







Consignes pour la vérification des apps

Les apps changent le monde, à la fois en enrichissant nos vies et en permettant aux développeurs d'innover comme jamais auparavant. Par conséquent, l'App Store est devenu un écosystème fascinant et dynamique pour des millions de développeurs et plus d'un milliard d'utilisateurs. Que vous soyez novice en matière de développement ou une grande équipe de programmeurs expérimentés, nous sommes ravis que vous créiez des apps pour nos plateformes, et nous souhaitons vous aider à comprendre nos directives afin que votre app passe rapidement la procédure de vérification.

Avril 2024

Introduction	4
Avant de soumettre votre app	5
1. Sécurité	6
1.1 Contenu répréhensible	6
1.2 Contenu généré par l'utilisateur	7
1.2.1 Contenu des créateurs	8
1.3 Catégorie Enfants	8
1.4 Blessures physiques 	9
1.5 Informations sur le développeur 	9
1.6 Sécurité des données 	10
1.7 Signalement d'une activité criminelle	10
2. Performances	10
2.1 Exhaustivité de l'app	10
2.2 Bêta-tests	10
2.3 Exactitude des métadonnées 	11
2.4 Compatibilité matérielle	13
2.5 Configuration logicielle requise	14
3. Monétisation	17
3.1 Paiements	17
3.1.1 Achats intégrés	17
3.1.1(a) Lien vers d'autres méthodes d'achat	18
3.1.2 Abonnements	19
3.1.2(a) Utilisations autorisées	19
3.1.2(b) Mises à niveau vers une version ultérieure ou antérieure	20
3.1.2(c) Informations d'abonnement	21
3.1.3 Autres méthodes d'achat	21
3.1.3(a) Apps de lecture	21
3.1.3(b) Services multiplateformes	21
3.1.3(c) Services aux entreprises	21
3.1.3(d) Services de personne à personne	22
3.1.3(e) Biens et services en dehors de l'app	22
3.1.3(f) Apps autonomes gratuites	22
3.1.3(g) Apps de gestion des publicités	22
3.1.4 Contenu dépendant d'un matériel spécifique	22
3.1.5 Cryptomonnaies	23
3.2 Autres problèmes liés au modèle commercial	23
3.2.1 Utilisation acceptable	23
3.2.2 Utilisation inacceptable	24

4. Conception	25
4.1 Plagiat	25
4.2 Fonctionnalités minimales	26
4.2.7 Clients de bureau à distance	26
4.3 Spam	27
4.4 Extensions	27
4.5 Sites et services Apple	28
4.6 Icônes d'apps alternatives	29
4.7 Mini apps, mini jeux, jeux en streaming, chatbots, modules et émulateurs de jeux	29
4.8 Services de connexion	30
4.9 Apple Pay	31
4.10 Monétisation des fonctionnalités intégrées	31
5. Aspects juridiques	31
5.1 Confidentialité	32
5.1.1 Collecte et stockage des données	32
5.1.2 Utilisation et partage des données	34
5.1.3 Santé et recherche médicale	35
5.1.4 Enfants	35
5.1.5 Service de localisation	36
5.2 Propriété intellectuelle	36
5.3 Jeux, jeux d'argent et loteries	37
5.4 Apps VPN	38
5.5 Gestion des appareils mobiles	38
5.6 Code de conduite des développeurs	38
5.6.1 Avis dans l'App Store	39
5.6.2 Identité du développeur	39
5.6.3 Fraude liée aux fonctionnalités de découverte	39
5.6.4 Qualité des apps	39
Une fois votre app soumise	40

Introduction

Le principe directeur de l'App Store est simple : nous souhaitons permettre aux utilisateurs d'obtenir des apps en toute sécurité et donner l'opportunité à tous les développeurs de connaître le succès. Pour ce faire, nous mettons à disposition l'App Store, une plateforme où chaque app est sélectionnée avec soin et évaluée par des spécialistes. Une équipe éditoriale aide également l'ensemble des utilisateurs à y découvrir chaque jour de nouvelles apps. Nous analysons également chaque app à la recherche de logiciels malveillants et d'autres logiciels susceptibles d'avoir un impact sur la sécurité et la confidentialité des utilisateurs. Grâce à ces efforts, les plateformes Apple garantissent aux utilisateurs et utilisatrices la meilleure sécurité au monde.

Dans l'Union européenne, les développeurs et développeuses peuvent également distribuer des apps iOS notariées sur d'autres marchés d'apps. En savoir plus sur [les magasins d'apps alternatifs](#) et [la notarisation des apps iOS](#). Vous pouvez voir quelles consignes s'appliquent à la notarisation des apps iOS en cliquant sur « Afficher uniquement les consignes de révision de la notarisation » dans le menu à gauche.

Pour tout le reste, il y a toujours Internet. Si le modèle et les consignes de l'App Store ou d'autres plateformes d'apps et la notarisation pour les apps iOS ne sont pas adaptés à votre idée d'app ou d'entreprise, nous proposons également Safari pour une excellente expérience web.

Vous trouverez ci-après la dernière version de nos directives organisées en cinq sections distinctes : Sécurité, Performances, Monétisation, Conception et Aspects juridiques. L'App Store évolue et s'améliore constamment pour répondre aux besoins de notre clientèle et de nos produits. C'est pour cette raison que vous devez vous aussi modifier et améliorer vos apps afin qu'elles puissent rester sur l'App Store.

Voici quelques autres points à garder à l'esprit concernant la distribution de votre app sur nos plateformes :

- Les enfants téléchargent de nombreuses apps. Le contrôle parental permet de protéger les enfants, mais vous devez également prendre une part active dans leur protection. N'oubliez pas que nous attachons une importance particulière à la protection des enfants.
- L'App Store est un excellent moyen de toucher des centaines de millions de personnes dans le monde. Si vous concevez une app que vous souhaitez montrer uniquement à votre famille et à vos proches, l'App Store n'est pas la meilleure plateforme pour cela. Envisagez d'utiliser Xcode pour que votre app puisse être installée gratuitement sur un appareil, ou d'utiliser la distribution ad hoc, qui est disponible pour les membres de l'Apple Developer Program. Si vous n'en êtes qu'à vos premières démarches, pour en savoir plus, accédez à [l'Apple Developer Program](#).
- Nous tenons vivement à ce que tous les points de vue soient représentés sur l'App Store, tant que les apps respectent les utilisateurs ayant des opinions divergentes et offrent une expérience de grande qualité. Nous refuserons les apps dont le contenu ou le comportement semblent dépasser les limites. Quelles limites, nous direz-vous ? Nous avons la certitude que vous saurez les reconnaître lorsque nous vous ferons comprendre que vous les avez dépassées.

- Si vous tentez de contourner le système (par exemple, en essayant d'utiliser la procédure de vérification de manière abusive, de voler des données utilisateur, de plagier le travail d'un autre développeur ou de manipuler les notes de vos apps et leur découverte sur l'App Store), vos apps seront supprimées de l'App Store, et nous procéderons à votre exclusion de l'Apple Developer Program.
- Il vous incombe de vérifier que tous les éléments de votre app sont conformes aux présentes directives, y compris les réseaux publicitaires, les services d'analyse et les kits de développement logiciel (SDK) tiers. Veillez donc à les examiner et à les sélectionner avec soin.
- Certaines fonctionnalités et technologies qui ne sont généralement pas disponibles pour les développeurs peuvent être fournies sous forme de droits pour certains cas d'utilisation. Par exemple, nous proposons des droits pour CarPlay Audio, HyperVisor et Privileged File Operations. Pour en savoir plus sur les droits, consultez nos documents qui y sont consacrés sur le site developer.apple.com.

Nous espérons que ces directives vous aideront à vous préparer à la procédure Review, et que les validations et les refus demeureront cohérents dans l'ensemble. Il s'agit d'un document évolutif. De nouvelles apps peuvent faire émerger de nouvelles questions et conduire à l'introduction de nouvelles règles à tout moment. Ce sera peut-être le cas de votre app. Nous apprécions cela et respectons votre travail. Nous faisons tout notre possible pour créer la meilleure plateforme au monde où exprimer et monétiser votre talent.

Avant de soumettre votre app

Pour mettre toutes les chances de votre côté lors de la validation de votre app, passez en revue les erreurs fréquemment commises indiquées ci-dessous. Celles-ci peuvent ralentir la procédure de vérification ou entraîner le refus de votre app. Si cela ne remplace pas les directives ni ne garantit la validation de votre app, la vérification de chaque élément de la liste constitue un bon point de départ. Si votre app ne fonctionne plus comme prévu ou que vous ne vous y consacrez plus de manière active, elle sera supprimée de l'App Store. [En savoir plus sur les améliorations apportées à l'App Store.](#)

Assurez-vous de suivre et respecter les instructions suivantes :

- Testez votre app pour détecter la présence de blocages et de bogues.
- Vérifiez que toutes les informations et les métadonnées de l'app sont complètes et exactes.
- Mettez à jour vos coordonnées au cas où l'équipe App Review aurait besoin de vous contacter.
- Donnez à l'équipe App Review un accès complet à votre app. Si votre app comprend des fonctionnalités nécessitant un compte, fournissez un compte de démo actif ou un mode démo complet, ainsi que tout autre matériel ou ressource nécessaire pour évaluer votre app (par exemple, des identifiants de connexion ou un exemple de code QR).
- Activez les services back-end afin qu'ils soient disponibles et accessibles lors de la vérification.
- Donnez des explications détaillées sur les fonctionnalités non apparentes et les achats intégrés dans les notes destinées à l'équipe App Review, notamment des documents permettant d'étayer vos explications, le cas échéant.

- Vérifiez que votre app respecte les consignes mentionnées dans d'autres documents, notamment les documents suivants :

Directives de développement

- [UIKit](#)
- [AppKit](#)
- [WatchKit](#)
- [Extensions d'app](#)
- [Directives sur le stockage de données iOS](#)
- [Apple File System](#)
- [Aide App Store Connect](#)
- [Aide pour le compte de développement](#)

Directives de conception

- [Directives d'interface humaine](#)

Directives sur les marques et le marketing

- [Directives sur les ressources marketing et le respect de l'identité](#)
- [Directives sur le marketing d'Apple Pay](#)
- [Directives relatives à Ajouter à Cartes d'Apple](#)
- [Directives d'utilisation des marques commerciales et des copyrights Apple](#)

Les directives qui incluent le symbole  s'appliquent à la [notarisation des apps iOS](#) dans l'UE.

1. Sécurité

Lorsque des utilisateurs installent une app depuis l'App Store, ils souhaitent être certains de le faire en toute sécurité, c'est-à-dire que l'app ne contient pas de contenu perturbant ou offensant, n'endommagera pas leur appareil, et n'est pas susceptible de provoquer des blessures physiques lors de son utilisation. Les principaux pièges sont indiqués ci-dessous. Si votre app vise à choquer et à offenser, elle n'a pas sa place dans l'App Store. Certaines de ces règles sont également incluses dans Notarisation pour les apps iOS.

1.1 Contenu répréhensible

Les apps ne doivent pas comporter de contenu offensant, inapproprié, perturbant, visant à écœurer, du plus mauvais goût ou tout simplement déplacé. De tels contenus incluent :

1.1.1 Le contenu à caractère diffamatoire, discriminatoire ou hostile, notamment les références ou les commentaires sur la religion, l'appartenance ethnique, l'orientation sexuelle, le genre, la nationalité, l'origine ethnique ou d'autres groupes ciblés, en particulier si l'app est susceptible d'humilier, d'intimider

ou de mettre en danger un individu ou un groupe ciblé. Les humoristes et les auteurs de satires politiques professionnels sont généralement exemptés de cette exigence.

1.1.2 Les représentations réalistes de personnes ou d'animaux tués, mutilés, torturés ou maltraités, ou le contenu encourageant la violence. Dans le cadre d'un jeu, les « ennemis » ne doivent pas cibler exclusivement une origine ethnique, une culture, un gouvernement, une entreprise ou toute autre entité réelle.

1.1.3 Les représentations encourageant l'utilisation illégale ou irresponsable d'armes et d'objets dangereux, ou promouvant l'achat d'armes à feu ou de munitions.

1.1.4 Le contenu à caractère ouvertement sexuel ou pornographique, défini comme étant une « description ou représentation explicite d'organes sexuels ou d'activités visant à éveiller un intérêt érotique plutôt qu'esthétique ou émotionnel ». Cela inclut les apps de rencontre et d'autres apps susceptibles de contenir de la pornographie ou d'être utilisées pour faciliter la prostitution, la traite et l'exploitation d'êtres humains.

1.1.5 Les commentaires religieux provocants ou les citations inexactes ou trompeuses de textes religieux.

1.1.6 ➡ Les informations et fonctionnalités erronées, notamment les données inexactes sur l'appareil ou les fonctionnalités permettant pièges et canulars, comme les faux traqueurs de localisation. Indiquer que l'app est proposée « à des fins de divertissement » ne permet pas d'être exempté de cette directive. Les apps permettant les appels ou les SMS/MMS anonymes ou les canulars seront refusées.

1.1.7 Les concepts nuisibles qui exploitent ou cherchent à tirer profit d'événements récents ou actuels, tels que des conflits violents, des attaques terroristes et des épidémies.

1.2 Contenu généré par l'utilisateur

Les apps incluant du contenu généré par une personne présentent des défis particuliers, de l'infraction de la propriété intellectuelle au harcèlement anonyme. Pour prévenir les abus, les apps comprenant du contenu généré par des personnes ou des services de réseaux sociaux doivent inclure ce qui suit :

- Une méthode permettant de refuser la publication de contenus répréhensibles.
- Un système permettant de signaler le contenu offensant et des réponses rapides aux préoccupations.
- La possibilité de bloquer l'accès au service pour les personnes injurieuses.
- Vos coordonnées afin que les utilisateurs puissent facilement vous contacter.

Les apps comprenant du contenu ou des services générés par l'utilisateur et étant au final essentiellement utilisées à des fins pornographiques, des expériences de type « Chatroulette », le traitement de personnes réelles comme des objets (par exemple, les votes sur l'apparence physique), le recours à des menaces physiques ou le harcèlement n'ont pas leur place sur l'App Store et en seront supprimées sans préavis. Si votre app comprend du contenu généré par l'utilisateur provenant d'un service web, elle peut afficher occasionnellement du contenu pour adultes, à condition que celui-ci soit masqué par défaut et s'affiche uniquement lorsque l'utilisateur active l'option sur votre site web.

1.2.1 Contenu des créateurs

Les apps qui mettent en avant du contenu provenant d'une communauté spécifique d'utilisateurs appelés « les créateurs » sont formidables si elles sont correctement modérées. Ces apps offrent une expérience unique et unifiée qui permet à la clientèle d'interagir avec divers types de contenus des créateurs. Elles proposent des outils et des programmes conçus spécialement pour cette communauté de créateurs qui n'ont pas d'expérience dans le développement d'apps, afin de les aider à concevoir, partager et monétiser des expériences générées par tous les utilisateurs. Ces expériences ne doivent pas modifier les caractéristiques et les fonctionnalités fondamentales de l'app native, le but étant plutôt d'ajouter du contenu à ces expériences structurées. Ces expériences ne correspondent pas à des « apps » natives codées par des développeurs : il s'agit de contenus disponibles au sein de l'app elle-même et qui sont traités par l'équipe App Review comme du contenu généré par les utilisateurs. Ce contenu des créateurs peut comprendre des vidéos, des articles, du contenu audio et même des jeux grand public. L'App Store soutient les apps proposant ce type de contenu généré par nos utilisateurs tant qu'elles respectent toutes les directives, notamment la directive 1.2 relative à la modération du contenu généré par un utilisateur, ainsi que la directive 3.1.1 relative aux paiements et aux achats intégrés. Les apps des créateurs doivent indiquer le contenu des créateurs qui présente la classe d'âge la plus élevée, ainsi qu'indiquer à tous les utilisateurs le type de contenu dont l'accès nécessite un achat supplémentaire.

1.3 Catégorie Enfants

La catégorie Enfants permet de trouver facilement des apps conçues pour les enfants. Si vous souhaitez participer à la catégorie Enfants, concentrez-vous sur la création d'une expérience spécialement destinée aux jeunes utilisateurs. Ces apps ne doivent pas inclure de liens redirigeant vers du contenu externe, de possibilités d'achat ou d'autres distractions pour les enfants, à moins qu'elles ne soient limitées à une zone désignée derrière une barrière parentale. Gardez à l'esprit qu'une fois que les clients attendent de votre app qu'elle satisfasse aux exigences de la catégorie Enfants, celle-ci devra continuer à les respecter dans les mises à jour ultérieures, même si vous décidez de sortir l'app de cette catégorie. En savoir plus sur les [barrières parentales](#).

Vous devez respecter la législation applicable dans le monde entier en matière de protection de la vie privée et de collecte des données des enfants sur Internet. Consultez la [section Confidentialité](#) de ces directives pour obtenir plus d'informations. En outre, les apps de la catégorie Enfants ont l'interdiction de transmettre à des tiers des informations à caractère personnel ou relatives à un appareil. Ces apps ne doivent pas non plus comprendre de publicités ou analyses tierces. Ces règles permettent de garantir une expérience plus sûre pour les enfants. Dans certains cas, des analyses tierces peuvent être autorisées, à condition que les services ne collectent ni ne transmettent l'IDFA (identifiant publicitaire) ou toute information à caractère personnel sur l'enfant (comme son nom, sa date de naissance ou son adresse e-mail), sa position géographique ou ses appareils. Cela comprend toutes les informations sur les appareils, les réseaux ou d'autres détails qui pourraient, que ce soit directement ou en étant mis en corrélation avec d'autres informations, servir à identifier les utilisateurs ainsi que leurs appareils. Les publicités contextuelles tierces peuvent également être autorisées dans certains cas, à condition que les services fournissent des pratiques publicitaires et des politiques accessibles au public et spécialement dédiées aux apps de la catégorie Enfants, qui exigent notamment un contrôle humain des créations publicitaires afin de vérifier qu'elles sont adaptées à l'âge des utilisateurs.

1.4 Blessures physiques 🚫

Votre app peut être refusée si elle est susceptible de provoquer des préjudices physiques. Par exemple :

1.4.1 🚫 Les apps médicales pouvant fournir des données ou des informations inexactes, ou être utilisées pour diagnostiquer ou traiter des patients, peuvent faire l'objet d'une évaluation plus minutieuse.

- Les apps doivent communiquer clairement les données utilisées et la méthodologie employée pour répondre aux demandes concernant l'exactitude des mesures de santé. Dans le cas où la méthodologie ou le niveau d'exactitude ne peut être validé, votre app sera refusée. Par exemple, les apps qui prétendent prendre des radiographies, mesurer la tension artérielle, la température corporelle, le taux de glycémie ou les niveaux d'oxygène dans le sang en utilisant uniquement les capteurs présents sur l'appareil ne sont pas autorisées.

- Les apps doivent rappeler aux utilisateurs de consulter un médecin en plus d'utiliser l'app et avant de prendre toute décision d'ordre médical.

Si votre app médicale a obtenu l'autorisation des autorités de réglementation, incluez un lien vers ce document dans votre app.

1.4.2 🚫 Les calculateurs de dosage de médicaments doivent provenir du fabricant du médicament, d'un hôpital, d'une université, d'une compagnie d'assurance maladie, d'une pharmacie ou d'une autre entité agréée, ou recevoir l'approbation de la FDA (agence américaine des produits alimentaires et médicamenteux) ou d'un organisme équivalent international. Compte tenu des risques pour les patients, nous devons avoir la certitude que l'app sera mise à jour sur le long terme et qu'une assistance sera assurée la concernant.

1.4.3 Les apps qui encouragent la consommation de tabac ou de produits de vapotage, de drogues illégales ou d'alcool en quantités excessives ne sont pas autorisées. Les apps qui encouragent les personnes mineures à consommer l'une de ces substances seront refusées. Il est interdit de faciliter la vente de substances réglementées (sauf pour les pharmacies agréées et les dispensaires de cannabis agréés ou autrement légaux) ou de tabac.

1.4.4 🚫 Les apps peuvent uniquement afficher les postes de contrôles routiers d'alcoolémie ou de dépistage de stupéfiants publiés par les autorités. Elles ne doivent jamais encourager la conduite en état d'ébriété ni d'autres comportements irresponsables comme les excès de vitesse.

1.4.5 🚫 Les apps ne doivent pas inciter les personnes à participer à des activités (paris, défis, etc.) ou à utiliser leurs appareils d'une manière qui risque de provoquer des préjudices physiques aussi bien sur elles-mêmes que sur autrui.

1.5 Informations sur le développeur 🚫

Les utilisateurs doivent savoir comment vous contacter en cas de questions ou de problèmes d'assistance. Assurez-vous que votre app et votre URL d'assistance permettent de vous contacter facilement. Ceci est particulièrement important pour les apps susceptibles d'être utilisées en classe. L'absence de coordonnées exactes et à jour frustre la clientèle et peut également enfreindre la loi dans certains pays ou certaines régions. Assurez-vous également que les cartes, billets et coupons de l'app Cartes comprennent les coordonnées valides de l'émetteur et sont signés à l'aide d'un certificat dédié attribué à la marque propriétaire de la carte, du billet ou du coupon.

1.6 Sécurité des données 🛡️

Les apps doivent mettre en œuvre toutes les mesures de sécurité appropriées pour garantir le traitement adéquat des informations sur les utilisateurs collectées conformément au contrat de licence de l'Apple Developer Program et aux présentes directives (voir la directive 5.1 pour plus d'informations) et empêcher que des tiers puissent y accéder, les utiliser ou les divulguer sans autorisation.

1.7 Signalement d'une activité criminelle

Les apps permettant de signaler une activité criminelle présumée doivent impliquer les autorités locales et ne peuvent être proposées que dans les pays ou régions autorisant une telle implication des autorités locales.

2. Performances

2.1 Exhaustivité de l'app

Les apps soumises à l'équipe App Review, notamment les apps que vous proposez en précommande, doivent être des versions finales comprenant toutes les métadonnées et les URL fonctionnelles nécessaires. Le texte de remplissage, les sites web vides et autres contenus temporaires doivent être supprimés avant que l'app soit envoyée. Assurez-vous que votre app a été testée sur l'appareil pour détecter la présence de bogues et vérifier sa stabilité avant de la soumettre sur l'App Store, et incluez les informations concernant le compte de démonstration si votre app nécessite un identifiant. N'oubliez pas d'activer votre service back-end. Si vous n'êtes pas en mesure de fournir un compte de démo en raison d'obligations légales ou de sécurité, vous pouvez inclure un mode démo intégré en lieu et place d'un compte de démo avec l'accord préalable d'Apple. Assurez-vous que le mode démo présente l'intégralité des caractéristiques et des fonctionnalités de votre app. Si votre app propose des achats intégrés, assurez-vous qu'ils sont complets, à jour et visibles pour l'évaluateur, ou expliquez pourquoi ce n'est pas le cas dans les notes destinées à l'équipe App Review. Ne considérez pas la procédure d'évaluation des apps comme un service de test de logiciels. Nous refuserons les lots et les fichiers binaires d'apps incomplets qui se bloquent ou présentent des problèmes techniques apparents.

2.2 Bêta-tests

Les versions de démonstration, versions bêta et versions d'essai de votre app n'ont pas leur place dans l'App Store. Utilisez plutôt TestFlight. Les apps soumises pour la distribution bêta par le biais de TestFlight doivent être destinées à la distribution au public et respecter les directives sur la procédure App Review. Cependant, notez que les apps utilisant TestFlight ne peuvent pas être distribuées à des testeurs en contrepartie d'une quelconque rémunération, notamment comme récompense pour un financement participatif. Les mises à jour importantes apportées à votre version bêta doivent être soumises à l'équipe TestFlight App Review avant d'être distribuées à votre équipe chargée des tests. Pour en savoir plus, consultez la page consacrée au [bêta-test TestFlight](#).

2.3 Exactitude des métadonnées 🚫

La clientèle doit savoir à quoi s'attendre lorsqu'elle télécharge ou achète votre app. Assurez-vous donc que toutes les métadonnées de votre app, notamment ses informations relatives à la confidentialité, sa description, ses captures d'écran et ses aperçus reflètent la principale expérience qu'elle propose, et mettez-les à jour à chaque nouvelle version.

2.3.1

(a) 🚫 N'incluez pas de fonctionnalités masquées, inactives ou non documentées dans votre app. Les fonctionnalités de celle-ci doivent être claires pour les utilisateurs et utilisatrices finaux et pour l'équipe App Review. Toutes les nouvelles caractéristiques, fonctionnalités et modifications apportées à l'app doivent être décrites en détail dans la section Remarques concernant la vérification d'App Store Connect (les descriptions trop générales seront refusées) et facilement accessibles pour simplifier leur vérification. De même, la commercialisation trompeuse de votre app, par exemple faisant la promotion d'un contenu ou de services qu'elle ne propose pas réellement (par exemple, les scanners de virus et de logiciels malveillants s'appuyant sur iOS) ou faisant la promotion d'un faux prix, aussi bien sur l'App Store qu'en dehors, constitue un motif de suppression de votre app de l'App Store ou de blocage de l'installation via une distribution alternative et de suspension de votre compte de développeur.

(b) Un comportement inacceptable ou répété peut entraîner votre exclusion de l'Apple Developer Program. Nous mettons tout en œuvre pour faire de l'App Store un écosystème fiable, et nous attendons de nos développeurs d'apps qu'ils en fassent de même. Si vous faites preuve de malhonnêteté, nous ne souhaitons pas travailler avec vous.

2.3.2 Si votre app propose des achats intégrés, assurez-vous que la description, les captures d'écran et les aperçus de votre app indiquent clairement si les articles, niveaux, abonnements, etc. présentés nécessitent des achats supplémentaires. Si vous décidez de promouvoir des achats intégrés sur l'App Store, assurez-vous que leur nom, leurs captures d'écran et leur description sont adaptés au grand public. Veillez à respecter les consignes indiquées sur la page [Promoting Your In-App Purchases](#) (Promotion de vos achats intégrés), et à faire en sorte que votre app gère correctement la [méthode SKPaymentTransactionObserver](#) afin que les clients puissent terminer le processus d'achat sans problème lorsque votre app se lance.

2.3.3 Les captures d'écran doivent présenter l'app en cours d'utilisation, et pas uniquement le titre, la page de connexion ou l'écran d'accueil. Elles peuvent également inclure du texte et des images en superposition (par exemple, pour décrire des mécanismes de saisie, comme un point de contact ou un Apple Pencil animé) et montrer une fonctionnalité étendue sur un appareil, comme la Touch Bar.

2.3.4 Les aperçus permettent aux clients de voir à quoi ressemble votre app et quelle est sa fonction. Pour garantir que les utilisateurs savent à quoi s'attendre avec votre app, les aperçus peuvent uniquement utiliser des captures d'écran vidéo de l'app elle-même. Par exemple, pour les extensions d'autocollants et iMessage, vous pouvez donner un aperçu de l'expérience utilisateur dans l'app Messages. Vous pouvez ajouter de la narration et des superpositions vidéo ou textuelles pour apporter des clarifications à la vidéo.

2.3.5 ➡ Sélectionnez la catégorie la plus adaptée à votre app et consultez les [définitions des catégories de l'App Store](#) au besoin. Si nécessaire, nous pouvons être amenés à modifier la catégorie si vous avez commis une erreur.

2.3.6 ➡ Répondez honnêtement aux questions permettant de déterminer la classe d'âge dans App Store Connect, afin que votre app soit gérée de manière appropriée par les fonctionnalités de contrôle parental. Si votre app n'est pas associée à la classe d'âge adéquate, la clientèle pourrait être surprise par son contenu, ou les organismes gouvernementaux de régulation pourraient ouvrir une enquête. Si votre app comprend du contenu multimédia qui nécessite l'affichage d'un système de classification de contenu ou d'avertissements (par exemple, pour des films, de la musique, des jeux, etc.), il vous incombe de vous conformer aux exigences locales de chaque territoire où votre app est disponible.

2.3.7 ➡ Choisissez un nom unique pour votre app et attribuez-lui des mots-clés qui la décrivent avec précision. N'essayez pas d'insérer des termes déposés, des noms d'apps populaires, des informations sur le prix ni d'autres expressions non pertinentes dans vos métadonnées, dans le seul but de contourner le système. Les noms d'apps sont limités à 30 caractères. Les métadonnées comme les noms d'apps, les sous-titres, les captures d'écran et les aperçus ne doivent pas inclure des prix, des termes ou des descriptions qui ne sont pas propres au type de métadonnées. Les sous-titres d'app sont un excellent moyen de fournir des informations supplémentaires sur l'environnement de votre app. Ces sous-titres doivent respecter nos règles standard en matière de métadonnées et ne doivent pas inclure de contenu inapproprié, faire référence à d'autres apps ou communiquer des informations sur des produits qui ne peuvent pas être vérifiées. Apple peut à tout moment modifier les mots-clés inappropriés ou prendre d'autres mesures appropriées pour prévenir les abus.

2.3.8 ➡ Les métadonnées doivent être appropriées pour tous les publics. Assurez-vous que les icônes, captures d'écran et aperçus associés à votre app et à vos achats intégrés sont adaptés à la classe d'âge 4 ans et +, même si votre app appartient à une classe d'âge supérieure. Par exemple, si votre app est un jeu contenant des scènes de violence, sélectionnez des images qui ne représentent pas une mort sanglante ou une arme braquée sur un personnage précis. L'utilisation de termes tels que « pour les enfants » dans les métadonnées de l'app est réservée dans l'App Store pour la catégorie enfants. Assurez-vous que vos métadonnées, notamment le nom et les icônes (petite, grande, app Apple Watch, icônes alternatives, etc.) de l'app, sont similaires pour éviter toute confusion.

2.3.9 Il vous incombe d'obtenir les droits nécessaires pour utiliser les éléments des icônes, captures d'écran et aperçus de votre app, et d'afficher des informations de compte fictives plutôt que les données d'une personne réelle.

2.3.10 Veillez à ce que votre app soit axée sur l'expérience iOS, iPadOS, macOS, tvOS ou watchOS, et n'incluez pas de noms, d'icônes ou d'images d'autres plateformes mobiles ou de marchée d'apps alternatives dans votre app ou vos métadonnées, à moins qu'il n'y ait une fonctionnalité interactive spécifique et approuvée. Assurez-vous également que les métadonnées de votre app sont centrées sur l'app elle-même et l'expérience qu'elle offre, et qu'elles ne contiennent pas d'informations non pertinentes.

2.3.11 Les apps que vous proposez en précommande sur l'App Store doivent être complètes et utilisables. Assurez-vous que l'app finale que vous lancez n'est pas foncièrement différente de celle que vous promouvez alors qu'elle est proposée en précommande. Si vous apportez des modifications importantes à l'app (par exemple, si vous changez de modèle commercial), vous devez reprendre à zéro la phase de précommande.

2.3.12 Les nouvelles fonctionnalités des apps et les modifications qui y ont été apportées doivent être clairement décrites dans la section Nouveautés des apps. Une description générale suffit pour les correctifs de bogues simples, les mises à jour de sécurité et les améliorations des performances, mais les modifications plus importantes doivent être décrites en détail dans cette section.

2.3.13 Les événements intégrés aux apps sont des événements qui se produisent à un moment précis au sein de votre app. Pour que votre événement apparaisse sur l'App Store, il doit appartenir à l'un des types d'événement répertoriés dans App Store Connect. Toutes les métadonnées relatives à un événement doivent être exactes et se rapporter à l'événement lui-même plutôt qu'à l'app dans son ensemble. Les événements doivent se produire aux dates et aux heures que vous avez sélectionnées dans App Store Connect pour tous les Stores choisis. Vous pouvez monétiser votre événement à condition de respecter les règles énoncées dans la section 3, qui est dédiée à la monétisation. Par ailleurs, le lien profond de votre événement doit rediriger directement les utilisateurs vers la destination adéquate au sein de votre app. Consultez la page [In-App Events](#) (Événements intégrés) pour obtenir des instructions détaillées sur les métadonnées des événements et leurs liens ciblés qui sont acceptables.

2.4 Compatibilité matérielle

2.4.1 Pour garantir que les personnes tirent le meilleur parti de votre app, les apps iPhone doivent fonctionner sur iPad lorsque cela est possible. Nous vous encourageons à développer des apps universelles afin que votre clientèle puisse les utiliser sur l'ensemble de leurs appareils. En savoir plus sur les [apps universelles](#).

2.4.2 ➡ Concevez votre app de sorte qu'elle soit économe en énergie et que son utilisation ne risque pas d'endommager l'appareil. Les apps ne doivent pas décharger rapidement la batterie, générer une chaleur excessive ou solliciter inutilement les ressources de l'appareil. Par exemple, les apps ne doivent pas encourager les utilisateurs à placer leur appareil sous un matelas ou un coussin pendant qu'il charge ou à réaliser un nombre excessif de cycles d'écriture sur le lecteur SSD (Solid State Drive). Les apps, y compris les publicités tierces qui y sont diffusées, ne doivent pas exécuter de processus en arrière-plan qui n'ont aucun rapport avec l'app, comme le minage de cryptomonnaie.

2.4.3 La clientèle doit pouvoir utiliser votre app Apple TV sans avoir à acheter du matériel en plus de la télécommande Siri Remote ou des manettes de jeu tierces. Cependant, n'hésitez pas à offrir des fonctionnalités avancées lorsque d'autres périphériques sont connectés. Si une manette de jeu est requise, assurez-vous de l'expliquer clairement dans vos métadonnées pour que la clientèle sache qu'elle a besoin d'un équipement supplémentaire pour jouer.

2.4.4 ➡ Les apps ne doivent jamais suggérer ni nécessiter un redémarrage de l'appareil ou des modifications des réglages du système sans rapport avec la fonctionnalité principale de l'app. Par exemple, n'encouragez pas les personnes à désactiver le Wi-Fi, à désactiver les fonctionnalités de sécurité, etc.

2.4.5 Les apps distribuées par le biais du Mac App Store sont soumises à des exigences supplémentaires :

- (i) Elles doivent être mises en bac à sable de manière appropriée et respecter les règles énoncées sur la page [macOS File System Documentation](#) (Documentation sur le système de fichiers macOS). De plus, elles doivent uniquement utiliser les API macOS appropriées pour modifier les données utilisateur stockées par d'autres apps (signets, Carnet d'adresses, données de Calendrier, etc.).
- (ii) Elles doivent être empaquetées et soumises à l'aide des technologies disponibles dans Xcode. Aucun programme d'installation tiers n'est autorisé. Elles doivent également se présenter sous forme de paquets d'installation d'apps uniques et autonomes et ne peuvent installer de code ou de ressources dans des emplacements partagés.
- (iii) Elles ne doivent pas se lancer automatiquement ou entraîner l'exécution automatique de code au démarrage ou lors de la connexion sans autorisation, ni engendrer des processus qui continuent de fonctionner sans autorisation après la déconnexion de l'utilisateur. Elles ne doivent pas ajouter automatiquement leur icône dans le Dock, ni placer des raccourcis sur le bureau de l'utilisateur.
- (iv) Elles ne doivent pas entraîner le téléchargement ou l'installation d'apps autonomes, de fichiers d'extension du noyau (Kext), de code supplémentaire ou de ressources dans le but d'ajouter des fonctionnalités ou d'apporter des modifications importantes à la version de l'app soumise lors de la procédure de vérification.
- (v) Elles ne doivent pas demander une remontée vers les privilèges root ou utiliser des attributs setuid.
- (vi) Elles ne doivent pas afficher d'écran de licence au lancement, exiger des clés de licence ou mettre en place leur propre protection contre la copie.
- (vii) Les mises à jour doivent être distribuées par le biais du Mac App Store. Toute autre méthode de mise à jour est interdite.
- (viii) Les apps doivent s'exécuter sur le système d'exploitation actuellement disponible et ne doivent pas utiliser de technologies obsolètes ou dont l'installation est facultative (par exemple, Java).
- (ix) Les apps doivent inclure l'assistance dans toutes les langues et variantes régionales dans un seul lot d'apps.

2.5 Configuration logicielle requise

2.5.1 Les apps peuvent utiliser uniquement des API publiques et doivent être compatibles avec le système d'exploitation actuellement disponible. En savoir plus sur les [API publiques](#). Maintenez vos apps à jour et assurez-vous de supprimer progressivement les fonctionnalités, frameworks ou technologies obsolètes qui ne seront plus pris en charge dans les versions futures d'un système d'exploitation. Les apps doivent utiliser les API et les frameworks aux fins prévues. Cette intégration doit être spécifiée dans la description de l'app. À titre d'exemple, le framework HomeKit doit offrir des services de domotique, et HealthKit doit être utilisé à des fins de santé et de forme et être intégré à l'app Santé.

2.5.2 ➡ Les apps doivent être autonomes et ne doivent pas lire ni écrire de données en dehors de leur conteneur, ni télécharger, installer ou exécuter du code qui ajoute ou modifie des fonctionnalités ou le fonctionnement de l'app, y compris d'autres apps. Les apps éducatives conçues pour enseigner, développer ou permettre aux élèves de tester du code exécutable peuvent, dans certaines circonstances, télécharger du code, à condition que ce code ne soit pas utilisé à d'autres fins. Ces apps doivent permettre à l'utilisateur de voir et de modifier complètement le code source fourni par l'app.

2.5.3 ➡ Les apps transmettant des virus, des fichiers, un code informatique ou des programmes susceptibles d'interrompre ou de perturber le fonctionnement normal du système d'exploitation ou des fonctionnalités matérielles, notamment les notifications push et Game Center, seront refusées. Les violations flagrantes et répétées entraîneront votre exclusion de l'Apple Developer Program.

2.5.4 ➡ Les apps multitâches peuvent uniquement utiliser des services d'arrière-plan aux fins prévues : VoIP, lecture audio, localisation, réalisation de tâches, notifications locales, etc.

2.5.5 Les apps doivent être pleinement fonctionnelles sur les réseaux uniquement IPv6.

2.5.6 ➡ Les apps permettant la navigation sur Internet doivent utiliser le framework WebKit approprié ainsi que WebKit JavaScript. Vous pouvez demander le droit d'utiliser un autre moteur de navigateur web dans votre app. [En savoir plus sur ces droits.](#)

2.5.7 Intentionnellement omis.

2.5.8 Les apps créant des écrans d'accueil ou des bureaux alternatifs ou simulant des expériences de widgets multi-apps seront refusées.

2.5.9 ➡ Les apps qui modifient ou désactivent la fonction des commutateurs standard, tels que le bouton de réglage du volume et le commutateur Sonnerie/Silencieux, ou d'autres éléments ou comportements de l'interface utilisateur native seront refusées. Par exemple, les apps ne doivent pas bloquer les liens redirigeant vers d'autres apps ou d'autres fonctionnalités dont les utilisateurs s'attendent à ce qu'elles fonctionnent d'une certaine manière.

2.5.10 Les apps ne doivent pas être soumises avec des bannières publicitaires ou des publicités de test vides.

2.5.11 ➡ SiriKit et Raccourcis

(i) Les apps intégrant SiriKit et Raccourcis doivent s'enregistrer uniquement pour les commandes qu'elles peuvent gérer sans l'aide d'une app supplémentaire et que les utilisateurs attendent de la fonctionnalité décrite. Par exemple, si votre app est une app de planification de repas, vous ne devez pas inclure une commande visant à démarrer un entraînement, même si votre app partage une intégration avec une app de fitness.

(ii) Assurez-vous que le vocabulaire et les expressions de votre fichier plist sont en rapport avec votre app et avec la fonctionnalité Siri des commandes pour lesquelles l'app s'est enregistrée. Les alias doivent être directement liés à votre app ou à votre nom d'entreprise et ne doivent pas être des termes génériques ni inclure des noms ou des services d'apps tierces.

(iii) Exécutez la demande Siri ou le Raccourci de la manière la plus directe possible et n'insérez pas de publicités ni d'autres contenus marketing entre la demande et son exécution. Présentez un message interstitiel uniquement lorsque cela s'avère nécessaire pour effectuer la tâche (par exemple, pour demander à l'utilisateur de choisir un type d'entraînement particulier).

2.5.12 ➡ Les apps qui utilisent CallKit ou intègrent une extension contre les fraudes par SMS doivent bloquer uniquement les numéros de téléphone confirmés comme étant indésirables. Les fonctionnalités de blocage d'appels, de SMS et de MMS ou d'identification de spam intégrées aux apps, ainsi que leurs critères utilisés pour identifier du spam et bloquer du contenu, doivent être clairement définis et expliqués dans le texte marketing qui accompagne ces apps. Vous ne pouvez pas utiliser les données accessibles via ces outils à des fins qui ne sont pas directement liées au fonctionnement ou à l'amélioration de votre app ou de votre extension (par exemple, vous ne pouvez pas les utiliser, les partager ou les vendre à des fins de suivi, de création de profils d'utilisateurs, etc.).

2.5.13 ➡ Les apps qui emploient la reconnaissance faciale pour l'authentification de compte doivent utiliser [LocalAuthentication](#) dans la mesure du possible (et non ARKit ou toute autre technologie de reconnaissance faciale), et doivent utiliser une autre méthode d'authentification pour les personnes âgées de moins de 13 ans.

2.5.14 ➡ Les apps doivent demander l'autorisation explicite de l'utilisateur ou de l'utilisatrice et fournir une indication visuelle et/ou sonore claire lorsqu'elles enregistrent, conservent ou conservent d'une autre manière l'activité de l'utilisateur ou de l'utilisatrice. Cela comprend toute utilisation de la caméra, du micro, des enregistrements d'écran ou d'autres données de l'utilisateur.

2.5.15 Les apps qui permettent de visualiser et de sélectionner des fichiers doivent inclure le contenu de l'app Fichiers et les documents iCloud de l'utilisateur.

2.5.16 ➡ Les widgets, les extensions et les notifications doivent être liés au contenu ou aux fonctionnalités de votre app.

(a) En outre, toutes les caractéristiques et fonctionnalités d'un extrait d'app doivent figurer dans le fichier binaire principal de l'app. Les extraits d'apps ne peuvent pas contenir de publicités.

2.5.17 ➡ Les apps qui prennent en charge Matter doivent utiliser le framework d'assistance d'Apple pour que Matter lance le jumelage. En outre, si vous choisissez d'utiliser dans votre app un composant logiciel Matter autre que le SDK (kit de développement logiciel) Matter fourni par Apple, ce composant logiciel doit être certifié par la [Connectivity Standards Alliance](#) pour la plateforme sur laquelle il est exécuté.

2.5.18 ➡ Les publicités d'affichage doivent se limiter au fichier binaire principal de votre app et ne doivent pas apparaître dans les extensions, extraits d'app, widgets, notifications, claviers, apps watchOS, etc. Les publicités affichées dans une app doivent être adaptées à la classe d'âge de l'app, permettre aux personnes de consulter toutes les informations servant à les cibler pour la publicité en question (sans les obliger à quitter l'app), et ne peuvent pas faire de publicité ciblée ou comportementale fondée sur des données utilisateur sensibles, comme des données de santé/médicales (par exemple, des données provenant des API HealthKit), des données d'établissements d'enseignement et de classes (par exemple, des données provenant de ClassKit), des données relatives à des enfants (par exemple, des données provenant d'apps de l'App Store de la catégorie Enfants), etc. Les publicités interstitielles ou les publicités

qui interrompent ou bloquent l'expérience utilisateur doivent clairement indiquer que ce sont des publicités, ne doivent pas manipuler ou tromper les personnes pour qu'elles les regardent, et doivent contenir des boutons servant à les fermer/passer qui sont facilement accessibles, visibles et suffisamment grands pour que les personnes puissent facilement les ignorer. Les apps qui contiennent des publicités doivent également permettre aux utilisateurs de signaler toute publicité inappropriée ou inadaptée à leur âge.

3. Monétisation

Il existe plusieurs façons de monétiser votre app sur l'App Store. Si votre modèle commercial n'est pas clair, assurez-vous d'apporter des précisions dans les métadonnées de l'app et les notes destinées à l'équipe App Review. Si nous ne parvenons pas à comprendre le fonctionnement de votre app ou que vos achats intégrés ne sont pas immédiatement reconnaissables, votre évaluation sera retardée et votre app pourrait être refusée. Bien que vous décidiez des tarifs, nous ne distribuerons pas les apps dont le prix et celui des achats intégrés qu'elles proposent sont abusifs. Nous refuserons les apps onéreuses dont le prix exorbitant risque de tromper les utilisateurs.

Si nous découvrons que vous avez tenté de manipuler les avis des utilisateurs, d'améliorer votre classement en ayant recours à des commentaires rémunérés, incités, filtrés ou faux, ou que vous avez demandé à des services tiers de le faire en votre nom, nous prendrons des mesures pour préserver l'intégrité de l'App Store, ce qui peut comprendre votre exclusion de l'Apple Developer Program.

3.1 Paiements

3.1.1 Achats intégrés

- Si vous souhaitez que des caractéristiques ou des fonctionnalités puissent être débloquées au sein de votre app (par exemple, des abonnements, des devises utilisables dans un jeu, des niveaux de jeu, du contenu premium ou le déverrouillage de la version complète de votre app), vous devez les proposer sous forme d'achats intégrés. Les apps ne doivent pas utiliser leurs propres mécanismes pour débloquer du contenu ou des fonctionnalités comme des clés de licence, des marqueurs de réalité augmentée, des codes QR, des cryptomonnaies et des portefeuilles de cryptomonnaies, etc.
- Les apps peuvent utiliser les devises associées aux achats intégrés pour permettre à la clientèle de « donner un pourboire » au sein de l'app au développeur ou aux fournisseurs de contenu numérique.
- Les crédits ou les devises de jeu acquis par le biais d'achats intégrés ne peuvent pas expirer. Assurez-vous de disposer d'un mécanisme de restauration pour les achats intégrés pouvant être restaurés.
- Les apps peuvent permettre d'offrir à une autre personne du contenu pouvant être acquis à l'aide d'un achat intégré. Un tel cadeau ne peut être remboursé qu'à la personne qui l'a acheté et ne peut pas être échangé.

- Les apps distribuées par le biais du Mac App Store peuvent héberger des modules externes ou des extensions compatibles avec des mécanismes autres que l'App Store.
- Les apps qui proposent des « loot boxes » (coffres à butin) ou d'autres mécanismes permettant d'acheter des objets virtuels aléatoires doivent indiquer à la clientèle les chances qu'elle a de recevoir chaque type d'objet avant l'achat.
- Les cartes cadeaux, les bons cadeaux et les coupons numériques qui peuvent être échangés contre des biens ou des services numériques ne peuvent être vendus dans votre app qu'au moyen d'un achat intégré. Les cartes cadeaux physiques vendues dans une app et envoyées ensuite par voie postale aux clients peuvent être réglées à l'aide d'autres modes de paiement que l'achat intégré.
- Les apps sans abonnement peuvent proposer une période d'essai gratuit avant de présenter une option permettant de déverrouiller toutes leurs fonctionnalités. Pour cela, il est nécessaire de configurer un article non utilisable et réglable par achat intégré au niveau de prix 0, qui respecte la convention d'appellation suivante : « Essai de XX jours ». Avant le début de l'essai, votre app doit clairement indiquer sa durée, le contenu ou les services qui ne seront plus accessibles au terme de l'essai, ainsi que tous les frais à régler pour déverrouiller toutes les fonctionnalités de l'app. Pour en savoir plus sur la gestion de l'accès au contenu et la durée de la période d'essai, consultez les pages dédiées aux [reçus](#) et aux services de [vérification des appareils](#).
- Les apps peuvent avoir recours aux achats intégrés pour vendre des jetons non fongibles (NFT) et des services liés à ceux-ci, tels que la frappe, l'inscription et le transfert. Les apps peuvent permettre aux utilisateurs de visualiser leurs propres NFT, à condition que la possession d'un NFT ne déverrouille pas des caractéristiques ou des fonctionnalités au sein de l'app. Les apps peuvent permettre aux utilisateurs de parcourir les collections NFT appartenant à d'autres personnes, à condition que les apps ne comprennent pas de boutons, de liens externes ou d'autres appels à l'action qui redirigent la clientèle vers des méthodes d'achat autres que les achats intégrés.

3.1.1(a) Lien vers d'autres méthodes d'achat

Les développeurs peuvent demander des droits permettant d'intégrer à leur app un lien vers un site web dont ils sont propriétaires ou responsables, et qui permet l'achat de contenus ou de services numériques. Veuillez consulter les informations supplémentaires ci-dessous.

- Droits de lien d'achat externe StoreKit : dans certaines régions, les apps disponibles dans l'App Store peuvent proposer des achats intégrés et utiliser un droit de lien d'achat externe StoreKit. Celui-ci permet d'inclure un lien vers le site web du développeur, informant les utilisateurs et utilisatrices qu'il existe d'autres moyens d'acheter des biens ou des services numériques. En savoir plus sur ces [droits](#). Conformément aux contrats de ces droits, le lien peut fournir des informations concernant la manière et l'endroit où ces articles intégrés peuvent être achetés, et sur le fait qu'ils peuvent être proposés à un prix relativement inférieur. Les droits sont limités à une utilisation dans des vitrines spécifiques de l'App Store iOS ou iPadOS. Dans toutes les autres vitrines, les apps et leurs métadonnées ne peuvent pas inclure de boutons, de liens externes ni d'autres appels à l'action dirigeant les utilisateurs et utilisatrices vers des méthodes d'achat autres que les achats intégrés.

- Droits de services de streaming de musique : dans certaines régions, les apps de streaming de musique peuvent utiliser les droits de services de streaming de musique pour inclure un lien (pouvant se présenter sous la forme d'un bouton d'achat) vers le site web du développeur, informant les utilisateurs et utilisatrices qu'il existe d'autres moyens d'acheter du contenu ou des services de musique numérique. Ces droits permettent également aux développeurs d'apps de streaming de musique d'inviter les utilisateurs et utilisatrices à fournir leur adresse e-mail dans le but explicite de leur envoyer un lien vers leur site web afin d'y acheter du contenu ou des services de musique numérique. En savoir plus sur ces [droits](#). Conformément aux contrats de ces droits, le lien peut fournir des informations concernant la manière et l'endroit où ces articles intégrés peuvent être achetés, ainsi que sur leur prix. Les droits sont limités à une utilisation dans des vitrines spécifiques de l'App Store iOS ou iPadOS. Dans toutes les autres vitrines, les apps de streaming de musique et leurs métadonnées ne peuvent pas inclure de boutons, de liens externes ni d'autres appels à l'action dirigeant les utilisateurs et utilisatrices vers des méthodes d'achat autres que les achats intégrés.
- Si votre app utilise des pratiques commerciales trompeuses, des escroqueries ou de la fraude en lien avec le droit, votre app sera supprimée de l'App Store et votre participation à l'Apple Developer Program peut être résiliée.

3.1.2 Abonnements

Les apps peuvent proposer des abonnements à renouvellement automatique pour les achats intégrés, quelle que soit leur catégorie sur l'App Store. Lorsque vous intégrez des abonnements à renouvellement automatique dans votre app, assurez-vous de suivre les directives ci-dessous.

3.1.2(a) Utilisations autorisées

Si vous proposez un abonnement à renouvellement automatique, vous devez fournir en continu un service de qualité à la clientèle. La période d'abonnement doit durer au moins sept jours, et l'abonnement doit être disponible sur tous les appareils de l'utilisateur ou de l'utilisatrice. Cette liste non exhaustive contient des exemples d'abonnements appropriés : nouveaux niveaux de jeu, contenu sous forme d'épisodes, prise en charge du mode multijoueur, apps qui offrent des mises à jour importantes et régulières, accès à de grandes collections de contenus multimédias ou à des contenus multimédias continuellement mis à jour, logiciel en tant que service (« SAAS ») et prise en charge du cloud. De plus :

- Des abonnements peuvent être proposés en même temps qu'une offre à la carte (par exemple, vous pouvez proposer un abonnement à un catalogue complet de films, tout comme l'achat ou la location d'un seul film).
- Vous pouvez proposer un abonnement unique qui peut être utilisé dans l'ensemble des apps et services que vous détenez.
- Les jeux inclus dans un abonnement à un service de jeux en streaming peuvent proposer un abonnement unique pouvant être utilisé dans plusieurs apps et services tiers. Toutefois, ces jeux doivent être téléchargés directement à partir de l'App Store, être conçus pour éviter que les personnes abonnées effectuent un paiement en double, et ne pas désavantager les personnes qui n'ont pas souscrit d'abonnement.

- L'abonnement doit fonctionner sur tous les appareils de l'utilisateur sur lesquels l'app est disponible. En savoir plus sur [l'utilisation d'un abonnement dans plusieurs apps](#).
- L'app ne doit pas obliger les utilisateurs à noter ou à évaluer l'app, à télécharger d'autres apps, ou à effectuer d'autres actions similaires afin d'utiliser l'app ou d'accéder à ses fonctionnalités ou à son contenu.
- Tout comme les autres apps, celles proposant un abonnement doivent permettre à tous les utilisateurs de bénéficier du service qu'ils ont acheté, sans avoir à réaliser de tâches supplémentaires, notamment publier du contenu sur les réseaux sociaux, charger des contacts, se connecter un certain nombre de fois à l'app, etc.
- Les abonnements peuvent comprendre des crédits consommables, des gemmes, des devises utilisables dans un jeu, etc. Vous pouvez aussi proposer un abonnement qui inclut l'accès à des biens consommables à prix réduit (par exemple, un abonnement Platine qui permet d'acheter des packs de gemmes à prix réduit).
- Si vous modifiez votre app existante pour adopter un modèle commercial fondé sur un abonnement, vous ne devez pas supprimer les fonctionnalités principales pour lesquelles les utilisateurs existants ont déjà payé. Par exemple, les personnes qui ont déjà payé pour déverrouiller le jeu complet doivent pouvoir continuer à accéder au jeu complet après l'introduction du modèle fondé sur l'abonnement pour la nouvelle clientèle.
- Les apps nécessitant un abonnement à renouvellement automatique peuvent proposer une période d'essai gratuite à la clientèle en lui fournissant les informations adéquates qui sont énoncées dans App Store Connect. [En savoir plus sur les offres d'abonnement](#).
- Les apps qui tentent d'escroquer les utilisateurs seront supprimées de l'App Store. Cela comprend les apps qui tentent d'inciter les personnes à souscrire un abonnement sous de faux prétextes ou qui ont recours à des escroqueries ou à des pratiques de « bait-and-switch » (vente frauduleuse par amorçage et substitution). Si votre app entre dans cette catégorie, elle sera supprimée de l'App Store, et nous procéderons éventuellement à votre exclusion de l'Apple Developer Program.
- Avec l'accord préalable d'Apple, des abonnements à des services musicaux et vidéo avec renouvellement automatique peuvent être inclus dans les apps d'un opérateur mobile lorsqu'ils sont achetés avec de nouveaux forfaits mobiles. Avec l'accord préalable d'Apple, d'autres abonnements à renouvellement automatique peuvent également être inclus avec de nouveaux forfaits de données mobiles, si les apps de l'opérateur mobile prennent en charge les achats intégrés pour les utilisateurs et les utilisatrices. Ces abonnements ne peuvent pas donner accès à des articles consommables ni offrir des remises sur ceux-ci, et les abonnements doivent être résiliés en même temps que le forfait de données mobiles.

3.1.2(b) Mises à niveau vers une version ultérieure ou antérieure

Les mises à niveau vers une version ultérieure ou antérieure doivent se faire en toute fluidité, et ne doivent pas permettre de s'abonner par erreur à plusieurs variantes du même abonnement. Consultez les [bonnes pratiques](#) en matière de gestion des options de mise à niveau vers une version ultérieure ou antérieure pour votre abonnement.

3.1.2(c) Informations d'abonnement

Avant de demander à une personne de s'abonner, vous devez décrire de manière claire l'ensemble des éléments qu'elle obtiendra en échange du paiement. Combien de publications par mois ? Quel espace de stockage dans le cloud ? Quel type d'accès à votre service ? Assurez-vous d'indiquer clairement les exigences décrites dans [l'annexe 2 du contrat de licence de l'Apple Developer Program](#).

3.1.3 Autres méthodes d'achat

Les apps ci-dessous peuvent proposer d'autres méthodes d'achat que l'achat intégré. Les apps de cette section ne peuvent en leur sein même encourager les utilisateurs à opter pour une méthode d'achat autre que l'achat intégré, sauf dans les cas décrits dans la directive 3.1.3(a). Les développeurs peuvent communiquer des informations en dehors de l'app à leur base d'utilisateurs au sujet de méthodes d'achat autres que l'achat intégré.

3.1.3(a) Apps de lecture

Ces apps peuvent permettre à la clientèle d'accéder à ses contenus ou à ses abonnements à des contenus achetés ou souscrits par le passé (en particulier les contenus suivants : magazines, journaux, livres, audio, musique et vidéo). Les apps de lecture peuvent proposer de créer un compte gratuitement et permettre aux utilisateurs existants de gérer leur compte. Les développeurs d'apps de lecture peuvent demander le droit de compte avec un lien externe afin d'intégrer à leur app un lien vers un site web dont ils sont propriétaires ou responsables et qui permet de créer un compte ou de le gérer. En savoir plus sur le [droit de compte avec un lien externe](#).

3.1.3(b) Services multiplateformes

Les applications qui fonctionnent sur plusieurs plateformes peuvent permettre aux utilisateurs d'accéder au contenu, aux abonnements ou aux fonctions qu'ils ont acquis dans votre application sur d'autres plateformes ou sur votre site web, y compris les éléments consommables dans les jeux multiplateformes, à condition que ces éléments soient également disponibles [sous forme d'achat dans l'app](#).

3.1.3(c) Services aux entreprises

Si vous vendez votre app uniquement à des organisations ou à des groupes pour leur personnel ou leurs élèves (par exemple, des bases de données professionnelles et des outils de gestion de classe), vous pouvez permettre aux utilisateurs de ces organisations ou groupes d'accéder au contenu ou aux abonnements achetés ou souscrits par le passé. Les ventes aux consommateurs, aux utilisateurs uniques ou aux familles doivent se faire par achat intégré.

3.1.3(d) Services de personne à personne

Si votre app permet de souscrire des services de personne à personne en temps réel entre deux individus (par exemple, des services de cours particuliers, des consultations médicales, des visites immobilières ou des entraînements sportifs), vous pouvez utiliser des méthodes d'achat autres que l'achat intégré pour encaisser ces paiements. Le système d'achat intégré doit être mis en place pour les services fournis en temps réel à une clientèle réduite ou à un grand groupe de personnes.

3.1.3(e) Biens et services en dehors de l'app

Si votre app permet l'achat de biens physiques ou de services qui seront consommés en dehors de l'app, vous devez utiliser des méthodes d'achat autres que l'achat intégré pour encaisser ces paiements, comme Apple Pay ou la saisie classique des informations d'une carte de crédit.

3.1.3(f) Apps autonomes gratuites

L'utilisation du système d'achat intégré n'est pas obligatoire pour les apps gratuites faisant office de complément autonome à un outil web payant (par exemple, VoIP, stockage dans le cloud, services de messagerie, hébergement web), à condition qu'elles ne proposent aucun achat et qu'elles ne contiennent aucun appel à l'action invitant à effectuer un achat externe.

3.1.3(g) Apps de gestion des publicités

Les apps dont le seul but est de permettre aux annonceurs (personnes ou sociétés qui font la publicité d'un produit, d'un service ou d'un évènement) d'acheter et de gérer des campagnes publicitaires sur différents types de médias (télévision, affichage public, sites web, apps, etc.) n'ont pas besoin d'utiliser les achats intégrés. Ces apps sont destinées à la gestion des campagnes et n'affichent pas elles-mêmes les publicités. Les achats numériques de contenu à consulter ou à consommer dans une app, notamment l'achat de publicités à afficher dans cette même app (comme les ventes de « boosts » pour les publications dans une app de réseaux sociaux), doivent se faire sous forme d'achats intégrés.

3.1.4 Contenu dépendant d'un matériel spécifique

Dans certaines circonstances, notamment lorsque des fonctionnalités dépendent d'un matériel spécifique pour fonctionner, l'app peut les débloquer sans les proposer sous forme d'achats intégrés (par exemple, une app d'astronomie offrant des fonctionnalités supplémentaires lorsqu'elle est synchronisée avec un télescope). Les fonctionnalités fonctionnant avec un produit physique approuvé (par exemple un jouet) à titre facultatif peuvent être débloquées sans passer par un achat intégré, à condition qu'une option d'achats intégrés soit également disponible. Cependant, vous ne pouvez pas exiger des utilisateurs qu'ils achètent des produits n'ayant aucun rapport avec l'app ou qu'ils s'impliquent dans des activités de publicité ou de marketing pour débloquer des fonctionnalités de l'app.

3.1.5 Cryptomonnaies

(i) Portefeuilles : les apps peuvent fournir un espace de stockage pour de la monnaie virtuelle, à condition qu'elles soient proposées par des développeurs inscrits en tant qu'organisations.

(ii) Minage : les apps ne peuvent pas miner de cryptomonnaies, sauf si ce processus est effectué hors de l'appareil (par exemple, minage dans le cloud).

(iii) Systèmes d'échange : les apps peuvent permettre d'effectuer des transactions ou des transmissions de cryptomonnaies via un système d'échange agréé, à condition que ces apps ne soient proposées que dans les pays ou régions où elles disposent des licences et autorisations adéquates pour fournir un échange de cryptomonnaies.

(iv) « Initial Coin Offerings » ou offre au public de jetons : les apps permettant d'effectuer des offres au public de jetons appelés aussi Initial Coin Offerings (ou ICO), des opérations de contrats à terme de cryptomonnaies et d'autres échanges de crypto-titres ou de quasi-titres doivent provenir de banques établies, de sociétés de valeurs mobilières, de Futures Commission Merchants (« FCM », commissionnaires sur les marchés à terme) ou d'autres institutions financières agréées, et doivent respecter toutes les lois en vigueur.

(v) Les apps de cryptomonnaies ne peuvent pas proposer de cryptomonnaie pour accomplir des tâches, comme télécharger d'autres apps, encourager d'autres personnes à télécharger, publier du contenu sur les réseaux sociaux, etc.

3.2 Autres problèmes liés au modèle commercial

Les listes suivantes ne sont pas exhaustives, et la soumission de votre app peut entraîner la modification ou la mise à jour de nos politiques. Voici certaines choses à faire et à éviter :

3.2.1 Utilisation acceptable

(i) Promouvoir l'achat ou le téléchargement de vos autres apps au sein de votre app, à condition que celle-ci ne soit pas un simple catalogue de vos apps.

(ii) Afficher ou recommander une collection d'apps tierces conçues pour un besoin approuvé spécifique (gestion de la santé, aviation, accessibilité, etc.). Votre app doit proposer un contenu rédactionnel solide pour ne pas ressembler à une simple vitrine.

(iii) Désactiver l'accès à un contenu de location approuvé spécifique (films, programmes télévisés, musique, livres, etc.) après l'expiration de la période de location. Tous les autres articles et services ne peuvent pas expirer.

(iv) Les cartes, billets et coupons de l'app Cartes peuvent être utilisés pour effectuer ou recevoir des paiements, transmettre des offres ou permettre une identification (par exemple des tickets de cinéma, des coupons et des identifiants VIP). D'autres utilisations peuvent entraîner le refus de l'app et la révocation des identifiants Cartes.

(v) Les apps d'assurance doivent être gratuites, conformes à la législation des régions dans lesquelles elles sont distribuées, et ne peuvent pas proposer d'achats intégrés.

(vi) Les organisations à but non lucratif approuvées peuvent collecter des fonds directement dans leurs propres apps ou dans des apps tierces, à condition que ces campagnes de collecte de fonds respectent toutes les directives sur la procédure App Review et proposent une assistance pour Apple Pay. Ces apps doivent communiquer la manière dont les fonds seront utilisés, respecter toutes les législations locales et nationales en vigueur, et garantir qu'une facture détaillée appropriée est mise à la disposition du donateur. Des informations supplémentaires seront transmises sur demande à l'équipe App Review. Les plateformes à but non lucratif qui mettent l'ensemble des donateurs en relation avec d'autres organisations à but non lucratif doivent s'assurer que chacune des organisations répertoriées dans l'app a également été soumise à la procédure de validation des organisations à but non lucratif. En savoir plus sur la marche à suivre pour devenir une [organisation à but non lucratif approuvée](#).

(vii) Les apps peuvent permettre aux utilisateurs individuels de faire un don en argent à une autre personne sans passer par les achats intégrés, à condition que (a) le don soit complètement volontaire, et que (b) l'intégralité du don soit versée au destinataire de celui-ci. Cependant, un don lié ou associé, à quelque moment que ce soit, à la réception de contenu ou de services numériques, doit passer par un achat intégré.

(viii) Les apps permettant d'effectuer des transactions financières, des investissements ou de gérer de l'argent doivent être soumises par l'établissement financier qui fournit ces services.

3.2.2 Utilisation inacceptable

(i) Créer une interface destinée à l'affichage d'apps, d'extensions ou de modules externes tiers similaire à l'App Store ou faisant office de collection d'intérêt général.

(ii) Intentionnellement omis.

(iii) Augmenter artificiellement le nombre d'impressions ou de clics sur les publicités, ainsi que les apps principalement destinées à l'affichage de publicités.

(iv) À moins que vous ayez le statut d'organisation à but non lucratif approuvée ou autorisée en vertu de la section 3.2.1 (vi) ci-dessus, lever des fonds au sein de l'app pour des organisations caritatives et des collectes de fonds. Les apps visant à lever des fonds pour de telles causes doivent être disponibles gratuitement sur l'App Store et peuvent uniquement collecter des fonds en dehors de l'app, par exemple par le biais de Safari ou par SMS.

(v) Restreindre arbitrairement l'utilisation de l'app à certains utilisateurs en fonction de leur emplacement géographique ou de leur opérateur.

(vi) Intentionnellement omis.

(vii) Manipuler artificiellement la visibilité, l'état ou le classement d'un utilisateur dans d'autres services, sauf autorisation accordée par les conditions générales d'utilisation du service en question.

(viii) Les apps qui permettent d'acheter et de vendre des options binaires ne sont pas autorisées sur l'App Store. Envisagez plutôt l'utilisation d'une app web. Les apps qui permettent d'acheter et de vendre des contrats pour la différence (« contracts for difference » ou CFD) ou autres services dérivés (par exemple, le FOREX) doivent être dûment agréées dans tous les pays où ces apps ou services sont distribués.

(ix) Les apps proposant des prêts personnels doivent indiquer de manière claire et visible toutes les conditions du prêt, y compris, sans toutefois s'y limiter, le taux d'intérêt annuel maximal correspondant et la date limite de paiement. Ces apps ne peuvent pas appliquer un taux d'intérêt annuel maximal supérieur à 36 % tous frais compris, et ne peuvent pas exiger le remboursement intégral dans un délai de 60 jours ou moins.

4. Conception

Les clients Apple attachent une grande importance aux produits simples, raffinés, innovants et simples à utiliser, et c'est exactement ce que nous souhaitons voir dans l'App Store. Vous êtes le seul responsable de la conception de votre app. Cependant, certaines normes minimales doivent être respectées afin que votre app soit acceptée dans l'App Store. Par ailleurs, n'oubliez pas que même une fois votre app approuvée, vous devez la mettre à jour afin qu'elle reste fonctionnelle et intéressante pour les clients nouveaux et existants. Les apps qui cessent de fonctionner ou qui offrent une expérience dégradée peuvent être supprimées de l'App Store à tout moment.

4.1 Plagiat

(a) Développez vos propres idées. Nous savons que vous en avez à revendre. À vous de les concrétiser. Ne vous contentez pas de copier la dernière app populaire sur l'App Store ou d'apporter quelques modifications mineures au nom ou à l'interface utilisateur d'une autre app pour la faire passer pour la vôtre. En plus de vous exposer à une plainte pour violation de la propriété intellectuelle, cela rend l'App Store plus difficile à parcourir et ce n'est pas juste pour les autres développeurs.

(b) ➡ L'envoi d'apps usurpant l'identité d'autres apps ou services est considéré comme une violation du code de conduite des développeurs et peut entraîner une exclusion de l'Apple Developer Program.

4.2 Fonctionnalités minimales

Votre app doit inclure des fonctionnalités, du contenu et une interface utilisateur qui la différencient d'un simple site web. Si votre app n'est pas particulièrement utile, unique ou adaptée au format d'app, elle n'a rien à faire sur l'App Store. Si votre app ne propose aucune forme de divertissement durable ou ne présente aucun intérêt pertinent, elle sera peut-être refusée. Les apps consistant uniquement en un morceau de musique ou un film doivent être soumises sur l'iTunes Store. Les apps consistant uniquement en un livre ou un guide de jeu doivent être soumises sur l'Apple Books Store.

4.2.1 Les apps utilisant ARKit doivent fournir des expériences de réalité augmentée riches et immersives. Le simple affichage d'un modèle en réalité augmentée ou la simple répétition d'une animation ne suffisent pas.

4.2.2 À part les catalogues, les apps ne doivent pas principalement consister en des supports marketing, des publicités, des découpages web, des agrégateurs de contenu ou une collection de liens.

4.2.3

(i) Votre app doit fonctionner de manière autonome, sans nécessiter l'installation d'une autre app.

(ii) Si votre app doit télécharger des ressources supplémentaires pour fonctionner au premier lancement, indiquez la taille du contenu à télécharger et prévenez les utilisateurs de ce téléchargement.

4.2.4 Intentionnellement omis.

4.2.5 Intentionnellement omis.

4.2.6 Les apps créées à partir d'un modèle commercialisé ou d'un service de génération d'app seront refusées, sauf si elles sont soumises directement par le fournisseur du contenu de l'app. Les fournisseurs de ces services ne doivent pas soumettre d'apps au nom de leur clientèle et doivent proposer à celle-ci des outils lui permettant de créer des apps personnalisées, innovantes et qui offrent des expériences uniques. Les fournisseurs de modèles peuvent opter pour une autre solution acceptable, à savoir créer un fichier binaire unique afin d'héberger tout le contenu du client dans un modèle de synthèse ou de « tri », comme une app de recherche de restaurants avec des entrées ou des pages personnalisées distinctes pour chaque restaurant du client, ou encore une app dédiée à l'évènementiel avec des entrées distinctes pour chaque événement du client.

4.2.7 Clients de bureau à distance

Si votre app de bureau à distance agit comme un miroir de logiciels ou de services spécifiques plutôt que comme un miroir générique de l'appareil hôte, elle doit respecter les obligations ci-dessous.

(a) L'app doit se connecter uniquement à un appareil hôte appartenant à l'utilisateur, à savoir un ordinateur personnel ou une console de jeu dédiée appartenant à l'utilisateur. L'appareil hôte et le client doivent être connectés à un réseau local (LAN).

(b) Tout logiciel ou service apparaissant dans le client doit être entièrement exécuté et affiché sur l'appareil hôte, et ne peut pas utiliser d'API ou de fonctionnalités de plateforme au-delà de ce qui est nécessaire pour diffuser en continu le bureau à distance.

(c) Toute action liée à la création et à la gestion de compte doit être effectuée à partir de l'appareil hôte.

(d) L'interface utilisateur visible dans le client ne doit ni s'apparenter à celle d'iOS ou de l'App Store, ni ressembler à l'interface d'une boutique. Elle ne doit pas permettre de parcourir, de sélectionner ou d'acheter des logiciels dont l'utilisateur n'est pas propriétaire ou ne possède pas la licence au préalable. Par souci de clarté, l'achat intégré n'est pas requis pour les transactions effectuées dans un logiciel en miroir, à condition que ces transactions soient traitées sur l'appareil hôte.

(e) Les clients légers utilisés pour les apps en cloud ne sont pas autorisés sur l'App Store.

4.3 Spam

(a) 🚫 Ne créez pas plusieurs identifiants de lot pour la même app. Si votre app se décline en plusieurs versions pour différents pays, équipes de sport, universités, etc., envisagez de soumettre une seule app et de proposer ses variantes sous forme d'achats intégrés.

(b) Évitez de contribuer à une catégorie déjà saturée. L'App Store comprend suffisamment d'apps de flatulence, de rot, de lampe torche, de voyance, de rencontre, de consommation d'alcool, de Kama Sutra, etc. Ces apps seront refusées sauf si elles offrent une expérience unique et de grande qualité. Spammer l'App Store peut entraîner votre exclusion de l'Apple Developer Program.

4.4 Extensions 🚫

Les apps hébergeant ou contenant des extensions doivent respecter le guide de programmation d'extension d'app [App Extension Programming Guide](#), la documentation sur les extensions d'app Safari [Safari App Extensions Documentation](#) ou la documentation sur les extensions web Safari [Safari Web Extensions Documentation](#) et proposer certaines fonctionnalités comme des écrans d'aide et des interfaces de réglages dans la mesure du possible. Vous devez indiquer de façon claire et précise les extensions disponibles dans le texte marketing de l'app. Par ailleurs, les extensions ne peuvent pas inclure de texte marketing, de messages publicitaires ou d'achats intégrés.

4.4.1 🚫 Les extensions de claviers sont soumises à des exigences supplémentaires.

Elles doivent :

- offrir une fonctionnalité de saisie de clavier (par exemple, les caractères saisis) ;
- respecter les directives relatives aux autocollants si le clavier comprend des images ou des emoji ;
- offrir un moyen d'accéder au clavier suivant ;
- rester fonctionnelles sans accès complet au réseau et sans nécessiter un accès complet ;
- collecter des données sur l'activité de tout utilisateur dans le seul but d'améliorer les fonctionnalités de l'extension de clavier de cette personne sur l'appareil iOS.

Elles ne doivent pas :

- lancer d'autres apps à l'exception de l'app Réglages ; ou
- réaffecter des touches du clavier à d'autres comportements (par exemple, maintenir la touche Retour pour lancer l'appareil photo).

4.4.2 Les extensions Safari doivent s'exécuter dans la version actuelle de Safari sous le système d'exploitation Apple approprié. Elles ne doivent pas interférer avec les éléments de l'interface utilisateur du système ou de Safari et ne doivent jamais inclure de contenu ou de code malveillant ou trompeur. Le non-respect de cette règle entraînera votre exclusion de l'Apple Developer Program. Les extensions Safari ne doivent pas demander l'accès à d'autres sites web que ceux strictement nécessaires à son fonctionnement.

4.4.3 Intentionnellement omis.

4.5 Sites et services Apple

4.5.1 Les apps peuvent utiliser des flux RSS Apple approuvés tels que le flux RSS iTunes Store, mais ne doivent ni extraire d'informations des sites Apple (comme le site apple.com, l'iTunes Store, l'App Store, App Store Connect, le portail de développement, etc.), ni créer de classements à l'aide de ces informations.

4.5.2 Apple Music

(i) MusicKit sous iOS permet à l'ensemble des utilisateurs de lire du contenu Apple Music et leur bibliothèque musicale locale en mode natif à partir de vos apps et jeux. Une fois que la personne a octroyé l'accès à son compte Apple Music, votre app lui permet de créer des playlists, d'ajouter des morceaux à sa bibliothèque et de lire tous les morceaux de son choix dans le catalogue Apple Music, qui contient des millions de morceaux. Les utilisateurs doivent pouvoir lancer la lecture en streaming d'un contenu Apple Music tout en naviguant à l'aide de commandes multimédias standard, comme « Lire », « Pause » et « Passer ». De plus, votre app ne doit pas exiger de paiement ou monétiser indirectement l'accès au service Apple Music (achats intégrés, publicités, demande d'informations d'utilisateur, etc.). Vous ne devez ni télécharger, ni charger, ni autoriser le partage de fichiers musicaux provenant des API MusicKit, sauf autorisation explicitement indiquée dans la documentation relative à [MusicKit](#).

(ii) Les API MusicKit ne constituent pas une méthode valable pour obtenir les licences dont vous pourriez avoir besoin pour une intégration musicale plus approfondie ou plus complexe. Par exemple, si vous souhaitez que votre app lance un morceau spécifique à un moment particulier, ou créer des fichiers audio ou vidéo pouvant être partagés sur les réseaux sociaux, vous devez contacter directement les titulaires des droits pour obtenir leur permission (à titre d'exemple, les droits de synchronisation ou d'adaptation). La pochette d'album et toute autre métadonnée peuvent être utilisées uniquement pour la lecture de musique ou des playlists (notamment les captures d'écran qui montrent les caractéristiques de votre app), et ne doivent pas être utilisées dans quelque contenu marketing ou publicitaire sans l'autorisation expresse des titulaires des droits. Assurez-vous de suivre les directives de la page [Apple Music Identity Guidelines](#) lorsque vous intégrez des services Apple Music à votre app.

(iii) L'accès aux données utilisateur d'Apple Music, comme leurs playlists ou leurs favoris, doit être clairement indiqué dans la description des apps qui utilisent de telles données. Aucune donnée collectée ne peut être partagée avec des tiers à d'autres fins que celles d'appuyer ou d'améliorer l'expérience fournie par l'app. Les données collectées ne peuvent pas être utilisées pour identifier des utilisateurs ou des appareils, ou pour envoyer de la publicité ciblée.

4.5.3 ➡ N'utilisez pas les services Apple pour mettre en place des campagnes de spam ou d'hameçonnage, ni pour envoyer des messages non sollicités aux utilisateurs et utilisatrices, y compris Game Center, les notifications push, etc. Ne tentez pas d'effectuer une recherche inversée, de tracer, relier, associer, extraire, recueillir ou exploiter autrement des identifiants de joueurs, des alias ou toute autre information obtenue par le biais de Game Center, ou nous procéderons à votre exclusion de l'Apple Developer Program.

4.5.4 ➡ Les notifications push ne doivent pas être nécessaires au fonctionnement de l'app et ne doivent pas servir à envoyer des informations personnelles ou confidentielles sensibles. Les notifications push ne doivent pas être utilisées à des fins de promotion ou de marketing direct, à moins que la clientèle n'ait explicitement accepté d'en recevoir par le biais d'une déclaration de consentement affichée dans l'interface utilisateur de votre app, et à moins que votre app contienne une option permettant de refuser de recevoir de tels messages. Toute utilisation abusive de ces services peut entraîner la révocation de vos privilèges.

4.5.5 ➡ Utilisez uniquement les identifiants de joueurs et de joueuses Game Center d'une manière autorisée par les conditions de Game Center. Ne les affichez pas dans l'app et ne les divulguez pas à des tiers.

4.5.6 ➡ Les apps et leurs métadonnées peuvent contenir des caractères Unicode générant des emoji Apple. Les emoji Apple ne peuvent pas être utilisés sur d'autres plateformes ou intégrés directement dans le fichier binaire de votre app.

4.6 Icônes d'apps alternatives ➡

Les apps peuvent afficher des icônes personnalisées dans le but, par exemple, de montrer une préférence pour une équipe sportive, à condition que chaque modification soit initiée par l'utilisateur et que l'app intègre des réglages permettant de revenir à l'icône d'origine. Toutes les variantes d'icône doivent se rapporter au contenu de l'app, et les modifications apportées doivent se répercuter sur tous les éléments du système, de sorte que les icônes affichées dans Réglages, Notifications, etc. correspondent à la nouvelle icône du springboard.

4.7 Mini apps, mini jeux, jeux en streaming, chatbots, modules et émulateurs de jeux

Les apps peuvent proposer des logiciels qui ne sont pas intégrés dans le fichier binaire, en particulier des mini apps et mini jeux au format HTML5, des jeux en streaming, des chatbots et des modules. De plus, les apps d'émulation de console de jeux rétro peuvent proposer le téléchargement de jeux. Vous êtes responsable de tous ces logiciels proposés dans votre app, et notamment de leur conformité aux présentes directives et à toutes les lois applicables. Les logiciels qui ne sont pas conformes à une ou plusieurs directives entraîneront le refus de votre app. Vous devez également vous assurer que le logiciel respecte les règles supplémentaires qui suivent dans les articles 4.7.1 et 4.7.5. Ces règles supplémentaires sont importantes pour préserver l'expérience attendue par les clients de l'App Store et pour garantir la sécurité des utilisateurs et utilisatrices.

4.7.1 Les logiciels proposés dans les apps qui sont soumises à cette règle doivent :

- suivre toutes les directives en matière de confidentialité, y compris, mais sans s'y limiter, les règles énoncées dans la directive 5,1 concernant la collecte, l'utilisation et le partage de données, notamment des données sensibles (telles que les données de santé et les données personnelles des enfants) ;
- inclure une méthode de filtrage de contenus répréhensibles, un mécanisme de signalement du contenu et des réponses rapides aux préoccupations, ainsi que la possibilité de bloquer les utilisateurs et utilisatrices abusifs ; et
- utiliser les achats intégrés pour proposer des biens ou des services numériques aux utilisateurs et utilisatrices finaux.

4.7.2 Votre app ne peut pas étendre ou exposer les API de la plateforme native au logiciel sans l'autorisation préalable d'Apple.

4.7.3 Votre app ne peut pas partager de données ou d'autorisations de confidentialité avec des logiciels individuels proposés dans votre app sans le consentement explicite de l'utilisateur ou de l'utilisatrice dans chaque cas.

4.7.4 Vous devez fournir un index des logiciels et des métadonnées disponibles dans votre app. Il doit inclure des liens universels qui mènent à tous les logiciels proposés dans votre app.

4.7.5 Votre app doit indiquer la classe d'âge du contenu qui présente la classe d'âge la plus élevée disponible dans votre application.

4.8 Services de connexion ↪

Les apps qui utilisent un service de connexion tiers ou de réseau social (comme les services de connexion avec Facebook, Google, Twitter, LinkedIn, Amazon ou WeChat) pour configurer ou authentifier le compte principal d'une personne doivent également proposer, comme option équivalente, un autre service de connexion présentant les fonctionnalités suivantes :

- le service de connexion limite la collecte des données au nom et à l'adresse e-mail de l'utilisateur ou de l'utilisatrice ;
- le service de connexion permet aux utilisateurs et utilisatrices de garder leur adresse e-mail confidentielle lors de la configuration de leur compte et
- le service de connexion ne collecte pas les interactions avec votre app à des fins publicitaires sans consentement.

Le compte principal d'une personne désigne le compte qu'elle crée auprès de votre app pour s'identifier, se connecter et accéder à vos fonctionnalités et services associés.

Un autre service de connexion n'est pas requis si :

- Votre app utilise exclusivement les systèmes de configuration de compte et de connexion détenus par votre entreprise.

- Votre app est un autre marché d'apps, ou une app distribuée à partir d'un autre marché d'apps, qui utilise une connexion spécifique au marché pour les fonctionnalités de compte, de téléchargement et de commerce.
- Votre app est axée sur l'éducation, l'entreprise ou l'économie et nécessite qu'une personne se connecte à l'aide d'un compte d'éducation ou d'entreprise existant.
- Votre app se sert d'un système d'identification des citoyens approuvé par le gouvernement ou le secteur ou d'un document d'identité électronique pour authentifier les utilisateurs.
- Votre app est le client d'un service tiers spécifique, et tout utilisateur doit se connecter directement à son compte de messagerie, son compte de réseaux sociaux ou à un autre compte tiers pour accéder à son contenu.

4.9 Apple Pay

Les apps utilisant Apple Pay doivent fournir à l'utilisateur ou à l'utilisatrice toutes les informations pertinentes concernant l'achat avant la vente d'un bien ou d'un service et doivent utiliser la marque et les éléments de l'interface utilisateur Apple Pay de manière appropriée, conformément aux pages Apple Pay Marketing Guidelines (Directives sur le marketing d'Apple Pay) et Human Interface Guidelines (Directives d'interface humaine). Au minimum, les apps utilisant Apple Pay pour proposer des paiements récurrents doivent fournir les informations suivantes :

- La durée de la période de renouvellement et le fait que le renouvellement sera poursuivi jusqu'à son annulation
- Ce qui sera fourni durant chaque période
- Les frais facturés au client
- La procédure d'annulation

4.10 Monétisation des fonctionnalités intégrées

Vous n'êtes pas autorisé à monétiser des fonctionnalités intégrées fournies par le matériel ou le système d'exploitation (par exemple, les notifications push, l'appareil photo ou le gyroscope), ou par des services et des technologies Apple (par exemple, l'accès à Apple Music, le stockage iCloud ou les API de temps d'écran).

5. Aspects juridiques

Les apps doivent respecter toutes les obligations légales en vigueur dans les pays où elles sont disponibles (en cas de doute, consultez un avocat). Tout cela peut paraître compliqué, mais vous êtes tenu de comprendre vos obligations et de vous assurer que votre app est conforme à la législation locale, et pas uniquement aux directives ci-dessous. Bien évidemment, les apps qui sollicitent, promeuvent ou encouragent un comportement criminel ou clairement irresponsable seront refusées. Dans les cas extrêmes où nous découvrons par exemple des apps qui facilitent la traite d'êtres humains et/ou l'exploitation d'enfants, les autorités compétentes seront informées.

5.1 Confidentialité ↻

La protection de la vie privée de l'ensemble des utilisateurs et des utilisatrices est essentielle dans l'écosystème Apple, et vous devez traiter les données personnelles avec précaution afin de vous assurer de respecter les [bonnes pratiques en matière de confidentialité](#), les lois en vigueur et les conditions du [contrat de licence de l'Apple Developer Program](#), sans oublier les attentes de la clientèle. Plus précisément :

5.1.1 Collecte et stockage des données ↻

(i) Politiques de confidentialité : toutes les apps doivent contenir un lien vers leur politique de confidentialité. Ce lien doit être facilement accessible et figurer au sein même de l'app ainsi que dans le champ de métadonnées d'App Store Connect. La politique de confidentialité doit clairement et explicitement :

- indiquer les données collectées, le cas échéant, par l'app ou le service, la manière dont ces données sont collectées et toutes les utilisations qui en sont faites ;
- garantir que tout tiers avec lequel une app partage des données utilisateur (conformément à ces directives), comme les outils d'analyse, les réseaux publicitaires et les SDK tiers, ainsi que toute société mère, filiale ou autre entité liée qui aura accès à ces données, assurera une protection des données utilisateur identique ou égale à celle énoncée dans la politique de confidentialité de l'app et exigée par les présentes directives ;
- expliquer ses politiques de conservation/suppression des données et décrire la manière dont une personne peut révoquer son consentement et/ou demander la suppression de ses données.

(ii) Autorisation : les apps qui collectent des données utilisateur ou d'utilisation doivent obtenir l'autorisation de la personne concernée pour collecter ces données, même si celles-ci sont considérées comme anonymes au moment de la collecte ou immédiatement après. Les fonctionnalités payantes ne doivent ni dépendre de ces données, ni en exiger l'accès auprès d'un utilisateur. Les apps doivent également permettre à la clientèle de retirer leur consentement de façon simple et compréhensible. Assurez-vous que vos chaînes d'objet décrivent de façon claire et exhaustive l'utilisation que vous ferez des données. Les apps qui collectent sans consentement des données pour un intérêt légitime en s'appuyant sur les conditions du Règlement général sur la protection des données (RGPD) de l'Union européenne ou d'une loi similaire doivent se conformer à toutes les conditions de cette loi. En savoir plus sur les [demandes d'autorisation](#).

(iii) Collecte minimale de données : les apps ne doivent demander l'accès qu'aux données nécessaires à leur fonctionnalité principale et doivent collecter et utiliser uniquement les données nécessaires pour exécuter une tâche pertinente. Dans la mesure du possible, utilisez le sélecteur hors processus ou une feuille de partage au lieu de demander un accès complet à des ressources protégées comme Photos ou Contacts.

(iv) Accès : les apps doivent respecter les réglages définis par l'utilisateur en matière d'autorisation et ne pas tenter de manipuler, de tromper ou de contraindre une personne de sorte qu'elle autorise l'accès à des données inutiles. Par exemple, les apps qui offrent la possibilité de publier des photos sur un réseau social ne doivent pas également exiger l'accès au micro avant de permettre à la

personne de charger des photos. Dans la mesure du possible, proposez des solutions alternatives aux personnes qui refusent de donner leur accord. Par exemple, si une personne refuse de partager sa position géographique, offrez-lui la possibilité de saisir manuellement une adresse.

(v) Connexion à un compte : si votre app ne comporte pas de fonctionnalités importantes nécessitant un compte, donnez la possibilité aux personnes d'en profiter sans identifiant. Si votre app offre la possibilité de créer un compte, elle doit également [permettre de supprimer un compte existant](#). Les apps ne peuvent pas exiger que les utilisateurs saisissent des informations personnelles, sauf lorsque celles-ci sont directement liées aux fonctionnalités principales de l'app ou sont requises par les lois en vigueur. Si la fonctionnalité principale de votre app n'est pas liée à un réseau social distinct (ex. : Facebook, WeChat, Weibo, X, etc.), vous devez proposer un accès sans identifiant ou par le biais d'un autre mécanisme. La récupération d'informations de profil de base, le partage de contenu sur les réseaux sociaux ou l'invitation de proches à utiliser l'app ne sont pas des actions considérées comme des fonctionnalités principales d'une app. L'app doit également intégrer un mécanisme permettant de révoquer les informations d'identification du réseau social et de désactiver l'accès aux données entre l'app et le réseau social depuis l'app elle-même. Une app ne peut pas stocker d'informations d'identification ou de jetons en lien avec des réseaux sociaux en dehors de l'appareil et ne peut utiliser ces informations d'identification ou jetons que pour se connecter directement au réseau social à partir de l'app elle-même pendant que celle-ci est utilisée.

(vi) Les développeurs qui se servent de leurs apps pour collecter subrepticement des mots de passe ou d'autres données privées seront exclus de l'Apple Developer Program.

(vii) SafariViewController doit être utilisé pour présenter visuellement des informations aux utilisateurs ; le contrôleur ne doit être ni caché ni obscurci par d'autres vues ou d'autres couches. Par ailleurs, une app ne doit pas se servir de SafariViewController pour suivre les personnes sans leur accord et sans les informer au préalable.

(viii) Les apps qui compilent des informations personnelles à partir de toute source ne provenant pas directement de l'utilisateur ou sans son consentement explicite, même les bases de données publiques, ne sont pas autorisées sur l'App Store ou sur les magasins d'apps alternatifs.

(ix) Les apps qui fournissent des services dans des domaines strictement réglementés (comme les services bancaires et financiers, la santé, les jeux d'argent, la consommation légale de cannabis et le transport aérien) ou qui nécessitent des informations sensibles sur l'utilisateur doivent être soumises par une entité juridique qui fournit les services, et non par un développeur. Les apps qui permettent la vente légale de cannabis ne doivent être disponibles que dans les pays autorisant cette activité.

(x) Les apps peuvent demander des coordonnées de base (comme le nom ou l'adresse e-mail) tant que la demande est facultative pour l'utilisateur, que les fonctionnalités et les services ne sont pas subordonnés à la communication de ces informations et que l'app respecte toutes les autres dispositions de ces directives, y compris les restrictions concernant la collecte d'informations auprès des enfants.

5.1.2 Utilisation et partage des données ↩️

(i) Sauf autorisation légale, vous ne pouvez pas utiliser, transmettre ni partager les données personnelles d'un individu sans avoir obtenu son accord au préalable. Vous devez donner accès à des informations concernant la manière et l'endroit où ces données seront utilisées. Les données collectées par le biais d'app peuvent être partagées avec des tiers uniquement pour améliorer l'app ou diffuser des publicités (conformément au [contrat de licence de l'Apple Developer Program](#)). Pour suivre l'activité de tout utilisateur, vous devez au préalable obtenir son autorisation explicite via les API dédiées à la transparence du suivi des apps. En savoir plus sur le [suivi](#). Votre app ne doit pas obliger les utilisateurs à activer des fonctionnalités du système (par exemple, les notifications push, le service de localisation, le suivi) pour accéder à des fonctionnalités et du contenu, utiliser l'app ou recevoir une compensation financière ou toute autre forme de compensation, y compris, sans toutefois s'y limiter, des cartes et codes cadeaux. Les apps qui partagent les données utilisateur sans consentement ou sans respecter les lois sur la confidentialité des données peuvent être retirées de la vente et peuvent entraîner votre exclusion de l'Apple Developer Program.

(ii) Les données collectées dans un but précis ne peuvent être réutilisées sans le consentement des personnes concernées, sauf si la loi l'autorise expressément.

(iii) Les apps ne doivent ni tenter d'établir subrepticement un profil utilisateur sur la base de données collectées, ni inciter ou encourager d'autres personnes à identifier des utilisateurs ou utilisatrices anonymes ou à reconstituer des profils utilisateur sur la base de données collectées à partir des API fournies par Apple ou de données qui, selon vos affirmations, ont été collectées de manière « anonyme », « agrégée » ou d'une toute autre manière non identifiable.

(iv) N'utilisez pas d'informations provenant de Contacts, Photos ou d'autres API qui accèdent aux données utilisateur en vue de créer une base de données de contacts pour votre propre usage ou pour la vente/distribution à des tiers, et ne collectez pas d'informations sur les autres apps installées sur l'appareil d'un utilisateur ou d'une utilisatrice à des fins d'analyse ou publicitaires/marketing.

(v) Ne contactez personne en vous servant d'informations collectées via l'app Contacts ou Photos d'un utilisateur, sauf sur demande explicite de cette personne ; n'intégrez pas d'option Sélectionner tout ou d'option de sélection de tous les contacts par défaut. Vous devez fournir à l'utilisateur une description claire du message que le destinataire verra avant de l'envoyer (par exemple, « Que dira le message ? » ou « Qui sera l'expéditeur ? »).

(vi) Les données recueillies depuis l'API HomeKit, HealthKit, l'API Clinical Health Records, les API MovementDisorder, ClassKit ou les outils de cartographie de profondeur et/ou de reconnaissance faciale (comme ARKit, les API Appareil photo ou Photos) ne peuvent pas être utilisées à des fins marketing, publicitaires ou d'exploration de données d'utilisation (« data mining »), y compris par des tiers. En savoir plus sur les bonnes pratiques à suivre pour mettre en place [CallKit](#), [HealthKit](#), [ClassKit](#) et [ARKit](#).

(vii) Les apps utilisant Apple Pay peuvent partager avec des tiers des données utilisateur obtenues via Apple Pay dans le seul but de faciliter ou d'améliorer la mise à disposition de biens et de services.

5.1.3 Santé et recherche médicale ↗

Les données sur la santé, sur la forme physique et médicales sont particulièrement sensibles. Les apps collectant de telles données doivent satisfaire à des exigences supplémentaires afin de garantir la protection de la vie privée de la clientèle :

(i) Les apps ne peuvent ni utiliser ni divulguer à des tiers des données collectées dans le cadre de la recherche médicale, sur la santé et la forme physique (notamment par le biais des API Clinical Health Records, HealthKit, Motion and Fitness, MovementDisorder ou d'une recherche médicale réalisée sur des sujets humains) à des fins publicitaires, de marketing ou d'exploration de données d'utilisation, ou à des fins autres que pour l'amélioration de la gestion de la santé ou la recherche médicale, et ce, uniquement sur autorisation. Les apps peuvent toutefois se servir des données relatives à la santé ou à la forme physique d'un utilisateur pour lui fournir directement un avantage (comme une réduction de prime d'assurance), à condition que l'app soit soumise par l'entité fournissant cet avantage et que les données ne soient partagées avec aucun tiers. Vous devez indiquer précisément les données de santé que vous recueillez à partir de l'appareil.

(ii) Les apps ne doivent pas écrire de données erronées ou inexactes dans HealthKit ou toute autre app de recherche médicale ou de gestion de la santé, et ne peuvent stocker d'informations de santé personnelles dans iCloud.

(iii) Les apps servant à la recherche médicale sur des sujets humains doivent obtenir le consentement des participants, ou des parents ou tuteurs s'il s'agit de mineurs. Un tel consentement doit inclure (a) la nature, l'objectif et la durée de la recherche ; (b) les procédures, les risques et les avantages pour les participants ; (c) des informations sur la confidentialité et le traitement des données (y compris tout partage avec des tiers) ; (d) un point de contact pour les questions des participants ; et (e) la procédure de rétractation.

(iv) Les apps servant à la recherche médicale sur des sujets humains doivent obtenir l'approbation d'un comité de déontologie indépendant. La preuve d'une telle approbation doit être fournie sur demande.

5.1.4 Enfants

(a) ↗ Il est essentiel de traiter les données personnelles des enfants avec précaution pour de nombreuses raisons. Nous vous encourageons à consulter soigneusement toutes les exigences prévues de conformité à des lois telles que le Children's Online Privacy Protection Act (COPPA), le Règlement général sur la protection des données (RGPD) de l'Union européenne ainsi que toute autre réglementation ou loi applicables.

Les apps peuvent demander la date de naissance et les coordonnées des parents dans le seul but de se conformer à ces lois, mais doivent inclure des fonctionnalités utiles ou offrir un divertissement, quel que soit l'âge de l'utilisateur.

Les apps destinées principalement aux enfants ne doivent pas contenir de publicités ou d'analyses tierces. Ces règles permettent de garantir une expérience plus sûre pour les enfants.

(b) Dans certains cas, les analyses et publicités tierces peuvent être autorisées, à condition que les services respectent les mêmes conditions que celles énoncées dans la [directive 1.3](#).

De plus, les apps de la catégorie Enfants ou celles qui collectent, transmettent ou sont capables de partager les informations personnelles (nom, adresse postale, adresse e-mail, localisation, photos, vidéos, dessins, conversations, autres données personnelles ou identifiants permanents utilisés en association avec l'un des éléments précédents) d'une personne mineure doivent intégrer une politique de confidentialité et respecter toutes les lois en vigueur sur la protection de la vie privée des enfants. Dans un souci de clarté, [l'exigence relative aux barrières parentales](#) pour les apps de la catégorie Enfants doit en règle générale être distinguée de l'obtention du consentement des parents pour la collecte de données personnelles en vertu de ces lois sur la protection de la vie privée.

Pour rappel, la [directive 2.3.8](#) exige que l'utilisation de termes tels que « Pour les enfants » et « Pour les petits » dans les métadonnées de l'application soit réservée à la catégorie Enfants. Les apps qui n'appartiennent pas à la catégorie Enfants ne peuvent pas inclure dans leur nom, leur sous-titre, leur icône, leurs captures d'écran ou leur description des termes qui laissent entendre que les enfants constituent leur public principal.

5.1.5 Service de localisation 📍

N'utilisez le service de localisation dans votre app que lorsqu'il est directement lié aux fonctionnalités et aux services proposés par l'app. Les API fondées sur la localisation ne doivent pas être utilisées pour fournir des services d'urgence ou permettre le contrôle autonome de véhicules, d'avions et d'autres appareils, sauf pour les petits appareils tels que les drones et les jouets légers, les systèmes d'alarme de voitures liés à une télécommande, etc. Assurez-vous d'informer les parties prenantes et d'obtenir un consentement avant de collecter, transmettre ou utiliser des données de localisation. Si votre app utilise le service de localisation, assurez-vous d'expliquer pourquoi. Reportez-vous à la page [Human Interface Guidelines](#) (Directives d'interface humaine) pour connaître les bonnes pratiques en la matière.

5.2 Propriété intellectuelle

Assurez-vous que votre app inclut uniquement du contenu que vous avez créé ou pour lequel vous possédez une licence d'utilisation. Votre app peut être supprimée si vous avez dépassé les limites et utilisé du contenu sans obtenir les autorisations nécessaires. De la même manière, cela signifie que les apps appartenant à une autre personne et ayant « emprunté » votre travail sans autorisation peuvent être supprimées. Si vous estimez que vos droits de propriété intellectuelle ont été enfreints par un autre développeur sur l'App Store, envoyez une réclamation par le biais de notre [formulaire web](#). Les lois diffèrent en fonction des pays et régions, mais assurez-vous au moins d'éviter les erreurs les plus courantes :

5.2.1 De façon générale : n'utilisez pas de contenu protégé appartenant à des tiers, comme des marques, des œuvres protégées par des droits d'auteur ou des idées brevetées dans votre app sans autorisation, et n'incluez pas de représentations, noms ou métadonnées trompeurs, erronés ou plagés dans votre lot d'apps ou dans votre nom de développeur. Les apps doivent être soumises par la personne ou l'entité juridique qui détient ou a mis sous licence les droits de propriété intellectuelle et tout autre droit concerné.

5.2.2 Sites/Services tiers : si votre app utilise, accède à, monétise l'accès à, ou affiche du contenu provenant d'un service tiers, assurez-vous d'avoir l'autorisation expresse de le faire en vertu des conditions d'utilisation du service. Cette autorisation doit être fournie sur demande.

5.2.3 Téléchargement audio/vidéo : les apps ne doivent pas encourager le partage illégal de fichiers ni offrir la possibilité d'enregistrer, de convertir ou de télécharger des fichiers multimédias provenant de sources tierces (comme Apple Music, YouTube, SoundCloud, Vimeo, etc.) sans l'autorisation expresse de ces dernières. La diffusion en streaming de contenu audio/vidéo peut également enfreindre les conditions d'utilisation. Assurez-vous que ce n'est pas le cas avant de permettre à votre app d'accéder à ces services. Cette autorisation doit être fournie sur demande.

5.2.4 Approbation d'Apple :

(a) Ne suggérez pas qu'Apple est une source ou un fournisseur de l'app, ou qu'Apple approuve une déclaration spécifique concernant la qualité ou les fonctionnalités de l'app.

(b) Si votre app est sélectionnée comme « Sélection de la rédaction », Apple appliquera automatiquement le badge correspondant.

5.2.5 Produits Apple Ne créez pas une app qui ressemble à s'y méprendre à un produit Apple, une interface (comme le Finder), une app (comme l'App Store, l'iTunes Store ou Messages) ou un thème publicitaire qui existe déjà. Les apps et les extensions, notamment les claviers et packs d'autocollants tiers, ne peuvent pas inclure d'emoji Apple. Les morceaux d'iTunes et les extraits de morceaux d'Apple Music ne doivent pas être utilisés à des fins de divertissement (par exemple, comme musique de fond d'un collage photo ou bande-son d'un jeu) ou de toute autre manière non autorisée. Si vous fournissez des extraits de morceaux d'iTunes ou d'Apple Music, vous devez inclure un lien redirigeant vers le morceau en question dans iTunes ou Apple Music. Si votre app affiche des anneaux Activité, elle ne doit pas permettre de visualiser les données Bouger, M'entraîner ou Me lever d'une manière semblable à la commande Activité. Consultez la page [Human Interface Guidelines](#) (Directives d'interface humaine) pour plus d'informations sur l'utilisation des anneaux Activité. Si votre app affiche les données de Météo d'Apple, elle doit respecter les exigences d'attribution détaillées dans la [documentation WeatherKit](#).

5.3 Jeux, jeux d'argent et loteries

Les jeux, jeux d'argent et loteries peuvent être délicats à gérer et constituent généralement les offres les plus réglementées sur l'App Store. N'incluez ces fonctionnalités que si vous avez pris connaissance de vos obligations légales dans les pays dans lesquels votre app est disponible et si vous êtes prêt à ce que la procédure de vérification de votre app prenne plus de temps. Voici quelques points à garder à l'esprit :

5.3.1 Tout développeur d'une app doit sponsoriser les tirages au sort et les concours.

5.3.2 Les règles officielles des tirages au sort, des concours et des tombolas doivent figurer dans l'app. Il doit être clairement indiqué qu'Apple n'agit ni à titre de sponsor, ni à titre de participant.

5.3.3 Les apps ne doivent pas utiliser les achats intégrés pour permettre l'achat de crédits ou de devises à utiliser avec des jeux en argent réel.

5.3.4 Les apps proposant des jeux d'argent réel (notamment les paris sportifs, poker, jeux de casino, courses de chevaux, etc.) ou des loteries doivent posséder les licences et les autorisations nécessaires dans les pays où elles sont utilisées, être limitées géographiquement à ces pays et être disponibles gratuitement sur l'App Store. Les aides aux jeux d'argent illégaux, notamment les compteurs de cartes, sont interdites dans l'App Store. Les apps de loterie doivent avoir une contrepartie, s'appuyer sur le hasard et proposer des gains.

5.4 Apps VPN ↻

Les apps proposant des services VPN doivent utiliser [l'API NEVPNManager](#) et ne peuvent être proposées que par des développeurs inscrits en tant qu'organisations. Vous devez indiquer clairement sur un écran de l'app quelles données seront collectées et comment elles seront utilisées avant que l'utilisateur n'achète ou n'utilise le service. Les apps proposant des services VPN ne peuvent vendre, utiliser ou divulguer aucune donnée à des tiers à quelque fin que ce soit, et doivent s'y engager dans leur politique de confidentialité. Les apps VPN ne doivent pas enfreindre la législation locale, et si vous choisissez de mettre votre app VPN à disposition sur un territoire qui exige une licence VPN, vous devez renseigner les informations relatives à votre licence dans le champ des notes destinées à l'équipe App Review. Les apps de contrôle parental, de blocage de contenu et de sécurité, entre autres, provenant de fournisseurs agréés peuvent également utiliser l'API NEVPNManager. Les apps qui ne respectent pas cette directive seront supprimées de l'App Store et bloquées pour être installées par d'autres moyens de distribution, et pourront entraîner votre exclusion de l'Apple Developer Program.

5.5 Gestion des appareils mobiles ↻

Les apps de gestion des appareils mobiles qui proposent des services de gestion des appareils mobiles (ou MDM) doivent en demander l'autorisation à Apple. Ces apps ne peuvent être proposées que par des entreprises commerciales, des établissements d'enseignement ou des organismes du secteur public et, dans certains cas, par des entreprises qui s'appuient sur la gestion des appareils mobiles pour fournir des services de contrôle parental ou assurer la sécurité des appareils. Vous devez indiquer clairement sur un écran de l'app quelles données seront collectées et comment elles seront utilisées avant que l'utilisateur n'achète ou n'utilise le service. Les apps MDM ne doivent pas enfreindre la législation en vigueur. Les apps proposant des services MDM ne peuvent vendre, utiliser ou divulguer aucune donnée à des tiers à quelque fin que ce soit, et doivent s'y engager dans leur politique de confidentialité. Dans certains cas, les analyses tierces peuvent être autorisées, à condition que les services ne collectent ou ne transmettent que des données sur les performances de l'app MDM du développeur, et non des données sur l'utilisateur, son appareil ou d'autres apps utilisées sur cet appareil. Les apps proposant des profils de configuration doivent également respecter ces exigences. Les apps qui ne respectent pas cette directive seront supprimées de l'App Store et bloquées pour être installées par d'autres moyens de distribution, et pourront entraîner votre exclusion de l'Apple Developer Program.

5.6 Code de conduite des développeurs ↻

Veillez traiter tout le monde avec respect, que ce soit dans vos réponses aux avis laissés sur l'App Store, pour les demandes d'assistance formulées par la clientèle ou dans vos communications avec Apple, notamment les réponses que vous apportez dans App Store Connect. Ne vous livrez pas à des actes de harcèlement de quelque nature que ce soit. Évitez toute pratique discriminatoire, d'intimidation ou de persécution, et n'encouragez pas d'autres personnes à se livrer à de telles pratiques. Un comportement manipulateur ou trompeur répété ou tout autre comportement frauduleux entraînera votre exclusion de l'Apple Developer Program.

La confiance des clients est un élément indispensable à l'écosystème d'apps. Les apps ne doivent jamais exploiter les utilisateurs ou tenter d'escroquer la clientèle, les inciter à effectuer des achats non désirés, les contraindre à partager des données inutiles, augmenter les prix de manière insidieuse, faire payer des fonctionnalités ou du contenu qui n'existent pas, ou se livrer à toute autre pratique de manipulation au sein de l'app ou en dehors.

Votre compte Developer Program sera suspendu si vous vous livrez à des activités ou à des actions qui ne respectent pas le code de conduite des développeurs. Pour rétablir votre compte, vous pouvez fournir une déclaration écrite détaillant les améliorations que vous comptez apporter. Si Apple approuve votre projet et que nous pouvons confirmer que les modifications ont bien été appliquées, votre compte pourra éventuellement être rétabli.

5.6.1 Avis dans l'App Store

Les avis laissés par les clients dans l'App Store peuvent faire partie intégrante de l'expérience fournie par l'app. C'est pourquoi vous devez traiter les personnes avec respect lorsque vous répondez à leurs commentaires. Vos réponses doivent se concentrer sur les commentaires de l'utilisateur et ne pas contenir de renseignements personnels, de spam ou d'informations marketing.

Utilisez l'API fournie pour inviter tout utilisateur à laisser un avis sur votre app. Cette fonctionnalité leur permet de donner une note et de rédiger un avis dans l'App Store, et ce sans avoir besoin de quitter votre app. Nous refuserons les invitations à rédiger un avis personnalisées.

5.6.2 Identité du développeur ↗

Il est essentiel que vous communiquiez des informations vérifiables à Apple et à la clientèle afin que celle-ci vous accorde toute sa confiance. Vous devez vous présenter vous même, présenter votre entreprise et vos offres avec exactitude sur l'App Store ou sur d'autres plateformes d'apps. Les informations que vous fournissez doivent être véridiques, pertinentes et à jour afin qu'Apple et la clientèle sachent qui vous êtes et puissent vous contacter en cas de problème.

5.6.3 Fraude liée aux fonctionnalités de découverte

Pour participer à l'App Store, vous devez faire preuve d'intégrité et vous engager à nouer et entretenir une relation de confiance avec la clientèle. La manipulation de tout élément de l'expérience clientèle sur l'App Store, comme les classements, la recherche, les avis ou les recommandations dirigées vers votre app, mine la confiance de la clientèle et n'est pas autorisée.

5.6.4 Qualité des apps

Les attentes des clients à l'égard de l'App Store sont très élevées, et le fait de leur proposer en permanence du contenu, des services et des expériences de grande qualité contribue à renforcer leur confiance. Certains signes indiquent que cette attente n'est pas satisfaite, notamment un nombre excessif de signalements de problèmes liés à votre app, comme des avis négatifs, et un nombre excessif de demandes de remboursement. L'incapacité à maintenir un niveau de qualité élevé peut nous aider à déterminer si un développeur respecte ou non le code de conduite des développeurs.

Une fois votre app soumise

Une fois que vous avez soumis votre app et vos métadonnées dans App Store Connect et que la procédure de vérification est en cours, voici quelques points à garder à l'esprit :

- **Délai** : l'équipe App Review examinera votre app dès que possible. Toutefois, si votre app est complexe ou présente de nouveaux problèmes, elle peut nécessiter un examen plus approfondi. Par ailleurs, n'oubliez pas que si votre app est refusée à plusieurs reprises parce qu'elle enfreint la même directive ou parce que vous avez tenté de manipuler la procédure de vérification des apps, l'évaluation de votre app prendra plus de temps. En savoir plus sur la [procédure de vérification des apps](#).
- **Informations sur l'état** : l'état actuel de votre app est indiqué dans App Store Connect pour vous permettre de le surveiller facilement.
- **Demande de vérification accélérée** : si vous rencontrez un problème de délai critique, vous pouvez [demander une vérification accélérée de votre app](#). Respectez les autres développeurs et demandez une vérification accélérée uniquement si vous en avez réellement besoin. Si nous découvrons que vous abusez de ce système, nous pourrions refuser vos futures demandes.
- **Date de sortie** : votre app n'apparaîtra pas sur l'App Store avant la date de sortie prévue, même si elle a été approuvée par l'équipe App Review. Rappelez-vous qu'un délai de 24 heures peut s'écouler avant que votre app n'apparaisse dans tous les Stores sélectionnés.
- **Refus** : notre objectif est d'appliquer ces directives de manière juste et cohérente, mais personne n'est parfait. Si votre app a été refusée et que vous avez des questions ou souhaitez fournir des informations supplémentaires, veuillez passer par App Store Connect pour communiquer directement avec l'équipe App Review. Cela pourra éventuellement nous aider à intégrer votre app à l'App Store, à améliorer la procédure de vérification des apps ou à déterminer si nos politiques doivent être clarifiées.
- **Procédures d'appels** : si vous n'êtes pas d'accord avec la décision découlant de notre évaluation, veuillez [faire appel](#). Cela pourra éventuellement nous aider à intégrer votre app à l'App Store. Vous pouvez également [suggérer des modifications à apporter aux directives](#) elles-mêmes pour nous aider à améliorer la procédure de vérification des apps ou à déterminer si nos politiques doivent être clarifiées.
- **Procédure d'envoi de correctifs** : pour les apps qui se trouvent déjà sur l'App Store ou sur un autre marché d'apps, les correctifs ne subiront pas de retards en raison d'infractions aux directives, à l'exception de celles liées à des problèmes juridiques ou de sécurité. Si votre app a été refusée et qu'elle répond aux critères de cette procédure, veuillez passer par App Store Connect pour communiquer directement avec l'équipe App Review afin de lui indiquer que vous souhaitez avoir recours à cette procédure et que vous comptez corriger le problème lors de votre prochain envoi.

Nous avons hâte de découvrir vos prochaines apps !

Dernière mise à jour : [5 avril 2024](#)