

Côté google :

Pour les données :

- Votre façon de gérer les données de l'utilisateur doit être transparente (p. ex., les renseignements recueillis d'un utilisateur ou le concernant, y compris les renseignements de l'appareil). Vous devez donc **divulguer l'accès aux données ainsi que la collecte, l'utilisation et la communication de celles-ci**. Vous devez en outre limiter l'utilisation des données aux fins précisées. Ces exigences de Google Play s'ajoutent aux exigences prescrites par les lois applicables de protection des données et de confidentialité.
- Limiter l'accès, la collecte, l'utilisation et la communication de données personnelles ou confidentielles collectées par l'application aux fins directement associées à l'offre et à l'amélioration des fonctionnalités de l'application (p. ex., fonction utilisateur anticipée, documentée et promue dans la description de l'application dans la boutique Play Store).
- Publier une politique de confidentialité à la fois dans le champ désigné de Play Console et dans l'application. **La politique de confidentialité doit, outre toutes divulgations intégrées à l'application, expliquer en détail la façon dont votre application accède, recueille, utilise et communique les données de l'utilisateur.** Votre politique de confidentialité doit stipuler **les types de données personnelles et confidentielles auxquelles votre application accède, qu'elle collecte, utilise et partage, et les types de tiers avec lesquels les données de l'utilisateur personnelles ou confidentielles sont partagées.**
- Gérer les **données de l'utilisateur personnelles ou confidentielles en toute sécurité**, y compris leur transmission à l'aide d'une cryptographie moderne (p. ex., sur HTTPS).
- Utiliser une **demande d'autorisations de temps d'exécution lorsqu'elle est disponible, avant d'accéder aux données gérées par les autorisations Android**.
- Ne pas vendre les données personnelles ou confidentielles de l'utilisateur.
- Obligation de divulgation et de consentement :
 - Dans les cas où les utilisateurs ne peuvent pas raisonnablement savoir que leurs données d'utilisateur personnelles ou confidentielles seront demandées pour offrir ou améliorer les caractéristiques ou les fonctionnalités conformes à la politique dans votre application (p. ex., la collecte de données a lieu en arrière-plan de votre application), vous devez répondre aux exigences suivantes :
 - Vous devez fournir une divulgation intégrée à l'application en ce qui concerne l'accès aux données ainsi que la collecte, l'utilisation et la communication de celles-ci. La divulgation intégrée à l'application :
 - doit être intégrée à l'application et non uniquement être publiée dans la description de l'application ou sur un site Web;
 - doit s'afficher dans le cadre de l'utilisation normale de l'application et ne pas nécessiter que l'utilisateur navigue dans un menu ni dans les paramètres;
 - doit décrire les données consultées ou collectées;

- doit expliquer la façon dont les données seront utilisées et partagées;
 - ne peut pas être uniquement incluse dans une politique de confidentialité ou dans des conditions d'utilisation; et
 - ne peut pas être incluse avec d'autres divulgations sans rapport à la collection de données confidentielles.
- La divulgation intégrée à votre application doit accompagner une demande de consentement de l'utilisateur et immédiatement la précéder. Elle doit en outre, dans la mesure du possible, comporter une autorisation du temps d'exécution associée. Vous ne pouvez pas accéder à des données personnelles ou confidentielles ni les collecter avant d'avoir reçu le consentement de l'utilisateur. La demande de l'application pour le consentement :
 - Doit présenter le dialogue de consentement clairement et sans ambiguïté;
 - Doit exiger une action affirmative de l'utilisateur (par exemple : toucher pour accepter, cocher une case);
 - ne doit pas interpréter comme un consentement le fait de quitter l'écran relatif à la divulgation (y compris le fait de toucher un autre endroit ou de cliquer sur le bouton de retour à la page d'accueil); et
 - ne doit pas utiliser des messages qui se ferment d'eux-mêmes ou qui expirent pour obtenir le consentement de l'utilisateur.

(<https://support.google.com/googleplay/android-developer/answer/9888076#1&2&3&4&5&6&7&87&9>)

Préparer votre application pour examen :

La page Contenu de l'application est l'endroit où vous fournissez et gérez les renseignements dont nous avons besoin pour assurer que votre application est sécuritaire pour les utilisateurs auxquels elle est destinée, qu'elle est conforme aux [politiques de Google Play](#) et qu'elle respecte les obligations juridiques.

Vous pouvez utiliser la page Contenu de l'application aux fins suivantes :

- Ajouter votre politique de confidentialité pour indiquer les façons dont vous traitez les données confidentielles de l'utilisateur et des appareils.
- Indiquer si votre application contient des annonces.
- Fournissez des instructions sur les façons d'accéder aux sections limitées de votre application et gérez-les.
- Fournir des détails sur le public cible et le contenu de votre application.
- Décrire la manière dont vous comptez utiliser les [autorisations à haut risque ou confidentielles](#), comme les [autorisations relatives aux messages texte et aux journaux d'appels](#).

Fournir les renseignements de l'application

Politique de confidentialité

L'ajout d'une politique de confidentialité à la fiche Google Play Store de votre application assure une transparence sur votre manière de traiter les données confidentielles de l'utilisateur et des appareils.

La politique de confidentialité doit, outre toutes divulgations intégrées à l'application, expliquer en détail les façons dont votre application collecte, utilise et communique les données de l'utilisateur, y compris les types de parties avec lesquelles elles sont partagées. Afin de vous renseigner sur les exigences, vous devriez consulter votre propre représentant légal.

- Pour les applications qui demandent un accès à des autorisations ou à des données confidentielles (comme définies dans les [politiques relatives aux données de l'utilisateur](#)) : vous devez fournir un lien vers une politique de confidentialité non seulement sur la fiche Google Play Store de votre application, mais aussi dans votre application. Assurez-vous que votre politique de confidentialité est accessible à l'aide d'une URL active, qu'elle s'applique à votre application et qu'elle couvre les règles de confidentialité.
- Pour les applications du programme [Conçu pour les familles](#) : vous devez fournir un lien vers une politique de confidentialité non seulement sur la fiche Google Play Store de votre application, mais aussi dans votre application, indépendamment de l'accès par votre application à des autorisations ou à des données confidentielles. Assurez-vous que votre politique de confidentialité est accessible à l'aide d'une URL active, qu'elle s'applique à votre application et qu'elle couvre les règles de confidentialité.

Ajouter une politique de confidentialité

1. Connectez-vous à [Play Console](#).
2. Sélectionnez une application.
3. Sélectionnez Présence dans la boutique > Contenu de l'application.
4. Sous la section « Politique de confidentialité », cliquez sur Démarrer.
 - Remarque : Si vous avez déjà ajouté une politique de confidentialité et si vous souhaitez apporter des modifications, cliquez sur Gérer.
5. Entrez l'URL hébergeant la politique de confidentialité en ligne.
6. Enregistrez vos modifications.

Accès des applications

Si l'accès à certains éléments ou à l'ensemble de votre application est limité en raison d'authentifiants de connexion, d'abonnements, de données de localisation ou de toute autre forme d'authentification, vous devez fournir des renseignements d'accès.

Ajouter des instructions concernant l'accès des applications

1. Connectez-vous à [Play Console](#).
2. Sélectionnez une application.
3. Sélectionnez Présence dans la boutique > Contenu de l'application.
4. Sous « Accès des applications », cliquez sur Démarrer.

- Remarque : Si vous avez déjà ajouté des instructions concernant l'accès des applications et si vous souhaitez apporter des modifications, cliquez sur Gérer.
5. Cliquez sur Ajouter de nouvelles instructions et fournissez vos renseignements d'accès.
- Remarque : Utilisez le champ « Toute autre instruction » pour nous faire savoir si votre mécanisme de connexion présente des particularités, comme l'utilisation d'un mot de passe à usage unique, une authentification multifacteur ou des connexions avec plus de deux champs.
6. Enregistrez vos modifications.

Remarque : Vous pouvez ajouter jusqu'à cinq ensembles d'instructions.

Public cible et contenu

Vous devez indiquer le groupe d'âge cible de votre application. Toutes les applications dont le public cible comprend les enfants doivent se conformer aux [exigences de la politique pour les familles](#) de Google Play.

Il est important de fournir des renseignements précis sur votre application. Selon les sélections du public cible effectuées, votre application peut être soumise aux politiques supplémentaires de Google Play. Vous pouvez prendre connaissance de ces politiques et découvrir comment [remplir la section « Public cible et contenu »](#) de la page Contenu de l'application.

Vous pouvez également en apprendre davantage sur le processus et consulter la liste de contrôle interactif sur le site de l'[Académie pour concepteurs d'applications](#).

Formulaire de déclaration des autorisations

Les demandes d'autorisation sont évaluées pendant le processus de publication après l'ajout de vos fichiers APK ou de vos collections d'applications. Si votre application demande d'utiliser des [autorisations à haut risque ou confidentielles](#) (p. ex., message texte ou journal des appels), vous devrez peut-être remplir le formulaire de déclaration des autorisations et recevoir l'approbation de Google Play.

Voici où vous pouvez en apprendre davantage sur le processus et comment [remplir le formulaire de déclaration des autorisations](#) sur la page Contenu de l'application.

La documentation Google étant trop longue (et donc moins lisible/compréhensible), je préfère fournir les liens des pages intéressantes :

https://support.google.com/googleplay/android-developer/answer/113469?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/9006925?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/7159011?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/7384423?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/9214102?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/9815348?hl=fr-CA&ref_topic=7072031

https://support.google.com/googleplay/android-developer/answer/6334282?hl=fr-CA&ref_topic=7072031

Généralement inutile du au mise à jour OTA, mais je précise au cas où :

https://support.google.com/googleplay/android-developer/answer/113476?hl=fr-CA&ref_topic=7072031

Pour la fiche google :

https://support.google.com/googleplay/android-developer/topic/3450987?hl=fr-CA&ref_topic=7072031

Info sur App Bundle :

<https://developer.android.com/guide/app-bundle>

Concernant les permissions (pour voir si une permission est considérée dangereuse, etc) :

https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions

Temps d'examen de l'application ou/et mise à jour :

<https://support.google.com/googleplay/android-developer/answer/6334282?hl=fr>

(« Dans le souci de mieux protéger les utilisateurs, nous pouvons soumettre les applications de certains comptes de développeur à un examen plus approfondi, ce qui peut étendre le délai à **sept jours (voire plus** dans certains cas exceptionnels). »)

Côté Apple :

Publish/upload sur app store

Publish permet de faire des modifs sur l'app en OTA, sans devoir regenerer une IPA et donc faire une maj de l'appli (et donc repasser par la review d'appStore) :

We can also improve this workflow by adding different channels! From now on, instead of publishing without specifying a channel, you can publish a production version of your app with the command.

expo publish --release-channel production.

This new build will subscribe to the production channel and listen for new updates. You just need to upload it to the Stores the first time.

Now, imagine you want to work on a new version of your app and show it to some test users without messing with the live production version. You simply need to create another channel, let's say

```
expo publish --release-channel staging
```

and build a new binary that will subscribe to this specific staging channel (*you can upload this build on Testflight for example and each time you will publish new changes on this channel, your Testflight users will be able to see the Work In Progress! For Android, you can upload this binary on a test release*).

Il est possible de voir l'historique des publications ainsi que les différents canaux utilisés, un peu comme les commits sur git :

In order to see everything that you've published, just do `expo publish:history`.

You will see something like this :

publishedTime	appVersion	sdkVersion	platform	channel	channelId	publicationId
2018-01-05T23:55:04.603Z	1.0.0	24.0.0	ios	staging	9133d577	d9bd6b80

If you want to promote your staging app to the production one, you just have to identify the publicationId you want to promote and do

```
expo publish:set --publish-id <publicationId> --release-channel production
```

That's it, your changes are now live in production! You can do `expo publish:history` again to see that the channel has changed!

What if you added a big regression to your users doing that?

No need to worry, just rollback the promotion channel doing `expo publish:rollback --channel-id <channelId>`

source: <https://hackernoon.com/how-to-publish-your-expo-application-to-the-app-stores-using-release-channels-un7a32ms>

Apple store review

5 points

Safety, Performance, Business, Design, and Legal

Make sure you :

- Test your app for crashes and bugs
- Ensure that all app information and metadata is complete and accurate
- Update your contact information in case App Review needs to reach you
- Provide an active demo account and login information, plus any other hardware or resources that might be needed to review your app (e.g. login credentials or a sample QR code)
- Enable backend services so that they're live and accessible during review
- Include detailed explanations of non-obvious features and in-app purchases in the App Review notes, including supporting documentation where appropriate.

Your apps should change and improve as well in order to stay on the App Store.

IOS data storage guidelines

Data that can be downloaded again or regenerated should be stored in the <Application_Home>/Library/Caches directory. Examples of files you should put in the Caches directory include database cache files and downloadable content, such as that used by magazine, newspaper, and map applications.

Realistic portrayals of people or animals being killed, maimed, tortured, or abused, or content that encourages violence. (pas d'images d'animaux trop 'choquantes').

Submissions to App Review, including apps you make available for pre-order, should be final versions with all necessary metadata and fully functional URLs included; placeholder text, empty websites, and other temporary content should be scrubbed before submission.

Data collection and storage

App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly [...]*.

*En anglais ?

Explicitly list all the permissions required by the application in the metadata (you can find them in info.plist).

Approval process

On average, 50% of apps are reviewed in 24 hours and over 90% are reviewed in 48 hours.

On average, over 40% of app rejections are for Guideline 2.1 – Performance: App Completeness.

En gros, inutile de se précipiter pour publish l'app si c'est pas 100% terminé, niveau fonctionnel/UI. Apple insiste bien sur le fait que l'app doit être finie et testée avant d'être publiée.

The current status of your app will be reflected in App Store Connect

If your app has been rejected and you have questions or would like to provide additional information, please use the Resolution Center to communicate directly with the App Review team.

All links in your app must be functional. A link to user support with up-to-date contact information and a link to your privacy policy is required for all apps.

Il faut aussi peaufiner la description de l'app pour l'app store, ainsi que fournir des screenshots montrant les fonctionnalités de l'appli.

TestFlight

A noter que le compte 'titulaire' de l'abonnement apple developer est le seul habilité à générer l'ipa, uploader sur apple store connect puis ajouter l'appli dans TestFlight.

Telecharger l'ipa : <https://docs.expo.io/distribution/building-standalone-apps/>

Voilà donc le lien pour le build généré le 27 août 2020 :

<https://expo.io/artifacts/70013202-da05-46bc-91ae-d335775ea0c2>

Uploader sur TestFlight : <https://www.raywenderlich.com/10868372-testflight-tutorial-ios-beta-testing>

Côté Expo :

Créer le fichier .apk ou .ipa selon le store : (<https://docs.expo.io/workflow/publishing/>)

Signature de l'application : <https://docs.expo.io/distribution/app-signing/>

Infos utiles sur le déploiement avec recommandations : <https://docs.expo.io/distribution/app-stores/>

Chaines, utile pour avoir 2 apk ou ipa (version prod et test) :

<https://docs.expo.io/distribution/release-channels/> et <https://docs.expo.io/distribution/advanced-release-channels/>

Etapes pour publier sur les 2 stores : <https://docs.expo.io/distribution/uploading-apps/>

Pour transférer le projet d'un compte à un autre (je ne recommande pas, mieux vaut essayer d'utiliser un même compte si possible) : <https://docs.expo.io/distribution/app-transfers/>

Optimisation : <https://docs.expo.io/distribution/optimizing-updates/> ,
<https://docs.expo.io/guides/preloading-and-caching-assets/>

Permissions : <https://docs.expo.io/versions/latest/sdk/permissions/>

Liste des propriétés app.json : <https://docs.expo.io/versions/latest/config/app/>

Coté loi en France :

<https://editioneo.com/blog/politique-confidentialite-apps-android/>