



RGPD & App mobiles

Recommandations et bonnes pratiques pour mettre en conformité une application mobile avec le RGPD

VERSION DU 23 AVRIL 2018

Préam- bule

Ce document n'a pas valeur juridique. Il s'appuie sur l'analyse métier de USERADGENTS, la lecture des documents & recommandations de la commission européenne*.

Il appartient à chaque entreprise & notamment au responsable du traitement des données, de s'assurer, avec l'appui d'experts juridiques, que ses applications mobiles soient conformes à la réglementation en vigueur.

Le règlement général sur la protection des données (RGPD) entrera en vigueur le 25 mai 2018.

** Cette présentation s'appuie notamment sur les documents suivants :*

« Avis 02/2013 sur les applications destinées aux dispositifs intelligents » du 27 Février 2013

« Smartphone Secure Development Guidelines for App Developers » ENISA 25 Novembre 2011

01 Les données



Objectif & périmètre du document

L'avis du groupe de travail vise à clarifier le cadre juridique régissant le traitement des données à caractère personnel dans le développement, la distribution et l'utilisation d'applications destinées aux dispositifs intelligents (ex : Smartphones, tablettes)



+ Le consentement

Accord préalable à la collecte, libre et informé de l'utilisateur.



+ Le traitement

Limitation de la finalité et minimisation des données. Facilitation de l'accès et limitation de la conservation.



+ La sécurité

Protection de l'accès et de l'intégrité des données de l'utilisateur.

Les principaux risques

Les applications mobiles, en interagissant avec l'OS notamment, sont susceptibles de collecter et de partager en temps réel, avec un écosystème fragmenté, des données à caractère personnel



+ Absence de transparence

Près de 40% des applications n'ont pas de politique de protection de la vie privée.



+ Absence de consentement

Le consentement libre et informé ne peut se résumer à une case à cocher d'acceptation des CGV de l'application.



+ Outrepassement de la finalité

La collecte de données décorrélée de l'usage de l'application et le partage incontrôlé de celles-ci à des tiers.



+ Insuffisance des mesures de sécurité

Le risque de violation des données chez l'éditeur ou dans l'application elle-même.

Les données collectées

Les applications mobiles accèdent à un certain nombre de données personnelles que l'on peut regrouper en différentes catégories



+ Identification

- Identifiants « techniques » (UDID, IMEI, IMSI, N° téléphone)
- Identité personne, téléphone
- Données d'authentification (login, mot de passe)
- Données biométriques.



+ Contenus

- Contacts
- Photos, Vidéos
- Journaux d'appels, SMS
- Emails.



+ Usages

- Géolocalisation
- Historique de navigation
- Carte de crédit & de paiement
- Capteurs (accéléromètre, camera, micro,...).

02 Les acteurs



Définir les rôles & les responsabilités des acteurs



La conception et la maintenance d'une application font appel à un écosystème complexe d'acteurs qui sont associés dans le traitement et la protection des données personnelles des utilisateurs.



+ Les développeurs

L'éditeur de l'application ou l'entreprise impliquée dans la conception, le développement ou la maintenance.



+ Les fabricants

Le fabricant du système d'exploitation (logiciel) et/ou du dispositif (matériel).



+ Les magasins

Le propriétaire du magasin d'application où sont téléchargées les applications des développeurs.



+ Les tiers

Les SDK (publicité, analytics, techniques) intégrées aux applications.

Définir le rôles & les responsabilités des acteurs



Les développeurs



+ Qui?

- **L'annonceur**, qui commande l'application, bien souvent à une société tierce.
- **L'agence / l'ESN** en charge de la conception, du développement & de la maintenance, dans le cadre d'un contrat de prestation de services avec l'annonceur.

+ Rôle

Dans la mesure où l'annonceur fixe les finalités et les moyens du traitement des données à caractère personnel dans les dispositifs intelligents, il devient le responsable du traitement.

Définir le rôles & les responsabilités des acteurs



+ Rôle (suite)

Les développeurs



- L'annonceur qui externalise une partie ou la totalité du traitement effectif des données à un tiers (ex : agence / ESN / hébergeur) et que ce tiers assume le rôle de sous-traitant, l'annonceur est tenu de respecter l'ensemble des obligations découlant du recours à un sous-traitant.
- L'annonceur qui autorise des tiers (ex : SDK) à accéder à des données personnelles, doit s'assurer de la conformité (consentement, co-responsabilité si usage par le tiers pour ses propres besoins, limitation de la finalité), au cas par cas selon le type d'accord avec le tiers.

Définir le rôles & les responsabilités des acteurs



Les fabricants



+ Qui?

- **Le propriétaire du système d'exploitation** du dispositif.
Généralement Apple (pour iOS), Google (pour Android) ou Microsoft (pour Windows).
- **Le fabricant du dispositif** : Apple, Samsung, HTC,...
- A noter que certains fabricants de dispositifs personnalisent l'OS du dispositif (notamment sous Android) et pourrait avoir une responsabilité sur l'OS également.

+ Rôle

- Ils devraient également être considérés comme responsables du traitement (et, le cas échéant, comme co-responsables du traitement) pour toutes les données à caractère personnel traitées pour leurs propres besoins (bon fonctionnement du dispositif, sécurité, etc.) ou les services qu'ils proposent eux-mêmes à l'utilisateur.

Définir le rôles & les responsabilités des acteurs



Les fabricants



+ Rôle

- Les propriétaires d'OS sont également responsables de l'accès qu'ils offrent aux développeurs via les APIs.
- Il doivent donc veiller à contrôler l'accès fourni aux développeurs & s'assurer d'un accès simple à la révocation de cet accès.
- Cela comprend l'information et la formation de l'utilisateur final sur les données auxquelles les applications peuvent accéder, et la mise à disposition des réglages appropriés permettant à l'utilisateur de modifier les paramètres du traitement.

Les magasins d'applications



+ Qui?

- Le propriétaire du magasin de téléchargement de l'application (« Applications Store »).
- Généralement lié au système d'exploitation ou au fabricant du dispositif. Ex Apple (pour App Store), Google (pour Google Play) ou Amazon (pour Alexa skills store).

+ Rôle

- Les magasins d'applications sont également considérés comme responsables du traitement pour toutes les données à caractère personnel traitées pour les besoins de la gestion des applications des développeurs (identifiants store, données de paiement, sécurité, restauration & mise à jour...).
- Ils ont également un rôle dans l'information aux utilisateurs des données accessibles par les applications des développeurs.

Définir le rôles & les responsabilités des acteurs



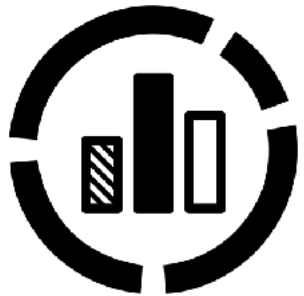
+ Qui?

- Bien souvent **les propriétaires des SDK tiers** intégrés dans les applications des développeurs : solutions d'analytics, de ciblage et d'affichage publicitaire, de notification, de messagerie, d'A/B testing, de monitoring technique,...
- Ces SDK, selon la finalité, sont intégrés à la demande de l'annonceur ou pour les besoins de l'agence/l'ESN (notamment sur le monitoring technique de l'application).

+ Rôle

- Si l'entreprise ne traite pas les données personnelles pour ses propres besoins, mais uniquement pour l'annonceur, elle sera un sous-traitant de l'annonceur.
- Si l'entreprise utilise les données personnelles pour ses propres besoins alors le tiers devient responsable du traitement et doit notamment s'assurer du consentement préalable et de la limitation de la finalité.

Les
tiers



03

Les bonnes pratiques



“

Proposer un consentement libre & informé

La gestion du consentement



**Libre,
informé &
spécifique**



+ Qui et quand ?

- La gestion du consentement utilisateur doit être intégrée aux phases de conception du service **entre l'annonceur et l'agence/ESN** (« **privacy by design** »).
- Le consentement doit avoir lieu **avant la collecte effective** de la donnée (notamment pour les données personnelles ne passant pas par un pop-up d'opt-in, ex : IMEI).
- Le consentement doit faire l'objet d'**une information claire & complète**.
- Certains magasins d'applications permettent aux utilisateurs de donner leur **consentement avant le téléchargement** de l'application (ex : Google Play), mais selon l'usage ce consentement ne pourra suffire pour le traitement de la donnée collectée.

La gestion du consentement



**Libre,
informé &
spécifique**



+ Quoi ?

- Le consentement doit être **libre** : l'utilisateur à la possibilité d'annuler / de refuser la collecte & le traitement de la donnée personnelle.
- Le consentement doit être **informé** : l'utilisateur doit disposer des informations nécessaires pour se forger une opinion exacte.
- Le consentement doit être **spécifique** : l'utilisateur doit être en mesure de donner un consentement détaillé, pour chaque type / catégorie de données auquel l'application est sur le point d'accéder. Un bouton « Installer » ou une case à cocher de CGV ne suffit pas. Exemples :
 - le consentement à la géolocalisation continue doit être spécifique
 - le consentement à l'accès aux contacts doit permettre une sélection individuelle des contacts.
- Le traitement de la donnée **ne doit pas être excessif et/ou disproportionné** vs le bénéfice présenté à l'utilisateur.

**Libre,
informé &
spécifique**



+ Bonnes pratiques

- Mettre un lien spécifique sur la gestion de la vie privée et des données personnelles dans la fiche de l'application sur le magasin (obligatoire sur iOS).
- Proposer lors du premier téléchargement (ou des mises à jour) des écrans d'informations clairs & didacticiels pour présenter les infos collectées, l'usage et le droit d'accès, avec les pop-up de consentement individuels associés si nécessaire, avec la possibilité de refuser.
- S'assurer que le développeur (ou les tiers, i.e SDK) ne collecte techniquement pas certaines données personnelles avant le consentement, notamment durant l'installation / le démarrage de l'application (ex : IMEI).
- Mettre un lien spécifique sur la gestion de la vie privée et des données personnelles au sein de l'application (rubrique infos, paramètres, compte, à propos par exemple), permettant également le droit d'accès et de modification / suppression / transfert (voir plus loin).

La limitation & minimisation



+ Qui & Quand ?

- La limitation de la finalité du traitement est définie par **l'annonceur** durant la conception.
- L'**agence/l'ESN** doit également s'assurer d'une approche de minimisation dans sa conception technique.

+ Quoi ?

- Principes fondamentaux qui sous-tendent la directive sur la protection des données.
- La **limitation de la finalité** permet à l'utilisateur de savoir précisément de quelle manière ses données sont utilisées et de pouvoir se fier à la description de la finalité restreinte pour comprendre à quelles fins ses données seront utilisées.
- Les finalités du traitement doivent dès lors être **bien définies et compréhensibles** pour un utilisateur moyen ne disposant pas de connaissances juridiques ou techniques approfondies.

La limitation & minimisation



+ Quoi ?

- La **minimisation des données** vise à prévenir la collecte et le traitement de données superflues à la finalité.
- Les développeurs d'applications doivent définir scrupuleusement les données qui seront **strictement nécessaires** à la réalisation de la fonctionnalité souhaitée.
- Au cours du projet il est important de **ne pas modifier le traitement** des données et sa finalité (attention aux mises à jour des apps).
- Les **tiers** accédant aux données doivent également respecter les principes de limitation & de minimisation.
- Les **propriétaires de systèmes d'exploitation** qui contrôlent les accès à certaines données doivent s'assurer de limiter l'accès exclusivement aux données strictement nécessaires à la fonctionnalité (licite) de l'application.

“

Assurer la sécurité des données utilisateurs

Protéger les données



+ Qui ?

- L'ensemble des acteurs portent une part de responsabilité dans la sécurisation des données
 - L'**annonceur** et son **agence** / **ESN** (focus de ce chapitre)
 - Le **fabricant du système d'exploitation** ou du **dispositif**
 - Le propriétaire du **magasin d'applications**
 - Les **tiers**.

+ Quoi ?

- Compte-tenu de la fragmentation des acteurs impliqués, les principes de protection de la vie privée doivent être intégrés par défaut par l'ensemble des acteurs dès la conception (« **privacy by design** »).
- La mise en place d'un «**plan de sécurité**» détaillé couvrant la collecte, le stockage et le traitement de toutes les données à caractère personnel, afin de prévenir la violation de ces dernières est à envisager.

+ Bonnes pratiques

- Exécuter les applications dans des «sandbox », afin de limiter les conséquences des applications ou des logiciels malveillants.
- S'assurer que les utilisateurs aient la dernière version de l'application & informer les utilisateurs, dans les meilleurs délais, lorsque la correction d'un problème de sécurité exige l'installation d'une mise à jour.
- Ne pas autoriser les mises à jour automatiques des SDK tiers dans l'application (utiliser un outil comme SafeDK pour monitorer et contrôler les SDK).
- Assurer des audits réguliers.

Le code



+ Bonnes pratiques

- Mettre en place des contrôles permettant d'éviter que des données ne soient accidentellement transférées ou compromises.
- Appliquer le principe du « moindre privilège par défaut », en vertu duquel les applications ne peuvent accéder qu'aux données dont elles ont réellement besoin pour garantir à l'utilisateur l'accessibilité d'une fonctionnalité.

Le code



Les identifiants & mots de passe



+ Bonnes pratiques

- Ne pas utiliser les identifiants permanents (spécifiques au dispositif) mais recourir au contraire à des identifiants spécifiques à l'application et à faible valeur entropique, ou à des identifiants de dispositif qui soient temporaires.
- Stocker les identifiants & mots de passe de manière encryptée et sûre, en tant que valeurs de hachage cryptographique avec chiffrement par clé.
- Proposer à l'utilisateur de vérifier la robustesse des mots de passe choisis est également une technique utile pour encourager l'utilisation de mots de passe plus adaptés (vérification de l'entropie).
- Si nécessaire (données sensibles), une authentification « forte » pourra être envisagée, à l'aide de facteurs multiples et de canaux différents (par exemple, un code d'accès envoyé par SMS) et/ou de données d'authentification liées à l'utilisateur final (plutôt qu'au dispositif).

Les identifiants & mot de passe



+ Bonnes pratiques

- Au lieu de mots de passe, utiliser des jetons d'autorisation pouvant être stockés en toute sécurité sur l'appareil.
- Utiliser des jetons limités dans le temps, spécifiques au service et révocables (si possible côté serveur).
- Utiliser les dernières versions des normes d'autorisation (ex: OAuth 2.0).
- Dans le cas où les mots de passe doivent être stockés sur l'appareil, utiliser les mécanismes de cryptage et de stockage de clés fournis par le système d'exploitation mobile.
- Ne stocker aucun mot de passe ou secret dans le fichier binaire de l'application.

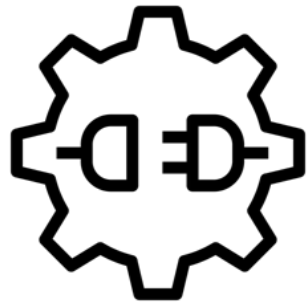
+ Bonnes pratiques

- S'appuyer sur des connexions HTTPS (SSL / TLS).
- Utiliser des certificats signés par des « trusted CA providers ».
- Utiliser des algorithmes de cryptage forts et reconnus (ex: AES).
- Établir les connexions sécurisées uniquement après vérification de l'identité du point d'extrémité distant (serveur).

Le réseau



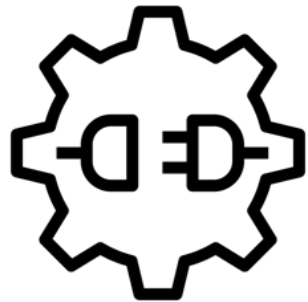
Les APIs & l'hébergement



+ Bonnes pratiques

- Contrôler spécifiquement les transferts involontaires de données sensibles au niveau du code de l'application (ex. l'emplacement ou d'autres informations incluses dans les métadonnées d'un fichier).
- Tester périodiquement la vulnérabilité des services back-end (Web Services / REST) en utilisant des outils d'analyseur de code statique et des outils de fuzzing pour tester et identifier les failles de sécurité.
- S'assurer que la plate-forme principale (serveur) fonctionne avec une configuration renforcée avec les derniers correctifs de sécurité appliqués au système d'exploitation, au serveur Web et aux autres composants de l'application.
- S'assurer que les logs adéquats sont conservés sur le back-end afin de détecter, répondre aux incidents et effectuer des investigations.

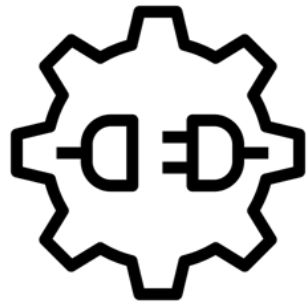
Les APIs & l'hébergement



+ Bonnes pratiques

- Utiliser la limitation et la limitation du débit par utilisateur / IP (si l'identification de l'utilisateur est disponible) pour réduire le risque d'attaque DDoS.
- Tester les vulnérabilités de DDoS où le serveur peut être engorgé par certains appels de l'application gourmands en ressources.
- Les services Web, REST et les APIs peuvent présenter des vulnérabilités similaires aux applications Web:
 - Effectuer des tests de cas d'abus, en plus des tests de cas d'utilisation.
 - Effectuer des tests du service Web, REST ou API back-end pour déterminer les vulnérabilités.

Les APIs & libs tiers



+ Bonnes pratiques

- Examiner la sécurité & l'authenticité de tout code / bibliothèque tiers utilisé dans votre application mobile (par exemple, s'assurer qu'ils proviennent d'une source fiable, avec une maintenance prise en charge, pas de chevaux de Troie back-end).
- Suivre tous les frameworks / API tiers utilisés dans l'application mobile pour les correctifs de sécurité. Une mise à jour de sécurité correspondante doit être effectuée pour les applications mobiles utilisant ces API / frameworks tiers.
- Porter une attention particulière à la validation de toutes les données reçues et envoyées à des applications tierces non approuvées avant le traitement dans l'application.
- Ne pas autoriser les mises à jour automatiques.

“
Faciliter l'information & le droit d'accès des utilisateurs

L'information

+ Qui ?

- Le responsable du traitement donc principalement l'**annonceur**, mais dans un certains cas les **tiers** si ces derniers exploitent les données personnelles pour leur propre besoin.

+ Quoi ?

- L'utilisateur a le droit de **connaître l'identité du responsable du traitement** des données à caractère personnel le concernant.
- L'utilisateur a le droit de **connaître la nature des données à caractère personnel**, l'objet du traitement, ainsi que **la finalité** escomptée de leur utilisation.
- La communication de ces informations **après le début du traitement** des données à caractère personnel (qui commence souvent pendant l'installation de l'application) n'est pas jugée suffisante et **est juridiquement sans valeur**.

+ Bonnes pratiques

L'infor- mation

- Le responsable du traitement concerné est tenu de fournir aux utilisateurs potentiels au moins les informations suivantes :
 - **l'identité** et les **coordonnées** du responsable du traitement;
 - les **catégories** précises des **données à caractère personnel** que le développeur d'applications entend collecter et traiter;
 - la **finalité** (les objectifs précis du traitement);
 - la confirmation d'une transmission éventuelle des données à des **tiers**;
 - la manière dont l'utilisateur peut **exercer ses droits** dans le cas d'un retrait de consentement ou de suppression de données.
- Le développeur d'applications devrait distinguer clairement les **informations obligatoires** de celles **facultatives**, et le système devrait permettre à l'utilisateur de refuser l'accès aux informations facultatives en sélectionnant des options par défaut privilégiant le respect de la vie privée.

+ Bonnes pratiques

L'infor- mation

- Il est également recommandé que le responsable du traitement fournisse à l'utilisateur des informations sur les points suivants :
 - le principe de **proportionnalité** applicable aux catégories de données collectées, ou auxquelles on a accédé, dans le dispositif;
 - les **durées de conservation** des données;
 - les **mesures de sécurité** mises en œuvre par le responsable du traitement.
- Enfin les développeurs d'applications incluent, dans leur politique de confidentialité, des informations destinées à l'utilisateur européen et précisent notamment dans quelle mesure l'application **respecte la législation européenne sur la protection des données.**

+ Bonnes pratiques

- La portée essentielle des informations relatives au traitement des données doit être disponible pour l'utilisateur préalablement à l'installation de l'application, par l'intermédiaire du **magasin d'applications** (ie : la fiche de l'app sur le magasin).
- Les informations pertinentes concernant le traitement des données doivent être également accessibles, après installation, **au sein même de l'application**.
- Afin de prendre en compte l'espace limité sur certains dispositifs, l'information via des **avis succincts** est considérée comme légalement acceptable si intégrée au sein d'une structure **multistrates** qui, dans sa totalité, assure la conformité.
- **Un lien spécifique** (vie privée / protection des données / politique de confidentialité) est recommandé pour faciliter l'identification par l'utilisateur (vs lien générique Infos éditeur / CGV,...).

La
forme

Le droit d'accès

+ Qui ?

- Le responsable du traitement donc principalement l'**annonceur**, mais dans un certains cas les **tiers** si ces derniers exploitent les données personnelles pour leur propre besoin.

+ Quoi ?

- Les droits d'**accès**, de **rectification**, d'**effacement** et d'**opposition** au traitement des données.
- Si un utilisateur exerce son droit d'accès, le responsable du traitement est tenu de fournir les informations relatives aux **données en cours de traitement** et aux **sources** de ces données.
- À la demande de l'utilisateur, le responsable du traitement doit également permettre la rectification, l'effacement ou le verrouillage de données à caractère personnel si celles-ci sont incomplètes, inexactes ou traitées de manière illicite, mais également la **portabilité** des données (sur des fichiers lisibles) .

+ Bonnes pratiques

- Mettre en oeuvre des **outils d'accès en ligne** simples mais sûrs au sein de l'application ou accessibles en suivant un lien vers une fonctionnalité en ligne.
- L'accès ne devrait être accordé que si **l'identité** de la personne concernée a été **établie**, afin d'éviter toute fuite de données vers des tiers.
- L'utilisateur doit y obtenir un accès immédiat à **l'ensemble des données en cours de traitement** et aux explications nécessaires correspondantes.
- L'utilisateur devrait toujours avoir la possibilité de **retirer son consentement** de manière **simple** et peu **fastidieuse**.

**Le droit
d'accès**

Le droit d'accès

+ Bonnes pratiques

- Il doit être possible de **désinstaller des applications** et, dès lors, de **retirer toutes les données** à caractère personnel, même sur les serveurs du/des responsable(s) du traitement.
- En principe, après la **désinstallation** de l'application par l'utilisateur, le développeur ne bénéficie **plus d'un fondement juridique** l'autorisant à poursuivre le traitement des données à caractère personnel relatives à cet utilisateur, et doit donc **supprimer toutes les données**.
- Un développeur d'applications souhaitant **conserver certaines données**, par exemple afin de **faciliter la réinstallation** de l'application, doit introduire une **requête de consentement séparée au cours du processus de désinstallation**, en demandant à l'utilisateur d'autoriser une durée de conservation supplémentaire bien définie.

+ Qui ?

- Le responsable du traitement donc principalement l'**annonceur**, mais dans un certains cas les **tiers** si ces derniers exploitent les données personnelles pour leur propre besoin.

+ Quoi ?

- Les **durées de conservation** spécifiques **dépendront de la finalité** de l'application et de l'importance des données pour l'utilisateur final.
- Il est rappelé que l'**obligation de conservation des données** imposée par l'Europe (directive 2006/24/CE) ne s'applique pas à l'ensemble des services de la société de l'information, parmi lesquels les applications, et qu'elle ne peut donc être invoquée comme fondement juridique pour poursuivre le traitement des données concernant l'utilisateur d'une application une fois que ce dernier a supprimé l'application.

La durée

+ Bonnes pratiques

- Les développeurs d'applications devraient prédéfinir **un délai d'inactivité** au terme duquel le compte serait considéré comme ayant expiré, et veiller à ce que l'utilisateur soit informé de ce délai.
- Au terme de ce délai, le responsable du traitement devrait avertir l'utilisateur et lui donner la **possibilité de récupérer les données** à caractère personnel.
- Si l'utilisateur ne réagit pas à cet avertissement, les données à caractère personnel concernant et relatives à l'utilisation de l'application devraient être **anonymisées de manière irréversible**, ou **supprimées**.

La durée

04

La check-list



+ Côté utilisateurs

1. Vérifier que la fiche sur le magasin d'applications dispose **d'un lien vers votre politique de données personnelles / confidentialité.**
2. Présenter à l'utilisateur les informations nécessaires (tutoriel, pop-up système) en vue d'obtenir un **consentement libre, informé et spécifique** sur chaque catégorie de données personnelles **avant** la collecte (par vous ou des tiers en faisant usage pour leurs propres besoins).
3. Intégrer une **rubrique spécifique**, facilement accessible sur votre politique de données personnelles dans l'app (ou un lien).
4. Proposer un **accès en ligne** permettant la visualisation des données personnelles en cours de traitement et leur modification / suppression/ transfert (portabilité) par l'utilisateur.
5. **Informé l'utilisateur en cas de fuite de données** en s'assurant de pouvoir diffuser les mises à jour correctives au plus vite.

**5#
points
clés**

+ En interne & avec vos partenaires

1. **Mettre à jour les contrats** sous-traitants pour intégrer les spécificités liées à RGPD.
2. **Mettre en place un PAQ / PAS** avec vos principaux fournisseurs (développement, maintenance & hébergement du service).
3. **Lister les informations personnelles collectées** par votre application & s'assurer de la conformité des consentements associés (préalable, libre, informé, spécifique).
4. **Lister les SDK** présents dans votre application & s'assurer notamment de leur rôle (sous-traitant vs responsable de traitement, en fonction de l'usage des données personnelles collectées), de la conformité de leur traitement vs RGPD et notamment du lieu de stockage des données collectées (Ex formulaire : <https://www.surveymonkey.com/r/safedk-gdpr-sdks>).
5. **Auditer régulièrement** votre infrastructure (interne et sous-traitants).

**5#
points
clés**

Document réalisé par :

Renaud Ménéral

Président @ USERADGENTS

r.menerat@useradgents.com



USERADGENTS

8 rue de la Rochefoucauld - 75009 Paris

01 77 75 65 90

www.useradgents.com