Projet de recommandation

Relative aux applications mobiles

Version soumise à consultation publique

jusqu'au 8 octobre 2023

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, à l'heure actuelle, les traitements de données mis en œuvre au sein des applications peuvent être opaques. En particulier, les informations sur l'existence de collectes de données et leurs objectifs sont souvent peu clairs. De même, 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.

Il est donc indispensable que les acteurs participant à la mise à disposition d'applications mobiles s'assurent du respect de leurs obligations en matière de protection des données et des droits des utilisateurs. Or, 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 est parfois incertaine.

La présente recommandation vise à clarifier ces règles afin que les acteurs de l'écosystème mobile aient une bonne compréhension de leurs obligations et des bonnes pratiques à mettre en œuvre, pour faciliter leur mise en conformité.

[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, 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 et à guider les professionnels de l'environnement des applications mobiles dans leur conformité à la réglementation relative à la protection des données.

Il s'adresse aux professionnels évoluant dans le secteur des applications mobiles décrits ci-dessous, 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 délégués à la protection des données de chacun de ces acteurs. Elle est également à l'usage de tous les conseils en matière de protection des données personnelles.

Elle a vocation en premier lieu à 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 les obligations qui lui incombent.

Les obligations et recommandations 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, celles-ci étant susceptibles de le concerner de manière incidente.

La recommandation s'intéresse aux traitements de données personnelles des personnes physiques utilisatrices des applications mobiles.

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.

- 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 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 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) ;
- Etc.

2.3. Quels sont les acteurs évoluant dans le secteur des applications mobiles ?

De multiples acteurs interviennent dans l'écosystème des applications mobiles, qui procèdent à des traitements de 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 pourrons 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). Ces applications étant préinstallées, il n'est en principe pas possible pour l'utilisateur final de les désinstaller.

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[3] 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] 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 et gère des identifiants propres à chaque terminal ou compte utilisateur, qui 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 propre compte 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, géolocalisation 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 mis en œuvre 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 publication 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 de l'application met à celle-ci 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 lui-même ou déjà présentes sur son terminal, données inférées de sa navigation. Il peut ainsi s'agir de toute donnée nécessaire à la fourniture d'un bien ou service au travers de cette application (données de contact, de paiement, de géolocalisation, etc.), comme de données liées au fonctionnement de l'application en elle-même (recueil de 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 cette occasion 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, le développeur développe l'application pour le compte de l'éditeur, ce qui peut l'amener à avoir accès à des données personnelles des utilisateurs de l'application pour réaliser les développements

demandés par l'éditeur et procéder à des opérations de maintenance (tests de préproduction, analyse des données [*analytics,* en anglais], remontées d'erreurs, etc.).

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, 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 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 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 permettant, à l'instar du code écrit par le développeur lui-même, de procéder à différentes opérations. 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.).

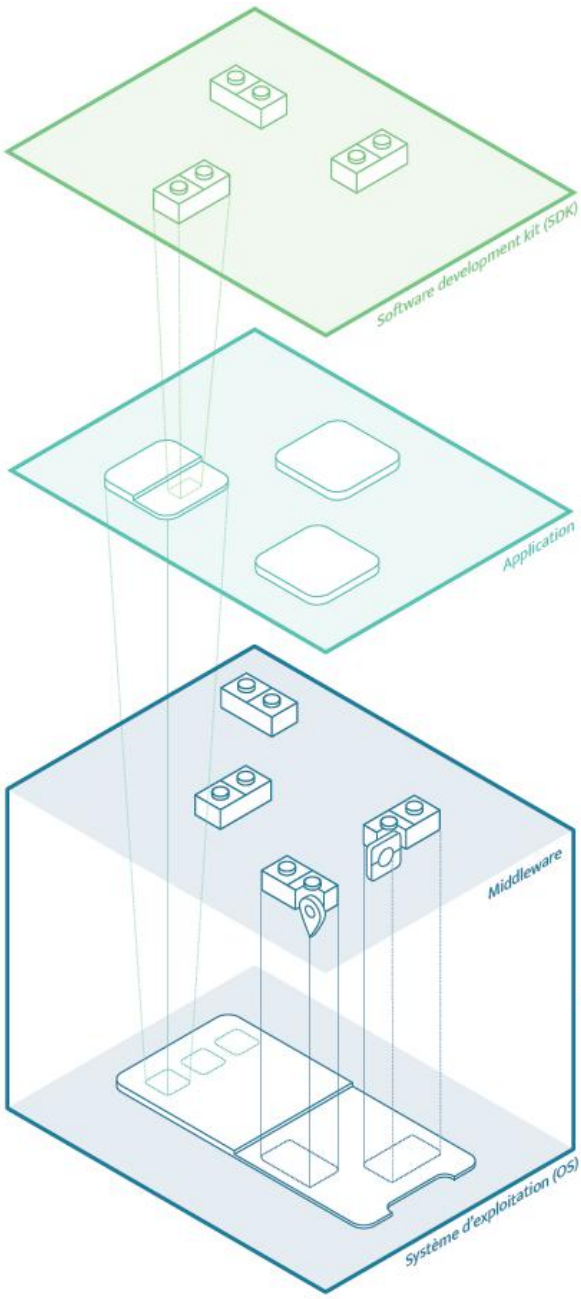
D'autres SDK permettent d'effectuer des demandes d'accès à l'OS, comme par exemple à l'identifiant publicitaire unique associé au terminal, ainsi que sa géolocalisation le cas échéant (en fonction des spécificités du SDK) et donc de tracer l'utilisateur de l'application à différentes fins : finalités marketing, publicitaires, etc.

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 ;
- etc.



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 : mise à disposition de code sous licence libre ou *open source*, mise à disposition de services logiciels destinés à être intégrés dans des OS, etc.

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 suivantes 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 « 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 du mobile** (identifiant unique du terminal, adresse MAC, etc.)[4] ;
- l'**accès à certaines informations contenues dans le terminal** (galerie photographique, contacts, etc.) ;
- l'**accès à certains capteurs du terminal** (appareil photo, microphone, géolocalisation etc.) ;
- etc.

Focus : le rôle des identifiants du mobile

- Dans l'écosystème des applications mobiles, ce sont des identifiants spécifiques à cet environnement qui permettent 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)[5], ou au compte de l'utilisateur authentifié au sein de l'environnement du système d'exploitation[6], 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

[4] 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).

[5] 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 d'*ordiphones*.

[6] Par exemple l'UDID dans l'environnement iOS (Apple), pour « *Unique Device IDentifier* », qui permet d'identifier un terminal Apple (iPhone, iPad, etc.).

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.

- 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[7]).

3.2. Application du RGPD

Champ d'application matériel

Le **RGPD** s'applique si l'application traite des données personnelles.

Si l'application traite des données personnelles, **le RGPD s'appliquera en principe à l'ensemble des traitements de données à caractère personnel mis en œuvre par l'application.**

Champ d'application territorial

Pour rappel et conformément à l'article 3 du RGPD, celui-ci s'applique :

- 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, 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 se trouvant 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, dès lors qu'une application serait destinée à des personnes dans l'UE et que l'application traite les données de ces mêmes personnes, le RGPD s'appliquera aux traitements réalisés au sein de cette application, quand bien même ceux-ci 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 exclusivement de l'exemption domestique. Ils doivent être réalisés par une personne physique et respecter les conditions posées par l'article 2.2.c et le considérant 18 du RGPD. Il s'agit d'une part d'activités « personnelles », qui sont souvent propres à l'activité d'un seul individu et effectuées en principe dans un cadre non professionnel ; d'autre part, d'activités « domestiques », qui sont communes à un nombre limité de personnes, dans un cadre familial ou amical.

[7] « *Cookies* et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », cnil.fr

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 ?

Lorsque l'exemption domestique s'applique à un traitement, **le RGPD ne s'applique pas à la personne physique effectuant ce traitement.**

Le RGPD s'applique toutefois aux tiers fournissant les moyens du traitement exempté si ces derniers peuvent être qualifiés de responsables de traitement ou de sous-traitants au sens du RGPD (considérant 18). L'exemption domestique a alors un effet limité. Si en revanche les tiers fournissant les moyens du traitement ne sont pas responsables de traitement, le RGPD ne s'appliquera pas au traitement des données personnelles effectué dans ce cadre.

Dans quels cas considère-t-on que le RGPD ne s'applique pas aux tiers fournissant les moyens du traitement exempté ?

La CNIL considère qu'en principe, si les deux critères cumulatifs suivants sont respectés, les tiers fournissant les moyens du traitement relevant de l'exemption domestique ne pourront revêtir aucune qualification au sens du RGPD (qu'il s'agisse de la qualification de responsable du traitement ou de sous-traitant) et le RGPD ne leur sera par définition pas applicable :

- le traitement est effectué à l'initiative, à la discrétion et pour le seul compte de la personne (ici l'utilisateur de l'application), c'est-à-dire décidé et mis en œuvre par cette dernière ;
- le traitement est effectué sous le contrôle de la personne, c'est-à-dire en parfaite autonomie, et dans un environnement cloisonné à savoir sans intervention possible de tiers sur ces données. Le tiers a fourni les moyens du traitement mais il n'agit plus en aval sur les données, ne les manipule pas.

En effet, dans ces conditions, l'acteur ne déterminera pas les finalités et les moyens du traitement effectivement mis en œuvre ni n'agira sur instruction d'un autre acteur déterminant les finalités et les moyens du traitement. Il ne fait que fournir un logiciel au service de l'utilisateur.

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

Ainsi, la CNIL a par exemple considéré que le RGPD ne s'appliquait pas, dans certaines conditions, aux éditeurs d'applications fournissant les moyens du traitement 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.

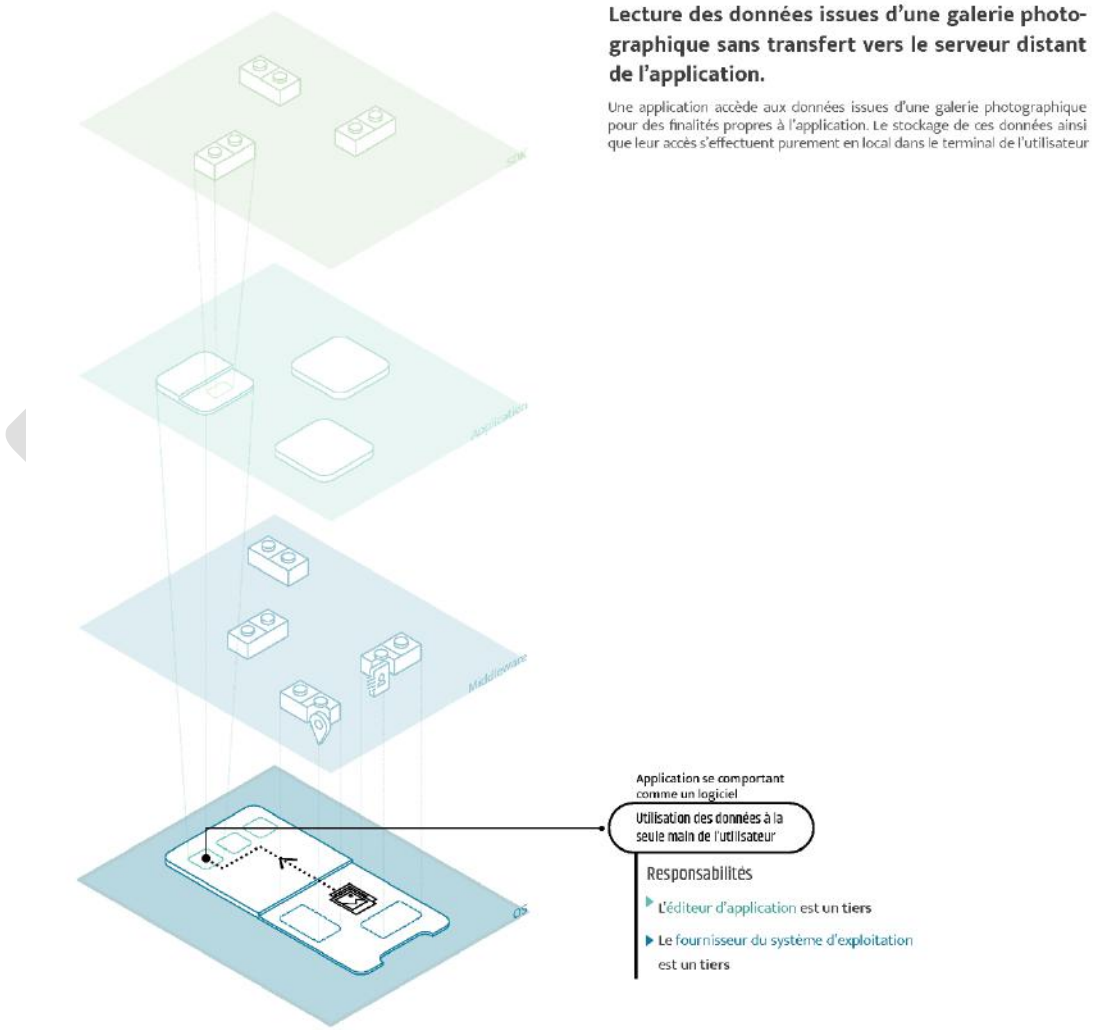
Le même raisonnement pourrait s'appliquer aux éditeurs d'applications fournissant les moyens du traitement dans les cas suivants :

- 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 (p. ex. : clavier avec configuration évolutive (« apprentissage ») locale sans fédération, fonctionnalités impliquant une interaction entre l'utilisateur et des données pré-enregistrées statiquement dans l'application).

En pratique, une application qui fonctionne sans aucune intervention de la part de son fournisseur ni transmission de données vers celui-ci a de fortes probabilités de pouvoir relever de l'exemption domestique. Une application qui pourrait continuer à fonctionner normalement malgré la disparition de son éditeur est particulièrement susceptible de répondre à ces critères.

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

Une application accède aux données issues d'une galerie photographique 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 à 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 encourage vivement 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 relèvent ainsi de l'exemption domestique et garantissent le respect de la vie privée dès la conception.

La CNIL formule toutefois deux recommandations complémentaires pour ces traitements domestiques :

- les applications relevant de l'exemption domestique étant sous le contrôle exclusif des utilisateurs, la CNIL les incite vivement à veiller à la sécurité de leurs applications : il leur est notamment recommandé de maintenir à jour les version de leurs applications et de ne pas utiliser une application pour laquelle des vulnérabilités logicielles sont connues. À titre de bonne pratique, dans ce dernier cas, la CNIL recommande à l'éditeur de l'application d'indiquer si celle-ci ne doit plus être utilisée, ou de la déréférencer du magasin d'applications ;
- les éditeurs et concepteurs de ces applications, quoique ne relevant pas du RGPD pour la mise en œuvre des traitements et n'étant donc pas soumis à ce titre à des obligations de sécurité, devraient concevoir celles-ci dans le respect des principes de minimisation et de sécurisation des données du RGPD afin de limiter les risques que courent les utilisateurs en cas de compromission.

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

Pour rappel, l'utilisateur de l'application respectant les conditions de l'exemption domestique ne pourra être qualifié de responsable du traitement ainsi exempté.

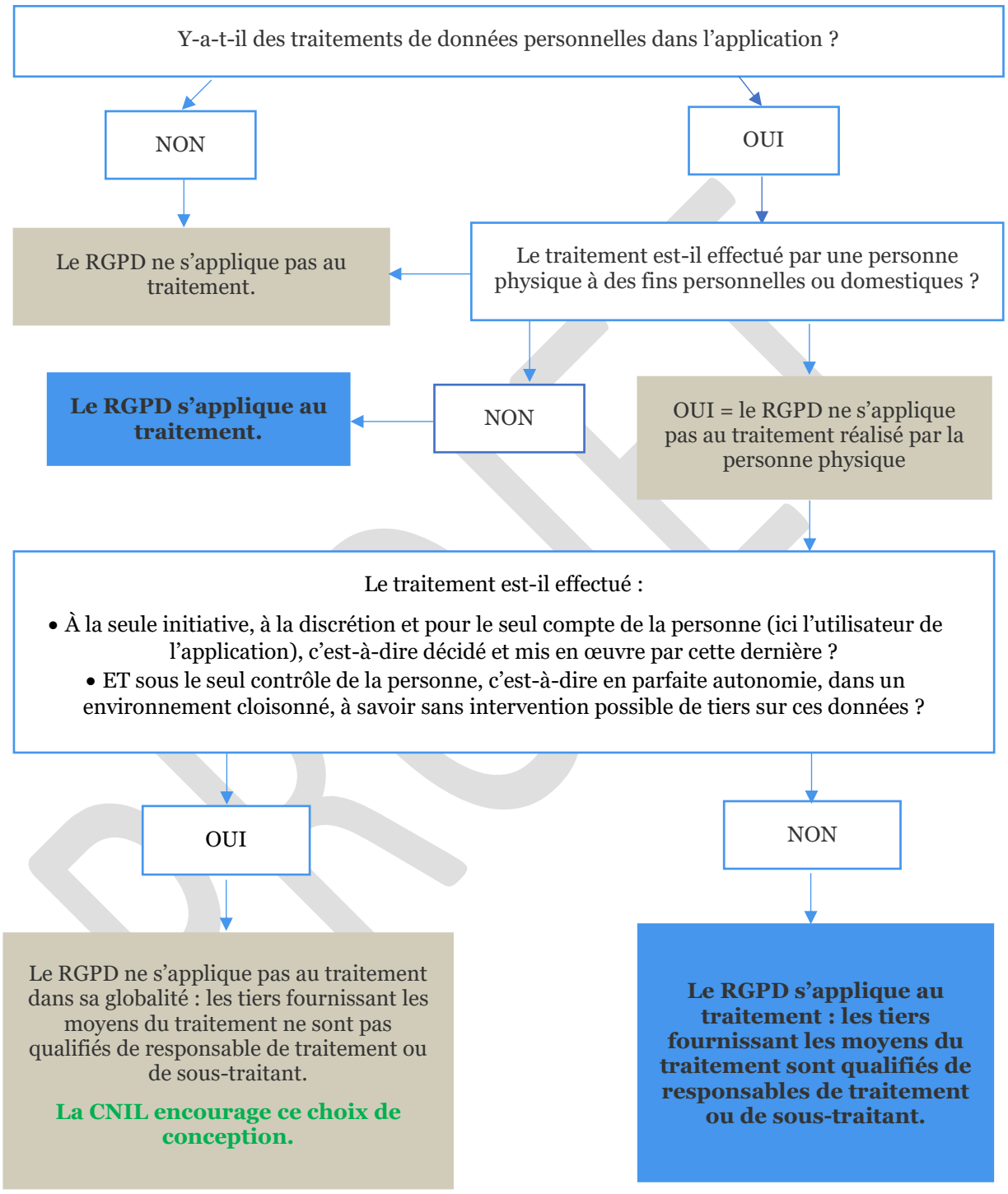
Le RGPD s'applique en revanche à l'éditeur de l'application, fournisseur des moyens du traitement, lorsque ce dernier ne respecte pas les conditions cumulatives précisées ci-dessus, auquel cas il doit être qualifié de responsable du traitement.

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

Dans cette hypothèse, le RGPD ne s'applique pas au créateur de l'album photo car ce traitement 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 de galerie photographique doit être qualifié de responsable du traitement dès le moment où l'album est stocké dans des serveurs de tiers (ceux de l'éditeur de l'application ou d'autres) pour être partagé entre les autres utilisateurs.

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

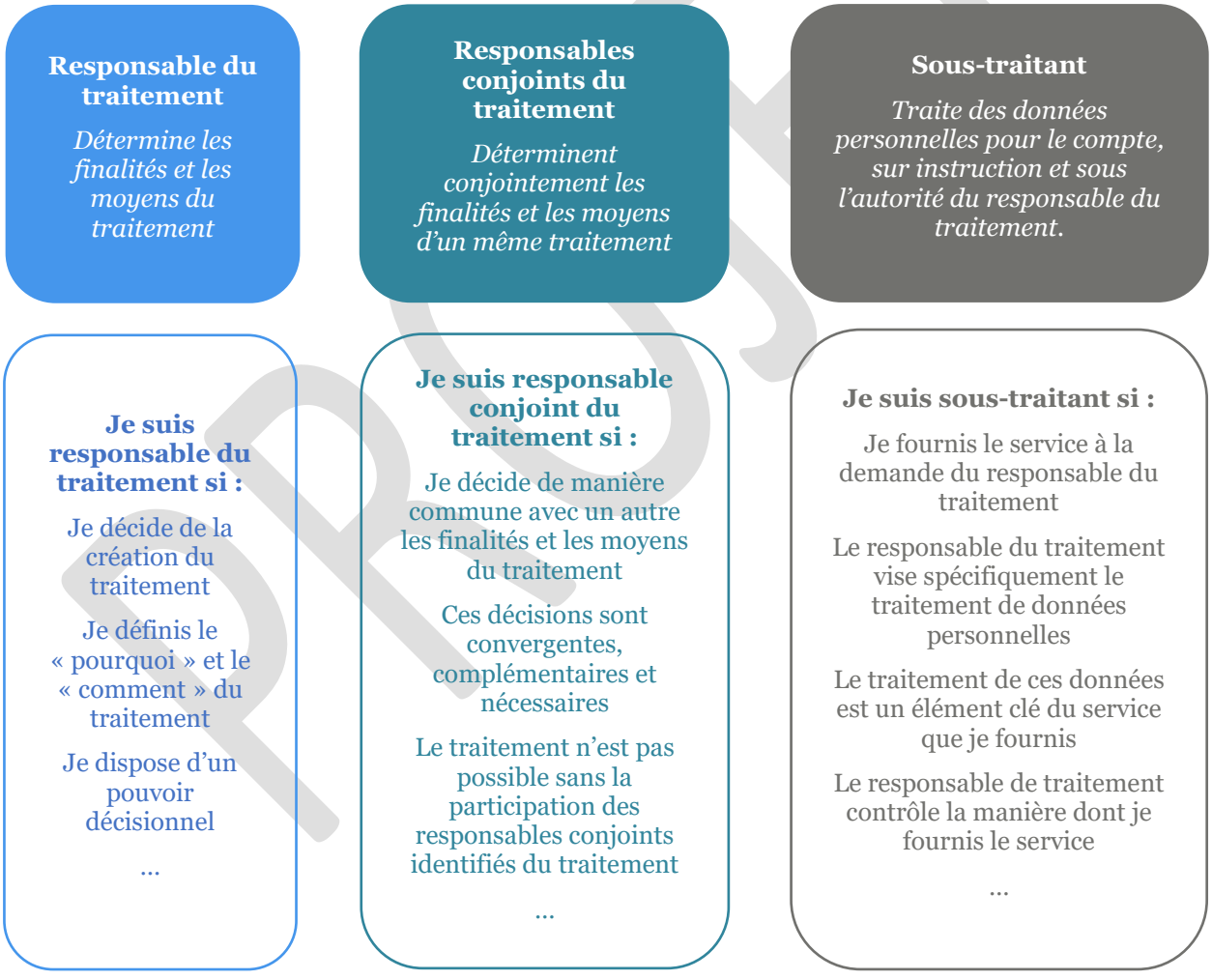
- Article 2 du RGPD
- Article 4 du RGPD
- Article 82 de la loi Informatique et Libertés

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 intervenant 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[8] ;
- Responsable conjoint du traitement ;
- Sous-traitant[9].



[8] 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).
[9] 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).

La ligne de partage entre ces trois qualifications peut parfois être délicate à fixer, dans la mesure où une multitude d'acteurs intervient dans le développement et le fonctionnement des applications mobiles et où la manière dont sont traitées les données personnelles est unique pour chaque application.

Il faut par ailleurs souligner que 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.

La question de la qualification de chaque acteur se pose pour chaque traitement de données personnelles réalisé au sein d'une application.

Conformément au principe de redevabilité (« *accountability* ») posé par le RGPD, il revient à chaque acteur de déterminer lui-même sa qualification au regard de son rôle effectif ; les acteurs ne peuvent pas choisir en opportunité la qualification qu'ils préfèrent : ils doivent être en mesure d'argumenter et 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 ? quelles sont les données personnelles collectées ? quelles en sont les durées de conservation ? quelles sont les mesures de sécurité mises en place ? etc. Les acteurs doivent démontrer qu'une réflexion approfondie a été menée pour déterminer la qualification à retenir, du point de vue des critères différenciant le responsable de traitement, le responsable conjoint de traitement et le sous-traitant. La réflexion menée sur la qualification des acteurs peut être formalisée dans différents types de supports tels que l'analyse d'impact relative à la protection des données.

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 la spécificité des situations particulières et des modes de fonctionnement auxquels les divers acteurs sont confrontés.

Les autorités de contrôle ne sont pas liées par les qualifications choisies par les parties, notamment au sein des contrats ; une requalification, appréciée au regard des justifications fournies, est donc toujours possible.

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 mais participe à son fonctionnement (par exemple, si ce fonctionnement implique des communications entre le terminal de l'utilisateur et des serveurs de l'éditeur), l'éditeur de l'application est, en principe, 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 au sein de l'application, durée de conservation des données, exigences de sécurité, etc.).

Il peut en particulier être **responsable** :

- **des traitements de données personnelles réalisés à l'occasion du recours aux services proposés à travers l'application, par exemple :**
  - les données issues de la gestion du compte de l'utilisateur (nom, prénom, adresse courriel, numéro de téléphone, etc.) ;
  - les données nécessaires à l'utilisation des services proposés au sein de l'application (adresse de livraison, données bancaires, numéro de carte de réduction, etc.) ;
- **des opérations de lecture et/ou d'écriture qu'il réalise lui-même 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 (en tant qu'éditeur d'application) 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 (en tant qu'éditeur d'applications système) de l'identifiant du compte de l'utilisateur pour suivre son activité pour améliorer les fonctionnalités de celles-ci ;
        - etc.
    - l'accès aux différents capteurs du terminal mobile (appareil photo, géolocalisation, etc.) lorsque les données sont transmises à travers un réseau pour diverses finalités, par exemple :
        - lecture de la géolocalisation 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 ;
        - etc.
    - 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 photo de l'utilisateur 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 ;
        - etc.
- **des opérations de lecture et/ou d'écriture réalisées par des tiers[10] (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 par un SDK tiers utilisé par l'application à des fins de profilage publicitaire des utilisateurs pour le compte de l'éditeur : l'éditeur de l'application est responsable du traitement s'agissant de l'opération consistant en la lecture de l'identifiant publicitaire (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 uniquement s'agissant de l'opération consistant en la lecture de l'identifiant technique ;
    - etc.
- **des opérations de lecture et/ou d'écriture effectués par des tiers pour le compte de l'éditeur ainsi que des traitements qui en sont issus et qui sont également effectués par ces tiers pour le compte de l'éditeur.** 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 ;
    - etc.

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, par une opération de collecte dont l'éditeur est co-responsable, le tiers doit dûment informer et obtenir l'accord de l'éditeur avant de récupérer les données pour mettre en œuvre de tels traitements pour son propre compte. Par exemple :

[10] 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 rendue par le Conseil d'État le 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.

- lecture d'un identifiant technique à travers l'application pour le compte du tiers pour réaliser des statistiques à des fins d'amélioration de son service : l'éditeur n'est pas responsable des traitements statistiques ultérieurs effectués par le tiers sur la base de cette opération ;
- lecture de l'identifiant publicitaire unique de l'application pour le compte du 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 sur la base de cette opération ;
- etc.

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[11]. Celle-ci est applicable aux traitements de données personnelles réalisés par des tiers pour leur propre compte à travers une application mobile.

Qualification du développeur

L'éditeur peut, selon les cas, faire développer son application par un développeur externe. Se pose alors la question de la qualification du développeur si le RGPD lui est applicable.

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

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 qu'il souhaite proposer au public, mais 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.

En pratique, cependant, le rôle du développeur est 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 juridiquement au responsable de traitement, la sécurité de l'application repose en pratique sur les choix du sous-traitant. La CNIL recommande donc, dans cette configuration :

- que le contrat liant le développeur à l'éditeur impose à celui-là de concevoir une application permettant que les données traitées le soient conformément au RGPD et dans une logique de respect de la vie privée 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.

Il est enfin rappelé que fournir une application dont le fonctionnement méconnaîtrait par lui-même le RGPD peut engager la responsabilité civile du développeur vis-à-vis de l'éditeur[12].

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

Le développeur pourra souvent être qualifié de **sous-traitant** s'il traite des données personnelles pour le compte de l'éditeur, agissant en tant que 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 relative à l'application mobile ;
- 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 ;
- etc.

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

Par exception, le développeur pourra 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 des autres applications qu'il développe ;

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

[12] 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).

- 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 ;
- etc.

Dès lors qu'il envisage d'utiliser des données collectées via l'application pour son propre compte, le développeur est tenu d'informer l'éditeur de l'application des finalités de cette collecte et d'obtenir son accord préalable avant de récupérer les données pour mettre en œuvre de tels traitements pour son propre compte.

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[13]. Celle-ci est applicable aux traitements de données personnelles réalisés par des tiers pour leur propre compte à travers une application mobile.

Qualification du fournisseur de SDK

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

Dans certains cas, l'éditeur peut y recourir de sa propre initiative, lorsqu'il procède lui-même au développement de son application ou lorsqu'il indique expressément à son développeur d'inclure un SDK en raison d'un accord commercial.

Dans d'autres cas, il ne décide pas directement d'y recourir, lorsque le développement de l'application et le choix du SDK est réalisé par un développeur externe.

En pratique, des échanges de données ont souvent lieu entre ces différents acteurs. Se pose alors la question de la qualification du SDK lorsque ce dernier traite des données personnelles, étant précisé que le RGPD ne s'applique pas au SDK qui ne traite aucune donnée personnelle issue de l'application pour réaliser les développements (p. ex : cela peut être le cas notamment lorsque le SDK fourni ne traite aucune donnée personnelle, et en particulier ne traite pas l'adresse IP de l'utilisateur de l'application).

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

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

Cela peut être le cas par exemple 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 géolocalisation de l'utilisateur d'une application mobile dans le but de le profiler pour le compte de l'éditeur.

Dans l'hypothèse où le développement de l'application serait assuré par un sous-traitant des données personnelles, le fournisseur du SDK mis en place dans l'application par le développeur externe serait considéré comme un sous-traitant ultérieur du développeur sous-traitant initial.

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

Le fournisseur de SDK peut être responsable de certains traitements de données personnelles effectués dans l'application, s'il en détermine les finalités et les moyens, c'est-à-dire l'objectif et la façon de les réaliser.

Il peut en particulier être responsable :

- **des opérations de lecture et/ou d'écriture qu'il réalise (conjointement avec l'éditeur qui permet cette collecte).** Il peut s'agir par exemple :
  - de la lecture de l'identifiant publicitaire unique à travers l'application à des fins de profilage publicitaire des utilisateurs ;

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

- de la lecture d'un identifiant technique du terminal de l'utilisateur à travers l'application pour réaliser des statistiques à des fins d'amélioration du service ;
- etc.

- **des traitements portant sur les données personnelles issues de ces opérations, lorsque ceux-ci sont réalisés pour son propre compte avec l'accord préalable de l'éditeur.** Le fournisseur de SDK est tenu de s'assurer de la bonne information de l'éditeur de l'application, responsable du traitement initial, avant de mettre 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 ;
  - etc.

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.

Celle-ci est applicable aux traitements de données personnelles réalisés par des tiers pour leur propre compte à travers une application mobile.

Qualification du fournisseur du système d'exploitation

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

Le fournisseur du système d'exploitation peut être considéré comme responsable des traitements du terminal, 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 moyens et finalités.

Ces traitements sont, pour une grande partie, indépendants des applications susceptibles d'être exécutées au sein du système d'exploitation, mais certains sont en lien avec elles, notamment parce qu'ils fournissent aux applications des informations et identifiants dont certains sont des données personnelles concernant l'utilisateur.

Certaines situations doivent faire l'objet d'une analyse au cas par cas pour déterminer la qualification du fournisseur du système d'exploitation, en fonction des paramètres et spécificités de chaque environnement, qu'il s'agisse notamment :

- de l'opération de création en local d'un identifiant mobile ;
- de la mise à disposition d'un identifiant mobile à un tiers, notamment un éditeur d'applications ;
- de 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 en l'état 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[14].

[14] Ainsi, à titre d'exemple, à la date d'adoption de la présente recommandation, 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

- 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.**

En tout état de cause, et 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, de 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 recommandations (voir la partie 8 des présentes recommandations : « Recommandations spécifiques au fournisseur d'OS »), indépendamment de leur responsabilité au sens du RGPD, s'agissant des configurations qu'ils déterminent (recueil des différentes permissions, accès aux API, etc.). Ces recommandations applicables aux OS sont susceptibles de constituer des obligations légales en cas de qualification de l'éditeur de l'OS de responsable du traitement.

Qualification du magasin d'applications

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

Le magasin d'applications appréhendé en tant qu'acteur édictant des règles relatives à la publication des applications au sein du magasin d'applications ne dispose pas à ce titre d'une qualification au sens du RGPD. En effet, s'il peut, dans une certaine mesure, influencer l'éditeur et/ou le développeur sur la conformité des applications au RGPD (par exemple en définissant des règles de présentation des demandes de permissions à l'utilisateur), cette circonstance est sans incidence sur ses responsabilités au titre du RGPD car il ne traite pas de données personnelles à cette occasion.

Et quand le fournisseur du magasin d'applications agit en tant qu'éditeur du magasin, en tant qu'application mobile ?

En revanche, l'éditeur du magasin, appréhendé en tant qu'éditeur d'applications, se verra appliquer les mêmes qualifications et obligations que pour n'importe quel éditeur d'applications. Ainsi, lorsque le 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 pourra être qualifié de responsable du traitement dès lors qu'il en définit les moyens et finalités.

Exemples

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

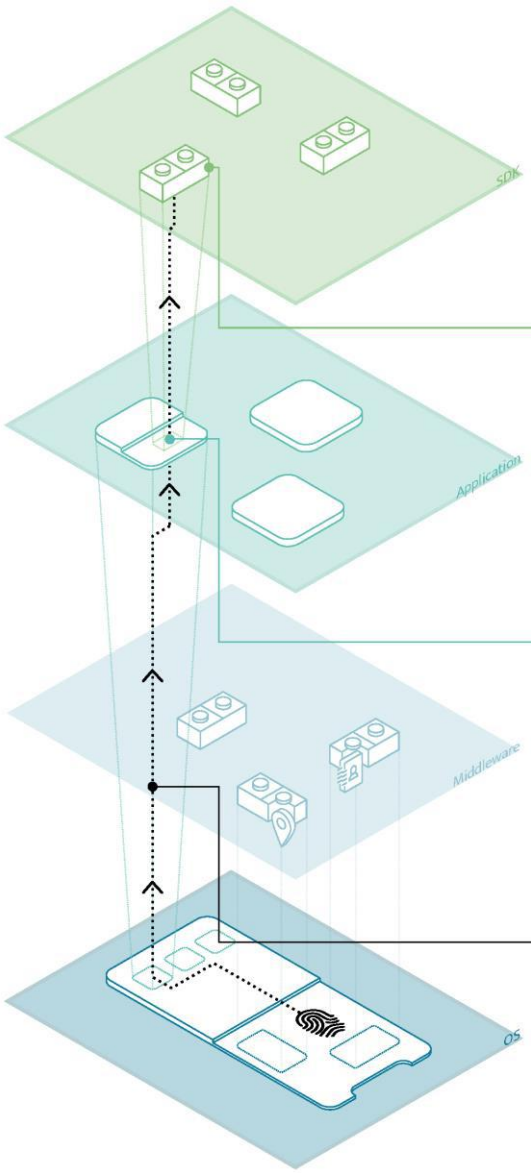
Un éditeur d'application fait appel aux services d'un fournisseur de SDK pour faciliter le développement de son application. Celui-ci introduit un SDK dans l'application ayant pour fonctionnalité d'accéder à l'identifiant publicitaire unique du mobile afin de pouvoir suivre le comportement de l'utilisateur dans l'application. 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 de l'application afin de lui permettre de connaître son audience et ainsi de monétiser les espaces publicitaires présents dans l'application auprès d'annonceurs. Les données collectées par le SDK permettent à son fournisseur de poursuivre par ailleurs 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'inclusion au sein de l'application d'un SDK ayant pour fonction d'accéder 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 ;
- s'agissant des traitements effectués par le fournisseur de SDK sur les données personnelles collectées grâce à l'accès à cet identifiant publicitaire pour le compte de l'éditeur (monétisation des espaces publicitaires dans l'application), l'éditeur est responsable du traitement et le fournisseur de SDK son sous-traitant ;

Google Play Services ni à GMS.

- 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 du 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 l'éditeur, responsable de traitement initial, lui en a donné l'autorisation.

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

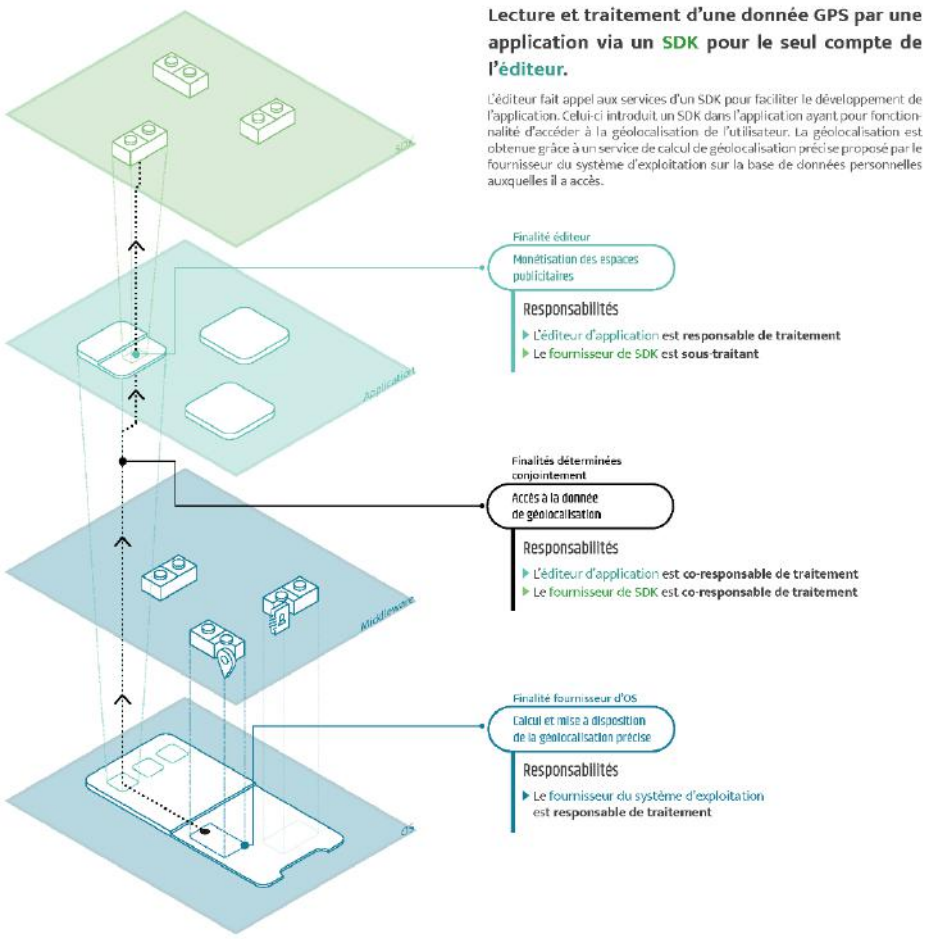
- L'éditeur d'application est **co-responsable de traitement**
- Le fournisseur de SDK est **co-responsable de traitement**

Lecture et traitement d'une donnée GPS 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 géolocalisation de l'utilisateur. Cette information est obtenue grâce à un service de calcul de géolocalisation 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 géolocalisation 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. Le SDK utilise par ailleurs cette information relative à la géolocalisation 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 et le fournisseur de SDK sont responsables conjoints du traitement s'agissant de l'inclusion au sein de l'application d'un SDK ayant pour fonction d'accéder à la donnée de géolocalisation (ce qui constitue une opération de lecture et/ou écriture au sens de l'article 82 de la loi Informatique et Libertés), car ils participent de manière conjointe à la détermination des finalités et des moyens du traitement ;
- s'agissant des traitements effectués par le fournisseur de SDK sur la donnée de géolocalisation 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 ;
- s'agissant des traitements effectués par le fournisseur de SDK pour son propre compte, le fournisseur de SDK est responsable de traitement ; dès lors que ce traitement utilise une donnée collectée via l'application, l'éditeur devra être informé de la finalité de cette collecte et y avoir donné son accord avant que le fournisseur de SDK n'utilise les données son propre compte. L'éventuel recueil du consentement doit se faire sur l'application avant la collecte de la donnée ;
- 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 géolocalisation précise à des tiers, incluant notamment l'éditeur de l'application.

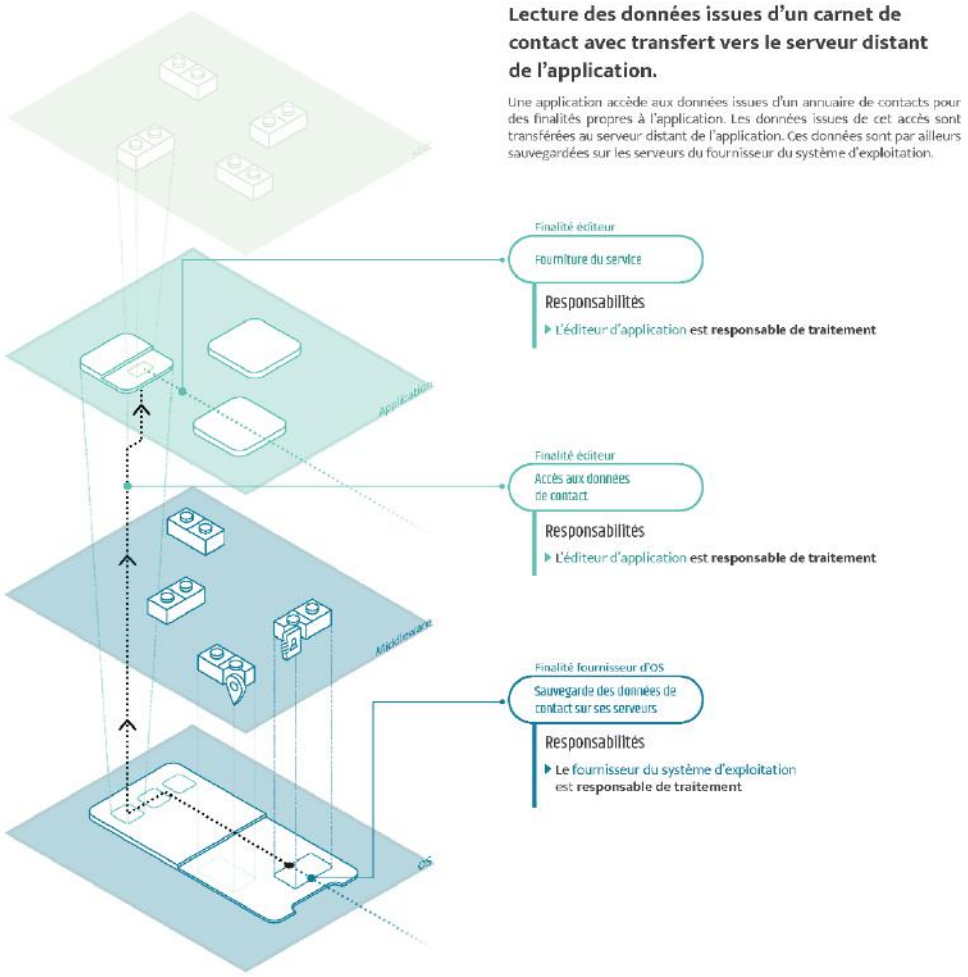


Lecture des données issues d'un carnet de contacts avec transfert vers le serveur distant de l'application

Une application accède aux données issues d'un carnet de contacts pour des finalités propres à l'application. Ces données sont sauvegardées sur les serveurs du fournisseur du système d'exploitation. Ces données sont par ailleurs transférées au serveur distant de l'éditeur de l'application.

Dans cette hypothèse :

- l'éditeur de l'application doit être considéré comme 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 ;
- de son côté, le fournisseur du système d'exploitation est responsable du traitement des données de l'utilisateur sauvegardées sur ses serveurs.



Références

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

5. Recommandations spécifiques à l'éditeur

Notice

À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **éditeurs d'applications**.
- Dans le contexte de ces recommandations, 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.
- Dans la pratique, 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* »).
- Si l'éditeur peut lui-même procéder au développement de l'application, il est fréquent qu'il se repose sur un développeur externe à cette fin. Dans ce cas, il faut considérer le rôle de l'éditeur comme donneur d'ordres, les recommandations relatives à l'activité de développement en elle-même étant prévues dans les recommandations spécifiques au développeur. **Dans le cas où le développeur et l'éditeur sont une même entité, ils sont invités à consulter simultanément les recommandations applicables à l'éditeur et au développeur**.
- Ces recommandations peuvent également être utilement consultées par tout acteur partenaire des éditeurs ou membre du public pour évaluer la conformité des démarches de ceux-ci.

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 ?

- Ces recommandations sont organisées en plusieurs sections, chacune correspondant 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 conseils et de bonnes pratiques à mettre en œuvre.
- Une **liste de vérifications récapitulative, regroupant les principales recommandations** destinées aux éditeurs, est proposée à la fin de cette partie. Les éditeurs sont invités à étudier cette liste et à l'utiliser, notamment lors de la rédaction de la documentation contractuelle, pour s'assurer, le cas échéant, de la prise en compte de ces recommandations par leurs partenaires.

Voir aussi

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

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

5.1. Concevoir son application

La prise en compte de la protection des données personnelles doit commencer dès la phase de conception des applications. C'est donc la responsabilité de l'éditeur, le cas échéant avec l'aide de ses partenaires, de définir clairement les traitements de données personnelles mis en œuvre.

1. Identifier l'existence de traitements de données personnelles

La première démarche de l'éditeur doit être d'identifier si des traitements de données personnelles seront mis en œuvre par l'intermédiaire de son application.

- **S'agit-il bien d'un traitement de données personnelles** ?
  - Pour rappel, une donnée à caractère personnel (ou, plus succinctement, « donnée personnelle ») est toute information se rapportant à une personne physique identifiée ou identifiable. Par exemple, dans le cas d'une application mobile, cela peut être le nom et prénom de l'usager, mais aussi son alias, sa position géographique, ses données d'activité dans l'application ou même les identifiants techniques du terminal qu'il utilise.
  - Dans de nombreux 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.)
  - Une application ne traitant pas de données personnelles n'entre pas dans le champ du RGPD.
  - L'éditeur devrait analyser la nécessité de collecter des données pour chaque traitement et envisager si des alternatives ne traitant pas de données personnelles sont possibles.

- **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 peut relever de l'exemption domestique, sans entraîner de responsabilité de l'éditeur d'application au sens du RGPD.
  - Pour rappel, ces conditions sont le respect cumulatif des deux critères suivants :
    - le traitement est effectué à l'initiative, à la discrétion et pour le seul compte de la personne (ici l'utilisateur de l'application), c'est-à-dire décidé et mis en œuvre par cette dernière ;
    - le traitement est effectué sous le contrôle de la personne, c'est-à-dire en parfaite autonomie, dans un environnement cloisonné, à savoir sans intervention possible de tiers sur ces données : l'éditeur ne fait que fournir le logiciel à l'utilisateur.
  - Pour chaque traitement, l'éditeur devrait privilégier une configuration répondant aux critères de l'exemption domestique, par exemple :
    - en ayant recours à des calculs locaux au lieu d'API interrogeant des serveurs distants,
    - en embarquant des bases de ressources au sein de l'application pour éviter les requêtes réseau,
    - en utilisant des outils de partage locaux des données entre plusieurs applications sous contrôle de l'utilisateur,
    - en permettant des communications entre utilisateurs en mode « pair-à-pair » (« *peer-to-peer* ») sans aucun stockage ou transit des données personnelles par un serveur centralisé.

Point d'attention

Il convient de ne 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 juridique des traitements

Si, au moment de la conception de l'application, l'éditeur identifie que des traitements de données personnelles seront mis en œuvre, chacun de ces traitements devra respecter l'ensemble des principes posés par le RGPD et la loi Informatique et Libertés.

- **Une finalité est-elle correctement définie pour chaque traitement ?**
- **Une base légale est-elle identifiée pour chaque traitement ?** L'éditeur doit identifier une base légale valable au sens de l'article 6.1 du RGPD. 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 consentementc, 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.
  - La base légale de l'intérêt légitime requiert une analyse de la balance des intérêts entre l'utilisateur dont les données sont traitées et le responsable de traitement. En principe, le profilage et la publicité personnalisée ne peuvent être justifiés par l'intérêt légitime de l'éditeur et nécessite le consentement[15].

- **Des accès au terminal de l'utilisateur sont-ils mis en œuvre ?**
  - 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. Ces opérations peuvent correspondre à un vaste éventail de techniques.
  - Sont notamment inclus, dans le contexte des applications mobiles, les identifiants mobiles (qu'ils aient une nature publicitaire ou non), les résultats d'opérations d'identification des caractéristiques (« *fingerprinting* »), les identifiants uniques, mais aussi 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 n'est pas forcément nécessaire pour l'ensemble des lectures ou écritures effectuées, les textes prévoyant des exemptions qui dépendent des finalités poursuivies. Les opérations nécessaires à la mise en œuvre de fonctionnalités expressément demandées par l'utilisateur ne sont ainsi pas visées par cette exigence de consentement. L'éditeur devrait fournir des instructions précises au développeur pour identifier quels traceurs et quels accès au terminal doivent être soumis au consentement.
  - Pour réaliser l'analyse technique des opérations mises en œuvre, et dont l'éditeur est responsable, l'aide du développeur est nécessaire.

[15] 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

Exemples :
• collecte de l'identifiant publicitaire à des fins publicitaires
• collecte des données de contact à des fins de découverte utilisateur
• 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></td><td>L'opération de lecture et/ou d'écriture a pour finalité exclusive de permettre ou de faciliter la communication par voie électronique

Exemple :
• utilisation d'identifiants à des fins de répartition de charge (load balancing) ou de routage</td><td colspan="2">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></td><td></td><td>Fonctionnalité demandée expressément par l'utilisateur

Exemples :
• accès au GPS pour fournir une fonctionnalité de localisation demandée
• utilisation d'identifiants d'authentification</td><td>Usage de sécurisation du service, centré sur la protection de l'utilisateur

Exemples :
• utilisation de traceurs pour prévenir d'attaques en déni de service
• utilisation de traceurs pour prévenir de bourrages d'identifiants (credential stuffing)</td></tr>
<tr><td></td><td></td><td></td><td>Mesure d'audience limitée

Exemple : simple comptage du nombre d'utilisateurs journaliers à des fins de dimensionnement du service</td></tr>
</table>

- **Une durée de conservation des données est-elle associée à chaque traitement ?**
  - Les données traitées au sein de l'application doivent être conservées pour une durée strictement nécessaire à l'objectif poursuivi par le traitement.
- **La collecte des données personnelles concernées est-elle nécessaire et minimisée**
  - L'éditeur devrait identifier les données qui devront être collectées pour chaque traitement, ainsi que le niveau de précision avec lequel il conviendra que l'application les traite afin de minimiser les données traitées (p. ex. : il est préférable de stocker seulement l'année de naissance en lieu et place de la date de naissance complète si l'application n'a besoin que de l'année).
- **Des traitements de données sensibles (au sens de l'article 9 du RGPD : données politiques, religieuses, de santé etc.) sont-ils mis en œuvre ?**
  - Ces traitements de données sensibles sont par principe interdits sauf s'ils reposent sur l'une des exceptions prévues à l'article 9.2 du RGPD, telle que le consentement de la personne concernée.
  - En particulier, toute catégorisation ou création de segments sur la base de telles données, aux fins de réaliser un tel profil et/ou d'adresser de la publicité personnalisée, doit répondre à une finalité légitime (article 5 du RGPD) et n'est en principe pas autorisée. Si elle est envisagée et licite dans un certain contexte, la catégorisation est soumise au recueil du consentement préalable du client concerné.

- 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 en principe s'exprimer de manière spécifique, par exemple en affichant un avertissement ou une information spécifique avant le recueil du consentement ou en ajoutant une case pour recueillir un consentement distinct[16].

- **Comment protéger les données des mineurs ?**
  - Il est fréquent que des éditeurs publient des applications qui s'adressent aux mineurs. Ceux-ci bénéficiant de protections particulières au titre de la réglementation, il est important de mettre en œuvre des mesures additionnelles pour protéger leurs données personnelles et respecter leur vie privée.
  - 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[17].

Point d'attention

Devraient être inclus dans l'analyse les traitements potentiellement effectués par des tiers.

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

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

Il est recommandé, pour chacun des traitements envisagés, d'analyser s'il est possible de 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* »)[18] :

- **Le traitement de données personnelles envisagé est-il indispensable à la fourniture du service ?**
  - Certains des traitements prévus peuvent ne pas être indispensables à la fourniture du service attendu (p. ex. : la géolocalisation permet de simplifier une recherche géographique, mais peut être remplacée par la saisie manuelle de l'adresse).
  - L'éditeur devrait laisser le choix à l'utilisateur final de choisir d'utiliser ou non les fonctionnalités non strictement nécessaires au bon fonctionnement de l'application.
  - L'éditeur ne devrait imposer la création d'un compte que si cela est nécessaire, et envisager des alternatives pour éviter de collecter adresses de courriel et mots de passe.

- **Les paramètres par défaut de l'application sont-ils les moins intrusifs possibles ?**
  - L'éditeur devrait déterminer, pour chacun des traitements, les paramètres minimaux permettant de fournir le service demandé (p. ex. : il ne devrait pas collecter par 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).
  - S'il identifie différentes catégories d'usagers, l'éditeur devrait analyser ces paramètres au regard de chacune de ces catégories (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).

- **La conception du système permet-elle par nature de protéger la vie privée des utilisateurs ?**
  - L'éditeur devrait analyser si des techniques de protection de la vie privée peuvent s'appliquer aux traitements mis en œuvre.

---

[16] 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.* »

[17] « Les droits numériques des mineurs », cnil.fr

[18] Article 25 du RGPD, cnil.fr

- Pour une revue de certaines de ces techniques et des exemples d'usage, l'éditeur peut se référer aux guides sur le sujet produits par l'OCDE[19] et par l'*Information Commissioner's Office* (ICO)[20], autorité britannique de protection des données.

- **Cette conception permet-elle de minimiser les risques pour les utilisateurs ?**
  - L'éditeur devrait, quand c'est possible, utiliser des mécanismes de chiffrement de bout en bout, cette pratique étant susceptible de réduire l'étendue de ses responsabilités, et de limiter les conséquences en cas de fuites de données.
  - L'éditeur devrait minimiser les données transmises à ses partenaires et, si possible, ne pas transmettre de données identifiantes (nom, alias, numéro d'identifiant unique, etc.).

4. Documenter son analyse

Depuis l'entrée en vigueur du RGPD, les responsables de traitement doivent adopter une démarche continue de conformité de leurs systèmes informatiques passant par la mise en œuvre de mécanismes et de procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Aussi, le principe de redevabilité des acteurs commande aux éditeurs d'adopter certains outils et procédures prescrits par le RGPD pour assurer la conformité de leurs traitements, en particulier :

- **Tenir et garder à jour un registre des traitements**. Il s'agit d'un outil de pilotage qui participe à la documentation de la conformité, permettant de recenser et d'analyser tous les traitements de données personnelles mis en œuvre et d'identifier et de hiérarchiser les risques associés. Celui-ci doit permettre une vision globale sur les données traitées, à quoi elles servent, qui peut y accéder, combien de temps elles sont conservées, si des transferts de données vers des pays tiers sont prévus, comment ces informations sont sécurisées.
- **Justifier et documenter les durées de conservation définies.** Une durée de conservation doit être déterminée par le responsable de traitement en fonction de l'objectif ayant conduit à la collecte de ces données.
- **Une analyse d'impact relative à la protection des données (AIPD) peut être requise lorsque le traitement est susceptible d'entraîner des risques importants pour les personnes.**
- **La nomination d'un délégué à la protection des données peut être obligatoire dans certains cas**. Dans les autres cas, elle est encouragée par la CNIL.

5.2. Cartographier ses partenaires

Il est fréquent que tout ou partie des traitements de données effectués à la suite de l'installation d'une application ne soient pas techniquement mis en œuvre par l'éditeur mais par des tiers. Il est donc primordial pour l'éditeur, en qualité de responsable de traitement, d'avoir une vision complète et un contrôle des rôles et de la conformité des mesures mises en œuvre par ses partenaires.

1. Encadrer les relations avec les développeurs

Dans la grande majorité des cas, l'éditeur va faire appel à un partenaire technique pour le développement de l'application. Il est indispensable de faire une analyse précise de cette relation.

- **La qualification du développeur est-elle claire pour les deux parties ?**
  - L'éditeur devrait identifier précisément et au préalable les traitements de données personnelles qui seront mis en œuvre par le développeur pour le compte de l'éditeur dans le cadre du développement et du fonctionnement de l'application. Le développeur agira alors en qualité de sous-traitant de l'éditeur responsable de traitement (voir la partie 4 des présentes recommandations).
  - Au titre de l'article 28 du RGPD, l'éditeur doit formaliser contractuellement (par exemple à travers un accord de traitement des données ou *data processing agreement – DPA* – en anglais) cette qualification et les obligations qui y sont liées.

[19] « *Emerging privacy-enhancing technologies* » (en anglais), oecd-library.org
[20] 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.

- **Le développeur est-il conscient de ses obligations en tant que sous-traitant ?**
  - L'éditeur doit faire figurer, dans le contrat qui le lie au développeur, l'ensemble des mentions figurant à l'article 28. Il est recommandé de sensibiliser le développeur à ses obligations[21], et notamment au fait qu'il ne doit agir que sur instruction de l'éditeur.

- **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 registre des traitements.
  - L'éditeur devrait mettre en place un point de contact clair concernant les problématiques de vie privée (par exemple le DPD / DPO).
  - L'éditeur devrait donner 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 »).
  - L'éditeur devrait prévoir dans la contractualisation 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.

- **L'éditeur peut 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.** 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. Le développeur doit être en mesure d'indiquer à l'éditeur l'ensemble des traitements mis en œuvre par des tiers qu'il a inclus.
- **L'éditeur devrait notamment demander à son développeur de mettre en œuvre les mécanismes de sélection des SDK décrits dans la partie 7 des présentes recommandations (« Recommandations spécifiques au fournisseur de SDK »)**, dès lors qu'en tant que responsable de traitement, l'éditeur assumera la responsabilité finale dans l'inclusion d'un SDK dans une application.

5.3. Gérer le consentement et les droits des personnes

Pour les traitements qui relèvent de sa responsabilité, l'éditeur doit s'assurer que, dans ses interactions avec les personnes, les droits des personnes sont respectés, que ce soit en termes d'information, de consentement ou d'exercice des droits, même quand la mise en œuvre pratique de ces droits est faite par un tiers.

1. Informer correctement ses utilisateurs

La première de ces obligations est de procéder à la correcte information des utilisateurs de l'application, étape indispensable pour assurer la transparence pour toute collecte de donnée, directe ou indirecte[22].

- **Quelles informations fournir aux utilisateurs de l'application dont les données sont traitées ?** Cette information, généralement regroupée dans un document intitulé « politique de confidentialité » devrait inclure :
  - les éléments obligatoires au titre de l'article 13 du RGPD[23] ;

[21] Ces obligations sont développées dans le guide du sous-traitant publié par la CNIL (PDF, 583 ko)
[22] Articles 13 et 14 du RGPD, cnil.fr
[23] « Fiche n°12 : Informer les personnes », guide de l'équipe de développement, lincnil.github.io

- le caractère obligatoire ou facultatif de chaque traitement (et en quoi le refus impacte l'usage de l'application) ;
- la liste des permissions d'accès aux données demandées, leur nature obligatoire ou facultative et les finalités poursuivies via ces permissions.

- **Comment mettre l'information à disposition des utilisateurs ?**
  - L'éditeur peut 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,
    - lister les permissions requises par l'application et les finalités justifiant l'accès aux données associées. Ces permissions pourront être scindées 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 devrait s'assurer que la politique de confidentialité est facilement accessible :
    - avant tout lancement ou téléchargement de l'application, par exemple sur son site ou sur la page de téléchargement de celle-ci. Si cela est possible, celle-ci devrait également être mise à disposition sur la page de l'application dans le magasin d'applications ;
    - au sein de l'application, par exemple directement depuis le menu de celle-ci
  - L'éditeur devrait s'assurer que la politique de confidentialité est concise, compréhensible par son public en utilisant un langage simple et illustré à l'aide d'éléments visuels. Pour s'adapter au médium, une présentation de cette information peut être envisagée en deux niveaux, avec un premier faisant l'usage d'icônes et de tableaux pour rendre celle-ci compréhensible.
  - 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 : il peut être nécessaire de contextualiser cette délivrance d'information lors de chaque collecte spécifique et d'utiliser dans ce cas des méthodologies de présentation simplifiées[24].
  - S'il est fréquent que l'OS mette à disposition des utilisateurs des outils pour les informer des collectes les plus intrusives (marqueur d'activité de la caméra ou de la géolocalisation), l'éditeur doit envisager dans les interfaces des applications la réinformation des personnes sur l'accès ou le partage de certaines données particulièrement intrusives (géolocalisation, carnet de contacts, microphone, etc.), par exemple via l'usage d'indicateurs persistants quand ces fonctionnalités sont activées.

2. Obtenir un consentement valide des utilisateurs

Si la base légale choisie pour un traitement est celle du consentement, ou si une opération de lecture et/ou d'écriture non soumise à exemption est mise en œuvre au titre de l'article 82 de la loi Informatique et Libertés, il convient de recueillir le consentement.

- **Comment recueillir un consentement dans le contexte des applications mobiles ?**
  - L'éditeur doit respecter les obligations en termes de recueil de consentement explicitées par la CNIL dans ses lignes directrices et recommandations sur les *cookies* et autres traceurs[25] lorsqu'une opération de lecture et/ou d'écriture est mise en œuvre.
  - L'éditeur devrait bien prendre en compte les spécificités de l'interface du mobile, notamment l'existence des fenêtres de permission et les limitations en termes d'espace disponible lors de ce recueil.
  - L'éditeur devrait clairement expliciter ses attentes à son développeur.
  - L'éditeur étant responsable en cas de manquement à l'obligation de recueil du consentement, il est indispensable qu'il mette en œuvre des mesures pour s'assurer du bon respect de ses instructions. Il peut à ce titre consulter la partie 5.4 des présentes recommandations (« Maintenir la conformité durant le cycle de vie de l'application »).

[24] « [Synthétiser] Résumé », design.cnil.fr
[25] « Sites web, *cookies* et autres traceurs », cnil.fr

3. Permettre l'exercice des droits

Il appartient aux éditeurs, responsables de traitement, de garantir et respecter l'exercice des droits des personnes, en prenant particulièrement en compte le contexte spécifique des applications mobiles

- **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[26].
  - En fonction de la base légale retenue, certains de ces droits ne sont pas applicables[27].

- **Par quel moyen y donner suite ?**
  - Si les textes ne prévoient pas de moyen privilégié pour répondre à l'exercice des droits, l'éditeur doit analyser les modalités les plus adaptées pour ce faire. Il est ainsi recommandé de mettre à disposition des personnes un centre de gestion des droits au sein de l'application où l'ensemble des droits peuvent être exercés. L'éditeur doit demander à son développeur de le conseiller dans cette démarche.
  - Il est primordial, lors de la contractualisation avec le ou les éventuels sous-traitants, d'assurer que les systèmes techniques et organisationnels permettent de répondre à ces droits, et notamment s'il est prévu qu'une réponse automatique soit apportée à ceux-ci (par exemple via des API de réponse aux demandes d'expressions des droits).

[26] « Fiche n° 13 : Préparer l'exercice des droits des personnes », guide de l'équipe de développement, lincnil.fr.github.io
[27] « 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

Les mesures relatives à la conformité de l'application ne s'arrêtent pas à la conception et à la publication de l'application. L'éditeur, en tant que responsable de traitement, doit mettre en place un ensemble de processus pour maîtriser et assurer cette conformité tout au long du cycle de vie de l'application.

1. Assurer le maintien de la sécurité au cours du temps

Si l'éditeur n'est pas l'acteur mettant directement en œuvre les mesures de sécurité, il a, du fait de son rôle de responsable de traitement, la responsabilité de donner des instructions précises à ses sous-traitants pour assurer la sécurité des données.

- **Comment exprimer les exigences de sécurité ?**
  - L'éditeur devrait formaliser les mesures techniques attendues en termes de sécurité (article 32 du RGPD) des données avec le développeur, en précisant que ces exigences sont applicables aux sous-traitants ultérieurs. Il peut par exemple *a minima* demander le respect de exigences formalisées par la CNIL dans la partie 6 des présentes recommandations (« Recommandations spécifiques au développeur ».
  - L'éditeur devrait 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.
  - 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 un délai cohérent avec le délai légal de première notification de 72h à l'autorité de protection des données (en France, la CNIL).

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 en termes de respect de la vie privée.

- **Comment mettre en œuvre des audits ?**
  - L'éditeur devrait rappeler dans la documentation contractuelle que le développeur est tenu de l'assister dans la tenue d'audits (article 28 du RGPD).
  - L'éditeur peut par exemple utiliser le *OWASP Mobile Application Security Testing Guide* (MASTG)[28] 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 devrait 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 :
    - Equiper 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.
  - En raison de la grande complexité de certaines briques applicatives, ces modalités ne peuvent permettre à elles-seules d'assurer le respect des obligations et sont uniquement un complément aux mesures organisationnelles (voir la partie 5.2 des présentes recommandations : « Cartographier ses partenaires »).

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 du niveau de conformité nécessaire, des processus doivent être

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

conçus en amont puis mis en œuvre de façon appropriée (sur une base régulière ou lorsqu'un développement significatif est entrepris).

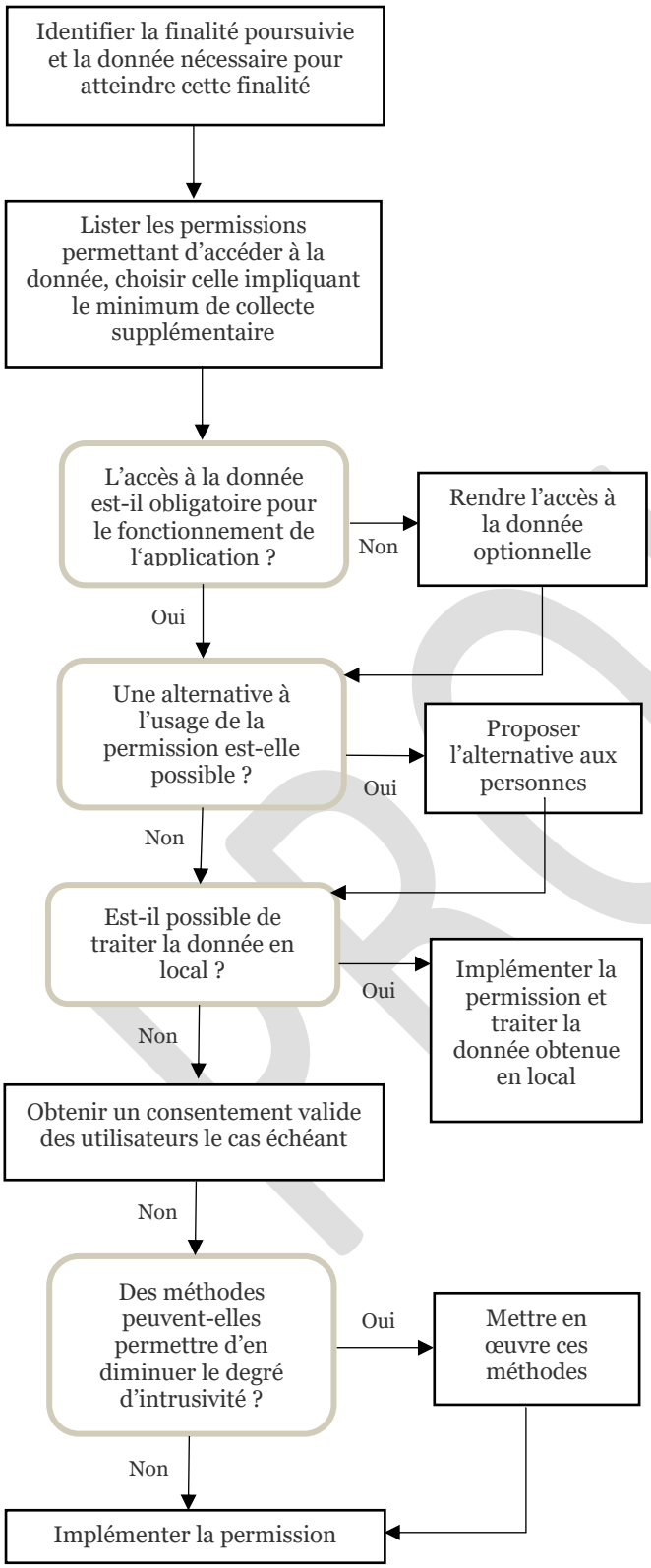
- **Est-ce que le contrôle des éventuelles évolutions des traitements de données est bien réalisé ?**
  - Il est souhaitable que l'éditeur mette en place un processus de validation afin que toute évolution impactant les conditions de mise en œuvre du traitement (choix de sous-traitant ultérieur, SDK, fonctionnalités, recueil de consentement) soit approuvée par celui-ci. Ces choix peuvent fréquemment être entérinés au cours d'opération de maintenance : l'éditeur devrait s'assurer que son processus prenne en compte ce point.
  - L'éditeur doit actualiser le registre des traitements afin de prendre en compte les évolutions des traitements de données mis en œuvre, ainsi que la politique de confidentialité des données.

- **Est-ce que des processus permettant d'assurer la confidentialité des données sont mis en place ?**
  - L'éditeur doit encadrer l'accès aux données personnelles par les sous-traitants. Une bonne pratique consiste à 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[29]. L'usage de données fictives ou synthétiques par les sous-traitants est une solution alternative.
  - L'éditeur devrait superviser et vérifier la suppression des données dont la durée de conservation est échue.

[29] 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.

5.5. Permissions et protection des données dès la conception

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



1. Utiliser les permissions

- **Comment analyser les permissions aux vues des textes applicables ?**

Les permissions en elle-même n'emportent pas forcément d'obligation au sens des textes et constituent une mesure technique indépendante. Ainsi l'accès à une ressource via une demande de permission, si cette ressource est ensuite traitée de manière purement locale, peut relever de l'exemption domestique. De même, dans ce contexte, les conditions d'applicabilité de l'article 82 de la loi Informatique et Libertés peuvent ne pas être réunies.

En outre, elles n'exigent pas de consentement préalable lorsque l'accès à des informations dans le terminal est nécessaire soit au fonctionnement du protocole de communication électronique, soit à la fourniture du service expressément demandé par l'utilisateur. Cependant dans de nombreux cas (et dès que la ressource accédée n'est pas traitée en local), un consentement peut être nécessaire du fait de l'article 82. La partie 5.3 des présentes recommandations « Gérer le consentement et les droits des personnes » explicite ces cas. La CNIL encourage la pratique consistant à prévoir que l'application doit systématiquement obtenir la « permission » de l'utilisateur pour accéder à certaines ressources sensibles stockés sur le terminal (géolocalisation, carnet de contact, appareils photographiques et photographies/films, etc.), indépendamment des obligations légales résultat de l'article 82 de la loi Informatique et Libertés.

De même, l'accès distant à une ressource protégée par une permission peut déclencher un traitement dont la base légale est le consentement.

- **Quelle information donner lors d'un recueil de consentement relatif à une permission ?**

Dans les cas où le consentement est la règle, il est indispensable d'obtenir un consentement valide. Des difficultés pratiques peuvent survenir dans l'articulation entre le consentement 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 »)

Il est par ailleurs nécessaire 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). Si plusieurs finalités de natures différentes sont poursuivies, il est important de respecter la granularité du consentement.

- **Comment mettre en œuvre une démarche de sélection des permissions ?**
  - Pour assurer une démarche de protection des données dès la conception, il convient 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 géolocalisation ?**
  - L'éditeur devrait identifier, parmi les permissions mises à disposition par l'OS, celle qui correspond au niveau de granularité minimum qui lui est nécessaire :
    - une localisation approximative plutôt que précise,
    - une permission limitée à une seule fois plutôt qu'une permission permanente,
    - une permission uniquement active quand l'appli 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).
  - Lorsque cela est possible au regard du service rendu, l'éditeur devrait 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 géolocalisation de la personne.
  - Si possible, l'éditeur devrait traiter la donnée de localisation en local. Par exemple, pour trouver le lieu le plus proche de son utilisateur parmi une liste de lieux, l'éditeur devrait intégrer la liste en question dans le contenu de l'application et calculer en local le lieu le plus proche en fonction de la localisation de la personne.
  - Le cas échéant, l'éditeur devrait obtenir un consentement valide pour la collecte distante de la donnée de localisation de la personne. Si le consentement n'est pas obtenu, il devrait envisager les méthodes alternatives identifiées plus haut. Avant tout envoi des données de localisation vers les serveurs de l'application, l'éditeur devrait identifier le niveau de précision minimal qui est nécessaire pour atteindre ses finalités et tronquer localement les coordonnées en fonction de celui-ci.
  - D'une manière générale, l'éditeur ne devrait pas conserver la donnée de localisation qu'il a utilisée sur un serveur distant mais préférer sa conservation en local dans l'application pour la reproposer à l'utilisateur (via un item : « ma dernière localisation »).
  - Par principe, et sauf pour des applications dont le fonctionnement dépend de la localisation en continu (navigation, certains jeux spécifiques dans l'espace public), l'éditeur ne devrait pas collecter la localisation quand l'application n'est pas activement utilisée par l'utilisateur.
  - Dans le cas où la permission donnée par l'utilisateur est permanente, l'éditeur devrait penser à lui rappeler l'existence de la permission de manière visible dans l'interface de l'application et à 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 ?**
  - L'éditeur devrait déterminer avec précision le besoin et les raisons d'accès à ces données de contact, et notamment si celui-ci est obligatoire pour le fonctionnement de l'application.
  - L'éditeur devrait identifier la permission associée la moins intrusive. Notamment, s'il souhaite uniquement lire les données, il ne devrait pas demander de droits en écriture.
  - Pour toute permission d'accès impliquant la sélection d'un contact de manière locale, il est exclu de faire cette sélection autrement que directement sur le terminal de l'utilisateur.
  - Si certaines permissions d'accès nécessitent la mise en commun de données de contacts entre plusieurs utilisateurs de l'application (par exemple, la découverte de contacts inscrit à une messagerie par exemple), il est indispensable de collecter un consentement pour la lecture de

ces données de contact sur le terminal de l'utilisateur et d'assurer l'information de l'ensemble des personnes susceptibles d'être concernées par le traitement[30]. L'éditeur devrait s'assurer de la bonne information de l'utilisateur quant à la nature de la collecte et son intrusivité et, en cas de refus, proposer des méthodes alternatives (p. ex. : entrée manuelle de numéro par la personne pour vérification ponctuelle de présence). En cas de mise en œuvre de telles alternatives, il devrait s'assurer 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 d'aspiration de données (« *scraping* »).

- Dans le cas précédent où le concepteur de l'application souhaite afficher à l'utilisateur lequel de ses contacts dispose déjà de l'application afin de lui proposer de le connecter, les opérations suivantes devraient être mises en œuvre :
  - À l'inscription, chaque utilisateur de l'application devrait consentir 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 ;
    - À cet égard, il n'est pas possible de considérer que la délivrance de la permission pour accéder aux « contacts » du téléphone est un 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 devrait avoir 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.).
  - L'accès et l'analyse de l'intégralité du carnet de contacts devrait utiliser les méthodes les plus adaptées pour limiter l'intrusivité de ce traitement (par exemple via des techniques de « *Private Set Intersection* »).
  - Les données de contacts qui auraient été stockées devraient être supprimées dès la fin de l'analyse et un nouvel accord pour le recours à cette permission devrait être sollicité pour tout nouvel accès. A défaut, 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 ?**
  - L'éditeur devrait déterminer avec précision le besoin et les raisons d'accès au microphone, et notamment si celui-ci est obligatoire pour le fonctionnement de l'application.
  - L'éditeur devrait identifier la permission associée la moins intrusive (notamment en termes de possibilité de captation concurrente de flux audio, qui peut présenter un risque important pour la personne).
  - Si le besoin est ponctuel, l'éditeur devrait révoquer la permission après la captation du son.
  - Si possible, l'éditeur devrait proposer des alternatives à l'accès au microphone (par exemple, dans le cadre d'une application de prise de notes vocales, l'éditeur devrait également proposer une prise de note manuelle).
  - Si possible, l'éditeur devrait traiter les contenus audio en local (par exemple s'il propose un accordeur, il devrait privilégier l'utilisation des capacités locales de calcul du téléphone plutôt que le traitement distant des contenus).
  - À défaut, l'éditeur devrait obtenir un consentement valide pour la collecte distante des données présentes dans ces contenus audio, en s'assurant de la bonne compréhension par la personne du fait que ces contenus seront envoyés vers ses serveurs. Si le consentement n'est pas obtenu, il doit envisager les méthodes alternatives identifiées plus haut.

[30] 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, l'EDPB 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 l'usage du microphone n'est utile que pour certaines actions dans l'application (par exemple enregistrer un message), l'éditeur devrait alerter l'utilisateur quand le microphone est activé, par exemple par le biais d'une icône clairement identifiée et dédiée.
- Avant tout envoi des contenus audio vers les serveurs de l'application, l'éditeur devrait proposer à ses utilisateurs de tronquer ou de réécouter les contenus partagés.
- D'une manière générale, l'éditeur ne devrait pas conserver les contenus audio collectés sur un serveur distant sauf cas d'usage précis et justifié. Plus particulièrement, il devrait rendre la mise en œuvre de sauvegardes sur serveur distant optionnelle, et obtenir à cette fin le consentement libre, spécifique et éclairé des utilisateurs concernés.

- **Comment gérer l'usage de l'appareil photographique ?**
  - L'éditeur devrait déterminer avec précision le besoin et les raisons d'accès à l'appareil photo, et notamment si celui-ci est obligatoire pour le fonctionnement de l'application. Notamment il devrait bien faire la distinction entre l'accès à l'appareil photo en lui-même ou l'accès aux photographies prises par la personne et stockées au sein de son terminal.
  - Partant de ce besoin, l'éditeur devrait identifier, parmi les permissions fournies par l'OS, celle qui présente le moins de risques pour la personne, et en particulier :
    - 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 devrait s'appuyer sur des permissions qui mettent l'utilisateur en capacité de sélectionner spécifiquement les contenus qu'il souhaite partager avec l'application ;
    - dans le cas où une prise de photo ou de vidéo en direct est nécessaire, privilégier les solutions déléguant cette captation aux applications système ;
    - si cela n'est pas possible (par exemple, pour des usages interactifs du flux vidéo), s'assurer de ne requérir que le strict minimum en termes d'autorisation matérielles (par exemple, ne pas activer l'enregistrement audio si ce n'est pas une nécessité).
  - Lorsque c'est possible, l'éditeur devrait proposer une alternative évitant l'accès à la caméra de l'utilisateur.
  - Si possible, l'éditeur devrait traiter la donnée en local (par exemple, s'il propose des outils de retouche, envisager l'utilisation des capacités de calcul locales du téléphone plutôt que le traitement distant des images). De même, l'éditeur devrait supprimer les métadonnées associées à l'image (géolocalisation, horodatage, données EXIF) si elles ne sont pas nécessaires.
  - À défaut, l'éditeur devrait obtenir un consentement valide pour la collecte distante des images. Si le consentement n'est pas obtenu, l'éditeur devrait envisager les méthodes alternatives identifiées plus haut.
  - Avant tout envoi des images vers ses serveurs, l'éditeur devrait analyser la nécessité de l'obtention de l'ensemble de l'image. À défaut, il devrait proposer des outils de sélection ou de floutage à l'utilisateur.
  - D'une manière générale, l'éditeur ne devrait pas conserver les images collectées sur un serveur distant sauf en cas d'usage précis et justifié. Plus particulièrement, il devrait rendre optionnelle la mise en œuvre de sauvegardes sur un serveur distant, et obtenir à cette fin le consentement libre, spécifique et éclairé des utilisateurs.

5.6. Liste de vérifications

Catégorie	Sous-Catégorie	Identifiant	Description
Concevoir son application	Identifier l'existence de traitements de données personnelles	1.1.1	Toute opération pouvant l'être est menée sans traiter de donnée à caractère personnel.
		1.1.2	Tout traitement pouvant l'être est réalisé de manière locale.
	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	Une durée de conservation des données est associée à chaque traitement.
		1.2.4	Aucune collecte de données non nécessaire n'est opérée. Celles nécessaires sont minimisées.
		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	1.3.1	La liste des traitements minimaux pour fournir le service demandé est déterminée.
		1.3.2	Les paramètres par défaut ont pour seul effet de mettre en œuvre des traitements de cette liste minimale.
		1.3.3	La possibilité d'intégrer des mécanismes de protection de la vie privée est étudiée dès la conception.
		1.3.4	La possibilité de mettre en œuvre des techniques de protection de la vie privée, tel que le chiffrement de bout en bout, a été étudiée.
	Documenter son analyse	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 remplis 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 figure dans le contrat avec le développeur.
		2.1.3	Le registre des traitements est mis à disposition du développeur.
		2.1.4	Les instructions données au développeur sur les traitements à mettre en œuvre sont claires et documentées. Un test d'acceptation (recette) figure dans le contrat avec le développeur. Un point de contact dédié aux problématiques de vie privée est mis à disposition du développeur.
	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 pour identifier s'il procède à des traitements de données personnelles.
Gérer le consentement et les droits des personnes	Informer correctement ses utilisateurs	3.1.1	Une politique de confidentialité complète est rédigée.
		3.1.2	La politique de confidentialité est accessible avant tout téléchargement ou installation de l'application. La politique de confidentialité est également accessible au sein de l'application.
	Obtenir un consentement valide des utilisateurs	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.
	Permettre l'exercice des droits	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	La mise à disposition des personnes d'un centre de gestion des droits au sein de l'application est envisagée.
Maintenir la conformité durant le cycle de vie de l'application	Assurer le maintien de la sécurité au cours du temps	4.1.1	Les exigences en termes de mesures techniques attendues sont formalisées auprès des sous-traitants.
		4.1.2	Le processus de mise à jour en cas de vulnérabilité est contractualisé avec les tiers.
		4.1.3	Les obligations en termes d'alerte de sécurité afin de permettre la notification de violations de données personnelles sont rappelées aux sous-traitants.
	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. Les audits à mener sont explicités au préalable.

	Mettre en place des processus robustes en termes de conformité	4.3.1	Des instructions sont données aux sous-traitant pour que toute évolution impactant les problématiques de vie privée soit approuvée avant mise en œuvre.
		4.3.2	Les mises à jour sont reflétées dans le registre des traitements et dans la politique de confidentialité.
		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	Mettre en œuvre une démarche pour la sélection des 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	La collecte des données non obligatoires pour le fonctionnement de l'application est optionnelle.
		5.1.3	Des alternatives à l'usage des permissions sont proposées aux personnes lorsque cela est possible.
		5.1.4	Les données collectées sont traitements localement lorsque cela est possible.
		5.1.5	Le consentement est valablement recueilli lorsqu'il est nécessaire (voir 3.2.1).
		5.1.6	Avant toute collecte distante, la précision de la donnée est diminuée au minimum nécessaire.

6. Recommandations spécifiques au développeur

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**.
- Dans la pratique, 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.
- Bien que le développeur agisse dans la majorité des cas comme exécutant des instructions de l'éditeur, en pratique, il prend en charge un certain nombre de choix techniques qui ont de forts impacts sur les caractéristiques des traitements qui seront mis en œuvre. **Dans le cas où le développeur et l'éditeur sont une unique entité, il devra consulter simultanément les recommandations applicables à l'éditeur et au développeur**.
- 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.
- À ce titre, il est indispensable que le développeur mette en œuvre une démarche pour assurer l'information et l'approbation de l'éditeur concernant les choix techniques opérés ainsi que leurs implications, et respecte ainsi son devoir de conseil. **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 ?

- Ces recommandations sont organisées en plusieurs sections, chacune correspondant à une étape dans l'activité de développement d'une application. Chaque partie 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 de vérifications** **récapitulative, regroupant les principales recommandations** destinées aux développeurs, est proposée à la fin de cette partie. Les développeurs sont invités à étudier cette liste et à l'utiliser notamment lors de la rédaction de leur documentation contractuelle pour s'assurer, le cas échéant, de la prise en compte de ces recommandations par leurs partenaires.

6.1. Formaliser sa relation avec l'éditeur

La relation centrale dans la conception et le développement d'une application est celle qui lie l'éditeur et le développeur. Il est primordial que les aspects relatifs à la protection des données personnelles des utilisateurs soient au cœur de la construction de cette relation contractuelle. 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

La relation contractuelle entre le responsable de traitement (éditeur) et le sous-traitant[31] (développeur) doit reposer sur une compréhension claire des responsabilités de chacun.

- **Des traitements seront-ils mis en œuvre sous le régime de la sous-traitance de données personnelles** ?
  - Le développeur peut se référer à la partie 4 des présentes recommandations pour déterminer sa qualification au titre du RGPD. Pour rappel, le fait que le développeur procède à certains choix techniques ne fait pas nécessairement de lui le responsable du traitement : un sous-traitant peut déterminer les « moyens » d'un traitement tant qu'ils sont non-essentiels[32].

- **Quelles demandes faire à l'éditeur** ?
  - Le développeur devrait demander à l'éditeur de lui fournir, comme partie intégrante du cahier des charges, le registre de traitements concernant l'application à développer. Dans le cas où ce registre des traitements n'existerait pas encore, le développeur devrait demander la fourniture d'un cahier des charges exhaustif et clair, qui permette de définir quelles données seront utilisées et ainsi mettre en œuvre par la suite un registre de traitements de l'application.
  - Lors de la contractualisation avec l'éditeur, le développeur devrait demander à l'éditeur une qualification claire de son rôle pour chacun des traitements concernés. En tant que développeur, il agira comme sous-traitant s'il intervient sur des traitements de données pour le compte et sur instruction du responsable de traitement, mais il est de sa responsabilité et de celle de l'éditeur de déterminer la qualification la plus adéquate pour chaque traitement.
  - Le contrat de sous-traitance liant l'éditeur et le développeur, conforme à l'article 28 du RGPD, doit notamment stipuler les conditions de mise en œuvre de chaque traitement.
  - Un point de contact doit être prévu par le contrat pour faire valider les choix ayant un impact en matière de traitements de données personnelles : il s'agit en général du DPD de l'éditeur.

- **Quelles obligations du côté du développeur ?**
  - En a qualité de sous-traitant, il incombe au développeur un certain nombre d'obligations au titre de l'article 28 du RGPD, détaillées dans cette partie, et notamment :
    - une obligation de transparence et de traçabilité ;
    - l'obligation de prendre en compte, au titre de son devoir de conseil, les principes de protection des données dès la conception et par défaut ;
    - l'obligation d'assister son client dans le respect de ses obligations 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 »).
  - Conformément à l'article 30.2 du RGPD, le développeur doit tenir de son côté un registre des activités de traitements mis en œuvre pour le compte de l'éditeur, qui devra être mis à la disposition de ce dernier.
  - Le développeur 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 charges exhaustif communiqué par l'éditeur. À défaut, il devrait alerter l'éditeur afin que ce document soit mis à jour.

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

- Dans tous les cas, le développeur est tenu d'agir strictement 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 procèdent à des opérations de lecture et/ou d'écriture, 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 » devront être validés par l'éditeur.
- Enfin, s'agissant des environnements propres au développeur (p. ex. : environnement technique de développement mutualisé entre ses clients) :
  - Le développeur doit déterminer sa responsabilité si des traitements sont mis en œuvre de son fait, et doit alors respecter l'ensemble des obligations du responsable de 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 (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, celui-ci ne peut prendre cette décision seul mais devrait au contraire impliquer l'éditeur dans le processus de décision.
    - À cet égard, il convient de bien distinguer, d'une part, l'environnement de test et de développement du développeur, dans lequel le développeur peut être amené à mettre en œuvre des tests de traitements de données ou d'intégration de SDK, à la demande de l'éditeur ou de sa propre initiative et, d'autre part, l'environnement de recette dans lequel il est proposé à l'éditeur une version de l'application conforme à ses instructions, comportant uniquement les traitements prévus.
    - Le point de contact établi au sein de l'éditeur à cette fin devrait être utilisé pour faciliter la communication.
  - Le développeur devrait présenter, au titre de son devoir de conseil, 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.
  - Une attention particulière devrait être portée 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 ?**
  - Le processus de décision décrit ci-dessus devrait être maintenu 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, les impacts que ces évolutions peuvent avoir sur les traitements de données mis en œuvre ne devraient pas être négligés. Certains outils peuvent aider le développeur à analyser les mises à jour des conditions d'utilisation des partenaires.
  - En cas d'évolution possible des conditions de mise en œuvre des traitements, l'éditeur devrait être informé de manière proactive. Par exemple, si des évolutions dans les permissions proposées par l'OS permettent de mieux protéger les personnes, la CNIL recommande de suggérer à l'éditeur une mise à jour, au titre de son devoir de conseil.

- **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.
  - À ce titre, le développeur devrait 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, devrait demander à l'éditeur de les lui transmettre.
  - Le compte de mise en ligne de l'application devrait 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 devrait 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. Il est indispensable d'identifier et de qualifier les responsabilités de chacun avec l'éditeur pour l'ensemble de ces traitements avant leur mise en œuvre.

- **Des traitements de données personnelles seront-ils impliqués par l'usage de fonctionnalités mises à disposition par l'OS ?**
  - Le développeur devrait 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 devrait 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[33]).
  - Le développeur devrait 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 de traitement.
  - Il lui est recommandé 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 devrait 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 devrait s'informer sur leurs caractéristiques pour permettre la qualification de 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 ? »).
  - Les informations qui devraient être recueillies à cet égard concernent notamment la liste des données personnelles collectées et 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, le développeur devrait en informer l'éditeur, et envisager de renoncer à l'usage du SDK. **Dans tous les cas, ces traitements additionnels ne peuvent être mis en œuvre sans l'information et l'accord préalable de l'éditeur.**
  - Cette analyse devrait être appliquée à l'ensemble des SDK utilisés, notamment ceux fournis par le fournisseur de l'OS.

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

6.2. Assumer son rôle de conseil envers l'éditeur

Le développeur, en tant que sous-traitant au sens du RGPD, est tenu d'assister et de conseiller l'éditeur dans sa conformité à certaines obligations posées par le RGPD, particulièrement en ce qui concerne les choix de mise en œuvre qui relèvent de son expertise. Il doit 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[34]. Il peut à cet effet proposer des moyens de traitements des données personnelles visant à assurer le respect des droits des personnes.

1. Proposer des développements respectant les principes de protection des données personnelles

Le développeur doit proposer des modalités de mise en œuvre et prodiguer des conseils prenant en compte les principes de minimisation et de protection des données dès la conception et par défaut.

- **Le principe de minimisation des données est-il pris en compte ?**
  - Qu'il soit sous-traitant ou qu'il se contente de fournir le code à l'éditeur, le développeur devrait s'assurer que les traitements qu'il propose de mettre en œuvre pour le compte de l'éditeur respectent le principe de minimisation des données collectées. Il peut également conseiller techniquement l'éditeur pour choisir et mettre en œuvre des solutions plus protectrices. La CNIL recommande :
    - 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[35]) ;
    - 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 devrait 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.
  - Si le développeur identifie que certaines données sont accessibles par des tiers (l'OS ou un SDK, par exemple), des solutions devraient être proposées pour limiter les risques de ces accès. De façon non exhaustive, la CNIL formule notamment les trois recommandations suivantes :
    - les données affichées dans les notifications émises par l'application peuvent être limitées, en indiquant simplement que celles-ci sont disponibles au sein de l'application. Dès que possible, le contenu des notifications devrait être chiffré, de sorte que le fournisseur d'OS ne soit pas en capacité d'y accéder ;
    - les contenus des sauvegardes peuvent être chiffrés, en permettant à l'utilisateur de l'application et à lui seul de conserver la maîtrise des clés cryptographiques utilisées pour ce chiffrement ;
    - la transmission d'identifiants inter-applications à des fournisseurs de SDK devrait être évitée. Si cette transmission est nécessaire, un hachage des identifiants devrait préalablement être opéré.
    - le développeur devrait s'assurer que les éventuelles permissions demandées sont strictement nécessaires au fonctionnement de l'application et aux finalités du traitement, afin de pouvoir conseiller l'éditeur sur les moyens de minimiser les collectes autorisées selon les niveaux de permissions. Lorsque c'est possible, il faudrait prévoir 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, il est recommandé que le développeur prévoie de signaler à l'utilisateur quand elles sont actives, via les fonctionnalités de l'OS ou au sein de l'application.

[34] 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).

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

- Si le développeur fait le choix d'activer certaines permissions dès l'installation de l'application, il devrait s'assurer que ce choix est compatible avec 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 »).

- **Des données sensibles au sens de l'article 9 du RGPD sont-elles traitées ?**

Qu'est-ce qu'une donnée sensible au sens de l'article 9 du RGPD ?

- **Voir la partie 5.1 des présentes recommandations :** « Assurer la conformité juridique des traitements »

  - Si les instructions fournies par l'éditeur impliquent le traitement de données sensibles, une distinction claire devrait être faite entre ces typologies de données et les autres, notamment au niveau de l'architecture du service.
  - Si le développeur identifie que des traitements de données sensibles sont mis en œuvre sans avoir reçu d'instruction en ce sens, l'éditeur devrait en être informé pour que ce dernier puisse analyser la conformité du traitement. A défaut, celui-ci est par principe interdit.
  - Le traitement de ces données doit faire l'objet d'une attention particulière, car leur traitement fait l'objet d'un régime spécifique, notamment en termes de transmission de ces données à des tiers. Par exemple, lors de l'intégration de SDK, le développeur devrait s'assurer qu'ils n'ont en principe aucun accès à ces données.
  - L'éditeur devrait 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).

2. Aider au bon respect des droits des utilisateurs

Le développeur a un rôle important à jouer dans le respect des droits des personnes. Il doit, à ce titre, lors de la conception de l'application, s'assurer que les droits pourront bien s'exercer de manière effective au sein de l'application. S'il a la qualité de sous-traitant, il doit aider l'éditeur pour la gestion des demandes des utilisateurs.

- **Les utilisateurs sont-ils bien informés ?**
  - Le développeur devrait rappeler à l'éditeur la nécessité de mettre à disposition la politique de confidentialité fournie par l'éditeur au sein de l'application. Celle-ci doit être lisible sur support mobile (voir les recommandations formulées à ce titre) et facilement accessible (p. ex. : affichée sur le menu principal de l'application, ou au niveau de la page du compte de la personne pour le cas d'une application authentifiée). Lorsqu'il y a des conditions générales d'utilisation de l'application, un document ou un lien spécifique pour accéder à la politique de confidentialité est en principe nécessaire.
  - De manière additionnelle, un écran d'information RGPD simplifié peut être mis à disposition au premier lancement de l'application, afin de garantir une information complète des personnes avant utilisation de l'application.
- **L'exercice des droits est-il possible au sein de l'application ?**
  - Le développeur devrait penser à l'exercice des droits dès la conception, notamment en termes de structuration des bases de données. En particulier, le droit de suppression s'il est exprimé doit être respecté, indépendamment des contraintes techniques.
  - Dans la mesure où les collectes ont lieu dans le cadre d'applications mobiles, il est recommandé 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 permettrait 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 ces droits 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.

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

En cas d'usage de traceurs, il est indispensable que l'éditeur puisse étudier l'éventuelle nécessité d'obtenir un consentement[36]. Il est ainsi recommandé au développeur, au titre de son devoir de conseil, d'alerter l'éditeur si des éléments du cahier des charges impliquent la mise en œuvre d'opérations de lecture et/ou d'écriture, et dans la mesure du possible, de participer à la bonne mise en œuvre des recueils de consentement. 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, en particulier « Des accès au terminal de l'utilisateur sont-ils mis en œuvre ? ».

- **Comment recueillir le consentement dans le cadre des applications mobiles ?**
  - Le consentement, dans le contexte des applications mobiles, doit répondre au niveau d'exigence décrit dans la recommandation « *Cookies* et autres traceurs » publiée par la CNIL, dont sont extraits les schémas ci-dessous.
  - Il est toutefois nécessaire d'adapter les interfaces pour permettre la lisibilité des fenêtres dans un environnement mobile.

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

[36] « *Cookies* et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation », cnil.fr

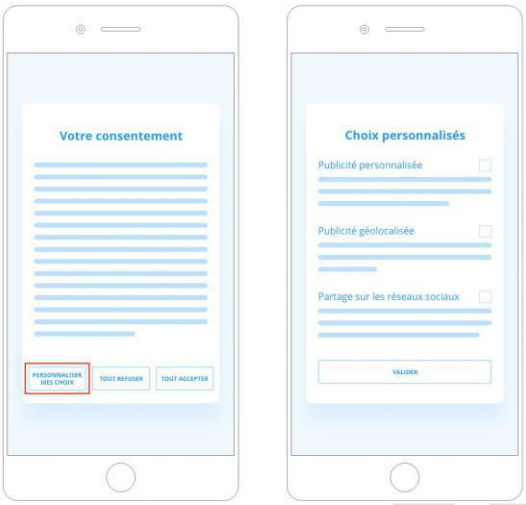


Figure 3 - La possibilité de consentir de manière granulaire peut-être offerte sur un second niveau d'information via un bouton « personnaliser mes choix » inséré sur le même niveau d'information (premier niveau) que les boutons permettant de « tout accepter » et de « tout refuser ».

- Pour éviter la fatigue du consentement et rendre le recueil du consentement plus compréhensible pour les ut²ilisateurs, il est recommandé de recueillir les consentements de manière contextuelle en fonctions des actions entreprises en lieu et place d'un unique écran initial.
- Les modalités de recueil du consentement doivent être convenues en accord avec l'éditeur et mises en place au sein de l'application sur la base de ses instructions. Le développeur devrait documenter cette démarche.

- **Comment articuler consentement et permissions ?**
  - Dans le cadre des applications mobiles, les développeurs peuvent utiliser les systèmes de permissions mis à disposition par l'OS pour l'accès à des fonctionnalités qui correspondent souvent en pratique à des accès au terminal nécessitant le consentement.
  - Le développeur devrait analyser les systèmes de permission fournis pour déterminer s'ils permettent ou non à eux seuls d'obtenir un consentement respectant les critères posés par les textes. En particulier, l'écran de recueil de consentement doit permettre de faire apparaître la finalité pour laquelle la permission est requise, et doit pouvoir abriter un lien permettant de renvoyer vers un document contenant l'ensemble des informations prévues aux articles 13 et 14 du RGPD. À défaut, il est nécessaire de mettre en œuvre une plateforme de gestion du consentement (« *Consent Management Platform* » ou CMP) de manière additionnelle à la fenêtre de permission (par exemple pour permettre une information complète ou assurer la granularité du consentement).
  - Le développeur devrait s'assurer que le recours à ces recueils additionnels de consentement ne vient pas créer de confusion chez les utilisateurs, et notamment lorsque le refus associé à une permission vient en réalité exprimer la volonté de s'opposer à l'usage de traceurs. Dans ce cas, le consentement donné à travers la CMP consécutivement à un refus exprimé lors d'une demande de permission ne pourra être considéré comme univoque, et ne sera ainsi pas valable au titre de la réglementation (par exemple, un consentement accordé dans une CMP large, incluant la collecte éventuelle de géolocalisation, suivi d'un refus de la permission système de collecte de géolocalisation).

6.3. Faire bon usage des SDK

En pratique, le développeur choisit les SDK qu'il propose à l'éditeur, auquel revient la décision finale d'intégration au sein de l'application. Il est fortement recommandé que le développeur mette en œuvre dans ce contexte une démarche rigoureuse de sélection et de mise en œuvre des SDK auxquels il entend recourir.

1. Sélectionner le SDK selon les bons critères

Avant toute proposition d'intégration d'un SDK, il est recommandé au développeur, lors de l'étude des outils qu'il souhaite mettre en œuvre, de suivre une méthodologie d'évaluation axée sur le respect de la vie privée.

- **Quels documents demander au fournisseur de SDK ?**
  - Des documents permettant de déterminer l'ensemble des traitements de données impliqués lors de l'intégration du SDK, par exemple sous la forme d'un registre des traitements, en fonction du paramétrage mis en œuvre, afin que le responsable du traitement puisse l'intégrer à son propre registre.
  - Les éléments permettant de déterminer la qualification du fournisseur de SDK pour chacun des traitements. Sur les critères pour qualifier le fournisseur de SDK, le développeur peut se référer à la partie 4 des présentes recommandations.
  - Les éléments permettant d'identifier d'éventuels transferts ou divulgations non autorisés de données personnelles (article 48 du RGPD).

- **Quelle analyse mener ?**
  - Si le développeur fait le choix de proposer l'intégration d'un SDK dans le développement de l'application, il devrait fournir à l'éditeur les éléments permettant de procéder à une qualification de sa responsabilité et demander son approbation écrite avant l'intégration du SDK. En effet, s'il agit en tant que sous-traitant et qu'un traitement implique le recours à un tiers sous-traitant ultérieur, le développeur doit, conformément à l'article 28 du RGPD, obtenir l'autorisation du responsable de traitement et s'assurer que les mêmes obligations en matière de protection des données qui lui incombent sont imposées à ce sous-traitant ultérieur dans un contrat ou tout autre acte juridique. Même dans l'hypothèse où le développeur n'est pas sous-traitant, il est nécessaire que l'éditeur soit informé et un contrat de sous-traitance devra en principe lier directement l'éditeur de l'application et le fournisseur du SDK.
  - Le développeur devrait 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).
  - Le développeur devrait s'assurer que le SDK permet de répondre aux demandes d'exercice des droits, notamment au droit au retrait du consentement. Les SDK mettant à disposition des API pour y répondre automatiquement devraient être privilégiés.
  - 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.

Point d'attention

Attention à l'effet « poupées russes », selon lequel l'intégration d'un SDK implique celle d'autres SDK. Dans ce cas, l'analyse devrait être répétée pour chacun des SDK ultérieurs.

2. Gérer le consentement des utilisateurs

Lors du choix d'un SDK, il est nécessaire d'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.

- **Quelles garanties pour permettre le recueil d'un consentement valide des utilisateurs ?**
  - Le développeur devrait veiller à ce que la configuration du SDK permette que ce 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 non exemptée de consentement et qui serait effectuée au premier lancement de l'application est à proscrire.
  - Le développeur ne devrait proposer que des SDK permettant le retrait du consentement.
  - Dans les cas où les SDK sélectionnés affirment qu'ils permettent de collecter le consentement de manière licite, cette obligation devrait être formulée contractuellement et son respect audité (voir la méthode proposée ci-dessous).

- **Comment assurer la granularité du consentement aux SDK ?**
  - Si plusieurs finalités sont poursuivies par le SDK, le développeur devrait veiller à ce que le SDK permette une 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 devront se limiter à cette unique finalité. Si plusieurs opérations techniques participent à la même finalité, le déclenchement de ces opérations peut découler d'un unique consentement (par exemple dans le cas de la publicité en ligne, la sélection de la publicité et la mesure d'audience de ladite publicité peuvent découler d'un unique consentement)
  - Le développeur ne devrait proposer que des SDK qui autorisent techniquement la suspension de leurs propres exécutions tant qu'ils n'ont pas reçu de signal de l'application leur indiquant quelles exécutions peuvent être mises en œuvre en fonction des finalités appropriées.

3. Auditer le bon fonctionnement des SDK

Au-delà de la collecte d'éléments contractuels et documentaires, il est recommandé que le développeur mette en œuvre des moyens suffisants, et 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 méthodologie d'audit par interception des communications réseaux devrait être envisagée.
  - Le développeur devrait au moins veiller, dans la mesure du possible, à vérifier les 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.
  - L'éditeur du SDK, en tant que sous-traitant ou sous-traitant ultérieur, a l'obligation de faciliter la tenue de ces audits.
  - En cas d'évolution du SDK, ces analyses devraient être mises à jour.
  - En raison de la grande complexité de certaines briques applicatives, ces modalités ne peuvent permettre à elles-seules d'assurer le respect des obligations et sont uniquement un complément aux mesures organisationnelles.

6.4. Assurer la sécurité de l'application

La sécurité des traitements mis en œuvre constitue une obligation incombant au développeur traitant des données pour le compte de l'éditeur, conformément à l'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

Parmi les mesures de sécurité à mettre en œuvre, certaines peuvent systématiquement être mises en œuvre par le développeur.

- **Quelles mesures de base est-il recommandé de mettre en œuvre ?**
  - 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[37] ;
  - 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 ;
  - Quelle que soit la donnée à caractère personnel concernée, prise en compte de la possibilité que l'OS effectue des sauvegardes automatiques de celles-ci. Désactivation des sauvegardes non souhaitées ou 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 et L2 des recommandations produites par l'OWASP[38].

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 ?**
  - Dans le cas général, le développeur devrait éviter 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, seul le défaut d'intégrité devrait être signalé, sans provoquer de blocage.
  - De manière similaire, les mesures d'épinglage de certificat (« *certificate pinning* ») ou d'obfuscation de code ne constituent pas des mesures de sécurité pertinentes.
  - Le service devrait être conçu de manière à maintenir le niveau de sécurité même avec des terminaux corrompus. Les bonnes pratiques en termes d'API[39] devraient être appliquées pour sécuriser les serveurs utilisés par l'application et les protéger contre des éventuelles tentatives d'abus.
  - Le développeur devrait 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.

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

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

La sécurité d'une application ne peut se considérer uniquement lors de sa première publication mais doit au contraire reposer sur des mesures pérennes.

- **Quelles mesures est-il recommandé de mettre en place pour assurer la sécurité au cours du temps ?**
  - Le développeur devrait mettre en œuvre des processus de déploiement qui assurent le maintien de la qualité des applicatifs distribués :
    - 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 développeur devrait maintenir 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* »[40]). Pour minimiser la surface d'attaque possible, en utilisant au minimum des éléments fournis par des tiers.
  - Le développeur devrait assurer une mise 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, 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, le développeur doit avertir 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 développeur devrait respecter les bonnes pratiques de conformité et de sécurité des développements informatiques, tels qu'indiqué dans le Guide RGPD de l'équipe de développement.

[40] « Chaîne d'attaque sur les prestataires de service et les bureaux d'étude : un nouveau rapport d'analyse de la menace », ssi.gouv.fr

6.5. Liste de vérifications

Catégorie	Sous-Catégorie	Identifiant	Description
Formaliser son interaction avec l'éditeur	Identifier les responsabilités et devoirs de chacun	1.1.1	Un registre des traitements comprenant la qualification de chacun des acteurs participants est fourni lors de la contractualisation.
		1.1.2	Les conditions de mise en œuvre de chaque traitement sont clairement stipulées dans le contrat.
		1.1.3	Un point de contact chez l'éditeur est désigné pour la validation de tout choix impactant les traitements de données personnelles.
		1.1.4	Un registre des traitements effectivement mis en œuvre est tenu et mis à disposition de l'éditeur, et en cas de divergence, celui-ci est alerté.
		1.1.5	Les obligations du développeurs (notamment article 28 et article 30.2 du 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	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.
Assumer son rôle de conseil envers l'éditeur	Proposer des développements respectant les principes de protection des données personnelles	2.1.1	Des solutions techniques à l'état de l'art sont analysées et proposées à l'éditeur pour minimiser les collectes et limiter l'impact de la mise à disposition des données aux tiers.
		2.1.2	La permission la moins intrusive est choisie pour chaque donnée collectée via ce système, et elle n'est déclenchée qu'au moment où elle est nécessaire.
		2.1.3	Les données sensibles (au sens de l'article 9 du RGPD) sont distinguées des autres types de données, notamment en termes d'architecture.
		2.1.4	Les données sensibles ne sont pas rendues accessibles aux tiers (par exemple, aux SDK).

	Aider au bon respect des droits des utilisateurs	2.2.1	Une politique de confidentialité lisible sur support mobile est fournie par l'éditeur et intégrée au sein de l'application, de manière accessible.
		2.2.2	L'exercice des droits est possible simplement, par exemple au moyen d'une page intégrée dans l'application.
		2.2.3	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.
	Participer à la conformité en matière d'usage de traceurs et de recueil du consentement	2.3.1	Les opérations visées par la nécessité du consentement sont identifiées et des instructions écrites spécifiques sont demandées à l'éditeur à ce sujet.
		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.
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	Les responsabilités sont qualifiées pour chacun des traitements mis en œuvre dans le cadre de l'intégration du SDK, et validées par l'éditeur.
		3.1.3	Le SDK respecte le consentement de l'utilisateur et répond aux demandes d'exercice des droits.
	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 ne procède à 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	Les niveaux L1 et L2 de l'OWASP MAS sont atteints.
	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 SDK

Notice

À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de kits de développement logiciel (ou SDK, pour « *software development kit* »)**.
- Le fournisseur de SDK est défini comme **l'entité personne 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**.**
- Dans la pratique, 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 la 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 donc essentiel que dans ces différentes configurations les rôles respectifs et qualification de chaque acteur à l'égard des traitements de données personnelles soient préalablement identifiés.
- 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 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 ?

- Ces recommandations sont organisées en plusieurs sections, chacune correspondant à une étape dans la mise à disposition d'un SDK par un fournisseur. Chaque partie 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 de vérifications récapitulative, regroupant les principales recommandations** destinées aux fournisseurs de SDK, est proposée à la fin de cette partie. Les fournisseurs de SDK sont invités à étudier cette liste et à l'utiliser notamment lors de la rédaction de leur documentation contractuelle.

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 vie privée 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.

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

Il est important de déterminer précisément les obligations qui incombent au fournisseur de SDK en fonction de sa qualification.

- **Quelles qualifications pour les traitements mis en œuvre ?**
  - Dans le cadre de la fourniture de SDK, différentes qualifications sont possibles en fonction des spécificités du traitement de données personnelles impliqué.
  - 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)[41].
  - Certaines recommandations propres à d'autres acteurs peuvent trouver à s'appliquer aux fournisseurs de SDK dans certains cas, en fonction de leur qualification pour chaque traitement.

- **Quels points d'attention spécifiques ?**
  - Le fournisseur de SDK devrait identifier si les données collectées constituent des données sensibles au sens de l'article 9 du RGPD (voir encadré ci-dessous).
  - Plus généralement, il devrait éviter, dans leur conception, que les outils qu'il propose procèdent à un recueil de données personnelles ; si ce recueil est indispensable, il ne doit jamais être réalisé à l'insu des personnes concernées.
  - Si le fournisseur de SDK est responsable de traitement ou responsable conjoint, il devrait veiller en particulier à s'assurer de l'information des personnes concernées (voir la partie 4 des présentes recommandations).
  - Si le SDK utilise des traceurs (y compris via la mise en œuvre d'une opération de lecture ou d'écriture sur le terminal de l'utilisateur, par exemple d'un identifiant logiciel ou matériel), cet usage devrait être précisément analysé, en fonction de la qualification et des responsabilités du fournisseur de SDK, en se référant notamment aux à la partie 6 de la présente recommandation (« Recommandations spécifiques aux développeurs »).
  - Le fournisseur de SDK devrait également s'assurer que ses clients ont connaissance du lieu de stockage des données, dans la mesure où un encadrement contractuel et/ou technique des transferts des données au sens du chapitre V du RGPD[42] pourrait être nécessaire[43].

Qu'est-ce qu'une donnée sensible au sens de l'article 9 du RGPD ?

- **Voir la partie 5.1 des présentes recommandations :** « Assurer la conformité juridique des traitements »

[41] 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

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

[43] 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

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

Il est recommandé, pour chacun des traitements envisagés et selon la qualification au sens du RGPD et les responsabilités du fournisseur de SDK, d'analyser si des mesures de protection des données personnelles dès la conception et par défaut peuvent s'appliquer.

- **Comment minimiser les données collectées ?**
  - Le principe de minimisation doit notamment conduire à limiter au strict nécessaire les données envoyées vers des serveurs (ceux du fournisseur de SDK, comme ceux de ses partenaires) au strict nécessaire, au regard des finalités poursuivies, pour atteindre la finalité du traitement.
  - Des configurations par défaut des SDK qui respectent ce principe devraient être proposées, y compris dans les exemples de configuration proposés dans ses documentations.
  - En particulier, la collecte et l'enregistrement d'identifiants de terminaux, de réseau (adresse IP, matériels réseau environnants) ou d'individus doivent être évités si l'usage du SDK ne le nécessite pas.
  - Lorsque le fournisseur d'OS ou un service tiers propose une fonctionnalité plus protectrice de la vie privée pour traiter certaines informations (par exemple une géolocalisation grossière au lieu d'une géolocalisation fine), qui semble plus pertinente en termes de minimisation de données, celle-ci devrait être mise en œuvre et les partenaires devraient être informés de la nécessité de mettre à jour leur SDK pour en tenir compte.

- **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 de traitement), la sélection indépendante de ces deux fonctionnalités par l'éditeur devrait 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 demandent le consentement, cette décorrélation technique peut également être nécessaire pour répondre à la nécessité du consentement de l'utilisateur.
  - Dans cette même logique, le fournisseur de SDK devrait 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 devrait 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 devrait pas rendre cette demande systématique.
  - Le fournisseur devrait veiller à choisir le niveau de permission le moins intrusif possible, ou à proposer différentes configurations au choix de l'utilisateur.
  - Le fournisseur de SDK doit aussi clairement distinguer les permissions relatives au service rendu à l'application des permissions et traitements de données subséquents qu'il réalise pour son compte propre et qui sont parfois liés à son modèle économique.
  - Il devrait veiller à rendre le SDK 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

Si la responsabilité de la conformité au RGPD d'une partie importante des traitements mis en œuvre dans l'application incombe à son éditeur, les traitements engendrés par l'intégration de SDK peuvent impacter sensiblement le travail de ces éditeurs dans l'information qu'ils communiquent et l'analyse des traitements mis en œuvre. Il est dès lors du ressort du fournisseur de SDK de documenter les informations nécessaires à la démonstration de la bonne application des textes.

1. Identifier les informations à rassembler

Il est important que le fournisseur de SDK s'assure de documenter l'ensemble des informations nécessaires au respect de ses obligations et/ou de celles de ses partenaires.

- **Quelles informations documenter sur les traitements mis en œuvre ?**
  - Quelles que soient les opérations réalisées par un SDK proposés par les fournisseurs de SDK, il est important que son fournisseur rédige et mette à disposition de ses clients une analyse claire des traitements entraînés par l'utilisation du SDK, et que le fournisseur se contente de fournir le logiciel ou joue un rôle opérationnel dans la mise en œuvre concrète des traitements.
  - Pour les traitements dans lesquels le fournisseur du SDK aura une responsabilité au sens du RGPD :
    - le fournisseur de SDK doit tenir et maintenir son propre registre des activités de traitement, selon sa qualification au sens du RGPD et conformément à l'article 30 du RGPD ;
    - pour chaque traitement, il doit identifier, le cas échéant avec ses partenaires, la qualification qui lui incombe au sens 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, conformément à l'article 28 du RGPD, 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.
- **Quelles informations documenter sur les usages de traceurs ?**
  - Le fournisseur de SDK doit informer précisément ses partenaires sur les traceurs utilisés qui mettent en œuvre 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 ces occurrences).
  - Il doit indiquer les finalités poursuivies par chacun de ces usages de traceurs, ou les fonctionnalités qu'ils permettent.
- **Quelles informations documenter sur les permissions ?**
  - Le fournisseur de SDK doit informer ses partenaires 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 doit préciser la nature optionnelle ou obligatoire de ces opérations selon les fonctionnalités proposées.

2. Présenter ces informations dans un format accessible

Ces informations sont idéalement 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 à 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.
  - Toute évolution du service impactant les questions de vie privée doit être mise à disposition des partenaires du fournisseur de SDK et leur 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 ?**
  - Lorsqu'il est responsable de traitement ou sous-traitant, le fournisseur de SDK doit tenir un registre de traitement comprenant l'ensemble des informations mentionnées à l'article 30 du RGPD :
    - 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 conseillé de mettre à disposition des partenaires un registre dynamique en fonction du paramétrage de chaque client. À défaut, les paramètres liés à chaque traitement devraient être soigneusement indiqués pour que les partenaires puissent aisément comprendre quels traitements sont mis en œuvre dans le cadre de leur configuration particulière.
    - Pour chaque traitement, les données collectées pour chaque traitement devraient être clairement 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.
    - Le registre devrait être 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.
  - De la même manière, lorsqu'il est responsable ou responsable conjoint du traitement pour ces opérations, le fournisseur de SDK doit documenter les opérations de lecture et/ou d'écriture qu'il met en œuvre. Il peut 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, mais aussi 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 est de son ressort d'assurer l'information des personnes. En effet, le SDK ayant vocation à être intégré dans une application mobile qui dépend d'un éditeur, cette information devra généralement être intégrée dans l'information fournie par l'éditeur à l'utilisateur
  - Il peut y veiller en exigeant contractuellement de l'éditeur ou du développeur qui a recours à ses services de procéder à cette information.
  - Il en va de même si un consentement est requis 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.

- **Comment s'assurer que les utilisateurs puissent facilement exercer leurs droits ?**
  - L'exercice des droits peut concerner des traitements sous la responsabilité de l'éditeur de l'application et le rôle du fournisseur de SDK, s'il est sous-traitant, est alors un rôle d'aide à la conformité, qui dépend des fonctions qui lui sont confiées contractuellement. Il peut aussi concerner les traitements sous la responsabilité propre du fournisseur de SDK, qui est 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.
  - Pour faciliter la mise en œuvre pratique de l'exercice des droits, la possibilité de l'automatiser devrait être 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 devrait veiller 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 devrait suffire pour permettre l'exercice des droits de la personne. À l'inverse et au regard de l'article 11 du RGPD, dans le contexte des applications mobiles, 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 serait alors nécessaire à la réidentification 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, l'assistance au responsable de traitement implique de conseiller celui-ci, 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 l'application nécessite le consentement de l'utilisateur, il est nécessaire de s'assurer qu'un consentement valable a été obtenu pour chaque finalité poursuivie.
- En conséquence, l'accès par le SDK à une ressource protégée et le traitement qui en résulte, s'ils nécessitent le consentement, ne peuvent pas systématiquement être opérés 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 peut être utilisée pour le SDK sans un nouveau consentement de la personne concernée.

- **Comment permettre un recueil de consentement valide ?**
  - 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) devraient être proposés, et ce jusqu'à ce qu'un consentement valable soit recueilli. Concrètement, cela signifie que le fournisseur devrait permettre que son SDK puisse suspendre son exécution tant qu'un consentement n'a pas été transmis.
  - 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, la conception et la documentation du SDK devrait prévoir la possibilité et anticiper les impacts fonctionnels d'une d'absence de consentement de l'utilisateur à celui-ci, 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. Notamment, le fournisseur de SDK devrait s'assurer 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 devrait 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.

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

Le fournisseur de SDK, doit, lorsqu'il est qualifié de sous-traitant, 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. Même dans les cas où le fournisseur de SDK est simple fournisseur de logiciel, il est encouragé à suivre ces recommandations.

- **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, ce dernier a l'obligation de contribuer à la réalisation d'audits (article 28.3.h du RGPD).

- **Comment faciliter la tenue d'audits ?**
  - Il appartient au fournisseur de SDK, en plus d'une transmission d'informations claires et d'une documentation technique à jour (voir ci-dessus) conformément à l'article 28, de faciliter la tenue d'audits, y compris de manière opérationnelle.
  - À ce titre, le fournisseur de SDK et ses sous-traitants peuvent être amenés à devoir répondre à des questions spécifiques sur les traitements mis en œuvre.
  - Ces questions peuvent faire suite à la simple diligence de leur client ou être transmises dans le cadre d'un contrôle d'une autorité de protection des données européennes ou suite à la réception d'une plainte ou d'une réclamation sur un ou plusieurs traitements précis d'une application liés au fonctionnement du SDK.
  - Le fournisseur de SDK devrait permettre, dans la mesure du possible, la transmission et l'obtention de réponses à celles-ci.
  - 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 ou les autorités de contrôle.

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

Le maintien de la conformité du SDK doit se concevoir 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 ?**
  - Des outils et méthodologies de signalement de vulnérabilité, en cas d'exploitation avérée de celle-ci, devraient être mis 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 et selon que le fournisseur de SDK est responsable ou responsable conjoint du traitement pour chaque traitement mis en œuvre par son SDK, il peut également être amené à devoir notifier lui-même la violation de données à l'autorité du pays dont l'entité dépend, ainsi éventuellement qu'aux personnes concernées (articles 33 et 34 du RGPD).

- **Comment prendre en compte les éventuelles évolutions de ses partenaires ?**
  - Il appartient au fournisseur de SDK de surveiller 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 constate qu'une information est manquante ou trop générale, il est de sa responsabilité de le signaler à son partenaire.
  - Le fournisseur de SDK devrait également 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. Le fournisseur devrait mettre à jour son SDK compte tenu des évolutions techniques de l'OS.

- Le fournisseur de SDK devrait notamment étudier si ces évolutions peuvent permettre de mettre en œuvre les traitements d'une manière respectueuse de la vie privée dès la conception. Si c'est le cas, il devrait mettre à jour et encourager l'utilisation des versions les plus récentes de son outil.

7.5. Liste de vérifications

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.
		1.1.3	La configuration par défaut du SDK permet à l'application qui l'utilise d'éviter qu'il n'entraine une collecte de données involontaire ou excessive.
		1.1.4	Les éventuelles lectures ou écritures opérées par le SDK sont définies et une documentation est mise à disposition des développeurs tiers.
	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, de manière à limiter strictement les finalités définies par le responsable de traitement.
		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	S'il n'est pas possible techniquement de décorréler les fonctionnalités 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	Un registre des traitements propre au SDK est tenu et maintenu à jour.
		2.1.3	Le registre indique pour chaque traitement la qualification des acteurs, au sens du RGPD.
		2.1.4	Pour chaque traitement impliquant le recours à un sous-traitant ultérieur, la liste des données collectées est établie, l'analyse des finalités est effectuée et l'autorisation du responsable de traitement est obtenue.
		2.1.5	La présence de traceurs mettant en œuvre une lecture ou une écriture sur le terminal de l'utilisateur final est indiquée précisément.
		2.1.6	Le caractère optionnel ou obligatoire pour chacun 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, permettant aux tiers partenaires d'analyser dans le temps ce qui les impacte.
		2.2.4	Lorsque ces traitements modifiés sont opérés en tant que sous-traitant, le recueil de leur autorisation est de nouveau effectué auprès de l'éditeur, préalablement à leur mise en œuvre.
		2.2.5	Le registre des traitements distingue clairement les finalités associées à chaque traitement.
		2.2.6	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 intégrer les éléments du registre qui correspondent à son paramétrage à son propre registre de traitements.
		2.2.7	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.
		2.2.8	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	Une vérification de recueil de consentement est opérée par le SDK lorsque c'est nécessaire, que l'accès à la ressource propre à l'utilisateur final soit effectué pour le compte du SDK ou pour le compte tiers partenaire, de sorte que l'accès à une permission système ne suffise techniquement pas au SDK pour collecter une donnée.
		3.2.2	Les permissions système nécessaires sont accordées dans les contextes d'usage où elles sont nécessaires à l'exécution du traitement prévu.
		3.2.3	Le SDK est conçu techniquement pour permettre une suspension de son exécution tant qu'un consentement valable, par finalité, n'est pas recueilli.
		3.2.4	Si plusieurs finalités sont poursuivies, le SDK permet techniquement la prise en compte d'un signal distinct par finalité, toujours indépendamment des permissions système.
		3.2.5	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.
		3.2.6	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).
		3.2.7	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	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 niveaux L1 et L2 de l'OWASP MAS sont atteints.
		4.1.4	Le modèle de sécurité ne repose pas sur l'intégrité du terminal.

		4.1.5	Toute détection de défaut d'intégrité est indiquée à l'utilisateur final et non utilisée pour bloquer celui-ci.
		4.1.6	La sécurisation du service est rendue effective par la sécurisation des API.
		4.1.7	Les données personnelles sont protégées contre des éventuels détournement internes ou par des sous-traitants ou sous-traitants ultérieurs.
		4.1.8	Toute violation de données personnelles, suspectée ou avérée, est signalée à l'éditeur ou au développeur partenaire, qu'il soit responsable de traitement ou responsable conjoint.
	Permettre la réalisation d'audits	4.2.1	Des rapports d'audits sont réalisés régulièrement et sont tenus à disposition des éditeurs partenaires et des autorités de protection des données qui en feraient la demande.
	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 politiques de confidentialité des partenaires, afin de pouvoir les assister et les informer si ces politiques ne correspondaient pas aux traitements mis en œuvre par le SDK.
		4.3.3	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, y compris en accompagnant les tiers partenaires.

8. Recommandations spécifiques au fournisseur d'OS

Notice

À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de systèmes d'exploitation (ou OS, pour *operating system*)**.
- Dans le contexte de ces recommandations, le fournisseur d'OS est défini comme **l'entité personne morale qui met à disposition un système d'exploitation sur un terminal.**
- Ce système d'exploitation peut, en fonction des situations :
  - être développé dans son intégralité par une entité pour usage exclusif sur des terminaux qu'elle met à disposition (par exemple iOS, développé par Apple) ;
  - être développé dans son intégralité par une entité pour usage sous licence sur des terminaux produits par des tiers (par exemple Android, développé par Google) ;
  - être 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 des terminaux (par exemple LineageOS, basé sur Android et développé par LineageOS LLC).
- Dans la pratique, le public cible de ces recommandations est notamment constitué :
  - des délégués à la protection des données (DPD ou *Data Protection Officer – DPO*) ;
  - des 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, dans le cadre du fonctionnement normal du terminal et des applications exécutées par l'utilisateur, peuvent être amenés à traiter des données personnelles. 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. Il est important que les fournisseurs d'OS permettent des configurations facilitant la conformité des applications.
- De plus, dans le cadre de la publication d'un OS sous une licence permettant sa réutilisation, 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. Il est donc important que des bonnes pratiques de protection de la vie privée dès la conception (« *privacy by design* ») puissent 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, indépendamment du fait de baser leur OS sur un OS préexistant, d'y intégrer un ensemble d'applicatifs tiers. Ces choix technologiques impliquent de nombreux traitements de données qu'il est important d'identifier, tant par les conséquences sur les personnes que pour les qualifications juridiques qui en découlent au sens du RGPD.

Comment utiliser ces recommandations ?

- Ces recommandations sont organisées en plusieurs sections, chacune correspondant 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. Chaque partie 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 de vérifications** **récapitulative, regroupant les principales recommandations** destinées aux fournisseurs d'OS, est proposée à la fin de cette partie. Les fournisseurs d'OS sont invités

à étudier cette liste et à l'utiliser notamment lors de la rédaction de leur documentation contractuelle pour s'assurer, le cas échéant, de la prise en compte de ces recommandations par ses partenaires.

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

Si ce n'est pas son rôle principal dans le contexte des applications mobiles, l'OS fournissant de manière principale des fonctionnalités à l'usage des développeurs d'applications, il est possible que certains traitements de données personnelles soient mis en œuvre à son initiative. À ce titre, il est nécessaire de répondre aux obligations concernant ces traitements.

1. Identifier et analyser 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 par ces entités.

- **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 devrait 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 de la présente recommandation, en particulier « Qualification du fournisseur du système d'exploitation ». En particulier, dans de nombreux cas, l'OS se limite à fournir des outils logiciels sans endosser de responsabilité.
  - 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 géolocalisation) ;
    - 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 bien 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 devrait permettre une utilisation fonctionnelle du terminal par l'utilisateur, et notamment de ses applications par défaut ou installées par ses propres moyens, sans qu'une création de compte ne soit nécessaire. Il doit 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[44].
- **Comment minimiser les données traitées par l'OS en tant que responsable de traitement ?**
  - Dans certains cas, les OS procèdent à des traitements de données en tant que responsable de traitement, de manière indépendante ou dans le cadre de la fourniture de fonctionnalité à des tiers (les applications par exemple) ou à l'utilisateur. Les mesures à mettre en œuvre dépendent alors des traitements opérés.
  - Concernant la transmission des notifications aux utilisateurs de l'application :
    - le fournisseur d'OS devrait 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 ;
    - il devrait 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 est recommandé d'indiquer clairement les modalités d'usage de ces outils dans la documentation à destination des développeurs
  - Concernant la télémétrie et la remontée de bogues :
    - il devrait 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 ;
    - il devrait permettre aux éditeurs et aux tiers, y compris lui-même, le cas échéant, d'obtenir le recueil d'un consentement des utilisateurs préalablement à chaque remontée de ces données ou à leur transmission à des tiers.
  - Concernant le stockage distant des sauvegardes :
    - il devrait s'assurer que celles-ci ne sont opérées qu'à la suite d'une demande explicite de l'application et non par défaut ;
    - il devrait 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 géolocalisation :
    - le fournisseur d'OS devrait permettre à l'application faisant usage des données de localisation, ainsi qu'à l'utilisateur, de facilement limiter l'usage de la géolocalisation 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 géolocalisation fondé sur des connexions environnantes, un mode de calcul de la localisation précise sur le terminal et non sur le serveur devrait être privilégié : à titre d'exemple, 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.

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

- le fournisseur d'OS devrait offrir la possibilité à l'utilisateur de pouvoir paramétrer facilement une suspension de la collecte constante de la géolocalisation, par l'OS lui-même ou par 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 devrait pouvoir choisir sans effort que sa géolocalisation 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

Les fournisseurs d'OS, du fait de leur expertise sur les traitements qu'ils opèrent et sur les fonctionnalités qu'ils proposent, 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 et claires pour favoriser la conformité des partenaires

Afin de faciliter la bonne compréhension des fonctionnalités de l'OS, il est recommandé de mettre à disposition une documentation exhaustive et claire, tant sur le plan technique que juridique.

- **À quel public adresser cette documentation ?**
  - S'il est courant que des documentations techniques soient mises à disposition, peuvent y être inclues également des éléments analysant le cadre législatif et normatif particulier de l'Union européenne, pour les éditeurs et développeurs qui souhaitent cibler le marché européen.
  - Ces éléments juridiques ne devraient pas être séparés des éléments techniques, et une compréhension commune des impacts qu'auront les décisions de chaque type devrait être favorisée pour permettre des décisions communes de la part de ces acteurs.
  - Ces éléments, et en particulier les contenus juridiques, devraient être rendus disponibles dans une langue comprise par le public visé.

- **Quels éléments inclure dans cette documentation ?**
  - Pour les éditeurs visant le marché européen, le fournisseur d'OS devrait alerter en particulier sur la nécessité de définir leur responsabilité et de mettre en place les mesures de conformité (finalité, information, droits, sécurité, etc.).
  - En plus des éléments techniques, il est recommandé d'intégrer des guides et outils spécifiques à l'attention des DPD, pour qu'ils puissent les intégrer directement dans leurs méthodologies d'analyse de risques et d'amélioration continues.
  - Si plusieurs méthodes de développement cohabitent sur le plan fonctionnel, le fournisseur d'OS devrait en préciser les caractéristiques, techniques comme juridiques, pour permettre à l'éditeur et au développeur de faire un choix éclairé prenant l'ensemble de ces critères. Les critères de rétrocompatibilité, de fin de support, de vulnérabilité, d'optimisation énergétique, de déport de la logique de calcul, de transferts, etc., devraient notamment être présentés.
  - Il est recommandé d'indiquer dans la documentation officielle si les outils mis à disposition peuvent permettre ou pas 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, notamment lorsque l'usage de fonctionnalité mises à disposition par l'OS aux applications entraine un traitement de la part de l'OS.

- **Quelle information mettre à disposition ?**
  - Le fournisseur d'OS devrait s'assurer 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.

- En particulier, il devrait 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[45].

- **Sur quels dispositifs informer les tiers ?**
  - Il est important de procéder à une information renforcée sur les dispositifs identifiés dans la partie précédente (sauvegardes, notification, télémétrie).
  - Le fournisseur d'OS devrait attirer 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).
  - L'impact des paramétrages et des fonctionnements par défaut de ces dispositifs devrait être expliqué de façon claire.

Qu'est-ce qu'une donnée sensible au sens de l'article 9 du RGPD ?

- **Voir la partie 5.1 des présentes recommandations :** « Assurer la conformité juridique des traitements »

3. Encourager l'utilisation des fonctionnalités les plus protectrices

Il est recommandé au fournisseur d'OS de mettre à disposition le détail des caractéristiques des différentes fonctionnalités qu'il propose. Cela 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.

- **Comment encourager l'adoption de technologies les plus respectueuses de la vie privée ?**
  - Le fournisseur d'OS devrait 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 devrait 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 devrait organiser la fin du support des fonctionnalités les plus problématiques, avec une période de transition suffisante pour permettre aux éditeurs de mettre à jour leurs applications.
  - Il devrait 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.

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

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

Si dans de nombreux cas, le fournisseur d'OS n'est pas partie prenante des traitements de données personnelles opérés au sein des applications, les fonctionnalités qu'il met à disposition des éditeurs et développeurs d'applications peuvent avoir un impact sur les traitements mis en œuvre et leur conformité. Il est donc important, à titre de bonne pratique de mettre ces problématiques au cœur de ses considérations lors de la conception de ces fonctionnalités.

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

Le système des permissions est au cœur de la protection des utilisateurs fournie par l'OS. À ce titre, il est important, lors de la conception de celui-ci, de mettre en œuvre le maximum de mesures permettant de protéger les données personnelles de l'utilisateur. En empêchant techniquement et/ou contractuellement les éditeurs d'applications d'accéder à certaines données, les permissions apportent une garantie technique forte de respect de la confidentialité des informations par les applications, et constituent une mesure positive majeure pour préserver la vie privée des personnes.

- **À quelles opérations appliquer les permissions ?**
  - Le fournisseur d'OS devrait appliquer 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).
  - Il devrait imposer l'information et le recueil de la permission de l'utilisateur pour l'ensemble de ces éléments, en évitant de masquer des permissions aux utilisateurs.
  - Il devrait prévoir le recueil d'une permission d'accès donnée par 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, la portée de celle-ci devrait être analysée sous trois axes distincts :
    - son degré de précision : 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 ;
    - sa portée matérielle : chaque permission peut s'appliquer à un ensemble plus ou moins large de données ou de fonctions. Toute permission trop large en termes de portée matérielle devrait être exclue en raison de la collecte excessive de données qu'elle provoque. Par exemple, toute permission globale d'accès aux fichiers stockés devrait être exclue, et un système d'accès par fichier ou dossier doit être privilégié ;
    - 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 devrait 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.
  - Le plus grand contrôle devrait être offert autant à l'éditeur de l'application qu'à l'utilisateur, pour restreindre la portée de chaque permission selon ces trois axes.

- **Quelles mesures additionnelles ?**
  - Le fournisseur d'OS devrait décourager voire ne pas permettre de conditionner le lancement d'une application à l'obtention de permissions. Au contraire, il devrait s'assurer de

systématiquement prévoir dans les applications la possibilité que l'utilisateur refuse les permissions demandées.
- Il devrait encourager, notamment 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.
- Il devrait permettre aux utilisateurs de décliner une permission sans que l'application soit automatiquement informée de ce refus. Par exemple, il devrait permettre de refuser l'accès aux contacts en renvoyant une liste vide ou partielle de contacts, à la localisation en renvoyant des coordonnées aléatoires ou prédéfinies manuellement, etc.
- Par défaut, il devrait permettre aux utilisateurs de n'autoriser l'accès qu'une seule fois ou uniquement quand l'application est active/en premier plan/utilisée, particulièrement pour les permissions les plus sensibles. Si l'application requiert une permission « à tout moment » (y compris quand l'application est fermée), l'information et le consentement de l'utilisateur devraient être renforcés.
- Il devrait révoquer périodiquement les autorisations permanentes des applications non utilisées, en prévenant l'utilisateur. Il devrait permettre à l'utilisateur de fixer la fréquence de ces rappels.
- Il devrait 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 droits et du consentement des utilisateurs

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

- **Comment aider au bon recueil du consentement ?**
  - Bien que ce ne soit pas systématique, il est très 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 fatigue du consentement des personnes, les fenêtres de permission devraient directement permettre d'obtenir un consentement valable.
  - À cette fin, il devrait être permis, au sein de ces fenêtres :
    - de préciser la finalité pour laquelle la permission est demandée ;
    - d'intégrer 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), notamment à la liste des listes de tiers intervenants comme responsable de traitement ;
    - de préciser les modalités pour révoquer son accès.
  - Si nécessaire, et en fonction de l'intrusivité des permissions, le fournisseur d'OS devrait 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, par exemple en proposant 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 de cette collecte et d'évaluer le degré de confiance qu'il porte dans l'éditeur d'une application.
  - Le fournisseur d'OS devrait également s'assurer, en fonction des instructions de l'éditeur que l'utilisateur est en mesure de comprendre si une permission est obligatoire ou facultative et l'impact de sa décision sur son accès à l'application.
  - Il devrait permettre de révoquer ou modifier facilement les permissions accordées par l'utilisateur.

- **Comment permettre la bonne information des utilisateurs ?**
  - 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, devraient être mises en œuvre.
  - L'utilisateur devrait avoir accès à un historique de l'activation des capteurs et des requêtes effectuées, filtrés par usage et par processus système ou par application.
  - Pour les permissions les plus intrusives (accès au microphone, à la caméra, à la géolocalisation, aux fichiers sur le téléphone, aux contacts, à l'agenda), il devrait être prévu de réitérer la demande de permission quelques semaines 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. De plus, un indicateur pourrait être affiché, par exemple dans la barre d'état, signalant quand la permission est utilisée.
- **Comment faciliter la portabilité des données ?**
  - Le fournisseur d'OS devrait mettre en œuvre une portabilité des données personnelles, au moyen d'un format ouvert. Cette portabilité devrait concerner les configurations et les applications installées sur le téléphone.
  - Le dialogue et la coopération avec les fournisseurs d'autres OS devrait à ce titre être favorisé, de manière à définir un « *format structuré, couramment utilisé et lisible par machine* », tel que mentionné par les articles 4-1 et 20 du RGPD, qui soit le plus 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.

- **Comment participer à la conformité des applications en ce qui concerne les utilisateurs mineurs ?**
  - Devraient être mis en œuvre au sein de l'OS 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. L'outil de contrôle parental doit pouvoir être utilisé directement sur le terminal sans avoir fournir d'informations complémentaires à un tiers (fournisseur de l'OS ou éditeur d'un système de contrôle parental), ni obliger à créer un compte utilisateur sur un service en ligne.
  - 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.
  - La minorité des utilisateurs devrait être prise en compte dans ces outils, concernant leur capacité à répondre aux permissions système via des outils de contrôle parental efficaces.
  - Il devrait ainsi être permis d'enregistrer plusieurs profils au sein des vecteurs d'authentification biométriques, en permettant de distinguer s'il s'agit du mineur ou de son représentant légal, de sorte qu'il soit 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 l'élément fondamental en termes de sécurité du terminal. À ce titre, les fournisseurs d'OS devraient, à titre de bonne pratique, s'assurer qu'ils mettent à disposition des éléments à l'état de l'art pour apporter cette garantie aux personnes.

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, devrait 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.
  - Si le terminal est utilisé à la fois dans la vie privée et professionnelle, un cloisonnement des usages personnels et professionnels au sein d'un même terminal au moyen de mesures techniques et de design d'interface devrait être mis en place. Pourraient par exemple être permis :
    - l'usage de profils utilisateurs distincts au sein de l'OS, en communiquant sur 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. En effet il est important, pour assurer la granularité des permissions et le contrôle des éventuels SDK par les éditeurs, d'assurer 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 ne devrait pas automatiquement étendre cette permission à l'ensemble des SDK intégrés dans cette application.
- **Quelles mesures techniques mettre en œuvre ?**
  - Un espace de stockage sécurisé dédié au stockage local des secrets (enclave, autrement appelé « *SecureElement* ») devrait être mis à disposition, lorsque le terminal sur lequel l'OS sera exécuté dispose du matériel nécessaire.
  - Le chiffrement des connexions réseaux devrait être imposé. À défaut, toute connexion non chiffrée devrait être signalée. L'usage du protocole TLS devrait ainsi être forcé dès que possible, ou bien son absence indiquée aux utilisateurs.
  - Des fonctionnalités de chiffrement à l'état de l'art devraient être mises à disposition des applications.
  - Des outils de partage local entre applications devraient être mis à disposition.
  - Les sauvegardes devraient être chiffrées par défaut, qu'elles soient locales ou placées sur des serveurs tiers. Les clés de chiffrement devraient être conservées sur le terminal.
  - Le fournisseur d'OS devrait indiquer les bonnes pratiques, 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.

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 ?**
  - Devraient être mis en place des outils adéquats, qu'ils soient contenus au sein même de l'OS ou proposés dans un environnement de développement, permettant 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 devraient être documentées, par exemple pour les développeurs concernant leurs propres applications mais également des traitements effectivement mis en œuvre par les SDK qu'ils peuvent être amenés à intégrer pour des questions de fonctionnalités ou de monétisation.

- Les utilisateurs devraient pouvoir générer des rapports de confidentialité simplifiés, afin qu'ils puissent comprendre 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 devrait mettre en place des processus pour assurer le maintien à jour du parc d'utilisateurs.

- **Comment préserver la sécurité des terminaux dans le temps ?**
  - Le fournisseur d'OS devrait 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.
  - Il devrait proposer systématiquement des mises à jour de sécurité de l'OS au moins jusqu'à 5 ans après l'achat du terminal. Le fait que certains éléments fonctionnels ne soient plus compatibles avec le terminal devrait être insuffisant à justifier la cessation des mises à jour de sécurité.
  - Quand cette durée est échue, le fournisseur d'OS devrait indiquer clairement à la personne les risques associés à l'absence de mise à jour. S'ils existent, la personne devrait être orientée vers des OS alternatifs qui supportent son terminal.

8.5. Liste de vérifications

Catégorie	Sous-Catégorie	Identifiant	Description
Assurer la conformité des traitements de données personnelles mis en œuvre	Identifier et analyser 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.
		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 géolocalisation 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 et claires pour favoriser la conformité des partenaires	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.
		2.1.2	Des éléments juridiques sont présents au sein de cette documentation, afin de favoriser les analyses et les impacts des développeurs tiers et des utilisateurs finaux.
		2.1.3	Les différentes documentations sont accessibles dans les langues des publics ciblés.
		2.1.4	Les documentations indiquent comment mettre en œuvre les demandes de recueil de consentement au sein de l'OS.
	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 redevabilité (« *accountability* »), les traitements impliqués ou induits par l'utilisation de l'OS.
	Encourager l'utilisation des fonctionnalités les plus protectrices	2.3.1	Les API proposées par l'OS permettent aux éditeurs et développeurs de répondre à leurs obligations légales.
		2.3.2	Les mises à jour de ces API améliorent le point précédent et une documentation spécifique est proposée aux développeurs et éditeurs pour les accompagner dans l'usage de ces nouvelles API ou nouvelles versions d'API.
		2.3.3	Des statistiques et recueils des retours des développeurs sont mis en place, de manière à identifier les fonctionnalités les plus utilisées et, à l'inverse, permettre de communiquer sur les fonctionnalités respectueuses de la vie privée qui sont ignorées.
		2.3.4	Les fonctionnalités et usages d'API obsolètes sont documentées et les dates de fin de support sont mises en avant. Les fonctionnalités permissives en termes de protection de la vie privée sont supprimées et les développeurs sont accompagnés dans la mise à jour de leurs applications depuis les fonctionnalités devenues obsolètes vers leurs remplaçantes.

Fournir des outils pour permettre le respect des droits et du consentement des utilisateurs	Concevoir des systèmes de permissions respectant le principe de protection des données dès la conception	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.
		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 d'accès aux données présentes sur les terminaux permettent de définir et compartimenter les espaces de stockage rendus accessibles par ces permissions.
		3.1.4	Les permissions peuvent être restreintes par l'utilisateur, sur une période temporelle et un nombre d'occurrences définis.
		3.1.5	L'exécution des applications est pensée de sorte qu'elles puissent être techniquement fonctionnelles indépendamment de l'obtention de permissions.
		3.1.6	Les documentations techniques à l'attention des développeurs référencent et encouragent les bonnes pratiques pour que leurs applications fonctionnent avec le strict minimum de permission accordées et soient accompagnées d'exemples concrets sur les méthodes alternatives qu'ils peuvent envisager (p. ex. : collecte d'un code postal dans un formulaire plutôt que mise en œuvre d'une géolocalisation, documentant la mise en place de ce formulaire).
		3.1.7	Les utilisateurs ont la possibilité de répondre à une permission par un refus de principe sans qu'il ne s'agisse d'un refus technique. Par exemple : suite à un refus de principe, renvoi à l'application d'un carnet de contacts vide, d'une photothèque vide ou partiellement vide (notion de compartimentation, ou « *storage scope* »), géolocalisation aléatoire, etc.
		3.1.8	Les utilisateurs ont accès à un tableau de bord détaillé leur permettant de consulter les permissions attribuées et celles qui ont été utilisées, leur proposant des alertes en cas d'utilisation anormale des permissions.
		3.1.9	Les permissions d'une application sont toutes révoquées lorsqu'une application n'est pas utilisée depuis un certain temps. L'utilisateur est averti de cette révocation.
	Aider au bon respect du consentement et des droits des utilisateurs	3.2.1	Les permissions rendent possible, dans leur format et leur contextualisation, d'emporter un consentement valide au sens du RGPD et de la directive « ePrivacy ». En pratique, elles permettent notamment de présenter la finalité du traitement, de lister les tiers et de préciser les modalités de leur révocation.

		3.2.2	Une information est dispensée, indépendamment de celle ajoutée par l'éditeur de l'application, permettant d'expliquer brièvement les capacités techniques relatives à une permission, afin que les utilisateurs puissent évaluer les bénéfices et les risques de l'accord d'une permission à une application donnée.
		3.2.3	Les écrans de permissions permettent aux développeurs tiers d'afficher à l'utilisateur si une permission est nécessaire au fonctionnement de l'application et aux traitements poursuivis, ou simplement souhaitée par le développeur.
		3.2.4	Les permissions peuvent être facilement révoquées. L'accès aux menus permettant cette révocation est intuitif.
		3.2.5	L'accès en cours aux capteurs physiques, aux matériels d'accès au réseau et aux espaces stockages des terminaux 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.
		3.2.6	L'utilisateur dispose d'un historique d'accès aux capteurs précités, horodaté et par application.
		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, sans qu'une création ou connexion à un compte soit nécessaire.
	Protéger les utilisateurs mineurs	3.3.1	Des outils de contrôles parental sont mis à disposition des utilisateurs finaux.
		3.3.2	Des outils de signalement de l'âge sont mis 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	La compartimentation mise en œuvre permet de restreindre l'accès à la mémoire ainsi que l'usage des permissions à une partie de l'application et non à son ensemble. Concrètement, il s'agit de permettre un refus de permission à un ou plusieurs SDK d'une

			application, tout en permettant une acceptation de permission à d'autres SDK ou aux traitements propres à l'application.
		4.1.4	Lorsque le matériel du terminal le permet, le stockage local de secret utilise le matériel dédié par défaut (enclave ou « *SecureElement* »).
		4.1.5	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.).
		4.1.6	Des systèmes de partages locaux inter-applications sont mis à disposition par l'OS.
		4.1.7	Un système de sauvegarde de l'OS, de son paramétrage et de son contenu est à disposition des développeurs et des utilisateurs finaux.
		4.1.8	Ce système de sauvegarde fonctionne localement par défaut. Aucune sauvegarde distante n'est possible par défaut.
		4.1.9	Ce système de sauvegarde, s'il propose une sauvegarde distante, conserve la clé de chiffrement exclusivement sous le contrôle de l'utilisateur.
		4.1.10	Des bonnes pratiques de conception et de développement en matière de sécurité sont communiquées aux développeurs tiers.
	Mettre à disposition des outils d'audit efficaces	4.2.1	Des outils et méthodologies d'audits sont mis à disposition des développeurs et des utilisateurs finaux (analyse fine du trafic réseau, des processus en cours, etc.).
		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* 5 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.
		4.3.4	Chaque nouvelle version d'un OS assure le plus haut niveau de rétrocompatibilité possible, de sorte que les applications mobiles puissent être fonctionnelles sur une large gamme de versions du même OS.

9. Recommandations spécifiques au fournisseur de magasin d'applications

Notice

À qui s'adressent ces recommandations ?

- Ces recommandations s'adressent aux **fournisseurs de magasins d'applications (*app stores* ou *stores* en anglais)**.
- Dans le contexte de ces recommandations, 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).
- Dans la pratique, le public cible de ces recommandations est par exemple constitué :
  - du délégué à la protection des données (DPD ou *Data Protection Officer – DPO*) de l'entité fournissant le magasin d'applications ;
  - des 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 consultés 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 peut cependant avoir un fort impact sur les traitements de données personnelles mis en œuvre via les applications lors de l'utilisation par les personnes de leurs terminaux. En effet, **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, pourront avoir un impact important 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 présente une information claire sur les traitements susceptibles d'être mis en œuvre au sein des applications distribuées et qu'il mette en œuvre des processus participant à assurer la conformité aux législations en vigueur des applications publiées. **Ces recommandations ont pour but d'aider les fournisseurs de magasin d'applications dans cette démarche.**

Comment utiliser ces recommandations ?

- Ces recommandations sont organisées en plusieurs sections, chacune correspondant à une étape dans l'activité du fournisseur de magasin d'applications. **Chaque partie 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 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 de vérifications récapitulative, regroupant les principales recommandations** destinées aux fournisseurs de magasin d'applications, est proposée à la fin de cette partie. Les fournisseurs de magasins d'applications sont invités à étudier cette liste et à l'utiliser 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 dont les éditeurs sollicitent la publication au sein du magasin d'applications, le fournisseur du magasin 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 recommandations suivantes s'appliquent notamment concernant les applications visant des utilisateurs au sein de l'Union européenne.

1. Centraliser et analyser les données relatives à la conformité

Conformément au principe de redevabilité (« *accountability* »), les éditeurs d'application ont l'obligation de mettre en œuvre tout un ensemble de processus et d'analyse des traitements de données personnelles auxquels ils vont procéder dans le cadre du fonctionnement de l'application. Ainsi, le fournisseur du magasin d'applications peut demander la transmission de la documentation préexistante constituée par l'éditeur afin d'encourager les bonnes pratiques en termes de protection des données personnelles et renforcer la transparence pour les utilisateurs.

- **Quelles informations obtenir de la part de chaque éditeur d'application ?**
  - Il est recommandé au fournisseur du magasin d'applications de solliciter *a minima* les informations suivantes :
    - 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 pays dans lequel les données seront stockées et traitées,
    - un historique des mises à jour, incluant les notes de mises à jour.
  - Il lui est recommandé 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 recommandé de permettre aux applications d'indiquer si elles visent uniquement, majoritairement ou potentiellement un public mineur.

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

Du fait de leur expertise, et souvent de leur grande connaissance des systèmes d'exploitation, les fournisseurs de magasin d'applications mobiles apparaissent comme des acteurs privilégiés pour encourager la mise en œuvre de bonnes pratiques lors 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, il est recommandé d'encourager les éditeurs d'applications 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.
  - De même, il est recommandé d'inviter 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 éditeurs devraient être invités 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.
- Cette information est d'autant plus importante que le système d'exploitation met en œuvre des restrictions logicielles empêchant un rétrogradage de version d'une application. L'utilisateur devrait ainsi avoir le choix, en toute connaissance de cause, de mettre à jour ou non son application, en particulier si celle-ci est fonctionnelle, ne bénéficierait d'aucun correctif de sécurité particulier ou se verrait ajouter des traitements de données personnelles supplémentaires.

3. Analyser les applicatifs pour détecter des failles de sécurité

De même, 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 ?**
  - Des analyses statiques devraient être mises en œuvre avant chaque publication d'une application, que cette publication corresponde à une publication initiale ou à une mise à jour. Ces analyses devraient aussi bien être automatiques que manuelles et spécifiques, notamment pour les applications dépassant un certain nombre de téléchargements ou ayant des caractéristiques justifiant de mener des analyses de sécurité et de confidentialité plus poussées.
- **Comment mettre en œuvre des analyses plus poussées ?**
  - Pour les applications les plus sensibles, des analyses dynamiques des applications devraient être mises en œuvre, 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

Il est important, tout au long de la démarche de publication des applications, que les fournisseurs de magasin d'applications agissent avec la plus grande transparence et facilitent les démarches des éditeurs.

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 serait utile que les processus de revue des applications intègrent certaines vérifications pouvant être réalisées par le magasin d'applications.

- **Quels critères de protection des données intégrer dans le processus de revue des applications ?**
  - Il pourrait être demandé à l'éditeur si les applications visent le marché européen et vérifier qui est informé des règles de protection des données applicables. En cas de réponse négative, l'application devrait être interdite sur les versions du magasin localisées au sein de l'Union européenne.
  - Pour les applications d'éditeurs installés hors de l'Union européenne mais visant le marché européen, il devrait être demandé à l'éditeur si l'application traite des données personnelles. Dans ce cas :
    - la fourniture d'un point de contact pour les utilisateurs de l'Union européenne souhaitant exercer leurs droits devrait être exigée,

        - il devrait être demandé à l'éditeur de soumettre dans le processus de revue les informations clés de protection des données : finalités poursuivies, données traitées, modalités d'exercice des droits, durées de conservation,
        - des conseils sur la mise en conformité avec les règles européennes de protection des données devraient être délivrés à l'éditeur.
    - Il serait utile que les magasins d'applications refusent les applications qui ne sont pas en mesure de fournir les éléments ci-dessus.
    - Par ailleurs, le fournisseur de magasin d'applications pourrait utilement proposer aux utilisateurs un mécanisme de signalement des applications ne respectant pas les règles ci-dessus, pouvant conduire à une exclusion de l'application du magasin.

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

Dans la mesure du possible, il serait utile pour l'ensemble des acteurs que les fournisseurs de magasin d'applications s'assurent de la clarté des exigences imposées aux applications candidates en termes de sécurité et de vie privée.

- **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.

3. Faciliter l'utilisation des outils mis à disposition

Les fournisseurs de magasin d'applications devraient également s'assurer qu'ils mettent à disposition des outils adéquats pour la gestion du processus de publication et de résolution de 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, une gestion fine des accès aux comptes éditeurs du magasin d'applications devrait être permise. Ainsi, lorsque plusieurs utilisateurs 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 ?**
    - Un canal clair de communication entre les entités publiant des applications mobiles sur le magasin d'applications et le fournisseur de magasin d'applications devrait 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 devrait être privilégiée.

4. Être transparent sur les causes de rejet et les voies de recours

Le besoin de transparence s'exprime tout particulièrement en cas de refus de procéder à la publication. À titre de bonne pratique, il est donc important de mettre en œuvre des dispositifs assurant la bonne compréhension des décisions prises dans ce contexte.

- **Les raisons de refus et suspensions sont-ils suffisamment compréhensibles ?**
    - Une communication transparente avec les éditeurs d'applications mobiles lors de l'application des critères de validité de publication devrait être assurée. Les causes du rejet et le processus de recours mobilisable par l'éditeur devraient être indiqués de manière claire et précise.

- En particulier, les raisons du refus et les méthodes de remédiation proposées devraient être spécifiées dans la documentation.
- Si 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, l'éditeur devrait en être informé de manière renforcée.
- Une communication avec les éditeurs d'applications dans leur langue est souhaitable.

9.3. Informer les utilisateurs et leur fournir des outils de signalement et d'exercice des droits

Pour la plupart des utilisateurs de terminaux mobiles, les magasins d'applications sont le point d'entrée de leurs usages de ceux-ci. Il est donc souhaitable que l'accès à ces applications leur offre un niveau suffisant d'information, leur permettant 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, donnant une description sommaire de chaque application. Chaque application dispose elle-même ensuite de sa propre page, au sein de laquelle un niveau de détail important peut être présenté, pour permettre d'éclairer le choix des utilisateurs potentiels de télécharger, ou non, une application.

- **À titre de bonnes pratiques, quelles informations afficher dans les pages de chaque application ?**
  - L'ensemble des informations citées dans la partie 9.1 (« *Quelles informations obtenir de la part de chaque éditeur d'application ?* ») devraient être mises à disposition de l'utilisateur.
  - Ces informations devraient 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, devrait être privilégiée. L'information mise à disposition pourrait notamment comprendre des informations relatives aux modalités de financement de l'application, notamment lorsque celui-ci repose directement sur une réutilisation des données personnelles de l'utilisateur pour d'autres finalités. Le cas échéant, l'information devrait être présentée de manière neutre et contextualisée.
- **Quelles informations afficher dans l'interface de recherche ?**
  - Des filtres contenant des critères relatifs à la vie privée pourraient être directement 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.
  - Si la création d'un tel score est envisagée, celui-ci devrait reposer sur une méthodologie préalablement définie et de manière transparente, de préférence 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 est susceptible d'être l'objet d'une certification, notamment pour assurer qu'il remplit ses objectifs en termes de transparence. Devraient également être mises 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.
  - Parmi les paramètres qui peuvent être pris en compte dans l'établissement de ce score peuvent figurer :
    - les types de données collectées (en fonction de leur sensibilité), leur volume et les finalités poursuivies,
    - le nombre et le type de permissions demandées par l'application dès l'installation, ainsi que celles susceptibles de l'être au court de l'utilisation de l'application,
    - le nombre et le type de SDK inclus dans l'application et les données qu'ils collectent en fonction des finalités,
    - les mesures de sécurité mises en œuvre,
    - la possibilité d'avoir accès au code source de l'application.

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 ?**
  - Il devrait être permis aux utilisateurs de signaler les applications qui ne remplissent pas leurs obligations directement depuis le magasin d'applications, notamment en termes d'exercice des droits, de design trompeurs (« *dark patterns* ») de manquements aux consentements, d'exécution de fonctionnalités SDK sans consentement préalable, de présence de transferts non encadrés, etc.
  - Ces remontées pourraient être utilisées pour orienter les contrôles sur les applications publiées et également impacter le score relatif aux critères de vie privées.

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 ?**
  - Le fournisseur du magasin d'applications devrait établir un protocole à adopter en cas de révélations de vulnérabilités dans une application pouvant affecter une partie importante des utilisateurs du magasin, en particulier lorsque la détection de la présence de cette vulnérabilité peut être analysée (notamment statiquement) à grande échelle en termes de nombre d'application concernées.
  - Une fois les applications vulnérables détectées, plusieurs mesures peuvent être appliquées, parfois simultanément. Il peut par exemple être envisagé :
    - de suspendre les mises à jour automatiques de tout ou partie du parc applicatif des utilisateurs ;
    - de 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 devrait 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

Catégorie	Sous-Catégorie	Identifiant	Description
Analyser les applications soumises par les éditeurs	Centraliser et analyser les données relatives à la conformité	1.1.1	Pour chaque soumission de publication (nouvelle application ou nouvelle version), les informations obligatoirement fournies par l'éditeur comportent *a minima* : • les 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 une liste des SDKs 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 pays dans lequel les données sont stockées et traitées ; • un historique des mises à jour, incluant les notes de mises à jour.

		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 les pratiques mieux-disantes lors de la publication et la mise à jour des applications	1.2.1	Avant de soumettre une application de version d'application pour validation, 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, en n'activant que celles qui seront nécessaires selon les fonctionnalités utilisées par les utilisateurs finaux.
		1.2.2	Les éditeurs sont invités à ne pas utiliser d'API de l'OS qui accorderaient des permissions trop larges ou seraient obsolètes, en particulier quand la version de l'OS détectée par le magasin permet de mieux respecter les principes de protection des données dès la conception et par défaut.
		1.2.3	Les éditeurs sont invités à publier des notes de mises à jour informatives pour les utilisateurs, afin de permettre aux utilisateurs finaux de définir eux-mêmes s'ils souhaitent installer ou non une nouvelle version de l'application, en particulier dans le cas où la mise à jour ne serait que fonctionnelle, sans apporter de correctifs de sécurité.
	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 nouvelles versions des applications dépassant un certain nombre de téléchargements, avant toute publication dans le magasin, afin de détecter des points de non-conformité qui résulterait de leur comportement dans le temps et à l'usage.
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	Une documentation à jour et exhaustive des exigences de prépublication est mise à disposition des éditeurs, à laquelle sont rattachés des exemples concrets d'éléments et de comportements bloquants ou problématiques à la publication dans le magasin.
		2.1.2	La question est posée aux éditeurs si leur application vise le marché européen. Si tel n'est pas le cas, l'application n'est pas disponible sur les magasins localisés au sein de l'union européenne.

		2.1.3	Si l'application, à l'inverse, cible le marché européen, plusieurs éléments devraient être demandés à son éditeur, notamment la fourniture d'un point de contact pour l'exercice des droits des personnes ainsi que la mise en œuvre des principes du RGPD, tels que les finalités poursuivies, les données traitées, les durées de conservation, etc. Si l'application vise le marché européen mais n'est pas en mesure de fournir ces éléments, elle n'est pas publiée sur le magasin.
	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.
	Être transparent sur les causes de rejet et les voies de recours	2.4.1	Les refus de publication et les correctifs à appliquer pour pallier ce refus sont indiqués clairement aux éditeurs et s'appuient sur les éléments de documentation dédiés.
		2.4.2	Un soin spécifique est apporté à l'exhaustivité et la clarté des explications fournies à l'éditeur dont la version de l'application est refusée lorsque ce refus est, en tout ou partie, dû à une problématique de sécurité impliquant un risque pour les données des personnes concernées.
		2.4.3	Les échanges et explications apportées aux éditeurs dans le processus de validation ont lieu dans la langue déclarée ou souhaitée au sein de leur profil
Informer les utilisateurs et leur fournir des outils de signalement et d'exercice des droits	Normaliser et mettre à disposition les données relatives à la conformité	3.1.1	L'ensemble des informations relatives à la vie privée, transmises par les éditeurs ou connue du 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.

		3.1.4	Les informations relatives à la vie privée doivent être publiées de manière exhaustive et synthétique. Pour ce faire, ces informations sont dispensées en premier lieu dans un format synthétique, permettant par exemple l'affichage d'un score de respect de la vie privée, ainsi qu'en second lieu de manière exhaustive, par exemple suite au clic sur un lien « En savoir plus ».
		3.1.5	L'affichage d'un score relatif aux paramètres de vie privée est apposé sur les applications disponibles au sein du magasin. De préférence, ce score repose sur une méthodologie définie préalablement, de manière transparente de sorte qu'il puisse être certifiable et défini par un ou plusieurs acteurs extérieurs au magasin d'application lui-même.
	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. Par exemple, il peut s'agir de la détection d'une bibliothèque logicielle considérée comme vulnérable mais qui ne présenterait un risque que dans le contexte de certaines applications, sans qu'il soit possible de le définir *a priori*.

10. Glossaire

Kit de développement logiciel ou SDK (« *software development kit* ») :

Le kit de développement logiciel 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.

Application mobile :

La notion d'application mobile désigne les logiciels applicatifs distribués dans l'environnement des 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. 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.

Exécution « en bac à sable » ou « *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. 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 l'OS, sous réserve de l'obtention d'une 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 expose toute un ensemble de fonctionnalités aux applications.

Système d'exploitation (ou « *operating system* », OS)

Le système d'exploitation 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, l'OS 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 (soit celles ajoutées a posteriori) 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 OS des terminaux mobiles pour permettre aux utilisateurs de choisir quelles fonctionnalités sont accessibles aux applications mobiles. Ces applications mobiles n'ont en effet par défaut qu'un accès limité à ces fonctionnalités, pour des raisons de sécurité et de protection de la vie privée. L'OS met dès lors à leur disposition des API leur permettant d'effectuer des requêtes afin de se voir autoriser des fonctionnalités additionnelles, sous réserve que l'utilisateur, via une interface fournie par l'OS, l'accepte.

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 l'OS, et qui peuvent, sous certaines conditions dépendantes de l'OS 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.