certains choix techniques ne fait pas nécessairement de lui un responsable du traitement : un sous-traitant peut déterminer les « moyens » non essentiels d'un traitement[38].
  - La CNIL recommande au développeur de se référer à la partie 4 des présentes recommandations pour déterminer sa qualification au titre du RGPD.
- **Quelles demandes faire à l'éditeur** ?
  - Lors de la contractualisation avec l'éditeur, il est recommandé au développeur de demander à l'éditeur une qualification explicite de son rôle pour chacun des traitements concernés.
  - Lorsqu'il est sous-traitant, le développeur doit demander à l'éditeur de lui fournir, dans le cahier des charges, des instructions sur les traitements à mettre en œuvre, permettant de définir quelles données seront utilisées.
  - Le contrat de sous-traitance doit prévoir dans ce cas que le développeur doit limiter les traitements mis en œuvre aux seules instructions fournies (article 28 du RGPD).
  - La CNIL recommande de prévoir dans le contrat un point de contact pour faire valider les choix ayant un impact en matière de traitements de données personnelles : il peut s'agir du délégué à la protection des données de l'éditeur.
- **Quelles obligations du côté du développeur ?**
  - Lorsqu'il a la qualité de sous-traitant, le développeur doit respecter un certain nombre d'obligations (article 28 du RGPD) et notamment :
    - une obligation de transparence et de traçabilité. A titre de bonne pratique, le développeur pourrait ainsi mettre à disposition de l'éditeur le code source de l'application ;
    - l'obligation d'assister son client, l'éditeur, dans le respect de ses obligations en termes de réponse aux exercices des droits au titre du RGPD (voir la partie 6.2 des présentes recommandations, « Assumer son rôle de conseil envers l'éditeur ») ;
    - l'obligation de garantir la sécurité des données traitées (voir la partie 6.4 des présentes recommandations « Assurer la sécurité de l'application »).
    - l'obligation d'alerter l'éditeur si les instructions fournies ne respectent pas le RGPD, notamment en termes de respect des principes de protection des données dès la conception et par défaut ;
  - Le développeur sous-traitant doit tenir un registre des activités de traitements mis en œuvre pour le compte de l'éditeur sous réserve des conditions prévus à l'article 30.3 du RGPD.
  - Le développeur sous-traitant doit s'assurer que les données personnelles qu'il collecte et traite sur instruction de l'éditeur correspondent à celles du registre de traitements ou du cahier des

[37] « Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les données personnelles », cnil.fr
[38] Lignes directrices 07/2020 du CEPD concernant les notions de responsable du traitement et de sous-traitant (PDF, 1,6 Mo), edpb.europa.eu

charges exhaustif communiqué par l'éditeur. À défaut, il lui est recommandé d'alerter l'éditeur afin que ce document soit mis à jour.

- Dans tous les cas, le développeur doit agir sur instructions documentées du responsable du traitement, en faisant valider le recours éventuel à des sous-traitants ultérieurs conformément à l'article 28 du RGPD.
- Si les sous-traitants ultérieurs recrutés par le développeur sous-traitant procèdent à des opérations de lecture et/ou d'écriture pour leur compte, ces derniers pourront être responsables ou responsables conjoints du traitement avec l'éditeur concernant ces opérations (voir la partie 4 des présentes recommandations : « Quels sont les rôles de chaque acteur dans le cadre de l'utilisation de l'application ? ») : le recours à ces prestataires ainsi que leur qualification au sens du RGPD et de la directive « ePrivacy » doit être validés par l'éditeur.
- Enfin, s'agissant des environnements propres au développeur (p. ex. : environnement technique de développement mutualisé entre ses clients) :
  - Si le développeur met en œuvre des traitements de données pour son propre compte, il doit, le cas échéant, respecter l'ensemble des obligations d'un responsable du traitement. Cela peut être le cas notamment si des données de tests sont utilisées pour les différentes applications développées par le développeur.
  - Le développeur ne procède à des traitements réutilisant les données qu'il détient en tant que sous-traitant, pour ses propres finalités, qu'avec l'accord préalable de l'éditeur et sous réserve que le traitement soit compatible avec les finalités initiales, conformément à l'article 6-4 du RGPD[39] (voir la partie 4 des présentes recommandations, « Quels sont les rôles de chaque acteur dans le cadre de l'utilisation de l'application ? »).

## 2. Mettre en œuvre des processus de maîtrise d'œuvre agréés par les deux parties

- **Quel processus de décision ?**
  - Si une décision impactant la vie privée des utilisateurs (choix technique, design d'interface, etc.) est identifiée par le développeur, la CNIL recommande de ne pas prendre cette décision seul mais au contraire d'impliquer l'éditeur dans le processus de décision.
  - La CNIL recommande que le point de contact identifié au sein de l'éditeur à cette fin soit utilisé pour faciliter la communication. Elle recommande que le développeur identifie également de son côté un référent pour toute question relative aux problématiques relatives à la protection des données (par exemple s'il existe le DPO de la structure).
  - La CNIL recommande de présenter les enjeux de manière claire et demander à ce que des instructions écrites lui soient transmises, afin de pouvoir démontrer qu'il agit bien sur instruction du responsable de traitement.
  - La CNIL recommande de porter une attention particulière aux sujets suivants :
    - choix des partenaires et plus particulièrement des SDK utilisés (voir la partie 6.3 des présentes recommandations : « Faire bon usage des SDK ») ;
    - choix des permissions qui seront sollicitées par l'application et les éventuelles alternatives en cas de refus ;
    - choix des modalités des éventuels recueils de consentement des utilisateurs ;
    - information des utilisateurs et exercice de leurs droits.

- **Quels processus pour assurer la conformité des traitements de données personnelles dans la durée ?**
  - La CNIL recommande de maintenir le processus de décision décrit ci-dessus pendant toute la durée de vie de l'application, en particulier à la suite d'une évolution externe ou d'une alerte (p. ex. : mise à jour d'un SDK, détection d'une faille de sécurité). Dans ces situations, elle recommande d'informer l'éditeur de manière proactive. Certains outils peuvent aider le développeur à analyser les mises à jour des conditions d'utilisation des partenaires.
  - A titre de bonne pratique, si des évolutions dans les permissions proposées par l'OS permettent de mieux protéger les personnes, le développeur peut suggérer à l'éditeur une mise à jour.

[39] « Sous-traitants : la réutilisation de données confiées par un responsable de traitement », cnil.fr

- **Quelle gestion pour la publication des applications ?**
  - Si la responsabilité relative à la publication d'une application ou de ses mises à jour dans un magasin d'applications repose sur l'éditeur, il est fréquent que cette opération soit effectuée en pratique par le développeur, notamment du fait des restrictions techniques imposées par les fournisseurs de magasins d'applications.
  - A titre de bonne pratique, le développeur peut s'assurer qu'il dispose bien de l'ensemble des éléments requis pour assurer la bonne information des personnes au sein de ces magasins et, sinon, peut demander à l'éditeur de les lui transmettre.
  - Le compte de mise en ligne de l'application doit être sécurisé, en excluant tout partage de mot de passe.
  - Si le développeur a pour instruction de distribuer l'application sans passer par un magasin d'applications, il doit s'assurer qu'il a la capacité à garantir l'intégrité du contenu distribué.

## 3. Identifier l'ensemble des traitements de données personnelles

Si la majorité des traitements seront répertoriés au registre fourni par l'éditeur ou dans un cahier des charges exhaustif, certains choix de développement peuvent impliquer la mise en œuvre de traitements additionnels. La CNIL recommande au développeur d'informer l'éditeur de l'existence de traitements de données personnelles identifiés et, en lien avec lui, de déterminer les responsabilités associées.

- **L'usage de fonctionnalités mises à disposition par l'OS implique-t-il des traitements de données personnelles ?**
  - Le développeur sous-traitant doit analyser, lorsqu'il utilise des outils fournis par l'OS, si leur usage implique le traitement de données personnelles.
  - Par exemple, lors de l'utilisation des fonctionnalités de sauvegarde de données (parfois activées par défaut), il doit d'informer l'éditeur et l'assister dans la qualification de ce traitement et des problématiques associées (par exemple en matière de transferts de données hors de l'Union européenne, au sens du chapitre V du RGPD[40]).
  - Il doit analyser de cette manière 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 du traitement.
  - La CNIL recommande de suivre les évolutions des OS et de leurs fonctionnalités, notamment en termes de minimisation des données traitées.

- **Des traitements sont-ils mis en œuvre à la suite de l'intégration de SDK ?**
  - Le développeur sous-traitant doit analyser, lorsqu'il a recours à des SDK, si l'usage de ceux-ci implique le traitement de données personnelles (par exemple, la collecte d'un identifiant unique propre au matériel, la collecte des adresses IP, des identifiants Wi-Fi environnants, etc.).
  - Si c'est le cas, il lui est recommandé de s'informer sur leurs caractéristiques pour qualifier ces tiers au sens du RGPD. Il peut se référer à ce titre à la partie 4 des présentes recommandations (« Quels sont les rôles de chaque acteur dans le cadre de l'utilisation de l'application ? »).
  - La CNIL recommande de recueillir à cette fin la liste des données personnelles collectées, l'objet, la nature et la finalité des traitements mis en œuvre sur ces données en fonction de la configuration de l'outil choisi. En cas d'absence de ces éléments, si des doutes subsistent sur les traitements effectivement impliqués par le recours au SDK, la CNIL recommande au développeur d'en informer l'éditeur, et d'envisager de renoncer à l'usage du SDK. En particulier, si le développeur sous-traitant estime que des traitements mis en œuvre suite à l'intégration du SDK contreviennent au RGPD, il a l'obligation d'en informer le responsable de traitement.
  - Cette analyse doit être appliquée à l'ensemble des SDK utilisés, notamment ceux fournis par le fournisseur de l'OS.

[40] « Transférer des données hors de l'UE », cnil.fr

## 6.2. Assumer son rôle de conseil envers l'éditeur

Le développeur, lorsqu'il est sous-traitant au sens du RGPD, doit assister et conseiller l'éditeur dans sa conformité à certaines obligations posées par le RGPD, particulièrement en ce qui concerne le respect des droits des personnes et les mesures de sécurité à mettre en œuvre (articles 28.3.e et 28.3.f du RGPD). Il a également l'obligation de l'informer s'il considère qu'une instruction donnée par celui-ci contrevient au RGPD. La CNIL recommande au développeur de s'assurer que le responsable du traitement est informé des choix techniques opérés et de leurs implications, pour lesquels le développeur engage sa responsabilité contractuelle[41].

### 1. Aider au bon respect des droits des utilisateurs

Si le développeur est sous-traitant, il doit assister le responsable de traitement afin d'assurer le respect des droits des personnes (article 28.3.e du RGPD). Il peut, à titre de bonne pratique, s'assurer, lors de la conception de l'application, que les droits pourront bien s'exercer de manière effective au sein de l'application indépendamment de sa qualification.

- **L'exercice des droits est-il possible au sein de l'application ?**
  - Le développeur sous-traitant doit prendre des mesures techniques et organisationnelles pour permettre l'exercice des droits, notamment en termes de structuration des bases de données. Par exemple, le droit de suppression doit être respecté, indépendamment des contraintes techniques.
  - La CNIL recommande que le développeur propose à l'éditeur d'offrir aux utilisateurs d'exercer leurs droits directement au sein de l'application, au moyen d'une page dédiée. Cela permet en particulier à l'éditeur d'éviter de collecter des données additionnelles pour répondre à l'exercice des droits, en faisant simplement usage des identifiants utilisés pour la collecte afin de le mettre en œuvre.
  - Le développeur doit s'assurer que, lorsque les droits d'accès ou à la portabilité sont exercés, l'ensemble des données concernées sont bien transmises à la personne. Cela nécessite, si des traitements sont effectués par des tiers comme des SDK et si l'éditeur souhaite apporter une réponse automatique aux demandes, que ces tiers fournissent des API de gestion des droits afin de rendre possible l'automatisation du processus.
- **Les utilisateurs sont-ils bien informés ?**
  - A titre de bonne pratique, le développeur peut rappeler à l'éditeur la nécessité de mettre à disposition la politique de confidentialité que ce dernier fournit au sein de l'application.
  - De manière additionnelle, un écran d'information relative à la protection des données peut être mis à disposition au premier lancement de l'application.

### 2. Proposer des développements respectant les principes de protection des données personnelles

- **Le principe de minimisation des données est-il pris en compte ?**
  - Le développeur, sous-traitant, doit s'assurer que les traitements qu'il met en œuvre pour le compte de l'éditeur respectent les instructions données par celui-ci en particulier concernant le principe de minimisation des données collectées.
  - A ce titre, si le développeur identifie que certaines données sont accessibles par des tiers (l'OS ou un SDK, par exemple), la CNIL recommande de proposer des solutions pour limiter les risques associés à ces accès et notamment :
    - limiter les données affichées dans les notifications émises par l'application, en indiquant simplement que celles-ci sont disponibles au sein de l'application. Dès que possible, chiffrer le contenu des notifications, de sorte que le fournisseur d'OS ne soit pas en capacité d'y accéder ;
    - chiffrer les contenus des sauvegardes, en permettant à l'utilisateur de l'application et à lui seul de conserver la maîtrise des clés cryptographiques utilisées pour ce chiffrement ;

[41] Le contrat liant l'éditeur de l'application et son développeur peut en particulier être frappé de nullité si le non-respect des obligations du cocontractant au titre du RGPD constitue une erreur sur les qualités essentielles de l'objet du contrat (voir en ce sens CA Grenoble, 12 janv. 2023, n° 21/03701, dans le cas de la conception d'un site web).

- éviter la transmission d'identifiants inter-applications à des fournisseurs de SDK. Si cette transmission est nécessaire, opérer un hachage des identifiants.

- Dans le cas où le développeur doit mettre en œuvre des fonctionnalités de navigation web au sein de l'application, la CNIL recommande de s'assurer que celles-ci ne permettent pas de collecter plus de données que lors d'une navigation utilisant les navigateurs web. Elle recommande de respecter les préférences et les réglages du terminal en utilisant le navigateur web choisi par l'utilisateur.
- Si le développeur ne dispose pas d'instructions spécifiques concernant les permissions à collecter, il doit s'assurer que celles qu'il va demander correspondent aux attentes de l'éditeur.
- La CNIL recommande de s'assurer que les permissions demandées sont nécessaires au fonctionnement de l'application et aux finalités du traitement, et de conseiller l'éditeur sur les moyens de minimiser les collectes autorisées selon les niveaux de permissions. Lorsque c'est possible, la CNIL recommande de proposer des méthodes de collecte de données alternatives et volontaires de la part de l'utilisateur en cas de refus de celles-ci (voir la partie 5.5 des présentes recommandations : « Permissions et protection des données dès la conception ») Pour les permissions les plus intrusives, le développeur peut, à titre de bonne pratique, proposer de signaler à l'utilisateur quand elles sont actives, via les fonctionnalités de l'OS ou au sein de l'application.
- Le développeur doit s'assurer que l'usage de permissions est compatible avec les instructions de l'éditeur concernant la nécessité d'obtenir un consentement valide avant toute opération de lecture et/ou d'écriture, en lien avec l'éditeur (voir la partie 6.2.3 des présentes recommandations : « Participer à la conformité en matière d'usage de traceurs et de recueil du consentement »). La CNIL recommande de limiter au maximum l'usage de permissions en bloc à l'installation (« *install-time permissions* »), en préférant l'usage de permissions déclenchables durant le fonctionnement de l'application (« runtime permissions »).
- A titre de bonne pratique :
  - le développeur peut conseiller techniquement l'éditeur pour choisir et mettre en œuvre des solutions plus protectrices. La CNIL encourage :
    - l'utilisation de techniques de protections de la vie privée (par exemple telles que décrites dans un guide sur le sujet produit par l'ICO[42]) ;
    - l'utilisation de méthodes visant à effectuer localement au sein du terminal les opérations et calculs sur les données, au lieu de recourir à des API distantes.
  - Le développeur peut analyser les instructions de l'éditeur pour identifier si les données qu'il lui est demandé de traiter sont bien nécessaires, et, si ce n'est pas le cas, lui proposer d'exclure certaines données du traitement.

- **Le traitement implique-t-il des données sensibles au sens de l'article 9 du RGPD ?**

**Pour la définition de la donnée sensible au sens de l'article 9 du RGPD : voir la partie 5.1 des présentes recommandations : « Assurer la conformité juridique des traitements »**

- Le développeur ne peut traiter de données sensibles qu'après avoir reçu instruction explicite en ce sens de l'éditeur (article 28.3.a du RGPD). A défaut, il doit informer l'éditeur s'il identifie des traitements de données sensibles pour que ce dernier puisse analyser la conformité du traitement et modifier ses instructions.
- L'éditeur doit être alerté en cas d'usage non pertinent voire illicite des données sensibles, par conception ou par erreur (p. ex. : usage de données sensibles pour cibler des publicités) au titre de l'article 28 du RGPD. Pour rappel, toute catégorisation ou création de segments sur la base de telles données à des fins de profilage publicitaire est interdite (article 26 du Règlement n° 2022/2065 sur les services numériques, dit « *Digital Services Act* » ou DSA).
- Le traitement de ces données doit faire l'objet d'une attention particulière, notamment en cas de transmission à des tiers. Par exemple, lors de l'intégration de SDK, la CNIL recommande au développeur de s'assurer qu'ils n'ont aucun accès à ces données.

[42] Chapter 5: Privacy-enhancing technologies (PETs) Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance (PDF, 722 ko), sept. 2022, ico.org.uk

- Si les instructions fournies par l'éditeur impliquent le traitement de données sensibles, la CNIL recommande au développeur de faire une distinction claire entre ces typologies de données et les autres, notamment au niveau de l'architecture du service.

## 3. Participer à la conformité en matière de recueil du consentement

La CNIL recommande au développeur d'alerter l'éditeur si des éléments du cahier des charges impliquent le recueil d'un consentement (en application de l'article 82 de la loi Informatique et libertés ou du RGPD) et, dans la mesure du possible, de participer à la bonne mise en œuvre de celui-ci. Pour plus de détails sur les contextes dans lesquels le consentement peut être nécessaire, voir la partie 5.1.2 des recommandations adressées aux éditeurs.

- **Comment recueillir le consentement dans le cadre des applications mobiles ?**
  - Les lignes directrices et la recommandation « *Cookies* et autres traceurs » publiées par la CNIL sont pertinentes dans le contexte des applications mobiles.
  - Il est nécessaire d'adapter les interfaces pour permettre la lisibilité des fenêtres dans un environnement mobile. La CNIL recommande de porter une attention particulière aux problématiques d'accessibilité pour permettre à tous de fournir un consentement valide.


*Figure 1- Le détail des finalités est disponible sous un bouton de déroulement que l'utilisateur peut activer sur le premier niveau d'information*


*Figure 2 - Le détail des finalités est disponible en cliquant sur un lien hypertexte présent sur le premier niveau d'information*

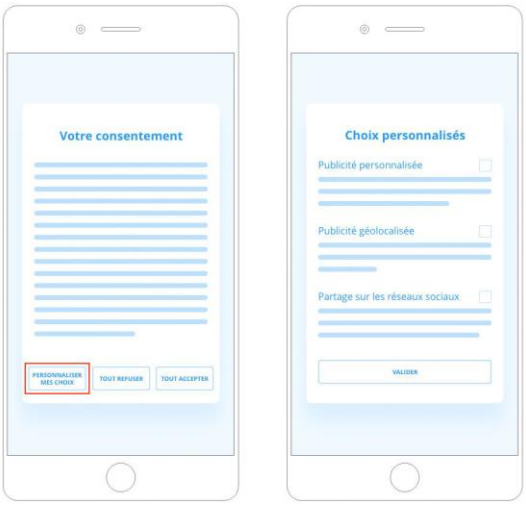
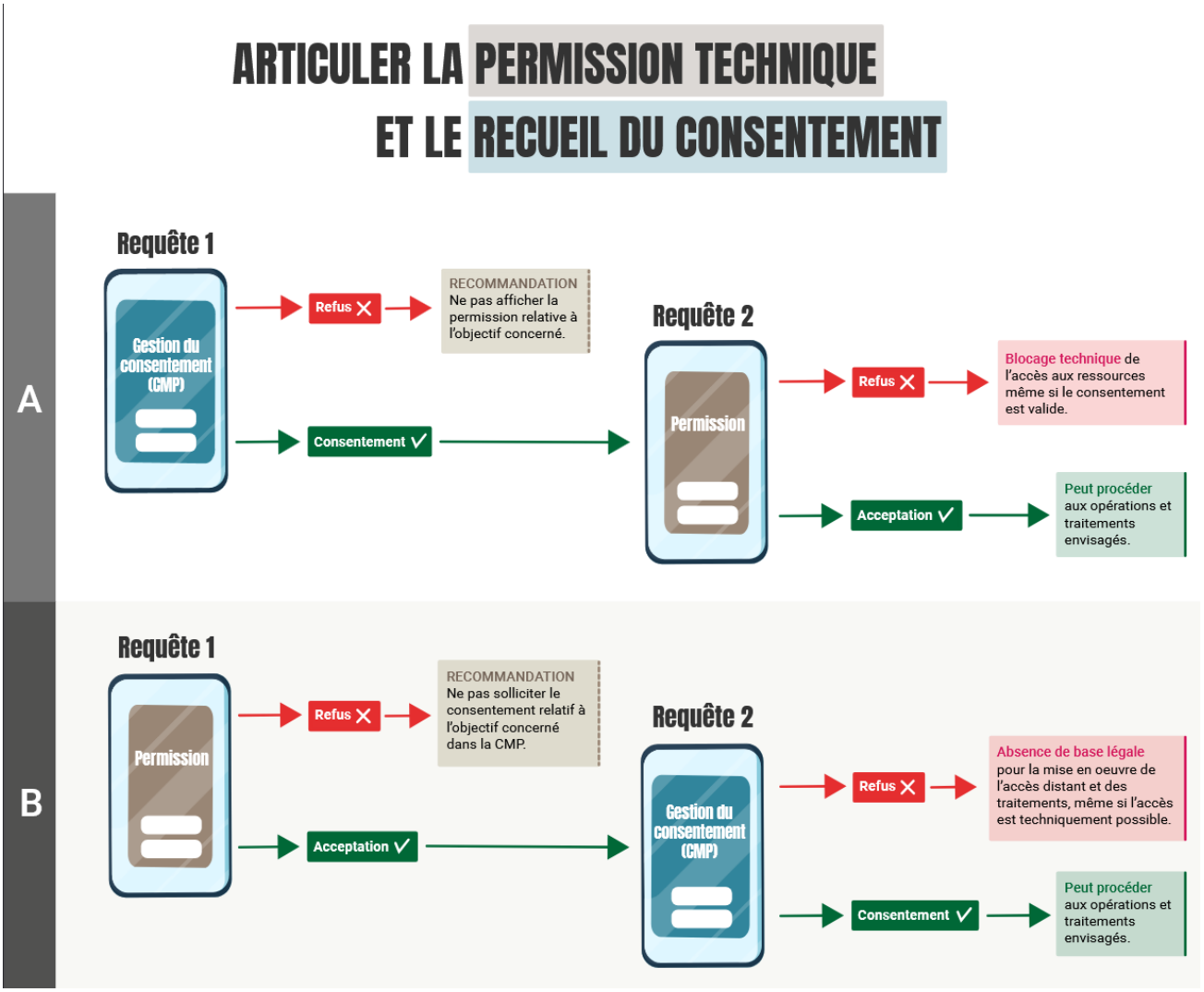



*Figure 3 - La possibilité de consentir de manière granulaire peut-être offerte sur un second niveau d'information via un bouton « personnaliser mes choix » inséré sur le même niveau d'information (premier niveau) que les boutons permettant de « tout accepter » et de « tout refuser ».*

- La CNIL recommande de convenir des modalités de recueil du consentement en amont avec l'éditeur et de les mettre en place au sein de l'application sur la base de ses instructions, en documentant cette démarche.
- Pour réduire la fatigue face à des requêtes excessivement longues et afin de rendre le recueil du consentement plus compréhensible pour les utilisateurs, la CNIL recommande, à titre de bonne pratique, de recueillir les consentements de manière contextuelle en fonctions des actions entreprises en lieu et place d'un unique écran initial.

- **Comment articuler le recueil du consentement et les permissions ?**
  - De manière générale, l'obtention de ces permissions permet de donner l'accès technique à la ressource visée. Néanmoins, la demande d'une permission ne permet pas nécessairement d'obtenir un consentement valide au titre du RGPD ou de l'article 82 de la loi Informatique et libertés.
  - Il est recommandé au développeur de convenir avec l'éditeur de la nécessité de mettre en œuvre une plateforme de gestion du consentement (« *Consent Management Platform* » ou CMP) de manière additionnelle à la fenêtre de permission.
  - Le consentement peut être obtenu indifféremment avant ou après la demande de permission. La CNIL recommande que le développeur, en lien avec l'éditeur, retienne la modalité qui soit la plus facile à comprendre pour l'utilisateur (par exemple en émulant ou annotant l'interface des permissions), en évitant de le solliciter de manière inutile (voir le tableau ci-après) : l'utilisateur devrait disposer des informations pertinentes pour comprendre à quoi il donne accès et pourquoi le plus tôt possible dans le processus de recueil de son autorisation.




*Cette infographie concerne l'articulation entre la fenêtre de sollicitation (CMP) et les permissions techniques et non les permissions visant à autoriser ou refuser la réalisation de certaines actions en vue d'une finalité précise.*

- Certains fournisseurs d'OS mettent à disposition des mécanismes pour recueillir l'approbation de l'utilisateur pour une finalité spécifique. Les fenêtres présentées dans le cadre de ces mécanismes ne peuvent constituer un moyen valide de recueillir le consentement que lorsqu'elles permettent de répondre aux exigences posées par le RGPD en termes d'information disponibles (finalités du traitement, identités des acteurs qui se prévalent du consentement donné) ou encore s'agissant de la possibilité de refuser ou de retirer le consentement aussi facilement que de le donner. Lorsque ces fenêtres ne permettent pas de recueillir un consentement valide, le développeur doit aider l'éditeur à analyser la nécessité et, le cas échéant, à mettre en œuvre une CMP de manière additionnelle. Si une CMP est utilisée pour recueillir le consentement pour cette même finalité, la CNIL souligne que celui-ci ne pourra être considéré comme valablement donné que si le caractère univoque du choix exprimé ne fait aucun doute ; tel ne sera pas le cas si le choix exprimé dans la permission et celui formulé au sein de la CMP diffère pour une même finalité.
- En tout état une cause, une CMP sera nécessaire pour recueillir le consentement pour les finalités qui ne sont pas couvertes par la permission.

## 6.3. Faire un bon usage des SDK

En pratique, lors de l'intégration de SDK procédant à des traitements, le développeur choisit les SDK qu'il propose à l'éditeur, auquel revient la décision finale d'intégration au sein de l'application. Le développeur sous-traitant ne doit pas engager un sous-traitant ultérieur sans approbation écrite, spécifique ou générale, de l'éditeur (article 28.2 du RGPD). De plus, dans le cas où le développeur sous-traitant intègre un SDK comme sous-traitant ultérieur, il doit s'assurer que ce SDK respecte l'ensemble des demandes du responsable du traitement en matière de protection des données et doit ainsi reproduire ses propres obligations au sein du contrat qui les lie (article 28.4 du RGPD). Il sera en effet responsable en cas de manquement de ce sous-traitant ultérieur. Même dans l'hypothèse où le développeur n'est pas sous-traitant, l'éditeur doit être informé et un contrat de sous-traitance doit lier directement l'éditeur de l'application et le fournisseur du SDK sous-traitant.

### 1. Sélectionner le SDK selon les bons critères

Avant toute proposition d'intégration d'un SDK, la CNIL recommande au développeur de suivre une méthodologie d'évaluation axée sur le respect de la protection des données.

- **Quels documents obtenir du fournisseur de SDK ?**
  - Le développeur doit s'assurer que le SDK procède uniquement aux traitements qui font partie des instructions documentées du responsable du traitement. La CNIL recommande de s'assurer de la mise à disposition, par le SDK, de documents permettant de déterminer l'ensemble des traitements de données qu'implique l'intégration du SDK en fonction du paramétrage mis en œuvre, par exemple grâce au registre des traitements.
  - Le développeur doit s'assurer de la mise à disposition des éléments permettant d'identifier d'éventuels transferts ou divulgations non autorisés de données personnelles, au sens du chapitre V du RGPD (articles 28.4 et du 28.3.a du RGPD).
- **Quelle analyse mener ?**
  - Le développeur doit s'assurer que le SDK permet de répondre aux demandes d'exercice des droits, notamment au droit au retrait du consentement (article 28.3.e du RGPD). La CNIL recommande de privilégier les SDK mettant à disposition des API pour y répondre automatiquement.
  - Elle recommande au développeur de s'assurer que le SDK présente des moyens de bloquer tout traitement ou accès à des données stockées sur le terminal ou mise en œuvre d'une permission jusqu'à ce qu'un consentement valable puisse être recueilli lorsqu'il est nécessaire (voir la partie 6.3.2 « Gérer le consentement des utilisateurs » ci-dessous).
  - Ces recommandations s'appliquent également aux SDK fournis par les fournisseurs d'OS ou à ceux qui sont proposés par défaut dans les documentations d'Apple et Google, respectivement pour iOS et Android.
  - A titre de bonne pratique, le développeur peut prendre en compte comme critère le paramètre du respect de la vie privée des utilisateurs, par exemple en choisissant des solutions qui ne se financent pas en monétisant les données de leurs utilisateurs.
- **Comment intégrer un SDK responsable de traitement ?**
  - Si le fournisseur de SDK met en œuvre des traitements pour son propre compte via le SDK intégré au sein de l'application, il est responsable de ces traitements. Cette collecte doit être prévue contractuellement avec l'éditeur.
  - Dans certains cas, il peut arriver que le fournisseur de SDK soit responsable de traitement et non sous-traitant pour certains traitements mis en œuvre pour son propre compte portant sur des données personnelles obtenues en tant que sous-traitant. Dans ce cas, le fournisseur de SDK doit obtenir du responsable du traitement initial une autorisation écrite spécifique pour la réutilisation des données[43].
  - Afin de permettre ce processus, la CNIL recommande que le développeur obtienne du fournisseur de SDK les éléments permettant de déterminer sa qualification pour les traitements visés (voir la partie 4 des présentes recommandations concernant la qualification du fournisseur de SDK).

**Point d'attention**

Il convient de veiller à l'effet « poupées russes » : lorsque l'intégration d'un SDK implique celle d'autres SDK, la CNIL recommande de s'assurer que le SDK initial apporte le niveau de garantie décrit dans ce paragraphe en ce qui concerne ses propres sous-traitants ultérieurs.

## 2. Gérer le consentement des utilisateurs

Lors du choix d'un SDK, il faut étudier la capacité des solutions proposées à permettre le bon recueil du consentement des utilisateurs lors de l'usage par ceux-ci de traceurs nécessitant le consentement au sens de l'article 82 de la loi Informatique et Libertés ou de la réalisation en tant que sous-traitant de finalités reposant sur la base légale du consentement, au titre de l'article 28.4 du RGPD.

- **Quelles garanties pour permettre le recueil d'un consentement valide des utilisateurs ?**
  - La configuration du SDK doit permettre qu'un consentement soit donné avant tout traitement reposant sur le consentement ou toute opération de lecture et/ou d'écriture provenant du SDK. En particulier, toute opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés qui nécessite un consentement qui serait effectuée au premier lancement de l'application est à proscrire.
  - Le développeur doit choisir des SDK qui permettent le retrait du consentement.
  - Dans les cas où les SDK sélectionnés affirment qu'ils permettent de collecter le consentement de manière licite pour le compte de l'éditeur, la CNIL invite le développeur, à titre de bonne pratique, à encadrer contractuellement cet engagement et à en auditer le respect (voir la méthode proposée ci-dessous) afin de permettre à l'éditeur de respecter ses obligations en la matière.

- **Comment assurer la granularité du consentement pour les traitements mis en œuvre via le SDK ?**
  - Si plusieurs finalités sont poursuivies par le SDK, il est recommandé au développeur de veiller à ce que le SDK supporte la granularité du consentement, qui est généralement nécessaire pour garantir que le consentement est donné librement. Cela signifie que si un consentement est obtenu pour une unique finalité, les opérations qui seront opérées par ce SDK se limiteront à cette unique finalité. Si plusieurs opérations techniques participent à la même finalité, ces opérations peuvent découler d'un unique consentement (par exemple la publicité ciblée en ligne inclura généralement la sélection de la publicité, la maitrise de la répétition publicitaire, la mesure d'audience de la publicité, la lutte contre la fraude publicitaire, etc.).
  - La CNIL recommande au développeur de ne retenir que des SDK qui permettent techniquement la suspension de leurs propres exécutions à un signal de l'application.

## 3. Auditer le bon fonctionnement des SDK

Le développeur peut, à titre de bonne pratique, mettre en œuvre des moyens adaptés à la complexité technique du processus, pour vérifier le respect des engagements des SDK qu'il propose.

- **Comment vérifier le respect des engagements pris par le SDK ?**
  - Une méthode d'audit par interception des communications réseaux peut être envisagée.
  - Le développeur peut vérifier l'effectivité des points suivants :
    - le SDK ne procède à aucune opération de lecture et/ou d'écriture (non exemptée) avant le recueil du consentement ;
    - en cas de consentement portant sur différentes finalités, le SDK respecte les choix exprimés par la personne ;
    - le SDK ne collecte pas plus de données que défini dans le registre fourni ;
    - le SDK n'accède pas aux ressources protégées lors de l'autorisation d'accès à celles-ci pour d'autres fonctionnalités ;
    - le SDK respecte le retrait du consentement.
  - En cas d'évolution du SDK, ces analyses peuvent être mises à jour.
  - Pour mémoire, l'éditeur du SDK, en tant que sous-traitant ou sous-traitant ultérieur, a l'obligation de faciliter la tenue de tels audits.

## 6.4. Assurer la sécurité de l'application

La sécurité des traitements mis en œuvre constitue une obligation incombant au développeur qui traite des données pour le compte de l'éditeur (article 28 du RGPD). Le développeur doit, s'il est qualifié de sous-traitant, mettre en œuvre toutes les mesures pertinentes à cette fin et a minima toutes les mesures requises en vertu de l'article 32 du RGPD.

### 1. Mettre en œuvre les mesures de sécurité minimales

- **Quelles mesures de base est-il recommandé de mettre en œuvre de manière systématique ?**
  - 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[44] ;
  - 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 ;
  - Désactivation par défaut des sauvegardes sur serveur effectuées par des tiers (par exemple l'OS) ou, à défaut, chiffrement des données sans inclure la clé de chiffrement dans celles-ci ;
  - Lorsqu'une authentification est nécessaire, recours à un moyen d'authentification correspondant au niveau de sécurité recherché (par exemple, si une personne doit être authentifiée avec certitude, ne pas recourir à un moyen d'authentification biométrique si le dispositif utilisé permet l'enregistrement de gabarits biométriques de personnes différentes) ;
  - De manière générale, respect des niveaux L1 des recommandations produites par l'OWASP[45].

### 2. Adopter un modèle de sécurité adéquat

Pour mettre en œuvre les mesures pertinentes, il est indispensable que le modèle de sécurité choisi corresponde au contexte des applications mobiles.

- **Sur quels principes est-il recommandé de faire reposer son modèle de sécurité ?**
  - Eviter de faire reposer son modèle de sécurité sur l'intégrité du terminal, sauf dans certains cas justifiés. Par exemple, dans le cas des applications bancaires, il peut être justifié de chercher à attester de l'intégrité du terminal, pour éviter l'accès malveillant à des mots de passe. Dans ce cas, il est recommandé de signaler le défaut d'intégrité, sans provoquer de blocage.
  - Ne pas 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'API[46] sont recommandées pour sécuriser les serveurs utilisés par l'application et les protéger contre des éventuelles tentatives d'abus.
  - 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.

### 3. Assurer le maintien de la sécurité au cours du temps

- **Quelles mesures est-il recommandé de mettre en place pour assurer la sécurité au cours du temps ?**
  - La mise en œuvre des processus de déploiement qui assurent le maintien de la qualité des applicatifs distribués :

---

[44] « Recommandations de sécurité relatives à TLS », ssi.gouv.fr
[45] « *OWASP MAS checklist* », mas.owasp.org
[46] « [Clôturée] API : la CNIL soumet à consultation publique un projet de recommandation technique », cnil.fr

    - en adoptant une méthodologie de déploiement d'intégration continue et de déploiement continu (« CI/CD » en anglais) pour permettre des mises à jour fréquentes des applications, notamment en cas de mise à jour de sécurité ;
    - en sécurisant le déploiement de code avec une phase préalable de revue de pairs.
- Le maintien de la vigilance relative aux éléments externes intégrés dans les applications :
    - en s'assurant que les versions utilisées sont les plus récentes ;
    - en s'assurant de l'absence d'évolution malveillante dans les SDKs mis en œuvre, ou les bibliothèques utilisées via des pratiques de sécurisation de la chaîne d'approvisionnement (« *supply-chain security* »[47]). Pour minimiser la surface d'attaque possible, en utilisant au minimum des éléments fournis par des tiers.
- Le maintien à jour des versions disponibles sur les magasins d'application pour ne pas mettre en danger les utilisateurs :
    - en vérifiant s'il est nécessaire d'imposer des versions récentes des OS, en fonction de la sensibilité des données traitées, et au regard des référentiels applicable en termes d'écoconception[48]. Et, si ce choix est fait, en ne laissant à disposition en tant que reliquat (dernière version d'une application disponible pour une version de l'OS donnée) que des versions présentant un risque minimal en termes de protection des données ;
    - en analysant, en fonction des problématiques de sécurité rencontrées, s'il est nécessaire de forcer la mise à jour des applications, par exemple en bloquant certaines fonctionnalités au niveau du serveur pour les versions non sécurisées de l'application.
- Si une violation de données personnelles est avérée ou même suspectée, l'alerte au plus tôt l'éditeur pour qu'il puisse, si cela est nécessaire, notifier cette violation, au titre de l'article 28 du RGPD.
- Le respect des bonnes pratiques de conformité et de sécurité des développements informatiques, tels qu'indiqué dans le Guide RGPD de l'équipe de développement.

## 6.5. Liste de vérifications

Ces vérifications ont pour objet de guider les développeurs dans la mise en œuvre de ces recommandations et sont présentées à titre indicatif. Certaines des vérifications à effectuer peuvent correspondre à des bonnes pratiques ou recommandations et non à des obligations : en cas de doute, se référer au texte de la recommandation.

| Catégorie | Sous-Catégorie | Identifiant | Description |
|---|---|---|---|
| **Formaliser sa relation avec l'éditeur** | Identifier les responsabilités et obligations de chacun | 1.1.1 | Des instructions exhaustives et claires sur les traitements à mettre en œuvre sont fournies lors de la contractualisation, incluant la qualification de chacun des acteurs. |
| | | 1.1.2 | Un point de contact chez l'éditeur est désigné pour la validation de tout choix impactant les traitements de données personnelles. |
| | | 1.1.3 | Les données ne sont traitées que sur la base des instructions spécifiques fournies. |

[47] « Chaîne d'attaque sur les prestataires de service et les bureaux d'étude : un nouveau rapport d'analyse de la menace », ssi.gouv.fr
[48] Référentiel général d'écoconception de services numériques (RGESN) – 2024, ecoresponsable.numerique.gouv.fr

| | | | |
|---|---|---|---|
| | | 1.1.4 | Les obligations du développeur sous-traitant (article 28 RGPD) sont identifiées et mises en œuvre. |
| | Mettre en œuvre des processus de maîtrise d'œuvre agréés par les deux parties | 1.2.1 | Toute décision impactant la vie privée des utilisateurs est validée par l'éditeur par écrit, après information et conseil du développeur. |
| | | 1.2.2 | Un processus de suivi des évolutions externes pouvant impacter les traitements est mis en œuvre, processus qui inclut l'alerte de l'éditeur. |
| | | 1.2.3 | L'ensemble des éléments nécessaires à la bonne information des personnes est transmis par l'éditeur en cas de délégation de la publication dans les magasins d'applications. |
| | Identifier l'ensemble des traitements de données personnelles | 1.3.1 | Les traitements mis en œuvre par l'OS à travers l'usage de fonctionnalités qu'il met à disposition sont identifiés et validés par l'éditeur. |
| | | 1.3.2 | Les traitements mis en œuvre suite à l'intégration des SDK sont identifiés et validés par l'éditeur. Sont collectés à cette fin auprès du SDK toutes les informations nécessaires pour cette qualification (liste des données personnelles collectées et l'objet, la nature et la finalité des traitements mis en œuvre sur ces données) |
| | | 1.3.3 | Si certains traitements mis en œuvre dans ce cadre contreviennent au RGPD, l'éditeur en est immédiatement averti. |
| **Assumer son rôle de conseil envers l'éditeur** | Aider au bon respect des droits des utilisateurs | 2.1.1 | L'exercice des droits est possible simplement, par exemple au moyen d'une page intégrée dans l'application. |
| | | 2.1.2 | L'exercice des droits inclut l'ensemble des traitements mis en œuvre au sein de l'application, y compris ceux effectués par des tiers comme les SDK. |
| | | 2.1.3 | Une politique de confidentialité lisible sur support mobile est fournie par l'éditeur et intégrée au sein de l'application, de manière accessible. |
| | Proposer des développements respectant les | 2.2.1 | Des solutions techniques à l'état de l'art sont analysées et proposées à l'éditeur pour minimiser les |

| | | | |
|---|---|---|---|
| | principes de protection des données personnelles | | collectes et limiter l'impact de la mise à disposition des données aux tiers. |
| | | 2.2.2 | Les permissions demandées sont strictement nécessaires au fonctionnement de l'application. Des alternatives à l'usage de permission sont prévues. |
| | | 2.2.3 | Les données sensibles (au sens de l'article 9 du RGPD) sont distinguées des autres types de données, notamment en termes d'architecture. |
| | | 2.2.4 | Les données sensibles ne sont pas rendues accessibles aux tiers (par exemple, aux SDK). |
| | Participer à la conformité en matière de recueil du consentement | 2.3.1 | Les opérations visées par la nécessité du consentement sont identifiées et les modalités de recueil sont validées en amont avec l'éditeur. |
| | | 2.3.2 | Les consentements obtenus répondent aux exigences décrites dans la recommandation « *Cookies* et autres traceurs », adaptées pour améliorer la lisibilité sur terminal mobile. |
| | | 2.3.3 | Si une même opération est visée par un consentement et une permission, l'articulation entre ces éléments n'est pas de nature à créer de la confusion chez les utilisateurs ou mène à les solliciter excessivement. |
| **Faire bon usage des SDK** | Sélectionner le SDK selon les bons critères | 3.1.1 | Des documents permettant de déterminer l'ensemble des traitements et données collectées lors de l'intégration du SDK est mis à disposition par le fournisseur de celui-ci. |
| | | 3.1.2 | Le SDK permet de répondre aux demandes d'exercice des droits. |
| | | 3.1.3 | Les responsabilités sont qualifiées pour chacun des traitements mis en œuvre dans le cadre de l'intégration du SDK, et validées par écrit par l'éditeur. |
| | Gérer le consentement des utilisateurs | 3.2.1 | Le SDK fournit une information permettant d'assurer la bonne information sur les finalités poursuivies lors du recueil du consentement. |
| | | 3.2.2 | Le SDK permet la granularité et le retrait du consentement. |

| | | | |
|---|---|---|---|
| | | 3.2.3 | Le SDK doit permettre une configuration en faisant aucune lecture et/ou écriture avant le consentement (notamment au premier lancement de l'application). |
| | Auditer le bon fonctionnement des SDK | 3.4.1 | Le respect des engagements pris par le fournisseur du SDK est audité, avec le concours de celui-ci. |
| **Assurer la sécurité de l'application** | Mettre en œuvre les mesures de sécurité minimales | 4.1.1 | Les communications sont systématiquement encapsulées dans un canal TLS. |
| | | 4.1.2 | Les suites cryptographiques de l'OS sont utilisées, ainsi que les protections matérielles des secrets. |
| | | 4.1.3 | Les sauvegardes (notamment automatiques) sont chiffrées avec une clé conservée localement. |
| | | 4.1.4 | Le niveau L1 de l'OWASP MAS est atteint. |
| | Adopter un modèle de sécurité adéquat | 4.2.1 | Le modèle de sécurité ne repose pas sur l'intégrité du terminal. |
| | | 4.2.2 | Toute détection de défaut d'intégrité est indiquée à l'utilisateur et non utilisée pour bloquer celui-ci. |
| | | 4.2.3 | Les API intègrent des éléments permettant de sécuriser les services. |
| | | 4.2.4 | Les données personnelles sont protégées contre d'éventuels détournement internes ou par des sous-traitants. |
| | Assurer le maintien de la sécurité au cours du temps | 4.3.1 | L'application est mise à jour aussi souvent que nécessaire en termes de sécurité. |
| | | 4.3.2 | Les éventuelles évolutions malveillantes des SDK ou bibliothèques utilisées sont surveillées dans le cadre de pratiques de « *supply-chain security* ». |
| | | 4.3.3 | L'application est mise à jour en cas d'évolution de l'OS à la suite de failles de sécurité, en fonction de la sensibilité des traitements. |
| | | 4.3.4 | Toute violation de données personnelles, suspectée ou avérée est signalée à l'éditeur. |

# 7. Recommandations spécifiques au fournisseur de kits de développement logiciel (SDK)

**Comment lire cette section ?**

Cette section rappelle les obligations posées par la règlementation (par exemple, « le responsable du traitement doit ») et formulent des recommandations pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer aux obligations, mais ils doivent alors pouvoir justifier leur choix et engagent leur responsabilité. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

## Notice

### À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de kits de développement logiciel (ou SDK, pour « *software development kit* »)**, dans la suite désignés comme « fournisseurs de SDK ».
- Le fournisseur de SDK est défini ici comme **l'entité, personne physique ou morale, qui met à disposition un ou plusieurs SDK destinés à être intégrés dans des applications mobiles,** impliquant souvent des serveurs de traitement, accompagnés de documentations relatives à leur intégration chez des tiers**.**
- Les obligations, recommandations et bonnes pratiques s'appliquent à l'ensemble des fournisseurs de SDK, y compris lorsque ceux-ci endossent par ailleurs le rôle de fournisseurs d'OS ou de magasin d'application.
- Ces recommandations s'adressent plus spécialement au sein du fournisseur de SDK :
  - au délégué à la protection des données (DPD ou *Data Protection Officer – DPO*) de l'entité éditrice du SDK ;
  - aux équipes techniques en charge du développement et de la maintenance du SDK ;
  - aux équipes chargées des relations commerciales avec les partenaires (développeurs ou éditeurs), pour faciliter l'intégration et l'encadrer contractuellement.
- Ces recommandations peuvent également être consultées par d'autres acteurs de l'écosystème mobile tels que les éditeurs et développeurs d'applications, les fournisseurs de magasins d'applications ou les fournisseurs de systèmes d'exploitation.

### Quel est l'objet de ces recommandations ?

- Ces recommandations concernent les fournisseurs de SDK traitant des données personnelles, dans le cadre de la mise en œuvre du SDK par les applications mobiles qui l'intègrent. Ces données peuvent être traitées par le fournisseur pour son propre compte, pour le compte de l'éditeur de l'application mobile, ou de manière conjointe par les deux acteurs. Il est impératif que dans ces différentes configurations les rôles respectifs et qualification de chaque acteur à l'égard des traitements de données personnelles soient préalablement identifiés, en particulier du fait qu'un fournisseur de SDK peut agir tant en tant que sous-traitant qu'en tant que responsable de traitement, au sens du RGPD.
- Néanmoins, il existe également des SDK destinés à être intégrés au sein des applications mobiles et ne proposant que des fonctionnalités locales, ou n'engendrant pas de traitements distants. À ce titre, leurs fournisseurs agissent uniquement en tant que fournisseurs de logiciels et ne revêtent pas nécessairement de qualification au sens du RGPD, du fait de l'absence de mise en œuvre par eux-mêmes de traitements de données personnelles. Ils sont néanmoins encouragés à s'assurer que la conception et l'architecture du logiciel qu'ils fournissent ne fait pas obstacle ou ne complexifie pas le respect du RGPD par le responsable de traitement qui l'utilisera, et à respecter les bonnes pratiques mises en avant dans le cadre de ces recommandations.

### Comment utiliser ces recommandations ?

- Chaque section correspond à une étape dans la mise à disposition d'un SDK par un fournisseur et expose les enjeux en matière de vie privée et regroupe une série de recommandations ainsi que de bonnes pratiques à mettre en œuvre.
- Une **liste récapitulative des principales vérifications à réaliser** est proposée à la fin de cette partie. Les fournisseurs de SDK sont invités à s'y référer, notamment lors de la rédaction de leur documentation contractuelle, afin d'évaluer le niveau de prise en compte des recommandations de la CNIL par leurs partenaires.

**Voir aussi**

Les fournisseurs de SDK sont invités à consulter également les recommandations applicables aux autres acteurs, susceptibles de les concerner de manière incidente, et en particulier les :

- Recommandations spécifiques à l'éditeur
- Recommandations spécifiques au développeur

## 7.1. Concevoir son service

La prise en compte du respect de la protection des données doit commencer dès la phase de conception des SDK mis à disposition des éditeurs d'application, le cas échéant par l'intermédiaire de leurs développeurs (article 25 du RGPD).

### 1. Identifier et analyser ses obligations au regard de la réglementation applicable en matière de protection des données personnelles

Le SDK doit déterminer précisément les obligations qui lui incombent en fonction de sa qualification.

- **Quelles qualifications pour les traitements mis en œuvre par le fournisseur de SDK ?**
  - 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 se référer à la partie 4 des présentes recommandations pour caractériser l'ensemble des traitements qu'il est susceptible de mettre en œuvre dans la fourniture des SDK. Une qualification de sous-traitant ou de responsable conjoint du traitement sont notamment possibles, au regard des critères fixés dans les lignes directrices 07/20 du Comité européen de la protection des données (CEPD)[49].
  - Dans le cas où le fournisseur de SDK est responsable de traitement, ou co-responsable de traitement, celui-ci est invité à consulter et se référer également aux recommandations spécifiques à l'éditeur.

- **Quels points d'attention spécifiques ?**
  - Le recueil de données personnelles par le SDK ne doit jamais être réalisé à l'insu des personnes concernées.
  - Si le fournisseur de SDK est responsable du traitement ou responsable conjoint, il doit veiller en particulier à s'assurer de l'information des personnes concernées (voir la partie 4 des présentes recommandations).
  - Le fournisseur de SDK, s'il est responsable ou co-responsable de traitement, doit identifier si les données collectées constituent des données sensibles, au sens de l'article 9 du RGPD (voir encadré ci-dessous).
  - Le fournisseur de SDK en tant que sous-traitant doit s'assurer que le responsable de traitement a connaissance de l'existence de transferts au sens du chapitre V du RGPD[50], afin de prévoir un encadrement contractuel et/ou technique adéquat[51].

[49] Lignes directrices 07/2020 concernant les notions de responsable de traitement et de sous-traitant au sens du RGPD (PDF, 1,6 Mo), edpb.europa.eu
[50] « Transférer des données hors de l'UE », cnil.fr
[51] Voir à cet égard les lignes directrices 01/2020 du CEPD sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE (PDF, 389 ko), edpb.europa.eu

**Pour la définition de donnée sensible au sens de l'article 9 du RGPD, voir la partie 5.1 des présentes recommandations :** « Assurer la conformité des traitements de données personnelles »

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

Le fournisseur de SDK doit, pour chacun des traitements qu'il met en œuvre en tant que responsable de traitement, analyser si des mesures de protection des données personnelles dès la conception et par défaut peuvent s'appliquer. Le fournisseur doit faire cette analyse sur l'ensemble des traitements opérés par le SDK.

- **Comment minimiser les données collectées ?**
  - Le principe de minimisation doit notamment conduire à limiter les données envoyées vers des serveurs (ceux du fournisseur de SDK, comme ceux de ses partenaires) au strict nécessaire, au regard des finalités poursuivies.
  - Des configurations par défaut des SDK qui respectent ce principe doivent être proposées, y compris dans les exemples de configuration proposés dans ses documentations.
  - En particulier, la collecte ou la conservation d'identifiants de terminaux, de réseau (adresse IP, matériels réseau environnants) pouvant être reliés à des individus doivent être évités si l'usage du SDK ne le nécessite pas.
  - La CNIL invite, à titre de bonne pratique, le fournisseur de SDK à s'informer régulièrement de l'existence de fonctionnalités plus à jour pour traiter certaines informations (par exemple une localisation approximative au lieu d'une localisation précise), qui seraient plus pertinentes en termes de minimisation de données afin, le cas échéant, de mettre à jour son SDK.

- **Comment cloisonner les différents services ?**
  - Il est recommandé que le fournisseur de SDK conçoive son service, dès l'origine, de sorte à ce que ses fonctionnalités puissent être décorrélées les unes des autres et ainsi permettre une configuration simple des différentes options, notamment si les traitements relatifs à ces différentes options impliquent des responsabilités différentes.
  - Par exemple, si le fournisseur de SDK fournit des services de qualification d'audience (en tant que sous-traitant) mais également de collecte de données à des fins de reciblage pour son propre compte (en tant que responsable du traitement), la sélection indépendante de ces deux fonctionnalités par l'éditeur pourrait être permise pour l'intégration du SDK, éventuellement avec une alternative payante si ce choix impacte le modèle économique du fournisseur de SDK. Si ces fonctionnalités nécessitent le consentement de l'utilisateur, cette décorrélation technique est nécessaire.
  - Dans cette même logique, la CNIL recommande au fournisseur de SDK d'éviter autant que possible de regrouper tous les services et fonctionnalités proposés au sein d'un même SDK, afin de permettre à l'éditeur d'utiliser uniquement le SDK qui lui est utile. Alternativement, le SDK peut être conçu de façon modulaire, afin que seuls les éléments correspondant aux fonctionnalités réellement utilisées soient intégrés dans l'application, ce qui contribue à limiter la présence de vulnérabilités éventuelles.

- **Quelles permissions système pour quels traitements ?**
  - Lors de la conception, le fournisseur de SDK doit analyser les permissions système utiles, en distinguant celles qui sont strictement nécessaires et celles qui sont souhaitées mais non indispensables, car elles simplifient l'expérience utilisateur mais ne sont pas essentielles à la fonctionnalité recherchée. Par exemple, un module d'assistant conversationnel peut souhaiter disposer d'une entrée vocale, qui nécessite les permissions d'accès au micro, mais ne doit pas imposer l'acceptation de cette permission pour fonctionner.
  - La CNIL recommande au fournisseur de veiller à choisir le niveau de permission le moins intrusif possible, ou de proposer différentes configurations au choix de l'utilisateur.
  - Le fournisseur de SDK doit également distinguer les permissions relatives au service rendu à l'application des permissions et traitements de données subséquents qu'il réalise pour son propre compte et qui sont parfois liés à son modèle économique.
  - Il est recommandé que le SDK soit le moins dépendant possible de l'obtention des permissions, notamment en étudiant l'usage d'alternatives telles que présenté dans la partie 5.5 des présentes recommandations (« Permissions et protection des données dès la conception »), que

ces alternatives soient à la main des utilisateurs directs (éditeurs ou développeurs) ou de l'utilisateur de l'application.

## 7.2. Documenter les bonnes informations

Le fournisseur de SDK doit fournir à ses partenaires (éditeur, développeur) la documentation nécessaire pour que ces derniers puissent assurer leur conformité. Dès lors qu'il agit en tant que responsable du traitement, il doit en outre documenter sa conformité.

### 1. Identifier les informations à fournir

- **Quelles informations documenter sur les traitements mis en œuvre ?**
  - La CNIL recommande que le fournisseur de SDK rédige et mette à disposition de ses clients une analyse des traitements qu'implique l'utilisation du SDK, que le fournisseur se contente de fournir le logiciel ou joue un rôle opérationnel dans la mise en œuvre concrète des traitements. La fourniture de ces informations permettra notamment à l'éditeur de répondre précisément aux impératifs des magasins d'applications, prérequis à la publication d'une nouvelle application ou de sa mise à jour sur le magasin.
  - Dès lors qu'un traitement mis en œuvre par le fournisseur de SDK est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, le fournisseur de SDK a l'obligation de rédiger une AIPD (voir article 35 du RGPD).
  - Pour chaque traitement, il doit identifier sa qualification au sens du RGPD.
    - La CNIL recommande que cette qualification soit définie en lien avec ses partenaires.
    - Selon cette qualification, lorsqu'il est responsable de traitement, le fournisseur de SDK doit tenir et maintenir son propre registre des activités de traitement, conformément à l'article 30 du RGPD ;
  - S'il agit en tant que sous-traitant et qu'un traitement implique le recours à un tiers sous-traitant ultérieur, il doit obtenir l'autorisation du responsable de traitement et s'assurer que les mêmes obligations en matière de protection des données qui lui incombent au titre du contrat passé avec le responsable de traitement, sont imposées à ce sous-traitant ultérieur, par contrat ou tout autre acte juridique (article 28 du RGPD).

- **Quelles informations documenter sur les usages de traceurs ?**
  - Le fournisseur de SDK doit informer précisément ses partenaires, soit le responsable du traitement si le fournisseur agit comme sous-traitant, soit d'éventuels autres responsables de traitements conjoints, des opérations de lecture et/ou écriture sur le terminal de l'utilisateur (il peut pour cela se référer aux recommandations spécifiques au développeur pour l'identification de telles occurrences).
  - Il doit indiquer les finalités poursuivies par chacun de ces usages de traceurs. S'il n'est ni responsable du traitement, ni sous-traitant, la CNIL invite, à titre de bonne pratique, le fournisseur de SDK à documenter les fonctionnalités comprenant des traceurs, pour permettre aux différents acteurs de répondre à leurs obligations éventuelles.

- **Quelles informations documenter sur les permissions ?**
  - Le fournisseur de SDK doit informer ses partenaires, soit le responsable du traitement si le fournisseur agit comme sous-traitant, soit d'éventuels autres responsables de traitements conjoints, des permissions requises par le SDK.
  - Pour chaque permission demandée, il doit indiquer en particulier si elle est associée à une opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés, susceptible de requérir un consentement spécifique de l'utilisateur.
  - Il est recommandé qu'il précise la nature optionnelle ou obligatoire de ces opérations selon les fonctionnalités proposées.

### 2. Présenter ces informations dans un format accessible

Ces informations peuvent idéalement être mises à disposition sous un format accessible et un formalisme facilitant leur analyse, quels que soient les paramétrages relatifs aux traitements mis en œuvre.

- **Quelles modalités de mise à disposition ?**
  - Le fournisseur de SDK doit s'assurer que les informations nécessaires (mentionnées ci-dessus) sont à jour et facilement accessibles par l'ensemble de ses partenaires, afin de leur permettre de répondre à leurs propres obligations.
  - Certaines de ces informations, s'agissant notamment des qualifications et obligations respectives des parties au sens du RGPD et du recueil des éventuels consentements, doivent être formalisées dans la documentation contractuelle.
  - La CNIL recommande que toute évolution du service impactant les questions de vie privée soit mis à disposition des partenaires du fournisseur de SDK et leur soit être expressément indiquée. Si le fournisseur de SDK est sous-traitant, ces évolutions doivent également être approuvées par le responsable de traitement avant leur mise en œuvre.

- **Quel formalisme adopter ?**
  - L'article 30 du RGPD rend obligatoire, pour les responsables de traitement (voir alinéa 1) ou pour les sous-traitants (voir alinéa 2) dont les effectifs comportent plus de 250 employés (voir aliéna 5), la tenue d'un registre de traitement, qui doit notamment comprendre :
    - Ce registre doit bien séparer chacun des traitements mis en œuvre, un traitement se définissant par sa finalité. Si des traitements dépendent des paramètres choisis, il est recommandé de mettre à disposition des partenaires un registre dynamique en fonction du paramétrage du SDK. À défaut, les paramètres liés à chaque traitement devraient être indiqués pour que les partenaires puissent comprendre quels traitements sont mis en œuvre dans le cadre de leur configuration particulière.
    - Pour chaque traitement, les données collectées doivent être explicitement indiquées. Pour faciliter la lecture et l'analyse, il est recommandé de choisir un format permettant une manipulation aisée des informations, par exemple via un fichier de tableur (permettant ainsi facilement d'identifier l'ensemble des traitements relatifs à une donnée).
    - Pour chaque traitement, il est obligatoire d'indiquer également la base légale identifiée et les obligations qui en découlent.
    - La CNIL suggère à titre de bonne pratique que le registre soit conçu de manière à pouvoir en extraire les informations utiles pour les partenaires du fournisseur de SDK, en identifiant notamment ce qui relève du secret des affaires.
  - A titre de bonne pratique, lorsqu'il est responsable ou responsable conjoint du traitement pour ces opérations, le fournisseur de SDK est encouragé à documenter les opérations de lecture et/ou d'écriture qu'il met en œuvre. Il peut par exemple présenter ces informations dans un tableau facilement lisible :
    - indiquant, pour chaque ligne, l'opération effectuée, la permission associée, les finalités poursuivies (et potentiellement la ligne du registre correspondante) ainsi que les moyens techniques permettant de bloquer ou d'activer cette lecture (afin de faciliter la mise en œuvre d'outils de gestion du consentement par les partenaires) ;
    - proposant, pour chaque ligne, des exemples de formulations pouvant être utilisées par le responsable du traitement pour informer les utilisateurs lors du recueil des consentements ;
    - documentant les versions du SDK qui recourent à chaque ligne, pour permettre aux partenaires de choisir la version adaptée et de comprendre les effets d'une éventuelle mise à jour du SDK qu'ils ont intégré.

## 7.3. Gérer le consentement et les droits des personnes

En tant que sous-traitant, le fournisseur de SDK peut avoir un fort impact quant au respect des droits des personnes, notamment en facilitant l'exercice des droits et en concevant des dispositifs facilitant le recueil du consentement.

### 1. Aider au bon exercice des droits des utilisateurs

Lorsqu'il est soumis au RGPD, et selon sa qualification, le fournisseur de SDK est tenu de répondre directement aux demandes d'exercice des droits (en tant que responsable du traitement), ou d'assister le responsable du traitement pour y répondre (en tant que sous-traitant).

- **Comment assurer l'information des personnes concernées sur les traitements de données personnelles liés au SDK ?**
  - Si le fournisseur de SDK est responsable de traitement ou responsable conjoint, il a l'obligation d'assurer l'information des personnes. Il est recommandé que cette information soit directement intégrée dans l'information fournie par l'éditeur à l'utilisateur.
  - En particulier, la transmission de données personnelles des utilisateurs à des partenaires commerciaux, par exemple à des fins de monétisation de l'application, doit être explicitement portée à la connaissance des personnes. Si les traitements en question nécessitent le consentement, les informations données doivent être de nature à permettre aux personnes concernées d'apprécier les conséquences de leur choix en les informant de l'étendue de celle-ci. La CNIL recommande de mettre en évidence, auprès des personnes concernées, le nombre et le secteur d'activité des partenaires qui seraient rendus destinataires des données.
  - La CNIL recommande que le fournisseur de SDK inclue dans son contrat avec l'éditeur ou le développeur, l'obligation pour ces derniers de procéder à l'information sur ses propres traitements.
  - Il en va de même de l'information devant accompagner une demande de consentement pour les traitements dont le fournisseur de SDK est responsable.
  - Le cas échéant, le fournisseur de SDK peut proposer un composant logiciel d'interface (type CMP) pouvant également être intégré dans l'application et permettant la collecte du consentement de l'utilisateur pour ces finalités peut être proposé.
  - Il est recommandé que le fournisseur de SDK surveille les évolutions des politiques de confidentialité des données des partenaires, pour s'assurer que les traitements mentionnés dans celles-ci correspondent bien aux traitements effectivement mis en œuvre. S'il est sous-traitant et qu'il constate qu'une information est manquante ou trop générale, la CNIL recommande de le signaler au responsable de traitement, au titre de l'article 28 alinéa 3 du RGPD.

- **Comment s'assurer que les utilisateurs puissent facilement exercer leurs droits ?**
  - L'exercice des droits est susceptible de concerner des traitements sous la responsabilité de l'éditeur de l'application. Le fournisseur de SDK, s'il est sous-traitant, a une obligation d'aide à la conformité vis-à-vis du responsable de traitement, dont le contenu dépend des fonctions qui lui sont confiées contractuellement. L'exercice des droits peut aussi concerner les traitements sous la responsabilité propre du fournisseur de SDK, qui doit alors pleinement en charge d'assurer le respect des droits ouverts aux personnes par le RGPD.
  - L'exercice des droits doit être pensé dès la conception, notamment en termes de structuration des bases de données. Le droit de suppression, notamment, doit pouvoir être respecté indépendamment des contraintes techniques.
  - En particulier, en cas de transmission de données personnelles des utilisateurs à des partenaires commerciaux, par exemple à des fins de monétisation de l'application, le fournisseur de SDK doit porter une attention particulière pour rendre possible l'exercice des droits applicables.
  - Pour faciliter la mise en œuvre pratique de l'exercice des droits, la CNIL recommande que la possibilité de l'automatiser soit analysée, notamment au moyen d'API intégrables au sein des applications ou au niveau du serveur des clients.
  - Dans ce cas, le fournisseur de SDK est invité à utiliser le moins d'identifiants additionnels possible pour traiter l'exercice de ces droits. Par exemple, si des données sont associées à la personne sur la simple base d'un identifiant publicitaire, celui-ci pourrait suffire pour permettre l'exercice des droits de la personne. À l'inverse, au regard de l'article 11 du RGPD, il est possible qu'une demande d'exercice des droits ne puisse pas recevoir de réponse effective. Par exemple,

dans le cas où la personne aurait réinitialisé son identifiant publicitaire et n'aurait plus connaissance du ou des précédents identifiants, une collecte d'information supplémentaire peut être nécessaire à l'identification de la personne.

## 2. Participer à la conformité en matière d'usage de traceurs et de recueil du consentement

Si la qualification du fournisseur de SDK est celle de sous-traitant au sens du RGPD, la CNIL recommande que celui-ci fournisse au responsable de traitement des conseils pratiques, notamment sur l'éventuelle nécessité de recueillir le consentement, de fournir les moyens techniques pour permettre la bonne prise en compte de celui-ci, ainsi que son retrait. Les cas dans lesquels le consentement est requis soit au titre de l'article 82 de la loi Informatique et Libertés, soit au titre du RGPD sont rappelés en partie 5.1 des présentes recommandations : « Assurer la conformité juridique des traitements ».

- **Les permissions accordées par l'utilisateur à l'application peuvent-elles être exploitées pour le recueil du consentement aux traitements effectués par le SDK ?**
  - 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. En particulier, si une permission est accordée à l'application pour une finalité distincte de celle du SDK, il n'est pas possible de considérer que cette permission comme un consentement valide de la personne concernée.

- **Comment permettre un recueil de consentement valide ?**
  - La CNIL recommande que des moyens techniques et organisationnels, permettant le blocage de tout traitement ou accès à des données stockées sur le terminal (ou permissions système le permettant) soit proposés, et ce jusqu'à ce qu'un consentement valable soit recueilli. Il est à ce titre recommandé que le fournisseur prévoie que son SDK puisse suspendre son exécution tant qu'un consentement n'a pas été obtenu.
  - 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 finalité).
  - À ce titre, si le traitement poursuit plusieurs finalités distinctes, les signaux relatifs au consentement de l'utilisateur doivent être pris en compte dans leur granularité, finalité par finalité, indépendamment du statut des permissions demandées.
  - Pour chacun des consentements recherchés, il est recommandé que la conception et la documentation du SDK prévoient la possibilité et anticipent les impacts fonctionnels d'une d'absence de consentement de l'utilisateur, afin de minimiser tout blocage non nécessaire de fonctionnalités en cas de refus.
  - La révocation du consentement pour ces finalités doit correctement être prise en compte après que celui-ci ait été initialement accordé. A ce titre, la CNIL recommande que fournisseur de SDK s'assure que la révocation n'entraîne pas une instabilité d'exécution de l'application ni ne provoque une demande constante de la permission révoquée, ce qui remettrait en cause la liberté du consentement.

- **Quelles meilleures pratiques mettre en œuvre ?**
  - Le fournisseur de SDK est invité à veiller à limiter au maximum l'usage de permissions en bloc à l'installation (« *install-time permissions* »), en préférant l'usage de permissions déclenchables durant le fonctionnement de l'application (« *runtime permissions* »), afin de faciliter l'éventuelle intégration aux outils de recueil de l'éditeur d'application et, lorsque cela est justifié, de manière à contextualiser les demandes de consentement. Ainsi, si la fonctionnalité en question n'est jamais utilisée, la permission relative ne devrait pas être affichée. La CNIL souligne que, dans certains cas, 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 configurer les traitements de données dans le sens le plus protecteur de la vie privée (*privacy by-design,* art. 25 du RGPD).

## 7.4. Participer au maintien de la conformité de l'application au cours du temps

Le fournisseur de SDK, lorsqu'il est qualifié de sous-traitant, doit participer à la mise en œuvre et au maintien de la conformité de l'application au cours du temps, en fournissant des éléments sécurisés, mais également en accompagnant la conformité des applications qui utilisent ses produits.

### 1. Proposer des SDK sécurisés

En tant que sous-traitant au sens du RGPD, le fournisseur de SDK est soumis aux mêmes exigences en termes de sécurité que les autres acteurs fournissant des éléments exécutables, tels que le développeur externe d'une application. Dans les cas où le fournisseur de SDK est simple fournisseur de logiciel, il est encouragé à suivre ces recommandations, à titre de bonne pratique.

- **Quelles mesures de sécurité mettre en œuvre ?**
  - Voir recommandations émises dans la partie 6.4 des présentes recommandations : « Assurer la sécurité de l'application ».

### 2. Permettre la réalisation d'audits

Dans le cas où la qualification du fournisseur de SDK au sens du RGPD est celle de sous-traitant, le contrat ou l'acte juridique qui encadre la sous-traitance doit prévoir l'obligation pour celui-ci de permettre la réalisation d'audits (article 28.3.h du RGPD).

- **Comment faciliter la tenue d'audits ?**
  - Pour faciliter la réalisation de tels audits, le SDK sous-traitant doit tenir à la disposition de son client toutes les informations nécessaires pour démontrer le respect de ses obligations au titre de l'article 28 du RGPD (ainsi que celui de ses sous-traitants ultérieurs éventuels), dont une documentation technique à jour (voir ci-dessus).
  - Il est recommandé au fournisseur de SDK de faire réaliser, régulièrement et à son initiative, des audits sur son SDK afin d'anticiper et de prévenir des problèmes qui pourraient être identifiés par la suite par ses partenaires, responsables ou responsables conjoints de traitements, ou par les autorités de contrôle.
  - A titre de bonne pratique, il est recommandé aux SDK de proposer une fonctionnalité de désactivation facilement actionnable par l'éditeur, à distance et en production, dans le cas où à la suite d'un audit, d'une incertitude juridique, d'un dysfonctionnement ou de tout autre événement, l'éditeur souhaiterait mettre en pause uniquement les traitements du SDK le temps de résoudre le problème, sans avoir à rendre l'ensemble de son application inopérante.

### 3. Mettre en place des processus robustes en termes de conformité

Le maintien de la conformité du SDK se conçoit dans le temps, en prévoyant des processus pour mettre à jour en fonction de l'évolution des conditions de mise en œuvre.

- **Quelles mesures mettre en place pour assurer la sécurité au cours du temps ?**
  - La CNIL recommande que des outils et méthodologies de signalement de vulnérabilité, en cas d'exploitation avérée de celle-ci, soient mises en place. En tant que sous-traitant, le fournisseur de SDK est tenu d'informer son responsable de traitement de manière à lui permettre de respecter ses obligations en matière de sécurité des données personnelles (articles 32 à 36 du RGPD).
  - En cas de violation de données personnelles au sens de la définition de l'article 4 du RGPD, le fournisseur de SDK qui est responsable oou responsable conjoint du traitement concerné doit notifier lui-même la violation de données à l'autorité du pays dont l'entité dépend ou s'assurer que(articles 33 et 34 du RGPD) ou s'assurer que cette notification a été effectuée par son responsable conjoint, le cas échéant.

- **Comment prendre en compte les éventuelles évolutions de ses partenaires ?**
  - Le fournisseur de SDK est également invité à surveiller les évolutions techniques des API proposées par les systèmes d'exploitation. En effet, il est fréquent que des mises à jour de l'OS entraînent des modifications du fonctionnement de certaines méthodes, ce qui peut avoir des impacts sur la protection de la vie privée. La CNIL considère comme une bonne pratique pour le fournisseur de mettre à jour son SDK en fonction des évolutions techniques de l'OS, notamment en étudiant si ces évolutions peuvent permettre de mettre en œuvre les traitements

d'une manière plus respectueuse de la vie privée. Si c'est le cas, il est invité à mettre à jour et encourager l'utilisation des versions les plus récentes de son outil.

## 7.5. Liste de vérifications

Ces vérifications ont pour objet de guider les fournisseurs de SDK dans la mise en œuvre de ces recommandations et sont présentées à titre indicatif. Certaines des vérifications à effectuer peuvent correspondre à des bonnes pratiques ou recommandations et non à des obligations : en cas de doute, se référer au texte de la recommandation.

| Catégorie | Sous-Catégorie | Identifiant | Description |
|---|---|---|---|
| **Concevoir son service** | Identifier et analyser ses obligations au regard de la réglementation applicable en matière de protection des données personnelles | 1.1.1 | Une qualification au sens du RGPD (responsable de traitement, responsable de traitement conjoint ou sous-traitant) est définie pour chaque traitement de données à caractère personnel opéré par le SDK. |
| | | 1.1.2 | Les données sensibles (au sens de l'article 9 du RGPD) sont identifiées et leur traitement modifié en conséquence. |
| | Appliquer les principes de protection des données dès la conception et par défaut | 1.2.1 | Les données collectées par le SDK ainsi que celles transmises aux partenaires sont minimisées. |
| | | 1.2.2 | Les différentes fonctionnalités proposées par le SDK peuvent être intégrées et exécutées de manière décorrélée, en particulier si elles n'impliquent pas toutes les mêmes responsabilités ou finalités. |
| | | 1.2.3 | Plutôt que de regrouper plusieurs fonctionnalités différentes au sein d'un même SDK, celles-ci sont scindées en plusieurs SDK distincts. |
| | | 1.2.4 | Les permissions requises pour l'exécution du SDK sont minimisées, en distinguant celles strictement nécessaires de celles souhaitées mais non indispensables. |
| | | 1.2.5 | Lorsque plusieurs permissions peuvent autoriser la collecte d'une donnée sous sa forme souhaitée, le choix est porté sur celles aux capacités techniques les moins intrusives. |
| **Documenter les bonnes informations** | Identifier les informations à rassembler | 2.1.1 | Une analyse claire des traitements entraînés par l'utilisation du SDK est réalisée et accessible. |
| | | 2.1.2 | Pour chaque traitement, la qualification des acteurs, au sens du RGPD, est identifiée. |
| | | 2.1.3 | Pour chaque traitement impliquant le recours à un sous-traitant ultérieur, l'analyse des finalités est effectuée et l'autorisation du responsable de traitement est obtenue. |

| | | | |
|---|---|---|---|
| | | 2.1.4 | La présence de traceurs mettant en œuvre une lecture ou une écriture sur le terminal de l'utilisateur final est indiquée précisément et explicitement, en explicitant les finalités poursuivies. |
| | | 2.1.5 | Le caractère optionnel ou obligatoire pour chacune des permissions requises par le SDK est indiqué, en fonction des fonctionnalités utilisées. |
| | Présenter ces informations dans un format accessible | 2.2.1 | Les documentations et informations précitées sont à jour. |
| | | 2.2.2 | Les informations précitées sont formalisées dans la documentation contractuelle lorsqu'elles doivent l'être. |
| | | 2.2.3 | Une information spécifique est délivrée lorsque les mises à jour du SDK impliquent une évolution des traitements mis en œuvre. |
| | | 2.2.4 | Le registre des traitements distingue clairement les finalités associées à chaque traitement. |
| | | 2.2.5 | Si les finalités poursuivies dépendent du paramétrage du SDK, un registre dynamique ou distinct est mis à disposition, en fonction des possibilités de paramétrage du SDK, de sorte que le responsable de traitement puisse facilement identifier les éléments du registre qui correspondent à son paramétrage. |
| | | 2.2.6 | Le format du registre, par exemple sous forme de tableau, permet d'identifier facilement et de manière exhaustive chaque donnée collectée, ainsi que les éléments juridiques (base légale, finalité, obligations) et techniques (lectures, écritures) associés. |
| | | 2.2.7 | Des exemples de formulation relatives aux traitements effectués sont directement proposés, de sorte qu'un tiers partenaire puisse facilement les réutiliser pour ses propres recueils de consentements. |
| **Gérer le consentement et les droits des personnes** | Aider au bon exercice des droits des utilisateurs | 3.1.1 | Des API sont mises à la disposition des tiers partenaires, lorsqu'ils reçoivent des demandes d'exercices de droits, de sorte que ces demandes puissent être répercutées de manière automatique dans les infrastructures techniques du SDK. |
| | | 3.1.2 | La mise en place de ces API n'utilise pas, ou le moins possible, d'identifiants additionnels, afin que ces demandes de droit puissent recevoir une réponse effective. |
| | Participer à la conformité en termes d'usage de traceurs et de recueil du consentement | 3.2.1 | La seule obtention d'une permission ne peut être considérée comme indiquant que le consentement a été valablement recueilli pour les traitements effectués par le SDK |
| | | 3.2.2 | Le SDK est conçu techniquement pour permettre une suspension de son exécution |

| | | | |
|---|---|---|---|
| | | | tant qu'un consentement valable, par finalité, n'est pas recueilli. |
| | | 3.2.3 | Si plusieurs finalités sont poursuivies, le SDK permet techniquement la prise en compte d'un signal distinct par finalité, toujours indépendamment des permissions système. |
| | | 3.2.4 | Des alternatives sont proposées aux tiers partenaires dans le cas d'un refus de l'utilisateur final, afin de ne pas altérer la bonne exécution de l'application intégrant le SDK. |
| | | 3.2.5 | La révocation d'un consentement n'altère pas la bonne exécution de l'application du tiers partenaire, tant fonctionnellement que vis-à-vis l'expérience utilisateur (telle qu'une demande de consentement affichée en boucle). |
| | | 3.2.6 | Les demandes de permissions système s'effectuent pendant l'exécution de l'application plutôt que lors de son installation, lorsque cela est possible. |
| **Participer au maintien de la conformité au cours du temps** | Proposer des SDK sécurisés | 4.1.1 | Se référer aux points 4.1.1-4.3.4 de la liste de vérifications relative aux développeurs. |
| | Permettre la réalisation d'audits | 4.2.1 | Des rapports d'audits du SDK sont réalisés régulièrement et sont tenus à disposition des éditeurs partenaires et des autorités de protection des données qui en feraient la demande. |
| | | 4.2.2 | Le SDK peut être mis en pause par l'éditeur, à distance et en production, dans le cas où le résultat d'un audit entrainerait une incertitude juridique ou un dysfonctionnement technique. |
| | Mettre en place des processus robustes en termes de conformité | 4.3.1 | Un processus technique et organisationnel relatif aux éventuelles violations de données est établi, qui prévoit la transmission d'informations aux responsables de traitement ainsi que le formalisme des notifications de violation aux autorités de protection des données. |
| | | 4.3.2 | Une veille régulière est appliquée sur les évolutions techniques des systèmes d'exploitation mobiles et des API qu'ils mettent à disposition, afin de renforcer les principes de protection dès la conception et de protection par défaut. |

# 8. Recommandations spécifiques au fournisseur de système d'exploitation (OS)

**Comment lire cette section ?**

Cette section comprend des éléments qui sont formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »). Elle rappelle également les obligations posées par la règlementation (par exemple, « le responsable du traitement doit ») et formulent des recommandations pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer aux obligations, mais ils doivent alors pouvoir justifier leur choix et engagent leur responsabilité. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

## Notice

### À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de systèmes d'exploitation (ou OS, pour *operating system*)** désignés comme « fournisseurs d'OS ».
- Le fournisseur d'OS est défini comme **l'entité qui met à disposition un système d'exploitation sur un terminal.**
- Il est possible que le système d'exploitation soit, en fonction des situations :
  - développé dans son intégralité par une entité pour usage exclusif sur des terminaux qu'elle met à disposition (par exemple iOS, développé par Apple) ;
  - développé dans son intégralité par une entité pour usage sous licence sur des terminaux produits par des tiers (par exemple Android, développé par Google) ;
  - basé sur un OS préexistant dont la licence permet la réutilisation, qui est ensuite modifié par une entité (selon un processus de branchement, ou « *fork* »), pour usage sur ses propres terminaux ou pour mise à disposition des utilisateurs finaux des terminaux (par exemple LineageOS, basé sur Android Open Source Project et développé par LineageOS LLC).
- Ces recommandations ne visent pas à couvrir les obligations qui s'appliquent au fournisseur d'OS, appréhendé en tant qu'éditeur d'application, ni en tant que fournisseur de SDK. **Le fournisseur d'OS également éditeur des applications systèmes (préinstallées ou non sur le terminal de l'utilisateur) ou fournisseur de SDK se voit appliquer à ce titre les mêmes qualifications et obligations que n'importe quel éditeur d'applications ou fournisseur de SDK,** respectivement. Il se réfère à cet effet aux recommandations applicables à ces acteurs.
- Ces recommandations s'adressent plus spécialement au sein de l'éditeur d'OS :
  - au délégué à la protection des données (DPD ou *Data Protection Officer – DPO*) ;
  - aux développeurs et juristes des entités qui fournissent ces OS.
- Ces recommandations peuvent également être consultées par d'autres acteurs de l'écosystème mobile : éditeurs et développeurs d'applications, fournisseurs de magasins d'applications, de kits de développement logiciel (SDK), etc.

### Quel est l'objet de ces recommandations ?

- Les fournisseurs d'OS sont souvent amenés à traiter des données personnelles dans le cadre du fonctionnement normal du terminal et des applications exécutées par l'utilisateur. À ce titre, les fonctionnalités des API qu'ils mettent à disposition des applications jouent un rôle majeur dans la capacité des éditeurs d'applications à proposer des contenus conformes aux règles applicables en matière de protection des données. **La CNIL encourage les fournisseurs d'OS à permettre des configurations facilitant la conformité des applications.**

- De plus, dans le cadre de la publication d'un OS sous une licence permettant sa réutilisation et dont le code source est accessible, les choix de conception sont susceptibles d'être répercutés, à l'identique ou sous une forme proche, par l'ensemble des acteurs réutilisant le code source publié. A titre de bonne pratique, des mesures de protection de la vie privée dès la conception (« *privacy by design* ») peuvent être mises en œuvre par les fournisseurs d'OS afin que l'ensemble des acteurs de la chaîne réutilisant le code puissent en bénéficier et, *in fine*, améliorer la protection de la vie privée des utilisateurs finaux de ces OS.
- Certains fournisseurs font le choix d'intégrer dans leur OS un ensemble d'applicatifs tiers. Ces choix technologiques impliquent de nombreux traitements de données qu'ils doivent identifier, tant par les conséquences sur les personnes que pour les qualifications juridiques qui en découlent au sens du RGPD.

### Comment utiliser ces recommandations ?

- Chaque section correspond à une étape dans la mise à disposition d'un OS par un constructeur lui-même, à destination d'autres constructeurs ou directement à destination d'utilisateurs finaux et expose les enjeux en termes de vie privée et regroupe une série de recommandations, ainsi que de bonnes pratiques à mettre en œuvre.
- Ces recommandations s'appliquent sans préjudice des règles applicables sur d'autres fondements juridiques que la protection des données personnelles, notamment le droit de la concurrence.
- Une **liste récapitulative des principales vérifications à réaliser** est proposée à la fin de cette partie. Les fournisseurs d'OS sont invités à s'y référer, notamment lors de la rédaction de leur documentation contractuelle.

## 8.1. Assurer la conformité des traitements de données personnelles mis en œuvre

Bien que le rôle de l'OS soit de fournir des fonctionnalités à l'usage des développeurs d'applications, il est possible que certains traitements de données personnelles soient mis en œuvre de son propre fait. À ce titre, le fournisseur d'OS doit répondre aux obligations concernant ces traitements.

### 1. Déterminer la part du fournisseur d'OS dans la conformité des traitements de données personnelles mis en œuvre

La première étape est la bonne identification des entités concernées ainsi que des traitements effectivement mis en œuvre.

- **Quelles entités peuvent participer à la mise en œuvre de traitements de données personnelles dans un OS ?**
  - L'OS n'étant pas forcément fourni dans son intégralité par une seule entité, chaque fournisseur doit mener une analyse de ses responsabilités, qui vont dépendre de la fourniture effective de briques fonctionnelles et de traitements utilisés par les applications et les personnes.
  - Cette analyse doit être effectuée lorsque le fournisseur d'OS détermine « *les finalités et les moyens du traitement* » (article 4.7 du RGPD), et est donc responsable du traitement opéré par un élément mis à disposition par lui.
  - Cela peut être le cas, selon une analyse à mener au cas par cas, quelle que soit la configuration de l'OS (voir la partie 2 des présentes recommandations « Quels sont les professionnels évoluant dans le secteur des applications mobiles ? ») :
    - s'il s'agit d'une entité développant et mettant à disposition un OS prévu pour être exécuté (uniquement ou majoritairement) sur ses propres terminaux ;
    - s'il s'agit d'une entité réutilisant des briques logicielles tierces pour son propre compte, afin de proposer un nouvel OS, par exemple destiné à être utilisé sur ses propres terminaux ;
    - s'il s'agit d'une entité développant et mettant à disposition un OS prévu pour être exécuté sur des terminaux tiers, dès lors que cette exécution met en œuvre des traitements pour son propre compte.

- **Quels traitements de données personnelles peuvent être concernés ?**

- La question des traitements pouvant emporter la responsabilité du fournisseur d'OS est détaillée dans la partie 4 des présentes recommandations, en particulier « Qualification du fournisseur du système d'exploitation ». Quand l'OS se limite à fournir des outils logiciel dont les traitements sont cantonnés au terminal, il n'est a priori ni responsable de traitement ni sous-traitant au sens du RGPD.
- Les traitements concernés peuvent être liés à des fonctions mises en œuvre dans différents contextes, par exemple :
  - le traitement de données relative à l'utilisation de capteurs (par exemple pré-traitement des données de localisation) ;
  - le traitement de données relative à la fourniture de fonctionnalités aux applications (par exemple, services de notification, de gestion de terminaison inopinée, dite « *crash* », et de sauvegardes distantes) ;
  - le traitement de données propre à l'OS (par exemple télémétrie et remontée de rapports de bogues).

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

Il est recommandé, pour chacun des traitements envisagés, d'analyser si des mesures de protection des données dès la conception et par défaut peuvent s'appliquer.

- **Le paramétrage par défaut de l'OS est-il le moins intrusif possible ?**
  - Le fournisseur d'OS doit vérifier qu'aucun traitement effectué pour son propre compte nécessitant le consentement de l'utilisateur et qu'aucune opération de lecture ou écriture sur le terminal non exemptée de consentement ne surviennent avant le recueil d'un consentement valable au titre du RGPD et de la loi Informatique et Libertés.
  - Il doit s'assurer que ce consentement est recueilli de manière spécifique et distincte de la validation des conditions d'utilisation du terminal. Lorsque les finalités pour lesquelles le consentement est requis ne sont pas strictement nécessaires à l'utilisation du terminal, il doit indiquer clairement à l'utilisateur le caractère facultatif du consentement pour ces finalités.
  - Il est recommandé que le fournisseur d'OS permette que l'utilisateur puisse utiliser son terminal, et notamment les applications par défaut ou celles installées par ses propres moyens, sans qu'une création de compte ne soit nécessaire. Il est recommandé d'éviter les schémas d'information trompeurs (« *dark patterns* ») destinés à l'inciter à créer un compte pour utiliser son terminal si ce n'est pas nécessaire[52].
- **Comment minimiser les données traitées par l'OS en tant que responsable de traitement ?**
  - Concernant la transmission des notifications aux utilisateurs de l'application, le fournisseur d'OS est invité, à titre de bonne pratique :
    - à permettre l'usage de serveurs de notifications tiers, en optimisant leur usage de manière à minimiser l'impact sur les capacités du terminal, par exemple en termes de batterie ;
    - à proposer aux développeurs, pour améliorer la confidentialité des données des utilisateurs, des outils à jour permettant un chiffrement des données contenues dans les notifications, quel que soit le système en charge de les transmettre. À ce titre, il peut indiquer clairement les modalités d'usage de ces outils dans la documentation à destination des développeurs.
  - Concernant la télémétrie et la remontée de bogues :
    - le fournisseur d'OS est invité à proposer un système de remontée de bogues et de gestion de terminaison inopinée (« *crash* ») qui n'implique pas de nouveaux traitements de données, en particulier vers des tiers ou vers lui-même : dans l'idéal, seul l'éditeur et ses sous-traitants ont accès aux données de remontées de bogues et de terminaison ;

[52] Voir à cet égard la décision n° SAN-2019-001 du 21 janv. 2019 de la CNIL.

        - il lui est recommandé de permettre aux éditeurs et aux tiers, d'obtenir le recueil d'un consentement (dès lors que celui-ci est nécessaire) des utilisateurs préalablement à chaque remontée de ces données ou à leur transmission à des tiers.
    - Concernant le stockage distant des sauvegardes :
        - il doit s'assurer que celles-ci ne sont opérées qu'à la suite d'une demande explicite de l'application et non par défaut ;
        - il est invité à permettre un chiffrement de celles-ci, de préférence par défaut, avec une clef qui ne soit pas accessible au fournisseur de l'OS lui-même.
    - Concernant le pré-traitement des données de localisation :
        - le fournisseur d'OS est invité à permettre à l'application faisant usage des données de localisation, ainsi qu'à l'utilisateur, de facilement limiter l'usage de la localisation à la seule donnée du capteur GPS, sans qu'il soit nécessaire de mobiliser d'autres services et capteurs tels que les connexions Wi-Fi ou Bluetooth environnantes.
        - pour le service de localisation fondé sur des connexions environnantes, un mode de calcul de la localisation précise sur le terminal et non sur le serveur doit être privilégié : à titre d'exemple et de bonne pratique, le terminal peut transmettre la liste des connexions environnantes à un serveur qui lui répond en lui fournissant toutes les informations relatives aux connexions dans un périmètre plus large, après quoi le terminal réalise localement le calcul de la localisation précise sur la base de ces informations précises.
        - le fournisseur d'OS est incité à offrir la possibilité à l'utilisateur de pouvoir paramétrer facilement une suspension de la collecte constante de la localisation, pour l'OS lui-même ou pour des tiers, de sorte que celle-ci ne soit à nouveau active que lorsqu'elle est nécessaire pour l'usage que fait un utilisateur d'une application. Ainsi, un utilisateur pourrait se voir offrir la possibilité que sa localisation ne soit pas collectée sauf lorsque ses usages le nécessitent, sans avoir à l'activer manuellement au préalable dans les paramètres de l'OS, puis avoir à y retourner pour la désactiver après chaque usage.

## 8.2. Assurer la bonne information des partenaires

Du fait de leur expertise sur les traitements qu'ils opèrent et sur les fonctionnalités qu'ils proposent, les fournisseurs d'OS sont les plus à même de fournir de la documentation et des conseils pour la bonne utilisation des fonctionnalités proposées. À titre de bonne pratique, un ensemble de mesures peuvent être mises en œuvre à cette fin.

### 1. Fournir des documentations exhaustives pour favoriser la conformité des éditeurs et développeurs

Afin de faciliter la bonne compréhension des fonctionnalités de l'OS, son fournisseur est invité à mettre à disposition une documentation exhaustive sur le plan technique, permettant à ses partenaires éditeurs et développeurs d'analyser et de qualifier juridiquement leurs responsabilités au sens du RGPD. À titre de bonne pratique, un rappel général des législations à prendre en compte pourrait être mis à disposition par les fournisseurs d'OS. Cependant, cette mise à disposition ne doit pas imposer aux partenaires des modalités particulières de mise en conformité.

- **À quel public adresser cette documentation ?**
    - S'il est courant que des documentations techniques soient mises à disposition, la CNIL suggère qu'y soient inclus des éléments rappelant le cadre législatif et normatif particulier de l'Union européenne, pour les éditeurs et développeurs qui souhaitent cibler le marché européen ;
    - Ces éléments juridiques pourraient ainsi être regroupés avec les éléments techniques afin de permettre des prises de décision éclairées sur leurs conséquences ;
    - La CNIL suggère que ces éléments, et en particulier les contenus juridiques, soient rendus disponibles dans une langue comprise par le public visé.

- **Quels éléments inclure dans cette documentation ?**
    - Pour les éditeurs visant le marché européen, la CNIL invite le fournisseur d'OS à alerter en particulier sur la nécessité de définir leur responsabilité et à mettre en place les mesures de conformité (finalité, information, droits, sécurité, etc.) ;

- En plus des éléments techniques, il est suggéré d'intégrer des guides et outils spécifiques à l'attention des délégués à la protection des données, pour qu'ils puissent les intégrer directement dans leurs méthodologies d'analyse de risques et d'amélioration continues.
- Dans l'hypothèse où l'OS met à disposition plusieurs fonctionnalité pouvant atteindre la même finalité (par exemple différentes API de localisation), la CNIL invite le fournisseur d'OS à en préciser les caractéristiques, techniques comme juridiques, pour permettre à l'éditeur et au développeur de faire un choix éclairé. Les critères de rétrocompatibilité, de fin de support, de vulnérabilité, d'optimisation énergétique, de déport de la logique de calcul, de transferts, etc., pourraient notamment être présentés.
- Il est recommandé d'indiquer dans la documentation officielle si les outils mis à disposition permettent ou non de répondre à des obligations juridiques telles que le recueil du consentement respectant les critères du RGPD (voir la partie 8.3 « Fournir des outils pour permettre le respect des droits et du consentement des utilisateurs »), et si oui avec quelle configuration.

## 2. Informer les tiers des traitements propres à l'OS

En ce qui concerne les traitements réalisés par le fournisseur d'OS, il est recommandé d'assurer la bonne information des tiers afin qu'ils puissent répondre à leurs obligations, lorsque l'usage de fonctionnalité mises à disposition par l'OS aux applications entraîne la mise en œuvre d'un traitement de la part de l'OS.

- **Quelle information mettre à disposition ?**
  - La CNIL recommande que le fournisseur d'OS s'assure que ses partenaires (développeurs tiers et éditeurs, magasins d'applications, constructeurs, etc.) sont en mesure de connaître, comprendre et documenter, conformément au principe de responsabilité, les traitements de données personnelles impliqués par l'utilisation de l'OS.
  - Dans ce cadre, il s'agira d'indiquer, pour les fonctions activées par ceux-ci :
    - les données traitées, de manière exhaustive, pour la configuration choisie ;
    - la qualification juridique, en particulier concernant la collecte, la conservation, la réutilisation d'une donnée pour le compte du fournisseur d'OS.
    - des points d'alertes spécifiques comportant notamment une plus grande précision sur l'implication d'éventuels transferts au sens du chapitre V du RGPD[53].

- **Sur quels dispositifs informer les tiers ?**

La CNIL recommande aux fournisseurs d'OS :

- de mettre à disposition à une information détaillée sur les dispositifs identifiés dans la partie précédente (sauvegardes, notification, télémétrie) ;
- d'appeler l'attention sur les risques liés aux traitement mis en œuvre, particulièrement s'ils sont susceptibles de traiter des données sensibles au sens de l'article 9 du RGPD (voir encadré ci-dessous) ;
- d'expliquer l'impact des paramétrages et des fonctionnements par défaut de ces dispositifs.

**Pour la définition de donnée sensible au sens de l'article 9 du RGPD, voir la partie 5.1 des présentes recommandations :** « Assurer la conformité des traitements de données personnelles »

## 3. Encourager l'utilisation des fonctionnalités les plus protectrices de la vie privée

La CNIL encourage le fournisseur d'OS à mettre à disposition le détail des caractéristiques des différentes fonctionnalités qu'il propose. Cette bonne pratique doit permettre aux éditeurs de prendre une décision éclairée concernant leur usage, dans le but de répondre aux exigences de la réglementation en matière de protection des données personnelles.

[53] « Transférer des données hors de l'UE », cnil.fr

Ainsi, lorsque le fournisseur d'OS propose une fonctionnalité plus protectrice de la vie privée pour traiter certaines informations (par exemple, une localisation approximative au lieu d'une localisation précise), qui semble plus pertinente en termes de minimisation des données, la CNIL suggère qu'il informe les éditeurs, les développeurs et les fournisseurs de SDK de son existence, ainsi que de la possibilité de mettre à jour leur code pour en bénéficier.

- **Quelles bonnes pratiques pour encourager l'adoption de technologies les plus respectueuses de la vie privée ?**
  - Le fournisseur d'OS peut informer davantage les éditeurs et développeurs d'applications, dans la durée, concernant leur utilisation des nouvelles API proposées par les OS :
    - en listant les diverses évolutions apportées et en présentant des cas pratiques ;
    - en précisant de manière circonstanciée et justifiée les conséquences juridiques pour ses partenaires (effets en termes de conformité, conséquences sur les obligations de l'éditeur, etc.) ;
    - en indiquant, le cas échéant, de manière circonstanciée et justifiée, les mises en œuvre qui respectent les principes de protection des données dès la conception et par défaut (article 25 du RGPD).
  - Le fournisseur d'OS peut établir des statistiques sur la prévalence de l'usage des fonctionnalités les plus avancées, et utiliser cette information pour communiquer de manière sélective sur les fonctionnalités ignorées.
  - Il peut organiser la fin progressive du support des fonctionnalités les plus intrusives et permissives en termes de collecte possible de données, avec une période de transition suffisante pour permettre aux éditeurs de mettre à jour leurs applications.
  - Il pourrait enfin organiser un dialogue (conférences, recherche et publications, forums, etc.) avec des développeurs, des experts de la protection des données et des régulateurs pour définir les priorités de développement de fonctionnalités de protection de la vie privée dans l'OS.

## 8.3. Fournir des outils pour permettre le respect des droits et du consentement des utilisateurs

Les fonctionnalités mises à disposition, par le fournisseur d'OS, aux éditeurs et développeurs d'applications peuvent avoir un impact sur la conformité des traitements mis en œuvre par ces derniers. La CNIL encourage, le fournisseur d'OS, à titre de bonne pratique, à en tenir le plus grand compte lors de la conception de ces fonctionnalités.

### 1. Des systèmes de permissions respectant le principe de protection des données dès la conception

Le système des permissions fourni par l'OS est au cœur de la protection des utilisateurs : en permettant de bloquer techniquement l'accès à certaines données en fonction du choix de l'utilisateur, les permissions apportent une garantie technique de respect de la confidentialité des informations par les applications et constituent un moyen direct pour les personnes de préserver leur vie privée

Ne sont ici considérées que les permissions techniques visant à donner ou bloquer l'accès à certaines ressources protégées, indépendamment des finalités pour lesquelles l'accès à celles-ci est demandé. Sont exclues les permissions visant à autoriser ou refuser la réalisation de certaines actions en vue d'une finalité précise (tel que le recueil d'un identifiant publicitaire), grâce à l'accès à certaines ressources mais également par d'autres moyens.

**Les permissions doivent en tout état de cause être conçues dans le respect des règles du droit de la concurrence.** En particulier, elles ne doivent pas conduire à favoriser les applications que le fournisseur d'OS a conçues ou préinstallées. Ainsi, les permissions conçues par le fournisseur d'OS doivent être présentées de la même manière que pour toute autre application. De plus, les permissions ne doivent pas être conçues dans le but d'empêcher les éditeurs d'accéder à des données pertinentes mais d'assurer que les personnes puissent avoir la main sur leurs données, dans le respect du DMA et du droit de la concurrence.

- **À quelles opérations appliquer les permissions ?**

La CNIL considère comme de bonnes pratiques que le fournisseur d'OS :

- applique les permissions d'accès au terminal utilisateur, que ce soit à ses capteurs (appareil photo, GPS, capteurs environnementaux), ses fonctionnalités (accès réseau, Bluetooth, NFC), ou son stockage (contacts, galerie photo, stockage de masse) ;
- impose l'information et le recueil de la permission de l'utilisateur pour l'ensemble de ces éléments, en préférant un usage systématique de permission qui soient visibles de l'utilisateur;
- prévoie, pour ces éléments le recueil d'une permission de l'utilisateur du terminal indépendamment de l'obligation légale de recueillir ou non un consentement au titre de l'article 82 de la loi Informatique et Libertés pour l'opération de lecture d'informations stockées sur le terminal.

- **Quelle portée choisir pour les permissions ?**
  - Quand une permission est définie, sa portée peut être analysée sous trois axes distincts :
    - le degré de précision de la donnée fournie : chaque permission peut être envisagée avec différents niveaux de précision pour permettre à l'application, ou à l'utilisateur, de choisir le niveau de précision strictement nécessaire au regard de la finalité poursuivie. Par exemple, dans le cas du GPS, cette donnée peut être mise à disposition avec différents niveaux de précision. Similairement, les permissions d'accès aux capteurs physiques (p. ex. : baromètre, thermomètre, photomètre, gyroscopes, accéléromètre) peuvent parfois proposer une limitation de leur précision ; à noter que le niveau de précision de la donnée devrait aussi être clairement indiqué à l'organisme qui utilise la données (éditeurs de l'application et ses sous-traitants) ;
    - sa portée matérielle : chaque permission peut s'appliquer à un ensemble plus ou moins large de données ou de fonctions. Les permissions trop larges en termes de portée matérielle sont susceptibles d'entraîner une collecte excessive de la part des applications (laquelle peut, dans certains cas, être contraire au principe de minimisation). Une bonne pratique consisterait par exemple à éviter les permissions globales d'accès aux fichiers stockés, en privilégiant un système d'accès par fichier ou dossier ;
    - sa portée temporelle : chaque permission peut être activée de manière ponctuelle, ou au contraire pour une durée prédéterminée. Ici encore, le choix de cette portée pourra revenir à l'utilisateur, éventuellement accompagné de suggestions de valeurs de la part de l'éditeur de l'application. Cette portée temporelle peut également prendre en compte des éléments contextuels, comme le fait que l'application soit active ou pas, en premier plan ou pas, ou au contraire inactive depuis une durée déterminée.
  - La CNIL invite le fournisseur d'OS à offrir le degré de contrôle le plus fin possible à l'utilisateur pour restreindre la portée de chaque permission selon ces trois axes.

- **Quelles mesures additionnelles ?**

A titre de bonne pratique, la CNIL invite le fournisseur d'OS à :

- systématiquement prévoir qu'une permission puisse ne pas être exigée avant le lancement de l'application mais seulement lorsque l'application en a besoin ;
- encourager, dans les documentations et les bonnes pratiques partagées avec les développeurs, le fait de recueillir les permissions de manière contextuelle, au moment où elles sont nécessaires ;
- laisser aux utilisateurs la possibilité de choisir le niveau d'information qu'ils souhaitent transmettre dans le cadre de cette permission. Par exemple, l'utilisateur pourrait avoir la possibilité, en cas de demande d'accès à ses contacts, d'en renvoyer une liste partielle. Dans ce cas, le fournisseur d'OS doit s'assurer que les informations transmises à l'application le sont dans le même format technique quel que soit le choix de l'utilisateur, afin de ne pas affecter le fonctionnement technique des applications. Cette possibilité de paramétrage laissée à l'utilisateur doit être mise en œuvre par le fournisseur d'OS dans des conditions transparentes, équitables et non-discriminatoires.

- permettre aux utilisateurs de n'autoriser l'accès qu'une seule fois ou uniquement quand l'application est active, en premier plan ou utilisée, en particulier pour les permissions les plus intrusives, c'est-à-dire celles présentant le plus de risques pour la vie privée des personnes, notamment du fait de la possibilité de les activer ponctuellement à l'insu de l'utilisateur voire en continu (ex : localisation, capteur de l'appareil photo, microphone). Si l'application requiert une permission « à tout moment » (y compris quand l'application est fermée), l'information lors de l'obtention du consentement de l'utilisateur peut être renforcée ;
- révoquer périodiquement les autorisations permanentes des applications non utilisées, en prévenant l'utilisateur de cette révocation, de sorte de permettre à l'utilisateur de fixer la fréquence de ces rappels (par exemple un mois, six mois, un an) ou de les désactiver s'il le souhaite ;
- mettre en place une isolation entre l'exécution de l'application proprement dite et l'exécution des SDK, de manière sécurisée, pour éviter qu'un SDK ne puisse bénéficier d'une permission qui n'aurait été accordée qu'à l'application ; en termes de finalités, de consentement et d'informations transmises à l'utilisateur.

## 2. Aider au bon respect des obligations d'information et de consentement des utilisateurs

En fournissant des outils à cet effet, le fournisseur d'OS est en mesure de simplifier la mise en œuvre du respect des droits et du consentement des utilisateurs.

- **Comment permettre la bonne information des utilisateurs ?**

Il est nécessaire que les systèmes de permissions, qui constituent généralement une étape pour déclencher un traitement de données à caractère personnel (localisation, contacts etc.) permettent techniquement à l'éditeur de fournir les informations pertinentes à l'utilisateur sur la portée de la permission qu'il donne (voir partie 5.5 des présentes recommandations, « Permissions et protection des données dès la conception »).

A titre de bonnes pratiques, la CNIL invite à prendre en compte les éléments de design suivants :

- Au-delà de la simple information préalable, il est souhaitable que l'utilisateur continue à être informé au cours du traitement et suite à celui-ci. À ce titre, des mesures de transparence sur l'accès aux capteurs, notamment via des indicateurs visuels sur les accès ponctuels, au moment où ils sont effectués par le système, mais également au moment où ils sont effectués par une application, en précisant alors laquelle, peuvent être mises en œuvre.
- L'utilisateur peut avoir accès à un historique de l'activation des capteurs et des requêtes effectuées, filtrés par usage et par processus système ou par application. De plus, un indicateur peut être affiché, par exemple dans la barre d'état, signalant quand la permission est utilisée.
- Pour les permissions les plus intrusives (accès au microphone, à la caméra, à la localisation, aux fichiers sur le téléphone, aux contacts, à l'agenda), il peut être prévu de réitérer la demande de permission un certain temps après la première autorisation, afin que l'utilisateur puisse revenir sur son choix initial au moment où il a mis en œuvre l'application pour la première fois. Ceci permettrait aux utilisateurs de revenir plus facilement sur leur choix concernant les permissions, y compris pour les applications préinstallées par le fournisseur d'OS. La mise en place d'un tel paramétrage suppose qu'il soit possible pour l'utilisateur de définir la fréquence ou l'activation même de ces rappels, par exemple lors de la configuration initiale de l'OS lors d'une première utilisation de l'appareil mobile.

- **Comment aider au bon recueil du consentement ?**
  - Il est fréquent que les demandes de permissions correspondent à des situations dans lesquelles un consentement est requis, au sens de la réglementation applicable en matière de protection des données personnelles.
  - Afin de faciliter la conformité des applications tout en minimisant la lassitude des utilisateurs, les fenêtres de permission peuvent, dans certains cas restreints, permettre d'obtenir directement un consentement valable. Parmi ces cas figure par exemple celui des permissions qui correspondent à un seul traitement, une seule finalité et un seul destinataire des données. À cette fin, ces fenêtres doivent alors contenir :

        - la seule finalité pour laquelle la permission est demandée ;
        - des liens hypertextes pour accéder à l'ensemble des informations prévues par la réglementation (articles 13 et 14 du RGPD) , art. 82 de la loi Informatique et Libertés) ;
        - les modalités pour révoquer son accès.
    - Dans ce cas, il appartient au développeur de veiller à une bonne articulation entre permission et recueil du consentement (voir tableau figurant dans la partie 6.2.3 des présentes recommandations).
    - La CNIL recommande qu'une certaine latitude soit laissée à l'éditeur en termes d'information présentée à l'utilisateur au moment de la demande de permission, afin d'assurer une information suffisante des personnes (voir partie 5.5 des présentes recommandations, « Permissions et protection des données dès la conception »).
    - A titre de bonne pratique et en fonction du caractère intrusif des permissions, le fournisseur d'OS peut s'assurer que l'utilisateur dispose d'une information suffisante sur l'impact de ses choix. Un lien permettant de comprendre cet impact pourrait être mis à sa disposition, en exposant une série d'exemples concrets et de risques associés. Par exemple, pour une permission d'accès aux SMS du terminal, il peut être précisé qu'il peut légitimement s'agir de récupérer un mot de passe temporaire dans le cadre d'une authentification multi-facteurs, mais également d'une capacité sans limite de temps pour une application malveillante de lire, transmettre ou modifier les SMS reçus. Une telle information serait de nature à permettre à l'utilisateur d'estimer l'intérêt d'autoriser une telle collecte en fonction du degré de confiance qu'il porte dans l'éditeur d'une application.
    - Enfin, il peut permettre de révoquer ou modifier facilement les permissions accordées par l'utilisateur.

- **Comment faciliter la portabilité des données ?**
    - Même dans les cas où il n'endosse pas de qualification de responsable de traitement, la CNIL considère comme une bonne pratique que le fournisseur d'OS permette de mettre en œuvre une portabilité des données personnelles, au moyen d'un format ouvert. Cette portabilité, qui devient une obligation pour le fournisseur d'OS s'il est responsable de traitement, pourra à ce titre concerner les configurations mais aussi les applications installées sur le téléphone, de sorte de favoriser le dialogue et la coopération avec les fournisseurs d'autres OS. A titre de bonne pratique, elle pourra considérer les articles 4-1 et 20 du RGPD, qui invitent à définir un « *format structuré, couramment utilisé et lisible par machine* », de sorte qu'il soit pertinent pour un utilisateur souhaitant porter ses données d'un OS à un autre.

## 3. Protéger les utilisateurs mineurs

Le traitement des données des utilisateurs mineurs par les éditeurs d'application est soumis à des obligations particulières. L'OS peut fournir des outils utiles à la mise en œuvre de celles-ci à titre de bonne pratique.

- **Comment participer à la conformité des applications en ce qui concerne les utilisateurs mineurs, au sens de l'article 8 du RGPD ?**
    - La CNIL invite les fournisseurs d'OS à fournir des outils de contrôles parentaux qui incluent, via une API ou d'autres modalités technologiques non-intrusives, la possibilité de signaler aux applications la tranche d'âge pertinente de la personne, en fonction des paramètres ayant pu être renseigné précédemment dans l'OS, notamment par le parent ou le tuteur légal de l'enfant.
    - L'outil de contrôle parental pourrait ainsi être utilisé directement sur le terminal sans avoir à fournir d'informations complémentaires à un tiers (tel que le fournisseur de l'OS lui-même ou l'éditeur d'un système de contrôle parental tiers), ni contraindre à créer un compte utilisateur sur un service en ligne uniquement pour cette raison.
    - Une telle solution permettrait d'aider les développeurs d'applications à définir si l'utilisateur est mineur, afin de faciliter le respect des obligations au regard du RGPD et en minimisant la nécessité de faire appel à des traitements distants.
    - Le fait qu'un utilisateur donné soit mineur pourrait être pris en compte directement dans ces outils, induisant leur capacité à répondre aux permissions système éventuelles via des outils de contrôle parental efficaces.

- La faculté d'enregistrer plusieurs profils au sein des vecteurs d'authentification biométriques, permettrait de distinguer si l'utilisateur authentifié est le mineur ou son représentant légal, de sorte qu'il serait possible pour les développeurs de configurer une application où la permission du mineur suffit pour certaines actions, et où la permission du représentant légal serait nécessaire pour d'autres actions.

## 8.4. Fournir une plateforme sécurisée

L'OS constitue le socle de la sécurité du terminal. À ce titre, les fournisseurs d'OS sont invités à s'assurer qu'ils mettent à disposition des éléments à l'état de l'art pour apporter cette garantie de sécurité aux utilisateurs.

### 1. Assurer la sécurité et le cloisonnement des terminaux

La sécurité sur les terminaux mobiles repose principalement sur des mesures de cloisonnement qui assurent une isolation des différentes applications.

- **Comment mettre en œuvre le cloisonnement des applications ?**
  - L'OS peut assurer, via un cloisonnement, la séparation stricte des applications entre elles et avec le système d'exploitation, notamment en termes d'accès mémoire, mais surtout, dans ce contexte, de permissions.
  - Lorsque le terminal est utilisé à la fois dans la vie privée et professionnelle, la CNIL considère comme une bonne pratique d'offrir un cloisonnement des usages personnels et professionnels au sein d'un même terminal au moyen de mesures techniques et de design d'interface soit mis en place. Pourraient par exemple être permis :
    - l'usage de profils utilisateurs distincts au sein de l'OS, en informant l'utilisateur de l'existence de cette fonctionnalité et en encourageant son utilisation ;
    - la possibilité d'avoir plusieurs instances simultanées et cloisonnées d'une même application de manière à permettre un usage simultané en fonction des contextes.
  - Le seul cloisonnement par application n'est pas toujours suffisant. La CNIL considère comme une bonne pratique de proposer également un cloisonnement entre les applications et les codes tiers qu'elles peuvent invoquer, notamment en termes d'obtention des permissions. En pratique, le fait de donner à une application la permission d'accéder à une ressource pourrait ne pas automatiquement étendre cette permission à l'ensemble des SDK intégrés dans cette application.
- **Quelles mesures techniques mettre en œuvre ?**
  La CNIL considère que les mesures suivantes correspondent à des pratiques à l'état de l'art :
  - mettre à disposition un espace de stockage sécurisé dédié au stockage local des secrets (enclave, autrement appelé « *SecureElement* »), lorsque le terminal sur lequel l'OS est exécuté dispose du matériel nécessaire ;
  - imposer le chiffrement des connexions réseaux ; à défaut, signaler toute connexion non chiffrée ; forcer l'usage du protocole TLS dès que possible, ou indiquer son absence aux utilisateurs.
  - mettre à disposition des applications des fonctionnalités de chiffrement à l'état de l'art ;
  - mettre à disposition des outils de partage local, entre applications au sein d'un même appareil ;
  - chiffrer les sauvegardes par défaut, qu'elles soient locales ou placées sur des serveurs tiers ; ne conserver les clés de chiffrement que sur le terminal ;
  - indiquer les bonnes pratiques, à l'état de l'art en termes de cybersécurité, qui sont susceptibles de concerner les éditeurs, accompagnées d'exemples permettant aux développeurs de déterminer les modèles de menaces de leurs utilisateurs et de mettre en place, le cas échéant, des mesures de sécurité supplémentaires permettant de répondre à ces menaces.

### 2. Mettre à disposition des outils d'audit efficaces

Il est souhaitable que les fournisseurs d'OS permettent à leurs utilisateurs et aux professionnels d'auditer le fonctionnement des terminaux auquel ils ont accès.

- **Quels outils mettre à disposition ?**
  - La CNIL considère comme une bonne pratique que soient mis en place des outils adéquats (qu'ils soient contenus au sein même de l'OS ou proposés dans un environnement de développement), qui permettent une analyse fine du trafic réseau, des processus en cours d'exécution, et de l'ensemble des communications, y compris celles effectuées vers et depuis les serveurs du fournisseur de l'OS.
  - Des méthodologies officielles d'audit pourraient être mises à disposition des éditeurs et développeurs pour faciliter leur audit des SDK qu'ils utilisent dans leurs applications et réduire l'asymétrie d'information entre ces acteurs.

- Le fournisseur d'OS peut également offrir la faculté de générer des rapports de confidentialité simplifiés, afin que les utilisateurs puissent comprendre plus facilement les impacts que peuvent avoir certaines applications.

### 3. Maintenir la sécurité dans le temps

Pour assurer la sécurité des terminaux dans le temps, le fournisseur d'OS sont invités, à titre de bonne pratique, à mettre en place des processus pour assurer le maintien à jour du parc d'utilisateurs.

- **Comment préserver la sécurité des terminaux dans le temps ?**
  - La CNIL invite le fournisseur d'OS à proposer aux utilisateurs un support des versions de l'OS le plus long possible dans le temps, en particulier lorsqu'une mise à jour d'une version à l'autre est incompatible, en termes de restriction matérielle, sur une partie importante du parc actuel de terminaux.
  - La CNIL considère comme une bonne pratique de proposer systématiquement des mises à jour de sécurité de l'OS au moins jusqu'à 7 ans après l'achat du terminal. Le fait que certains éléments fonctionnels ne soient plus compatibles avec le terminal de suffisant pas à justifier la cessation des mises à jour de sécurité.
    - A ce titre, la CNIL rappelle que cette suggestion s'inscrit également dans les critères du Référentiel Général d'Ecoconception de Services Numériques[54].
  - Quand cette durée est échue, le fournisseur d'OS est invité à informer les utilisateurs concernés des risques associés à l'absence de mise à jour. Le fournisseur pourrait orienter de tels utilisateurs vers des OS alternatifs qui supportent son terminal et maintenus en condition de sécurité.

## 8.5. Liste de vérifications

Ces vérifications ont pour objet de guider les fournisseurs d'OS dans la mise en œuvre de ces recommandations et sont présentées à titre indicatif. Certaines des vérifications à effectuer peuvent correspondre à des bonnes pratiques ou recommandations et non à des obligations : en cas de doute, se référer au texte de la recommandation.

| Catégorie | Sous-Catégorie | Identifiant | Description |
|---|---|---|---|
| **Assurer la conformité des traitements de données personnelles mis en œuvre** | Déterminer la part du fournisseur d'OS dans la conformité des traitements de données personnelles mis en œuvre | 1.1.1 | Une analyse des responsabilités est menée, portant sur le socle de l'OS, sur les briques fonctionnelles ajoutées à celui-ci ainsi que les traitements susceptibles d'être mise en œuvre par les applications et utilisés par les personnes. |
| | Appliquer les principes de protection des données dès la conception et par défaut | 1.2.1 | Aucun traitement effectué pour le compte du fournisseur d'OS n'est effectué avant le recueil d'un consentement valide, y compris lors du premier lancement de celui-ci. |
| | | 1.2.2 | La création d'un compte n'est pas nécessaire pour utiliser l'OS et les applications préinstallées. |
| | | 1.2.3 | L'utilisation de serveurs de notifications tiers est possible. Leur utilisation est optimisée, notamment en termes d'exécution en tâche de fond et d'impact sur la batterie. |

[54] https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

| | | | |
|---|---|---|---|
| | | 1.2.4 | Des outils permettant le chiffrement du contenu des notifications est proposé, quel que soit le serveur de notification responsable de leur transmission. La mise à disposition de ces outils est accompagnée d'une documentation claire. |
| | | 1.2.5 | Un système de remontée de bogues et de gestion de terminaison inopinée conforme au principe de minimisation est proposé, incluant un consentement à la remontée du rapport de bogue. |
| | | 1.2.6 | Si un système de sauvegarde distant des paramètres et du contenu de l'OS est proposé, il n'est pas activé par défaut. Il fait l'objet d'un recueil de consentement et les données correspondantes sont transmises et stockées de manière chiffrée, au moyen d'une clé à laquelle le fournisseur de l'OS n'a pas lui-même accès. |
| | | 1.2.7 | La mise à disposition des données de localisation peut être limitée uniquement à l'utilisation du capteur GPS, sans mobiliser d'autres traitements. |
| **Assurer la bonne information des partenaires** | Fournir des documentations exhaustives pour favoriser la conformité des éditeurs et développeurs | 2.1.1 | La documentation à l'attention des développeurs tiers ainsi que celle à l'attention des utilisateurs finaux de l'OS sont à jour, facilement compréhensibles et exhaustives et comprennent des exemples pratiques. |
| | | 2.1.2 | Des éléments juridiques sont présents au sein de cette documentation et comprennent des exemples pratiques. |
| | | 2.1.3 | Les différentes documentations sont accessibles dans les langues des publics ciblés. |
| | Informer les tiers des traitements propres à l'OS | 2.2.1 | Les partenaires (développeurs tiers et éditeurs, magasins d'applications, constructeurs, etc.) sont en mesure de connaître, comprendre et documenter, conformément au principe de responsabilité (« *accountability* »), les traitements impliqués ou induits par l'utilisation de l'OS. |
| | Encourager l'utilisation des fonctionnalités les plus protectrices de la vie privée | 2.3.1 | Les API proposées par l'OS permettent sont documentées pour permettre une décision éclairée quant à leur usage. |
| | | 2.3.2 | Une documentation spécifique est proposée aux développeurs et éditeurs pour les accompagner dans l'usage de nouvelles API ou nouvelles versions d'API dans la mesure où elles sont plus protectrices de la vie privée. |
| **Fournir des outils pour permettre le respect des droits et du** | Des systèmes de permissions respectant le principe de protection des | 3.1.1 | Les accès aux capteurs physiques, aux matériels d'accès au réseau et aux espaces de stockage des terminaux ne peuvent être effectués qu'après validation d'une permission par l'utilisateur final. |

| | | | |
|---|---|---|---|
| **consentement des utilisateurs** | données dès la conception | 3.1.2 | Les permissions permettant différents niveaux de précision laissent à l'utilisateur final, et non uniquement au développeur d'une application, le choix de ce niveau. |
| | | 3.1.3 | Les permissions peuvent être restreintes par l'utilisateur, sur une période temporelle et un nombre d'occurrences définis. |
| | | 3.1.4 | Les utilisateurs ont la possibilité de choisir le niveau d'information qu'ils souhaitent transmettre dans le cadre des permissions, notamment via une saisie manuelle de l'information à transmettre. Par exemple : transmettre une partie de son carnet de contact ou de sa médiathèque plutôt que l'intégralité (compartimentation de l'information). |
| | | 3.1.5 | Les permissions d'une application sont révoquées lorsqu'une application n'est pas utilisée depuis un certain temps. L'utilisateur est averti de cette révocation. |
| | Aider au bon respect des obligations d'information et de consentement des utilisateurs | 3.2.1 | Les systèmes de permissions permettent à l'éditeur de fournir les informations pertinentes sur la portée de la permission demandée. |
| | | 3.2.2 | L'accès en cours aux capteurs physiques fait l'objet d'un signal visuel ou sonore au sein de l'interface de l'OS présentée à l'utilisateur final (pastille de couleur, sonnerie, vibration, etc.), permettant à l'utilisateur de déterminer quelle application est en train d'accéder à quel capteur. |
| | | 3.2.3 | L'utilisateur dispose d'un historique d'accès aux capteurs précités, horodaté et par application. |
| | | 3.2.4 | L'utilisateur dispose d'un moyen simple de définir si un rappel lui est proposé, concernant les permissions requises par les applications qu'il utilise, lui permettant de paramétrer une désactivation par défaut ou un rappel d'information des permissions requises après un certain temps de non-utilisation de ses applications. |
| | | 3.2.6 | Les permissions peuvent être facilement révoquées. L'accès aux menus permettant cette révocation est intuitif. |
| | | 3.2.7 | L'OS propose une portabilité des données, au sens du RGPD, permettant à l'utilisateur de migrer ses données et configurations vers un autre OS ou vers un même OS sur un autre terminal. |
| | Protéger les utilisateurs mineurs | 3.3.1 | Des outils de contrôles parental sont mis à disposition des utilisateurs finaux. |
| | | 3.3.2 | Ces outils mettent un signal de minorité à disposition des développeurs, de sorte que l'utilisation de leurs applications puissent être |

| | | | |
|---|---|---|---|
| | | | restreinte ou bloquée en fonction des paramètres relatifs à un âge connu par l'OS. |
| **Fournir une plateforme sécurisée** | Assurer la sécurité et le cloisonnement des terminaux | 4.1.1 | Une compartimentation (« *sandboxing* ») est mise en œuvre, permettant de limiter et contrôler les interactions, l'accès à la mémoire et l'usage des permissions, entre l'OS et les applications. |
| | | 4.1.2 | Une compartimentation, à la fois technique et d'interface, est mise en œuvre dans l'OS, afin de pouvoir distinguer usages personnels et professionnels sur un même terminal physique. |
| | | 4.1.3 | Lorsque le matériel du terminal le permet, le stockage local de secret utilise le matériel dédié par défaut (enclave ou « *SecureElement* »). |
| | | 4.1.4 | Une contrainte technique et d'interface est appliquée sur la mise en œuvre des connexions réseaux (p. ex. : signalement de connexions non chiffrées, de certificat obsolète, forçage de TLS, etc.). |
| | | 4.1.5 | Des systèmes de partages locaux inter-applications, par exemple par API, sont mis à disposition par l'OS, de sorte qu'une application puisse communiquer des données de manière sécurisée à une autre application, sans que celles-ci ne nécessitent une transmission vers des serveurs extérieurs. |
| | | 4.1.6 | Les sauvegardes sont chiffrées par défaut, avec conservation de la clé de chiffrement exclusivement sous le contrôle de l'utilisateur. |
| | Mettre à disposition des outils d'audit efficaces | 4.1.1 | Des bonnes pratiques de conception et de développement en matière de sécurité sont communiquées aux développeurs tiers. |
| | | 4.2.2 | Une documentation de ces outils et méthodologies d'audit est mise à disposition, de manière à faciliter le travail des acteurs amenés à les utiliser et à s'assurer de leur pleine compréhension des résultats observés. |
| | Maintenir la sécurité dans le temps | 4.3.1 | Le support de chaque version de l'OS est assuré le plus longtemps possible. |
| | | 4.3.2 | Des mises à jour de sécurité sont proposées le plus longtemps possible, *a minima* 7 ans, indépendamment des mises à jour fonctionnelles. |
| | | 4.3.3 | Lorsque le support d'une version de l'OS s'achève, une information claire est délivrée aux développeurs et aux utilisateurs finaux. |

# 9. Recommandations spécifiques au fournisseur de magasin d'applications

**Comment lire cette section ?**

Cette section comprend des éléments qui sont formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »). Elle rappelle également les obligations posées par la règlementation (par exemple, « le responsable du traitement doit ») et formulent des recommandations pour s'y conformer (par exemple, « la CNIL recommande »). Il est possible que les responsables de traitement identifient des manières alternatives de se conformer aux obligations, mais ils doivent alors pouvoir justifier leur choix et engagent leur responsabilité. Certains éléments sont également formulés à titre de bonnes pratiques et permettent d'aller plus loin que le respect de la règlementation (par exemple, « A titre de bonnes pratiques, la CNIL encourage »).

## Notice

### À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de magasins d'applications (*app stores* ou *stores* en anglais)**.
- Le fournisseur de magasins d'applications est défini comme **l'entité personne morale qui développe et maintient un magasin d'applications, c'est-à-dire une application mobile qui indexe, met en avant et permet le téléchargement d'autres applications mobiles.** Il peut s'agir d'une entité commerciale ou non, elle-même potentiellement rattachée juridiquement à une autre entité (constructeur, éditeur, fournisseur d'OS).
- Ces recommandations ne s'appliquent pas au fournisseur du magasin, appréhendé en tant qu'éditeur d'application. En effet, **l'éditeur de l'application mobile que constitue le magasin d'applications doit se voir appliquer les mêmes qualifications et obligations que n'importe quel éditeur d'applications**. Il se réfèrera à cet effet aux recommandations applicables aux éditeurs d'applications.
- Ces recommandations s'adressent plus spécialement au sein du fournisseur de magasin d'application :
  - au délégué à la protection des données (DPD ou *Data Protection Officer – DPO*) de l'entité fournissant le magasin d'applications ;
  - aux équipes juridiques et techniques des fournisseurs d'OS, notamment des constructeurs, amenés à autoriser ou intégrer les magasins d'applications tiers ;
- Ces recommandations peuvent également être consultées par des éditeurs et développeurs d'applications mobiles souhaitant rendre accessible leurs applications sur différents magasins d'applications.

### Quel est l'objet de ces recommandations ?

- Si certains systèmes d'exploitation permettent l'installation d'applications suite à un téléchargement direct, la majorité des utilisateurs installent des applications via le magasin d'applications proposé par défaut sur leur équipement. Quel que soit le système d'exploitation utilisé, le fournisseur du magasin d'applications ne sera généralement pas responsable des traitements mis en œuvre au sein des applications elles-mêmes.
- Le fournisseur du magasin d'applications met en général en place un processus de revue des applications proposées, que ce soit pour la publication initiale ou la mise à jour de celle-ci, processus pouvant aboutir à la publication de l'application sur le magasin ou au rejet de celle-ci, le plus souvent dans le cadre d'un processus permettant à l'éditeur de modifier sa soumission pour aboutir à la publication. Il est également fréquent que le fournisseur de magasin d'applications, suite à des signalements ou des évolutions de ses critères, procède à la suspension d'applications préalablement publiées.

- Le fournisseur du magasin d'applications est cependant susceptible d'avoir une influence sur les applications que les personnes choisissent d'utiliser sur leurs terminaux. Par conséquent, **ses choix de conception, la clarté des informations qu'il propose et sa capacité à contrôler les applications qu'il met à disposition, avant et pendant leur mise à disposition, ont *in fine* un impact sur les droits et libertés des personnes dans leurs usages numériques mobiles**.
- À ce titre, il est souhaitable que le fournisseur du magasin d'applications joue un rôle de relai pour permettre d'informer les utilisateurs sur les traitements susceptibles d'être mis en œuvre au sein des applications distribuées et qu'il mette en œuvre des processus participant à faciliter la conformité aux législations en vigueur des applications publiées. **Ces recommandations et bonnes pratiques ont pour but d'aider les fournisseurs de magasin d'applications dans cette démarche.**

### Comment utiliser ces recommandations ?

- Chaque section correspond à une étape dans l'activité du fournisseur de magasin d'applications **et expose les enjeux en matière de vie privée et regroupe une série de recommandations ainsi que de bonnes pratiques à mettre en œuvre**.
- Ces recommandations sont sans préjudice des règles applicables sur d'autres fondements juridiques que la protection des données personnelles, notamment le droit de la concurrence.
- Une **liste récapitulative des principales vérifications à réaliser** est proposée à la fin de cette partie. Les fournisseurs de magasins d'applications sont invités à s'y référer, notamment lors des contrôles opérés préalablement à la publication d'une application dans le magasin, ainsi que lors de la mise à jour des interfaces utilisateur du magasin.

## 9.1. Analyser les applications soumises par les éditeurs

Lors du processus de revue des applications avant leur publication au sein du magasin, le fournisseur du magasin d'applications a la possibilité de procéder à la collecte d'informations et à l'analyse de l'applicatif proposé afin de favoriser le respect des droits des utilisateurs finaux. Les bonnes pratiques suivantes s'appliquent en particulier aux applications visant des utilisateurs au sein de l'Union européenne.

### 1. Centraliser et analyser les données relatives à la conformité

Conformément au principe de responsabilité (« *accountability* »), les éditeurs d'application ont l'obligation de documenter les traitements de données personnelles auxquels ils vont procéder dans le cadre du fonctionnement de l'application. Le fournisseur du magasin d'applications peut demander la transmission d'une partie de la documentation préexistante constituée par l'éditeur afin de renforcer la transparence pour les utilisateurs.

- **Quelles informations obtenir de la part de chaque éditeur d'application ?**
  - La CNIL invite le fournisseur du magasin d'applications à solliciter la mise à disposition des informations suivantes de la part de l'éditeur :
    - les catégories de données collectées et les finalités poursuivies pour chacun des traitements,
    - les tiers qui ont accès aux données ou qui sont susceptibles d'y avoir accès, ce qui peut inclure la liste des fournisseurs de SDK utilisés,
    - la liste exhaustive des permissions système demandées par l'application, comprenant leur nature obligatoire ou optionnelle, ainsi que les finalités pour lesquelles celles-ci sont demandées, telles qu'elles seront présentées à l'utilisateur lors de l'usage de l'application,
    - le cas échant, le pays tiers dans lequel les données seront stockées et traitées,
    - un historique des mises à jour, incluant les notes de mises à jour.
  - Il lui est suggéré de demander la mise à disposition d'un point de contact pour les questions de vie privée, à destination des utilisateurs, ainsi que la politique de confidentialité ;
  - Il lui est également suggéré de permettre aux applications d'indiquer si elles visent uniquement, majoritairement ou potentiellement un public mineur.

La CNIL rappelle qu'aucune des informations précitées n'est confidentielle. Elles correspondent à des informations qui doivent être mises à disposition par le responsable du traitement, tel que le prévoient les articles 13 et 14 du RGPD. Par ailleurs, ces données ne doivent pas être utilisées par les contrôleurs d'accès en concurrence avec les entreprises utilisatrices, ainsi que le prévoit l'article 6-2 du Règlement 2022/1925 du 14

septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique (dit Règlement sur les marchés numériques, « *Digital Markets Act* » ou DMA). La CNIL invite à ce que chacune de ces informations soit fournies dans leur version la plus à jour possible.

### 2. Encourager des pratiques mieux-disantes en termes de protection la vie privée lors de la publication et la mise à jour des applications

Du fait de leur expertise et de leur connaissance des systèmes d'exploitation, les fournisseurs de magasin d'applications mobiles apparaissent bien positionnés pour encourager les bonnes pratiques à l'occasion de la publication et des mises à jour des applications.

- **Quelles bonnes pratiques pour encourager la conformité des applications ?**
  - Lors du processus de revue des applications, qu'elles soient nouvelles ou qu'il s'agisse de mises à jour, la CNIL invite les fournisseurs des magasins d'applications à encourager les éditeurs à ne pas demander des permissions en bloc lors de l'installation mais plutôt à gérer des permissions à l'exécution, en n'activant que celles qui seront nécessaires aux seules fonctionnalités utilisées par les utilisateurs finaux ; pour aller plus loin, le fournisseur de magasin d'applications pourrait réserver l'accès à son magasin à des applications qui effectuent des demandes de permission contextuelles.
  - Le fournisseur de magasin d'applications peut inciter les éditeurs d'applications à ne pas utiliser d'API de l'OS qui seraient trop larges ou obsolètes, en particulier si les versions les plus récentes permettent de mieux respecter les principes de protection des données dès la conception et par défaut.
- **Comment améliorer les notes de mises à jour ?**
  - Les fournisseurs de magasins d'applications pourraient inviter les éditeurs à publier des notes de mises à jour informatives pour les utilisateurs. Les notes de mises à jour sont un moyen simple et accessible pour les utilisateurs de connaître à l'avance les conséquences de la mise à jour de leur application, en particulier sur le plan de la sécurité (correction de vulnérabilités) et sur la mise en œuvre de traitement de données personnelles supplémentaires. L'utilisateur pourrait ainsi avoir le choix, en toute connaissance de cause, de mettre à jour ou non son application.

### 3. Analyser les applicatifs pour détecter des failles de sécurité

Les fournisseurs de magasin d'applications ont la capacité de mettre à disposition des éditeurs d'applications des outils d'analyse afin de détecter au plus tôt d'éventuelles failles de sécurité.

- **Comment mettre en œuvre des analyses statiques ?**
  - Le fournisseur d'applications pourrait mettre en œuvre des analyses statiques avant chaque publication ou mise à jour d'une application. Ces analyses pouvant aussi bien être automatiques que manuelles et spécifiques, dans le cas d'applications dépassant un certain nombre de téléchargements ou demandant un ensemble particulièrement intrusif de permissions.
- **Comment mettre en œuvre des analyses plus poussées ?**
  - Pour les applications les plus sensibles, la CNIL invite les fournisseurs de magasins d'applications à mener des analyses dynamiques, aussi bien automatiques que manuelles, afin de détecter des comportements anormaux à l'usage et échappant à une analyse statique.
  - Peuvent par exemple être étudiés :
    - le chargement dynamique de bibliothèques logicielles *a posteriori* ;
    - l'exécution en tâche de fond, pouvant notamment impacter l'autonomie de la batterie ;
    - l'usage de comportements propres aux applications malveillantes, documentés notamment dans la littérature scientifique, la presse spécialisée et les publications de CVE (*Common Vulnerabilities and Exposures*).

## 9.2. Mettre en œuvre des processus transparents de revue des applications qui intègrent la vérification des règles élémentaires de protection des données

La CNIL encourage les fournisseurs de magasin d'applications à agir avec la plus grande transparence et à faciliter les démarches de conformité des éditeurs. Cela passe notamment par une communication avec les

éditeurs dans leurs langues respectives. Au regard du droit de la concurrence et du DMA, lorsqu'une entité recouvre à elle seule plusieurs des catégories d'acteurs de cette recommandation (éditeur, développeur, fournisseur d'OS, fournisseur de magasin d'applications), il est impératif que le processus de vérification des applications publiées dans son magasin d'applications ne soit pas plus complexe pour les applications tierces que pour les applications qu'elle développe.

## 1. Intégrer la vérification des règles élémentaires de protection des données dans les processus de revue des applications

Afin d'accompagner dans leur conformité au RGPD les éditeurs souhaitant destiner une application au marché européen, il est souhaitable que les processus de revue des applications par le magasin d'applications intègrent les vérifications suivantes.

- Si l'application vise le marché européen, il peut être demandé à l'éditeur si l'application traite des données personnelles. Dans ce cas, la CNIL encourage le magasin d'applications à vérifier la présence ou non des éléments suivants parmi les informations offertes aux usagers[55], que l'éditeur a l'obligation de fournir sur le fondement du RGPD :
  - l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement (article 13.1 a) et 14.1 a)) ;
  - les finalités du traitement ainsi que sa base juridique (article 13.1 c) et 14.1 c)) ;
  - la durée de conservation des données personnelles (article 13.2 a) et 14.2 a)) ;
  - selon la base légale, l'existence d'un moyen d'expression des droits (article 13.2 b) et 14.2 b)) ;
  - le droit d'envoyer une plainte à l'autorité compétente (article 13.2 d) et 14.2 d)).
- La CNIL rappelle qu'aucune des informations précitées n'est confidentielle : elles correspondent strictement aux informations qui doivent être mises à disposition du public, tel que le prévoient les articles 13 et 14 du RGPD. Par ailleurs, ces données ne doivent pas être utilisées par les contrôleurs d'accès en concurrence avec les entreprises utilisatrices, ainsi que le prévoit l'article 6-2 du DMA. La CNIL invite à ce que chacune de ces informations soit fournies dans leur version la plus à jour possible.
- La CNIL invite les magasins d'applications à refuser les applications visant le marché européen, traitant des données à caractère personnel, qui ne sont pas en mesure de fournir les éléments ci-dessus.
- À titre de bonne pratique, un rappel général des législations à prendre en compte pourrait également être mis à disposition par le magasin d'application.

## 2. Exprimer clairement les attentes et les processus mis en œuvre

La CNIL estime qu'il serait bénéfique pour l'ensemble des acteurs que les fournisseurs de magasin d'applications s'assurent de la clarté, l'exhaustivité et l'uniformité des exigences imposées aux applications candidates en termes de sécurité et de vie privée, dans les limites posées par l'article 6-12 du règlement sur les marchés numériques qui mentionne que « *le contrôleur d'accès applique aux entreprises utilisatrices des conditions générales d'accès équitables, raisonnables et non discriminatoires à ses boutiques d'applications logicielles* ».

- **Quelles bonnes pratiques pour l'information des éditeurs d'application ?**
  - La mise à disposition d'une documentation complète concernant les points d'exigence étudiés ;
  - Pour chacune de ces exigences, la publication d'exemples concrets de comportements problématiques et de solutions pour y remédier,
  - La mise à disposition d'une description précise du processus de validation, des étapes de vérification et des temporalités associées à chaque étape, y compris pour les différents processus de remédiation en cas de rejet,
  - En cas de mise à jour des règles applicables, une communication proactive aux éditeurs concernant celles-ci, en allouant une période raisonnable pour leur prise en compte. Si ces mises à jour ont vocation à provoquer le rejet de solutions précédemment acceptées, des exemples de techniques de remédiations peuvent également être publiés.

[55] Le fournisseur de magasin d'applications peut par exemple demander de renseigner ces informations au sein d'un formulaire.

### 3. Faciliter l'utilisation des outils mis à disposition

Les fournisseurs de magasin d'applications sont également invités à mettre à disposition des outils adéquats pour la gestion du processus de publication et la résolution des rejets.

- **Les éditeurs d'application ont-ils les outils à leur disposition pour publier efficacement leur application ?**
  - Les organisations internes des entités qui publient des applications peuvent être très diverses.
  - À ce titre, la CNIL encourage les fournisseurs de magasins d'applications à permettre une gestion fine des accès aux comptes éditeurs. Ainsi, lorsque plusieurs acteurs participent à la publication de l'application, cela permettrait que ceux-ci disposent d'accès distincts aux dépôts, aux signatures de versions, aux notes de mises à jour, ainsi qu'aux informations utiles à l'utilisateur.
- **Les éditeurs d'application ont-ils un canal de communication identifiable à leur disposition ?**
  - A titre de bonne pratique, un canal de communication entre les entités publiant des applications mobiles sur le magasin d'applications et le fournisseur de magasin d'applications pourra être établi, afin d'éviter les situations de blocage.
  - L'utilisation de la plateforme de publication pour la mise en œuvre du processus de résolution de rejets et les communications subséquentes avec l'organisation demandant la publication étant à privilégier.
- **Quelles bonnes pratiques pour la gestion des refus et des suspensions d'applications ?**
  - Informer rapidement l'éditeur quand une faille de sécurité est détectée, et en particulier si cela peut mener à la désactivation de l'application ou à une communication aux utilisateurs finaux.
  - Assurer une communication transparente avec les éditeurs d'applications mobiles lors de l'application des critères de validité de publication.
  - Indiquer les causes du rejet et le processus de recours mobilisable par l'éditeur.
  - Mettre à disposition des conditions générales d'accès comportant notamment un mécanisme de règlement extrajudiciaire des litiges (DMA, art. 6-12).

## 9.3. Informer les utilisateurs et leur fournir des outils de signalement

La CNIL encourage les fournisseurs de magasins d'applications à offrir un niveau d'information suffisant, notamment la liste des SDK tiers utilisés par chaque application, pour permettre aux utilisateurs d'exercer leurs droits plus facilement.

### 1. Normaliser et mettre à disposition les données relatives à la conformité

Un magasin d'applications dispose le plus souvent d'une interface de recherche qui donne une description sommaire de chaque application. Chaque application dispose elle-même de sa propre page, au sein de laquelle un niveau de détail supérieur peut être présenté afin de permettre d'éclairer les utilisateurs potentiels.

- **À titre de bonnes pratiques : quelles informations afficher dans les pages de chaque application ?**
  - La CNIL encourage la mise à disposition à l'utilisateur de l'ensemble des informations citées dans la partie 9.1 (« *Quelles informations obtenir de la part de chaque éditeur d'application ?* ») .
  - Ces informations pourraient être accessibles avant l'achat ou installation de l'application.
  - Dans le contexte des interfaces mobiles, il peut être complexe de rendre compréhensible l'ensemble de ces informations. Afin d'en faciliter la lecture, l'utilisation de représentations graphiques, par exemple l'utilisation d'icônes et de tableaux, en choisissant ceux-ci de manière à souligner les éléments ayant le plus d'impact en termes de protection de la vie privée, pourra être privilégiée.
  - L'utilisation de données à caractère personnel à des fins commerciales doit faire l'objet d'une information de la personne concernée préalablement à la conclusion du contrat[56]. La CNIL

[56] Les éditeurs d'applications ont l'obligation de délivrer au consommateur (ici l'utilisateur de l'application) les informations précontractuelles prévues à l'article L. 221-5 du code de la consommation, issu de la transposition de la directive 2011/83 sur les droits des consommateurs, dont les informations sur les caractéristiques essentielles du bien, du service, du service numérique ou du contenu numérique (C. consom., art. L. 221-5 I 1°).

encourage à rendre accessible cette information pour les utilisateurs directement au sein de la page de l'application.
    - L'information doit être présentée de manière neutre et contextualisée.

- **Quelles informations afficher dans l'interface de recherche ?**

    - A titre de bonnes pratiques, des filtres contenant des critères relatifs à la vie privée pourraient être mis à disposition dans l'interface de recherche. Ceux-ci pourraient être relatifs à l'utilisation de certaines permissions, la collecte de certaines données ou bien même relativement à un « score » relatif à des critères de vie privée.
    - Toujours à titre de bonnes pratiques, et si la création d'un tel score est envisagée, celui-ci devrait reposer sur une méthodologie préalablement définie, de manière transparente, par un acteur tiers au fournisseur de magasin d'applications et idéalement agréée entre les différents acteurs de l'écosystème et de la société civile. Le processus de calcul de ce score devrait également être également confié à un tiers, ou à défaut faire l'objet d'une certification par un tiers, notamment pour assurer qu'il remplit ses objectifs en termes de transparence. Une mise à disposition les données sources permettant le calcul de ce score dans un format ouvert et facilement exploitable, afin que des méthodologies alternatives puissent être proposées, est encouragée. A cet égard, il est rappelé qu'au terme de l'article 6-5 du DMA, le contrôleur d'accès « *n'accorde pas, en matière de classement ainsi que pour l'indexation et l'exploration qui y sont liées, un traitement plus favorable aux services et produits proposés par le contrôleur d'accès lui-même qu'aux services ou produits similaires d'un tiers. Le contrôleur d'accès applique des conditions transparentes, équitables et non discriminatoires à ce classement* ».
    - La CNIL rappelle, dans l'hypothèse de la mise en œuvre d'un tel score, que les applications éditées par les acteurs qui fournissent également des systèmes d'exploitation et/ou des SDK devraient être soumises aux mêmes règles que les applications tierces, en vertu du droit applicable en matière de concurrence.

## 2. Mettre à disposition des modalités claires de signalement

L'interface du magasin d'applications est un canal privilégié pour permettre la prise en compte des retours des utilisateurs.

- **Comment mettre à profit les retours et signalements des utilisateurs ?**
    - Conformément à l'article 16 du Règlement n° 2022/2065 sur les services numériques (dit « *Digital Services Act* » ou DSA), les fournisseurs de services d'hébergement, dont font partie les fournisseurs de magasins d'applications, doivent mettre en place des « *mécanismes permettant à tout particulier ou à toute entité de leur signaler la présence au sein de leur service d'éléments d'information spécifiques que le particulier ou l'entité considère comme du contenu illicite* ».
    - La CNIL recommande que les fournisseurs de magasins d'applications incluent dans ce dispositif la possibilité de signaler des pratiques possiblement contraires au RGPD, qui sont susceptibles d'entrer dans le champ des contenus illicites tels que définis à l'article 3.h du DSA (par exemple : manquement à l'exercice des droits, manquement aux obligations entourant le recueil du consentement, y compris à travers l'usage de designs trompeurs ou « *dark patterns*[57] », exécution de fonctionnalités SDK sans consentement préalable, présence de transferts non encadrés, etc.).
    - Ces remontées pourraient, à titre de bonne pratique, être utilisées pour orienter les contrôles opérés par le magasin sur les applications qu'il héberge.

## 3. Prévenir en cas de détection de vulnérabilité ou de nécessité de mise à jour

Le magasin d'applications est, sur le plan technique, l'acteur le plus en capacité de protéger massivement les utilisateurs contre les risques de sécurité. À titre de bonne pratique, il peut donc participer à la protection des utilisateurs.

- **Que faire en cas de détection de vulnérabilités actives ?**
    - La CNIL encourage le fournisseur du magasin d'applications à établir un protocole en cas de révélation de vulnérabilités dans une application ou d'un SDK largement déployés.

[57] A l'exclusion des pratiques couvertes par l'article 25 du DSA.

- Le fournisseur de magasin d'applications peut notamment mettre en œuvre des analyses (notamment statiques) pour déterminer les applications affectées par une vulnérabilité.
- Une fois les applications vulnérables détectées, plusieurs mesures peuvent être appliquées :
  - suspendre les mises à jour automatiques de tout ou partie du parc applicatif des utilisateurs ;
  - procéder au retrait temporaire de l'ensemble des applications vulnérables, rendant leur téléchargement impossible et protégeant les potentiels et futurs utilisateurs, tant qu'elles n'ont pas été mises à jour et que cette mise à jour ne passe pas le test de sécurité établi lors de la détection des applications vulnérables.
- Le fournisseur du magasin d'applications pourrait également analyser si une information de l'utilisateur est nécessaire. Si la vulnérabilité engendre des risques élevés pour les personnes concernées, il peut par exemple être envisagé d'afficher une notification système aux utilisateurs, leur indiquant qu'une ou plusieurs de leurs applications sont vulnérables.

## 9.4. Liste de vérifications

Ces vérifications ont pour objet de guider les fournisseurs de magasins d'applications dans la mise en œuvre de ces recommandations et sont présentées à titre indicatif. Certaines des vérifications à effectuer peuvent correspondre à des bonnes pratiques ou recommandations et non à des obligations : en cas de doute, se référer au texte de la recommandation.

| Catégorie | Sous-Catégorie | Identifiant | Description |
|---|---|---|---|
| **Analyser les applications soumises par les éditeurs** | Centraliser et analyser les données relatives à la conformité | 1.1.1 | Des éléments relatifs aux traitements, permissions demandées ou tiers accédants aux données sont demandés pour leur mise à disposition lors du processus de revue des applications. |
| | | 1.1.2 | Une politique de confidentialité et un point de contact sont définis et accessibles aux utilisateurs finaux, pour chaque éditeur d'application ayant au moins une application publiée dans le magasin. |
| | | 1.1.3 | Lorsqu'une application est destinée uniquement, majoritairement ou potentiellement à un public mineur, cette information est indiquée dans la page du magasin relative cette application. |
| | Encourager des pratiques mieux-disantes en termes de protection la vie privée lors de la publication et la mise à jour des applications | 1.2.1 | Lors du processus de revue, les éditeurs sont invités à ne pas demander des permissions en bloc lors de l'installation et sont encouragés à avoir une gestion des permissions à l'exécution. |
| | | 1.2.2 | Le fournisseur de magasin d'applications peut inciter les éditeurs d'applications à ne pas utiliser d'API de l'OS qui seraient trop larges ou obsolètes |
| | | 1.2.3 | Les éditeurs sont invités à publier des notes de mises à jour informatives pour les utilisateurs afin qu'ils puissent évaluer la nécessité de la mise à jour. |

| | | | |
|---|---|---|---|
| | Analyser les applicatifs pour détecter des failles de sécurité | 1.3.1 | Des analyses statiques sont effectuées sur chaque nouvelle application ou version d'application, avant toute publication dans le magasin. |
| | | 1.3.2 | Des analyses dynamiques sont effectuées sur les applications plus sensibles afin de détecter des comportements anormaux. |
| **Mettre en œuvre des processus transparents de revue des applications qui intègrent la vérification des règles élémentaires de protection des données** | Intégrer la vérification des règles élémentaires de protection des données dans les processus de revue des applications | 2.1.1 | Dans le cas où l'application traite des données personnelles, est vérifié la présence des éléments suivants dans les informations aux usagers :<br>• l'identité et les coordonnées du responsable du traitement<br>• les finalités du traitement ainsi que sa base juridique<br>• la durée de conservation des données personnelles<br>• selon la base légale, l'existence d'un moyen d'expression des droits<br>• le droit d'envoyer une plainte à l'autorité compétente |
| | | 2.1.2 | Les applications visant le marché européen qui ne sont pas en mesure de fournir ces éléments ne sont pas publiées dans le magasin d'application. |
| | Exprimer clairement les attentes et les processus mis en œuvre | 2.2.1 | Les éditeurs d'applications sont correctement informés, notamment sur les éléments de conformité qui leur incombent selon les critères du magasin. La mise à jour de ces éléments, dans le temps, leur est communiquée. |
| | Faciliter l'utilisation des outils mis à disposition | 2.3.1 | Une gestion fine des accès aux comptes éditeurs du magasin d'applications est proposée, de sorte que plusieurs utilisateurs puissent avoir un usage distinct des dépôts, des signatures de versions, des notes de mises à jour. |
| | | 2.3.2 | Un canal clair de communication entre les entités publiant des applications mobiles et le magasin d'applications est affiché, en favorisant un canal intégré au magasin d'applications lui-même. |
| | | 2.3.3 | Les refus de publication et les correctifs à appliquer pour pallier ce refus ainsi que les éventuels recours sont indiqués clairement aux éditeurs et s'appuient sur les éléments de documentation dédiés. |
| **Informer les utilisateurs et leur fournir** | Normaliser et mettre à disposition les données | 3.1.1 | L'ensemble des informations relatives à la vie privée, transmises par les éditeurs ou connue du |

| | | | |
|---|---|---|---|
| **des outils de signalement** | relatives à la conformité | | magasin, sont accessibles à l'utilisateur final avant achat ou téléchargement. |
| | | 3.1.2 | L'ensemble des informations, requises ou utiles, à destination de l'utilisateur final sont affichées dans un format adapté au système dans lequel elles sont amenées à être consultées. |
| | | 3.1.3 | Des filtres relatifs à la vie privée sont proposés parmi les options de recherche. |
| | Mettre à disposition des modalités claires de signalement | 3.2.1 | Les utilisateurs finaux ont la possibilité de signaler des applications qui ne remplirait pas leurs obligations, directement depuis le magasin. |
| | Prévenir en cas de détection de vulnérabilité ou de nécessité de mise à jour | 3.3.1 | Un protocole est défini concernant les actions à mener lors de la détection, via une analyse statique ou dynamique, d'une vulnérabilité au sein d'une application mobile déjà publiée dans le magasin. |
| | | 3.3.2 | Un affichage spécifique est proposé aux utilisateurs finaux, intégré à la page de l'application dans le magasin, sur un potentiel risque pour la sécurité. |

# 10. Glossaire

## Application mobile

La notion d'application mobile désigne les logiciels applicatifs distribués dans l'environnement des mobiles multifonctions (ou « *smartphones* ») et tablettes.

Ces applications sont exécutées de manière isolées (ou en mode « bac à sable ») par un système d'exploitation qui limite les fonctionnalités auxquelles elles peuvent accéder via un système de permissions.

## Kit de développement logiciel ou SDK

Le kit de développement logiciel (« *software development kit* » ou SDK) désigne un ensemble d'outils utilisés pour le développement de l'application, en fonction du système d'exploitation utilisé.

Cette pratique, extrêmement développée dans l'écosystème mobile, est notamment due au fait que les SDK permettent le plus souvent de faciliter ou d'accélérer le développement de fonctionnalités logicielles, en évitant au développeur d'écrire l'intégralité du code de l'application.

Ces SDK sont en général intégrés par l'ajout du code offert par ceux-ci dans l'application développée, code qui va éventuellement permettre de s'interfacer avec l'infrastructure du fournisseur de SDK pour mettre en œuvre la fonctionnalité. Ils recouvrent de nombreuses fonctionnalités, mais les plus fréquentes sont l'analyse d'audience (« *analytics* »), la sélection et la diffusion de publicités ou les fonctionnalités de commerce électronique.

## Mode « bac à sable » (« sandboxing »)

L'exécution en mode « bac à sable » ou « *sandboxing* » est un mécanisme de sécurité mis en œuvre par un système d'exploitation pour isoler une application exécutée vis-à-vis du cœur du système d'exploitation, mais aussi des autres applications exécutées sur le terminal (ordinateur, mobile, etc.).

Cette isolation permet de réduire le risque qui pourrait être lié à l'abus de fonctionnalités du terminal, mais aussi à des tentatives d'une application pour accéder à des données ou perturber le fonctionnement d'une application tierce.

En général, les applications s'exécutant en mode « bac à sable » ont des fonctionnalités par défaut assez réduites, n'ayant la possibilité d'utiliser que des API fournies par le système d'exploitation, avec la permission de l'utilisateur.

## Interface de programmation d'application (API)

Une API (*application programming interface* ou « interface de programmation d'application ») est une interface logicielle qui permet de mettre en relation un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

Les API donnent de nombreuses fonctionnalités, comme la portabilité des données, la mise en place de campagnes de courriels publicitaires, des programmes d'affiliation, l'intégration de fonctionnalités d'un site sur un autre ou l'accès à des entrepôts de données ouverts. Leur accès peut être gratuit ou payant.

Dans le contexte des applications mobiles, les API sont également le moyen par lequel le système d'exploitation (OS) expose toute un ensemble de fonctionnalités aux applications.

## Système d'exploitation (OS)

Le système d'exploitation (ou « *operating system* », OS) est la brique logicielle la plus proche du matériel informatique, allouant les ressources disponibles (ressources de calcul, mémoire, accès aux périphériques) aux différents éléments applicatifs qui en font la requête.

Dans le contexte des applications mobiles, le système d'exploitation est la brique logicielle qui définit et permet l'ensemble des interactions possibles entre l'utilisateur et le terminal, mais également entre les applications mobiles tierces (c'est-à-dire celles ajoutées *a posteriori* par l'utilisateur) et le terminal. Il met en œuvre notamment l'exécution en « bac à sable » (« *sandboxing* ») des applications, ainsi que le système de permission permettant l'accès aux fonctionnalités du terminal.

## Permission d'accès

Les permissions d'accès sont des dispositifs mis en œuvre par les systèmes d'exploitation (OS) des terminaux mobiles pour permettre aux utilisateurs de choisir quelles fonctionnalités sont accessibles aux applications mobiles.

Ces applications mobiles n'ont, en effet, qu'un accès limité à ces fonctionnalités par défaut, pour des raisons de sécurité et de protection de la vie privée. Le système d'exploitation met donc à leur disposition des API leur permettant d'effectuer des requêtes afin de se voir autoriser des fonctionnalités additionnelles, sous réserve que l'utilisateur l'accepte via une interface fournie par le système d'exploitation.

Il existe en pratique différents types de permissions. Les permissions techniques visent ainsi à donner ou bloquer l'accès à certaines ressources protégées, indépendamment des finalités pour lesquelles l'accès à ces ressources est demandé. D'autres permissions visent quant à elles à autoriser ou refuser la réalisation de certaines actions en vue d'une finalité précise, grâce à l'accès à certaines ressources mais également par d'autres moyens.

## Mesure d'audience (« *analytics* »)

La gestion d'un site web ou d'une application mobile peut impliquer dans de nombreux cas l'utilisation de services permettant de collecter des statistiques de fréquentation ou de performance, en général regroupées sous le terme de mesure d'audience ou d'« *analytics* ». Ces outils peuvent en pratique être de natures très diverses, allant de mesures très simples qui peuvent parfois se révéler indispensables pour la bonne gestion du service à des outils proposant des fonctionnalités complexes d'analyse, telles que de les « tests A/B » ou « *AB testing* » (présentant différentes versions du site à différents utilisateurs), des cartes de chaleur ou « *heatmap* » (présentant l'agrégation des navigations des utilisateurs) ou du rejeu de session (permettant de visualiser le parcours d'un utilisateur unique). Certains outils commerciaux (d'analyse des sources de trafic ou de publicité ciblée) sont parfois abusivement présentés comme des solutions de mesure d'audience.

## Identifiant publicitaire

Les identifiants publicitaires sont des identifiants numériques, souvent représentés sous forme de chaînes de caractères, générés et associés à un terminal par le système d'exploitation (OS), et qui peuvent, sous certaines conditions dépendantes du système d'exploitation en question, être mises à disposition des applications qui en font la demande.

Ces identifiants sont spécifiquement conçus pour permettre l'identification d'un unique utilisateur par différentes applications, identification rendue en dehors de celui-ci impossible par l'exécution en mode « bac à sable » (« *sandboxing* ») des applications.

Cette identification permet notamment le ciblage publicitaire. Par exemple, si un utilisateur est connecté sur un réseau social depuis son téléphone et que des applications tierces embarquent le module de ciblage de ce réseau social, l'accès à l'identifiant publicitaire permettra d'utiliser les données relatives au profil de la personne pour cibler de la publicité dans le contexte de ces applications tierces.

## Géolocalisation

La géolocalisation est une technologie permettant de déterminer la localisation d'un objet ou d'une personne en renvoyant le résultat sous la forme de coordonnées géographiques. La technologie s'appuie généralement sur le système GPS ou sur les interfaces de communication d'un téléphone mobile, et peut renvoyer des résultats avec une précision plus ou moins importante. Les applications et finalités de la géolocalisation sont multiples : de l'assistance à la navigation, à la mise en relation des personnes, mais aussi à la gestion en temps réel des moyens en personnel et en véhicules des entreprises, etc. Cette technique fait partie du groupe plus général des techniques de localisation, mais celles-ci peuvent sortir du concept de géolocalisation, par exemple en renvoyant la localité plutôt que les coordonnées géographiques.