Règlement du programme pour les développeurs (à compter du 1er octobre 2020)

Créons ensemble le site de jeux et d'applications le plus fiable au monde

Notre réussite commune repose sur vos innovations, qui entraînent inévitablement des responsabilités. Le Règlement du programme pour les développeurs, ainsi que le Contrat relatif à la distribution (pour les développeurs), nous permettent de continuer à proposer, ensemble, les applications les plus innovantes et fiables du monde à plus d'un milliard d'utilisateurs sur Google Play. Nous vous invitons à consulter nos règles ci-dessous.

Contenu non autorisé

Chaque jour, des internautes du monde entier utilisent Google Play pour accéder à des applications et à des jeux. Avant d'envoyer votre application, demandez-vous si elle est appropriée pour Google Play et si elle respecte les lois locales.

Mise en danger de mineurs

Les applications présentant des contenus sexualisant des mineurs seront immédiatement supprimées du Play Store,-y compris, sans s'y limiter, les applications qui encouragent la pédophilie ou les interactions inappropriées avec un mineur (par exemple, attouchements ou caresses).

De plus, les applications qui peuvent plaire aux enfants, mais qui contiennent des thèmes réservés aux adultes, y compris, mais sans s'y limiter, les applications qui contiennent de la violence ou du sang, ou qui représentent ou encouragent des activités dangereuses, sont interdites. Nous n'autorisons pas non plus les applications donnant une représentation négative du corps ou de soi, par exemple en montrant à des fins de divertissement des interventions de chirurgie plastique, des pertes de poids et d'autres altérations de l'apparence physique.

Si nous détectons la présence de contenus avec des images d'abus sexuels sur des mineurs/enfants, nous le signalons aux autorités compétentes et nous supprimons les comptes Google des personnes impliquées dans leur diffusion.

Contenu inapproprié

Afin que Google Play reste une plate-forme sûre et respectueuse, nous avons mis en place des normes définissant et interdisant les contenus dangereux ou inappropriés pour nos utilisateurs.

Contenu à caractère sexuel ou grossier

Nous n'autorisons pas les applications présentant ou faisant la promotion de contenu à caractère sexuel ou grossier, y compris de la pornographie, ou tout autre contenu ou service destiné à apporter une gratification sexuelle. Les contenus présentant des scènes de nudité peuvent être autorisés si celles-ci ne sont pas gratuites, mais à visée éducative, documentaire, scientifique ou artistique.

Voici quelques exemples courants de non-respect des règles :

- Représentations de nudité sexuelle ou de positions sexuellement explicites dans lesquelles le sujet est nu, flou ou minimalement vêtu, et/ou dont la tenue ne serait pas autorisée dans un contexte public approprié
- Représentations, animations ou illustrations d'actes sexuels, poses suggestives ou représentation sexualisée de parties du corps
- Contenu représentant ou constituant des accessoires sexuels, guides sexuels, thèmes sexuels illégaux et fétiches
- Contenu obscène ou grossier, y compris, sans s'y limiter, tout contenu pouvant contenir des grossièretés, des insultes, du texte explicite, des mots clés réservés aux adultes ou à caractère sexuel dans la fiche Play Store ou dans l'application
- Contenu représentant ou décrivant de la zoophilie, ou y incitant
- Applications faisant la promotion de divertissements à caractère sexuel, de services d'hôtesses ou d'autres services susceptibles d'être interprétés comme une proposition de relations sexuelles en échange de rémunération
- Applications qui humilient ou objectifient des personnes

Incitation à la haine

Nous n'autorisons pas les applications incitant à la violence ou à la haine envers des individus ou des groupes définis par leur race, origine ethnique, religion, handicap, âge, nationalité, statut d'ancien combattant, orientation sexuelle, genre, identité de genre ou toute autre caractéristique identifiée comme motif de discrimination ou de marginalisation.

Les applications avec des contenus éducatifs, documentaires, scientifiques ou artistiques liés au nazisme peuvent être bloquées dans certains pays, conformément aux lois et réglementations locales.

Voici des exemples courants de non-respect des règles :

- Contenus ou discours affirmant qu'un groupe protégé ne fait pas partie de l'espèce humaine, est inférieur ou mérite d'être haï
- Applications contenant des insultes, théories ou stéréotypes haineux attribuant à un groupe protégé des caractéristiques négatives (par exemple, malveillance, corruption, cruauté, etc.), ou prétendant explicitement ou implicitement que le groupe constitue une menace
- Contenu ou discours visant à encourager les autres à croire que certaines personnes méritent d'être haïes ou discriminées parce qu'elles font partie d'un groupe protégé
- Contenu faisant la promotion de symboles incitant à la haine, comme des drapeaux, des symboles, des insignes, des accessoires ou des comportements associés à des groupes incitant à la haine

Violence

Nous n'autorisons pas les applications qui représentent ou favorisent la violence gratuite ou d'autres activités dangereuses. Les applications qui représentent de la violence fictive dans le cadre d'un jeu, comme les dessins animés, la chasse ou la pêche, sont généralement autorisées.

Voici quelques exemples courants de non-respect des règles :

- Représentations visuelles ou descriptions de violence réaliste ou de menaces violentes contre des personnes ou des animaux
- Applications encourageant l'automutilation, le suicide, l'intimidation, le harcèlement, les troubles alimentaires, les jeux d'étranglement ou autres actes comportant des risques de blessure grave ou de mort

Contenu à caractère terroriste

Nous n'autorisons pas les organisations terroristes à publier des applications sur Google Play à quelque fin que ce soit, y compris pour le recrutement.

Nous n'acceptons pas les contenus à caractère terroriste, tels que la promotion d'actes terroristes, l'incitation à la violence ou l'apologie d'attentats terroristes. Si vous publiez des contenus liés au terrorisme dans un objectif pédagogique, documentaire, scientifique ou artistique, vous devez fournir suffisamment d'informations aux utilisateurs pour qu'ils comprennent le contexte.

Événements sensibles

Nous n'autorisons aucune application qui peut être considérée comme exploitant une catastrophe naturelle, un crime, un conflit, un décès ou tout autre événement tragique, ou faisant preuve d'un manque de sensibilité concernant de tels événements. Les applications dont le contenu est lié à un événement sensible sont généralement autorisées si ce contenu a une portée éducative, documentaire, scientifique ou artistique, s'il a pour but d'alerter ou de sensibiliser les utilisateurs au sujet de l'événement en question.

Voici des exemples courants de non-respect des règles :

- Manquer de sensibilité en ce qui concerne le décès d'une personne ou d'un groupe de personnes réelles en raison d'un suicide, d'une overdose, de causes naturelles, etc.
- Nier un événement tragique important
- Tirer profit d'un événement tragique sans que cela offre un avantage apparent pour les victimes.

Intimidation et harcèlement

Nous n'autorisons pas les applications qui comportent ou favorisent les menaces, le harcèlement ou l'intimidation.

Voici des exemples courants de non-respect des règles :

- Intimidation de victimes de conflits internationaux ou religieux
- Contenu ayant pour but d'exploiter les autres, par des pratiques d'extorsion ou de chantage, par exemple
- Publication de contenu pour humilier publiquement quelqu'un
- Harceler les victimes d'un événement tragique ou leurs proches

Produits dangereux

Nous n'autorisons pas les applications qui facilitent la vente d'explosifs, d'armes à feu, de munitions ou de certains accessoires pour armes à feu.

- Les accessoires interdits comprennent ceux qui permettent à une arme à feu de simuler un tir automatique ou de la transformer en arme à tir automatique (par exemple, les bump stocks, les manivelles Gatling, les gâchettes automatiques insérables et les kits de conversion), ainsi que les magasins ou les ceintures de plus de 30 cartouches.

Nous n'autorisons pas les applications qui fournissent des instructions pour la fabrication d'explosifs, d'armes à feu, de munitions, d'accessoires interdits pour armes à feu ou de toute autre arme. Cela comprend les instructions sur la façon de transformer une arme à feu en vue de déclencher ou de simuler un tir automatique.

Marijuana

Nous n'autorisons pas les applications qui facilitent la vente de marijuana ou de produits à base de marijuana, qu'ils soient légaux ou non.

Voici quelques exemples courants de non-respect des règles :

- Applications autorisant les utilisateurs à commander de la marijuana via une fonctionnalité de panier d'achat dans l'application
- Applications permettant aux utilisateurs d'organiser la livraison ou la collecte de marijuana
- Applications facilitant la vente de produits contenant du THC (tétrahydrocannabinol), y compris des produits tels que les huiles de CBD contenant du THC

Tabac et alcool

Nous n'autorisons pas les applications qui facilitent la vente de tabac (y compris les cigarettes électroniques) ou qui encouragent la consommation illégale ou inappropriée d'alcool ou de tabac

Voici des exemples courants de non-respect des règles :

- Applications représentant ou encourageant la consommation ou la vente d'alcool ou de tabac auprès des mineurs
- Applications suggérant que la consommation de tabac peut améliorer le statut social ou les performances sexuelles, professionnelles, intellectuelles ou esthétiques
- Applications présentant la consommation excessive d'alcool, y compris les beuveries et les concours, sous un jour favorable

Services financiers

Nous n'autorisons pas les applications qui exposent les utilisateurs à des produits et services financiers trompeurs ou nuisibles.

Dans le cadre de ce règlement, les produits et services financiers désignent toute solution de gestion ou d'investissement d'argent et de cryptomonnaies, y compris tout service de conseil personnalisé.

Si votre application contient ou met en avant des produits et services financiers, vous devez respecter les réglementations nationales et locales en vigueur dans les régions ou pays ciblés par votre application. Par exemple, vous devez inclure toute mention spécifique requise par la législation locale.

Options binaires

Nous n'acceptons pas les applications permettant la négociation d'options binaires.

Cryptomonnaies

Nous n'autorisons pas les applications qui valident les transactions en cryptomonnaies sur les appareils. En revanche, nous autorisons celles qui gèrent à distance ce processus de validation.

Prêts personnels

Par prêt personnel, nous entendons tout prêt ponctuel accordé par un individu, une organisation ou une entité au bénéfice d'un consommateur individuel, à des fins autres que le financement d'études ou d'un actif immobilisé. Les consommateurs qui souhaitent souscrire un prêt personnel doivent disposer d'informations précises sur les produits proposés (qualité, caractéristiques, frais, échéancier de remboursement, risques et bénéfices) afin de faire leur choix en toute connaissance de cause.

- Exemples : prêt personnel, prêt sur salaire, prêt entre particuliers, prêt sur titre de propriété
- Types de prêts non inclus : emprunt immobilier, financement automobile, prêt étudiant, crédit renouvelable (cartes de crédit, marges de crédit personnelles, par exemple)

Les applications qui proposent des prêts personnels, y compris, mais sans s'y limiter, les applications proposant directement des prêts, les applications de génération de prospects et celles qui mettent les consommateurs en relation avec des prêteurs tiers, doivent inclure les informations suivantes dans leurs métadonnées :

- La durée minimale et maximale de la période de remboursement
- Le taux annuel effectif global maximal, qui comprend généralement le taux d'intérêt plus les frais et autres coûts pour une année, ou tout autre taux similaire calculé conformément à la législation locale
- Un exemple représentatif du coût total du prêt avec tous les frais applicables
- Des règles de confidentialité décrivant de manière exhaustive les méthodes d'accès, de collecte, d'utilisation et de partage de toutes les informations personnelles et sensibles sur l'utilisateur

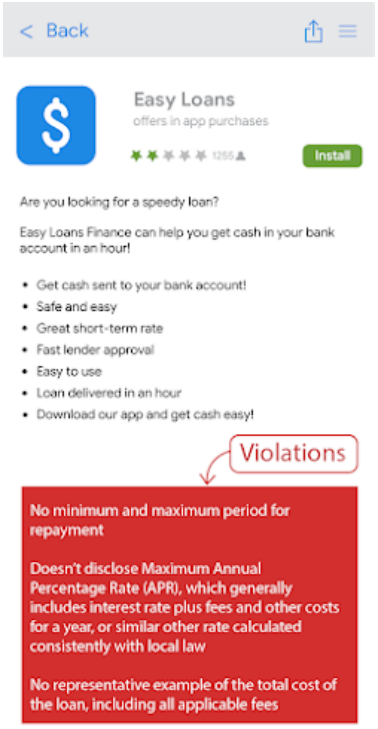
Nous n'autorisons pas les applications qui favorisent les prêts personnels nécessitant un remboursement intégral dans un délai de 60 jours ou moins à compter de la date d'octroi du prêt (appelés "prêts personnels à court terme").

Prêts personnels avec un taux annuel effectif global élevé

Aux États-Unis, nous n'acceptons pas les applications de prêts personnels dont le taux annuel effectif global est supérieur ou égal à 36 %. Le taux annuel effectif global maximal doit obligatoirement être indiqué pour chaque application de ce type aux États-Unis, et calculé conformément à la Loi américaine TILA (Truth in Lending Act) sur la transparence des prêts.

Ces règles s'appliquent aux applications proposant des prêts directement, aux applications de génération de prospects et à celles qui mettent les consommateurs en relation avec des prêteurs tiers.

Voici un exemple courant de non-respect des règles :



Jeux d'argent et de hasard utilisant de l'argent réel, jeux et concours

Nous n'autorisons les applications de jeux d'argent et de hasard utilisant de l'argent réel, les annonces liées à de tels jeux, ainsi que les applications de mini ligue fantasy que si elles répondent à certaines exigences.

Applications de jeux d'argent et de hasard

(Actuellement autorisées en France, en Irlande et au Royaume-Uni uniquement)
Pour tous les autres pays, nous n'autorisons pas les applications dont le contenu ou les services visent à faciliter l'accès à des jeux d'argent et de hasard en ligne.

Nous autorisons les contenus et les services en relation avec des jeux d'argent et de hasard en ligne s'ils respectent les conditions suivantes :

- Le développeur doit faire une demande, et sa demande doit être acceptée pour qu'il puisse distribuer son application sur Google Play.
- L'application doit respecter l'ensemble des lois applicables et des standards dans l'industrie de chaque pays dans lequel elle est diffusée.
- Le développeur doit disposer d'une licence de jeu valide pour chaque pays où l'application est diffusée.
- L'application doit empêcher les utilisateurs n'ayant pas l'âge minimal requis de jouer.
- L'application ne doit pas pouvoir être utilisée dans les pays où la licence de jeu n'a pas été octroyée au développeur.
- L'application NE DOIT PAS être proposée sous forme d'application payante sur Google Play ni utiliser la facturation des achats in-app dans Google Play.
- L'application doit pouvoir être téléchargée et installée gratuitement depuis le Play Store.
- L'application doit être classée dans la catégorie "Réservé aux adultes" ou dans une catégorie équivalente de l'IARC.
- L'application et la fiche associée doivent afficher clairement des informations relatives au jeu responsable.

Autres applications de concours, de tournois et de jeux utilisant de l'argent réel

Nous n'autorisons pas les contenus ou services qui permettent ou facilitent des paris, mises ou participations avec de l'argent réel (y compris les éléments intégrés à l'application achetés avec de l'argent réel) afin de remporter un prix dans une valeur monétaire réelle. Cela inclut, sans s'y limiter, les casinos en ligne, les paris sportifs, les loteries qui ne répondent pas aux exigences des applications de jeux d'argent et de hasard mentionnées ci-dessus, et les jeux offrant des prix en espèces ou autre valeur réelle.

Voici quelques exemples de non-respect des règles :

- Jeux acceptant de l'argent en échange de la possibilité de remporter un prix physique ou une somme d'argent
- Jeux avec des points de fidélité (par exemple, engagement ou activité) qui (1) sont cumulés ou augmentés via des achats avec de l'argent réel et (2) peuvent être échangés contre des articles ou des prix dans une valeur monétaire réelle
- Applications qui acceptent ou gèrent des paris de jeux d'argent et de hasard, des devises intégrées à l'application requises pour participer, gagner ou effectuer des dépôts afin d'obtenir ou d'accélérer la possibilité de remporter un prix physique ou une somme d'argent
- Applications qui intègrent une "incitation à l'action" pour parier, miser ou participer avec de l'argent réel dans des jeux, des concours ou des tournois, telles que des applications avec des éléments de navigation (éléments de menu, onglets, boutons, etc.) qui invitent les utilisateurs à "S'INSCRIRE" ou à "PARTICIPER" pour tenter de gagner un prix en espèces

Annonces pour des jeux d'argent et de hasard, ou des jeux, concours et tournois utilisant de l'argent réel, dans des applications distribuées sur Google Play

Nous autorisons les applications qui font la promotion de jeux d'argent et de hasard, ou de jeux, concours et tournois utilisant de l'argent réel, si elles répondent aux exigences suivantes :

- L'application et l'annonce (y compris les annonceurs) doivent respecter l'ensemble des lois applicables et des standards dans l'industrie du pays où l'annonce est affichée.
- L'annonce doit respecter les conditions locales d'octroi de licence pour tous les produits et services de jeux d'argent et de hasard dont elle fait la promotion.
- L'application ne doit pas afficher d'annonce faisant la promotion de jeux d'argent et de hasard s'il est établi que l'utilisateur a moins de 18 ans.
- L'application ne doit pas être inscrite au programme Pour la famille.
- L'application ne doit pas cibler des personnes de moins de 18 ans.
- Si vous faites la promotion d'une application de jeux d'argent et de hasard (telle que définie ci-dessus), l'annonce doit clairement afficher des informations sur le jeu responsable sur sa page de destination, dans la fiche de l'application elle-même ou dans l'application.
- L'application ne doit pas fournir de contenu de simulation de jeux d'argent et de hasard (applications de casino sur les réseaux sociaux, applications avec machines à sous virtuelles, etc.).
- L'application ne doit pas fournir de fonctionnalités propres aux jeux d'argent et de hasard ni aux jeux, loteries et tournois utilisant de l'argent réel (facilitant, par exemple, les paris, les paiements, le suivi de cotes ou résultats sportifs, ou la gestion de fonds de participation).
- Vous ne devez pas détenir de participation dans les services de jeux d'argent et de hasard, ou de jeux, loteries et tournois utilisant de l'argent réel, promus dans l'application.

- Le contenu de l'application ne doit pas promouvoir de services de jeux d'argent et de hasard, ou de jeux, loteries et tournois utilisant de l'argent réel, ni diriger les utilisateurs vers de tels services.

Seules les applications de jeux d'argent et de hasard (telles que définie ci-dessus) ou qui répondent à toutes ces exigences sur les annonces pour de tels jeux peuvent inclure des annonces pour des jeux d'argent et de hasard ou des jeux, loteries et tournois utilisant de l'argent réel.

Voici quelques exemples de non-respect des règles :

- Application conçue pour les mineurs et diffusant une annonce pour des services de jeux d'argent et de hasard
- Simulation de casino faisant la promotion de casinos utilisant de l'argent réel ou dirigeant les utilisateurs vers de tels casinos
- Application de suivi des cotes sportives intégrant des annonces de jeux d'argent et de hasard qui redirigent l'utilisateur vers un site de paris sportifs
- Application d'actualités qui diffuse des annonces pour un service de jeux d'argent et de hasard détenu ou géré par le développeur de l'application
- Applications dont les annonces relatives aux jeux d'argent et de hasard ne respectent pas nos règles sur les annonces mensongères, comme les annonces présentées aux utilisateurs sous forme de boutons, d'icônes ou d'autres éléments interactifs intégrés à l'application

Applications de mini ligue fantasy

Nous n'autorisons les applications de mini ligue fantasy, tel que défini par la législation locale applicable, que si elles respectent les exigences suivantes :

- L'application est soit 1) distribuée uniquement aux États-Unis, soit 2) éligible conformément aux exigences concernant les applications de jeux d'argent et de hasard mentionnées ci-dessus.
- Le développeur doit envoyer le formulaire de candidature spécifique à la mini ligue fantasy, et sa demande doit être acceptée pour qu'il puisse distribuer son application sur Play.
- L'application doit être conforme à l'ensemble des lois en vigueur et des standards dans l'industrie pour les pays dans lesquels elle est distribuée.
- L'application doit empêcher les utilisateurs n'ayant pas l'âge minimal requis d'effectuer des paris ou des transactions monétaires dans le cadre de son utilisation.
- L'application NE DOIT PAS être proposée sous forme d'application payante sur Google Play ni utiliser la facturation des achats in-app dans Google Play.
- L'application doit pouvoir être téléchargée et installée gratuitement depuis le Play Store.
- L'application doit être classée dans la catégorie "Réservé aux adultes" ou dans une catégorie équivalente de l'IARC.
- L'application et la fiche associée doivent afficher clairement des informations relatives au jeu responsable.

Si elle est distribuée aux États-Unis, les exigences supplémentaires suivantes s'appliquent :

- L'application doit être conforme à l'ensemble des lois en vigueur et des standards dans l'industrie pour tout État ou territoire américain où elle est distribuée.
- Le développeur doit détenir une licence valide pour chaque État ou territoire américain exigeant une telle licence pour une application de mini ligue fantasy.
- L'application ne doit pas être utilisable dans un État ou territoire américain pour lequel le développeur ne possède pas la licence requise pour les applications de mini ligue fantasy.
- L'application ne doit pas être utilisable dans les États ou territoires américains où les applications de mini ligue fantasy ne sont pas autorisées.

Activités illégales

Nous n'autorisons aucune application favorisant ou faisant la promotion d'activités illégales.

Voici quelques exemples courants de non-respect des règles :

- Applications qui permettent la vente ou l'achat de drogues illégales ou de médicaments délivrés sur ordonnance en l'absence de prescription
- Applications représentant ou encourageant la consommation de drogues, d'alcool ou de tabac par des mineurs
- Applications fournissant des instructions pour la culture ou la fabrication de drogues illégales

Contenu généré par l'utilisateur

Un contenu généré par l'utilisateur est, dans une application, un contenu auquel l'utilisateur contribue et qui est visible ou accessible par les autres utilisateurs de cette application ou une partie d'entre eux.

Les applications incluant ou présentant un contenu généré par les utilisateurs doivent :

- exiger que les utilisateurs acceptent les conditions d'utilisation et/ou les règles relatives aux utilisateurs de l'application avant de les autoriser à créer ou à importer de tels contenus ;
- définir les contenus et les comportements inappropriés (d'une manière conforme au règlement du programme Google Play pour les développeurs) et les interdire dans les conditions d'utilisation ou les règles relatives aux utilisateurs de l'application ;
- mettre en œuvre une modération fiable, efficace et continue des contenus générés par les utilisateurs de façon raisonnable et adaptée aux types de contenus hébergés par l'application ;
  - dans le cas des applications de streaming en direct, supprimer les contenus générés par les utilisateurs problématiques en temps quasi réel, autant que possible ;
  - dans le cas des applications de réalité augmentée (RA), la modération des contenus générés par l'utilisateur (y compris le système de signalement intégré à l'application) doit tenir compte des contenus RA générés par l'utilisateur inappropriés (par exemple, une image RA sexuellement explicite) et du lieu d'ancrage RA (par exemple, un contenu RA ancré dans une zone faisant l'objet de restrictions, comme une base militaire ou une propriété privée, où l'ancrage de la RA peut poser des problèmes au propriétaire) ;
- fournir un système intégré facile à utiliser pour signaler les contenus inappropriés générés par les utilisateurs et prendre des mesures à leur encontre, le cas échéant ;
- supprimer ou bloquer les utilisateurs mal intentionnés qui ne respectent pas les conditions d'utilisation et/ou les règles relatives aux utilisateurs de l'application ;
- fournir des garanties pour empêcher que la monétisation dans l'application n'encourage un comportement indésirable des utilisateurs.

Toute application conçue principalement pour proposer des contenus inappropriés générés par les utilisateurs sera supprimée de Google Play. De même, une application sera supprimée si elle est essentiellement utilisée pour l'hébergement de contenus inappropriés générés par les utilisateurs, ou si elle a acquis la réputation, auprès de ces derniers, d'être une application où de tels contenus dominent.

Voici quelques exemples courants de non-respect des règles :

- Applications faisant la promotion de contenus à caractère sexuel explicites générés par les utilisateurs, y compris la mise en œuvre ou l'autorisation de fonctionnalités payantes qui encouragent principalement le partage de contenu répréhensible
- Applications comportant du contenu généré par les utilisateurs et qui n'offrent pas de protection suffisante contre les menaces, le harcèlement ou l'intimidation, en particulier pour les mineurs
- Applications contenant des publications, commentaires ou photos principalement destinés à harceler un individu ou à l'isoler au moyen d'injures, d'attaques ou de moqueries
- Applications non modifiées malgré les réclamations récurrentes de la part d'utilisateurs à propos de contenus inappropriés

Substances non approuvées

Google Play interdit les applications qui vendent des substances non approuvées ou en promeuvent la consommation, que ces substances soient légales ou non. Exemples :

- Tous les éléments répertoriés dans cette liste non exhaustive de produits et suppléments pharmaceutiques non approuvés
- Produits contenant de l'éphédra
- Produits contenant de l'hormone hCG (hormone chorionique gonadotrope humaine) dans le cadre du contrôle ou de la perte de poids, ou présentés en association avec des stéroïdes anabolisants
- Compléments alimentaires ou produits de phytothérapie contenant des principes pharmaceutiques actifs ou des ingrédients dangereux
- Allégations fausses ou trompeuses sur la santé, y compris les déclarations insinuant qu'un produit est aussi efficace que des produits délivrés sur ordonnance ou des substances contrôlées
- Produits ne disposant pas d'une accréditation gouvernementale et présentés comme étant sans risque ou efficaces pour la prévention ou le traitement d'une maladie, ou de troubles médicaux
- Produits ayant fait l'objet d'actions ou d'avertissements de la part d'un gouvernement ou d'une entité de réglementation
- Produits dont les noms peuvent être confondus avec ceux de produits pharmaceutiques ou compléments alimentaires non approuvés ou de substances contrôlées

Pour en savoir plus sur les produits et suppléments pharmaceutiques non approuvés ou trompeurs que nous surveillons, consultez le site www.legitscript.com.

Propriété intellectuelle

Lorsque des développeurs copient les créations d'un tiers ou les utilisent sans l'autorisation requise, cela peut nuire au propriétaire de ce travail. Abstenez-vous d'utiliser le travail d'autrui sans autorisation.

Propriété intellectuelle

Nous interdisons les applications ou les comptes de développeurs qui portent atteinte aux droits de propriété intellectuelle d'autrui (y compris les brevets, les marques, les secrets industriels, les droits d'auteur et les autres droits de propriété). Nous n'acceptons pas non plus les applications qui favorisent ou entraînent une atteinte aux droits de propriété intellectuelle.

Nous répondrons à tout avis clairement formulé d'atteinte aux droits d'auteur. Pour en savoir plus ou pour déposer une demande de suppression DMCA, veuillez consulter nos procédures concernant les droits d'auteur.

Pour déposer une réclamation concernant la vente ou la promotion d'articles de contrefaçon dans une application, veuillez envoyer un avis de contrefaçon.

Vous êtes propriétaire d'une marque et vous pensez qu'une application sur Google Play porte atteinte à vos droits de propriété intellectuelle ? Nous vous recommandons de contacter directement le développeur pour résoudre le problème. Si vous ne parvenez pas à trouver une solution auprès de celui-ci, veuillez déposer une réclamation en remplissant ce formulaire.

Si vous détenez un document écrit prouvant que vous êtes autorisé à utiliser du contenu protégé par les droits de propriété intellectuelle d'un tiers dans votre application ou dans la fiche correspondante (par exemple des noms de marque, des logos ou des éléments graphiques), contactez l'équipe Google Play en amont de votre envoi pour que votre application ne soit pas rejetée pour non-respect des règles relatives à la propriété intellectuelle.

Utilisation non autorisée de contenu protégé par des droits d'auteur

Nous n'autorisons pas la distribution d'applications portant atteinte aux droits d'auteur. L'utilisation comme la modification d'un contenu protégé peuvent constituer une atteinte aux droits d'auteur. Le justificatif des droits d'utilisation d'un contenu protégé pourra être demandé aux développeurs, le cas échéant.

Soyez vigilant si vous utilisez un contenu protégé pour illustrer le fonctionnement de votre application. En règle générale, il est plus sûr de créer un contenu original.

Voici quelques exemples de contenu protégé par des droits d'auteur fréquemment utilisé sans autorisation ni raison juridiquement valable :

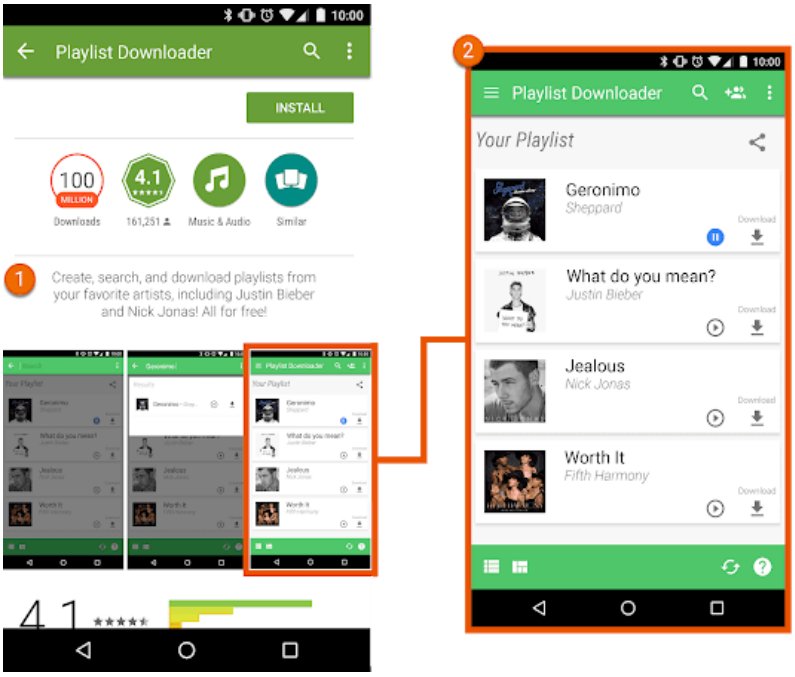
- Images illustrant les pochettes d'albums ou de jeux vidéo et les couvertures de livres
- Images publicitaires provenant de films, de la télévision ou de jeux vidéo
- Affiches ou images provenant de bandes dessinées, de dessins animés, de films, de clips musicaux ou de la télévision
- Logos d'équipes de sport amateur et professionnel
- Photos prises sur un compte de réseaux sociaux d'une personnalité publique
- Images professionnelles de personnalités publiques
- Reproductions ou œuvres de "fan art" identiques à l'œuvre originale protégée par des droits d'auteur
- Applications permettant de lire des sons extraits d'un contenu protégé par des droits d'auteur
- Reproduction intégrale ou traduction de livres qui ne sont pas tombés dans le domaine public

Incitation à l'atteinte aux droits d'auteur

Nous n'autorisons pas les applications qui favorisent les atteintes aux droits d'auteur ou y incitent. Avant de publier votre application, vérifiez si elle présente des éléments incitant à porter atteinte aux droits d'auteur. Le cas échéant, demandez un avis juridique.

Voici quelques exemples courants de non-respect des règles :

- Applications de diffusion en streaming permettant de télécharger une copie locale de contenu protégé par des droits d'auteur sans autorisation
- Applications qui incitent à télécharger et à lire en streaming des œuvres protégées, notamment de la musique et des vidéos, alors que les lois sur les droits d'auteur l'interdisent :



① La description figurant sur la fiche Play Store incite l'utilisateur à télécharger du contenu protégé par des droits d'auteur sans autorisation.
② La capture d'écran figurant sur la fiche Play Store incite l'utilisateur à télécharger du contenu protégé par des droits d'auteur sans autorisation.

Atteinte aux marques

Nous interdisons les applications qui portent atteinte aux marques de tiers. Une marque est un mot, un symbole ou une combinaison qui identifie la source d'un bien ou d'un service. Après le dépôt d'une marque, son propriétaire détient des droits exclusifs sur son utilisation concernant certains biens ou services.

L'atteinte aux marques consiste à utiliser abusivement ou sans autorisation une marque identique ou similaire de façon à prêter à confusion quant à la source du produit en question. Si votre application utilise des marques de tiers d'une manière susceptible de prêter à confusion, elle risque d'être suspendue.

Contrefaçon

Nous n'autorisons pas les applications qui vendent des articles de contrefaçon ou qui en font la promotion. Les articles de contrefaçon comportent une marque ou un logo identique, ou presque, à la marque ou au logo d'un autre produit. Ils imitent les caractéristiques d'une marque afin d'être confondus avec le produit authentique du propriétaire de celle-ci.

Confidentialité, tromperie et utilisation abusive des appareils

Nous nous engageons à protéger la confidentialité des informations des utilisateurs et à leur offrir un environnement sécurisé. Les applications trompeuses, malveillantes ou qui visent à un usage abusif des réseaux, des appareils ou des données à caractère personnel sont strictement interdites.

Données utilisateur

Vous devez faire preuve de transparence concernant la façon dont vous gérez les données utilisateur, telles que les informations fournies par l'utilisateur ou obtenues à son sujet, y compris les informations provenant des appareils. Autrement dit, vous devez informer l'utilisateur en cas de collecte, d'utilisation et de partage desdites informations, et les utiliser exclusivement aux fins indiquées. En outre, si votre application gère des données utilisateur sensibles ou à caractère personnel, nous vous invitons à vous reporter également aux exigences supplémentaires détaillées dans la section "Informations personnelles et sensibles" ci-après. Ces exigences Google Play viennent compléter celles imposées par les lois applicables sur la confidentialité et la protection des données.

Informations personnelles et sensibles

Les données utilisateur à caractère personnel et sensible incluent, sans toutefois s'y limiter, les informations personnelles, financières, de paiement et d'authentification, le répertoire téléphonique et les contacts, la position de l'appareil, les données concernant les SMS et les appels, les données du micro et de l'appareil photo, ainsi que d'autres données sensibles sur l'appareil ou son utilisation. Si votre application gère des données utilisateur sensibles, vous devez respecter les exigences suivantes :

- Limiter la consultation, la collecte, l'utilisation et le partage de données sensibles ou à caractère personnel aux fins directement liées à la mise à disposition et à l'amélioration des fonctionnalités de l'application (par exemple, les fonctionnalités attendues par l'utilisateur qui sont détaillées et mises en avant dans la description de l'application sur le Play Store). Toute application qui utilise également ces données à des fins publicitaires doit respecter nos Règles relatives aux annonces.
- Publier des règles de confidentialité dans l'application même et dans le champ correspondant de la Play Console. Ces règles de confidentialité, ainsi que les communiqués au sein de l'application, doivent indiquer de manière exhaustive comment celle-ci accède aux données utilisateur, les collecte, les utilise et les partage. Ces règles doivent également préciser les types de données sensibles ou à caractère personnel auxquelles elle accède, qu'elle collecte, qu'elle utilise et qu'elle partage, ainsi que les types de parties avec lesquelles ces données sont partagées.
- Gérer de manière sécurisée toutes les données utilisateur sensibles ou à caractère personnel, y compris en les transmettant à l'aide d'une technologie de chiffrement moderne (HTTPS, par exemple).
- Afficher une requête d'autorisations d'exécution dès que possible avant d'accéder à des données protégées par des autorisations Android.
- Ne pas vendre de données utilisateur sensibles ou à caractère personnel.

Exigences concernant la visibilité des communiqués et les demandes de consentement

Dans les cas où l'utilisateur ne s'attend pas, dans la mesure du raisonnable, à ce que ses données sensibles ou à caractère personnel servent au fonctionnement ou aux fonctionnalités conformes de votre application (par exemple, collecte des données en arrière-plan dans votre application), ni à leur amélioration, vous devez respecter les exigences suivantes :

Vous devez afficher un communiqué au sein de l'application concernant l'accès aux données et leur collecte, leur utilisation et leur partage, lequel :

- doit figurer dans l'application même, et pas seulement dans la description de celle-ci ou sur un site Web ;
- doit être facilement consultable sans que l'utilisateur ait besoin de parcourir un menu ni de chercher dans les paramètres ;
- doit préciser les informations auxquelles vous accédez et que vous collectez ;
- doit expliquer comment les données sont utilisées et/ou partagées ;
- **ne doit pas** figurer uniquement dans les règles de confidentialité ou les conditions d'utilisation ;
- **ne doit pas** être inclus avec d'autres informations sans rapport avec la collecte de données sensibles ou à caractère personnel.

Le communiqué affiché dans l'application doit s'accompagner d'une demande de consentement de l'utilisateur, et doit précéder celle-ci. Il doit également être accompagné de l'autorisation d'exécution associée, le cas échéant. Vous ne devez pas accéder à des données utilisateur sensibles ou à caractère personnel, ni collecter de telles données, tant que l'utilisateur n'y a pas consenti. La demande de consentement de l'application :

- doit faire apparaître la boîte de dialogue de collecte du consentement de façon claire et non équivoque ;
- doit nécessiter une action de la part de l'utilisateur pour indiquer le consentement (appuyer pour accepter, cocher une case, etc.) ;
- **ne doit pas** considérer le fait de quitter la section concernant la déclaration de collecte de données (en appuyant ailleurs, en revenant à l'accueil ou en appuyant sur un bouton "Retour", par exemple) comme un consentement ;
- **ne doit pas** utiliser de messages éphémères ou qui disparaissent automatiquement pour obtenir le consentement de l'utilisateur.

Voici quelques exemples courants de non-respect des règles :

- Application qui accède à l'inventaire des applications installées par l'utilisateur et qui ne traite pas ces informations comme des données sensibles ou à caractère personnel soumises aux règles de confidentialité, ainsi qu'aux exigences concernant la gestion des données, la visibilité des communiqués et le consentement indiquées ci-dessus
- Application qui accède aux numéros de téléphone ou aux contacts de l'utilisateur, et qui ne traite pas ces informations comme des données sensibles ou à caractère personnel soumises aux règles de confidentialité, ainsi qu'aux exigences concernant la gestion des données, la visibilité des communiqués et le consentement indiquées ci-dessus
- Application qui enregistre l'écran de l'utilisateur et qui ne traite pas ces informations comme des données sensibles ou à caractère personnel soumises à ce règlement
- Application qui collecte la position de l'appareil sans indiquer de manière exhaustive comment elle utilise cette information ni obtenir le consentement de l'utilisateur conformément aux exigences indiquées ci-dessus

- Application qui collecte des autorisations restreintes en arrière-plan, y compris à des fins de suivi, de recherche ou de marketing, sans indiquer de manière exhaustive comment elle utilise ces informations ni obtenir le consentement de l'utilisateur, conformément aux exigences indiquées ci-dessus

Restrictions spécifiques concernant l'accès aux informations sensibles

En plus des exigences indiquées ci-dessus, le tableau suivant décrit les exigences à respecter pour certaines activités :

Activité	Exigence
Votre application gère des informations financières ou de paiement, ou des numéros d'identification officiels.	Votre application ne doit jamais divulguer publiquement des informations sensibles ou à caractère personnel sur l'utilisateur, que ce soit des informations financières ou de paiement, ou des numéros d'identification officiels.
Votre application traite des coordonnées ou un répertoire téléphonique non publics.	Nous n'autorisons pas la publication ni la divulgation non autorisées des coordonnées privées des contacts des utilisateurs.
Votre application possède des fonctionnalités de sécurité contre les virus, les logiciels malveillants ou d'autres risques.	Votre application doit inclure des règles de confidentialité et des communiqués qui précisent quelles données utilisateur sont collectées et transmises, dans quel but et avec qui elles sont partagées.

Bouclier de protection des données UE-États-Unis (EU-U.S. Privacy Shield)

Bouclier de protection des données

Si vous consultez, utilisez ou traitez des informations personnelles mises à disposition par Google, qui identifient directement ou indirectement une personne et qui proviennent de l'Union européenne ou de la Suisse (dénommées ci-après "Informations personnelles"), vous êtes alors tenu de vous conformer aux obligations suivantes :

- Respecter l'ensemble des lois, des directives, des réglementations et autres règles applicables en matière de confidentialité et de protection des données
- Consulter, utiliser ou traiter les Informations personnelles provenant de l'Union européenne uniquement aux fins consenties par la personne à laquelle se rapportent ces informations
- Mettre en œuvre les mesures appropriées sur le plan technique et de l'organisation afin de protéger les Informations personnelles provenant de l'Union européenne en cas de perte, d'usage abusif, d'accès non autorisé ou illicite, de divulgation, d'altération ou de destruction
- Fournir le même niveau de protection que celui établi dans les Principes du Privacy Shield (Bouclier de protection des données)

Il vous incombe de vérifier régulièrement que vous respectez bien ces conditions. Si, à tout moment, vous n'êtes plus en mesure de vous y conformer (ou s'il est très probable que vous ne puissiez plus les honorer), vous devez nous avertir immédiatement par e-mail à l'adresse data-protection-office@google.com. Vous devez alors cesser de traiter des Informations personnelles provenant de l'Union européenne ou prendre immédiatement les mesures nécessaires et appropriées pour rétablir un niveau adéquat de protection.

Autorisations

Une demande d'autorisation doit avoir du sens pour l'utilisateur. Vous ne pouvez demander une autorisation que si elle est nécessaire pour mettre en œuvre des fonctionnalités ou services déjà disponibles dans votre application et mis en avant dans votre fiche Play Store. Vous ne pouvez pas demander une autorisation d'accès à des informations sur l'utilisateur ou à celles provenant des appareils à des fins non stipulées ou pour des fonctionnalités qui ne sont pas activées ou mises en œuvre. Vous ne devez jamais vendre les données sensibles ou personnelles auxquelles vous êtes autorisé à accéder.

Demandez l'autorisation d'accéder à ces informations en précisant le contexte (par le biais d'une autorisation supplémentaire), afin que l'utilisateur comprenne pourquoi vous avez besoin de cette autorisation. N'utilisez ces informations qu'aux fins pour lesquelles l'utilisateur a donné son autorisation. Si par la suite, vous voulez les utiliser à d'autres fins, vous devez vous assurer auprès de l'utilisateur que celui-ci accepte ces nouvelles dispositions.

Autorisations restreintes

Outre ces considérations, des exigences et restrictions supplémentaires s'appliquent aux autorisations dangereuses, spéciales ou avec signature, dites "autorisations restreintes" :

- Vous pouvez communiquer à des tiers les données sensibles sur l'utilisateur ou l'appareil auxquelles vous accédez par le biais d'autorisations restreintes, mais seulement si elles sont nécessaires pour fournir ou améliorer les fonctionnalités ou services déjà disponibles dans l'application à partir de laquelle vous collectez ces données. Vous êtes également autorisé à transférer ces données si cela est nécessaire pour vous conformer à la loi applicable ou dans le cadre d'une fusion, d'une acquisition ou d'une cession d'actifs, à condition de fournir aux utilisateurs un avis de confidentialité jugé adéquat sur le plan juridique. Tout autre transfert ou toute vente de données utilisateur sont interdits.
- Respectez le choix de l'utilisateur s'il refuse votre demande d'autorisation restreinte. Il est interdit de manipuler les utilisateurs ou de les forcer à accepter une autorisation non essentielle. Vous devez prendre des dispositions raisonnables pour vous adapter aux utilisateurs qui choisissent de ne pas accorder l'accès à des autorisations sensibles (par exemple, en leur permettant de saisir manuellement un numéro de téléphone si l'accès au journal d'appels est restreint).

Certaines autorisations restreintes peuvent faire l'objet d'exigences supplémentaires, détaillées ci-dessous. Ces restrictions ont pour but de protéger la vie privée des utilisateurs. Nous pouvons accorder des exceptions limitées aux exigences ci-dessous dans les cas, très rares, où des applications fournissent une fonctionnalité essentielle ou très intéressante, et où il n'existe actuellement aucune alternative à cette fonctionnalité. Nous évaluons les exceptions proposées en fonction de leur impact potentiel sur la sécurité et la vie privée des utilisateurs.

Autorisations associées aux SMS et au journal d'appels

Les autorisations associées aux SMS et au journal d'appels sont considérées comme des données utilisateur sensibles et à caractère personnel. À ce titre, elles sont soumises au règlement sur les informations personnelles et sensibles, ainsi qu'aux restrictions suivantes :

Autorisation restreinte	Exigence
Le fichier manifeste de votre application demande le groupe d'autorisations du journal d'appels (par exemple, READ_CALL_LOG, WRITE_CALL_LOG et PROCESS_OUTGOING_CALLS).	L'application doit avoir été activement désignée comme gestionnaire par défaut du téléphone ou de l'Assistant sur l'appareil.
Le fichier manifeste de votre application demande le groupe d'autorisations des SMS (par exemple, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH et RECEIVE_MMS).	L'application doit avoir été activement désignée comme gestionnaire par défaut des SMS ou de l'Assistant sur l'appareil.

Les applications qui ne disposent pas de la fonctionnalité de gestionnaire par défaut des SMS, du téléphone ou de l'Assistant ne peuvent pas déclarer l'utilisation des autorisations ci-dessus dans le fichier manifeste. (Cela inclut le texte d'espace réservé dans le fichier manifeste.) Pour inviter l'utilisateur à accepter l'une des autorisations ci-dessus, les applications doivent en outre avoir été activement désignées comme gestionnaires par défaut des SMS, du téléphone ou de l'Assistant. Dès lors qu'elles n'en sont plus les gestionnaires par défaut, elles doivent immédiatement cesser d'utiliser l'autorisation. Les utilisations et exceptions autorisées sont répertoriées sur cette page du Centre d'aide.

Les applications ne peuvent utiliser l'autorisation (et toutes les données qui en découlent) que pour assurer le fonctionnement de base approuvé. Le "fonctionnement de base" correspond à la finalité principale de l'application. Il peut être assuré par un ensemble de fonctionnalités de base, qui doivent toutes être documentées et mises en avant de façon visible dans la description de l'application. Sans ces fonctionnalités, l'application est défectueuse ou inutilisable. Le transfert, le partage ou l'utilisation sous licence de ces données ne doivent servir qu'à fournir les fonctionnalités ou services de base de l'application. L'utilisation desdites données ne peut être étendue à d'autres fins (que ce soit, par exemple, pour améliorer d'autres applications ou services, ou à des fins publicitaires ou de marketing). Vous ne pouvez pas utiliser d'autres méthodes (y compris d'autres autorisations, API ou sources tierces) pour récupérer des données attribuées aux autorisations associées au journal d'appels ou aux SMS.

Autorisations d'accéder à la position

La position de l'appareil est considérée comme une information sur l'utilisateur sensible et personnelle soumise au règlement sur les informations personnelles et sensibles, ainsi qu'aux exigences suivantes :

- Les applications ne peuvent pas utiliser les données protégées par des autorisations d'accéder à la position (par exemple, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION et ACCESS_BACKGROUND_LOCATION) une fois que celles-ci ne sont plus requises pour mettre en œuvre les fonctionnalités ou services déjà disponibles.
- Vous ne devez en aucun cas demander à l'utilisateur l'autorisation d'accéder à sa position dans un but exclusivement publicitaire ou d'analyse. Toute application qui utilise également l'accès autorisé à ces données à des fins publicitaires doit respecter nos Règles relatives aux annonces.

- Vous ne devez demander que le niveau d'accès le plus bas nécessaire (c'est-à-dire un accès à la position approximative plutôt que précise, et au premier plan plutôt qu'en arrière-plan) pour fournir la fonctionnalité ou le service requérant la position. Les utilisateurs doivent raisonnablement s'attendre à ce que la fonctionnalité ou le service en question ait besoin de la position demandée. Par exemple, nous pouvons refuser les applications qui demandent la position ou y accèdent en arrière-plan sans justification convaincante.
- L'accès aux données de localisation en arrière-plan ne peut être utilisé que pour fournir des fonctionnalités utiles liées au fonctionnement de base de l'application.

Les applications sont autorisées à accéder à la position en utilisant un service de premier plan (lorsque l'application ne dispose que d'un accès au premier plan, de type "si l'application est ouverte") si cette utilisation :

- a commencé par une action déclenchée par l'utilisateur dans l'application ;
- prend fin dès que l'utilisation prévue par cette action est terminée.

Les applications spécialement conçues pour les enfants doivent en outre respecter le règlement du programme Pour la famille.

Autorisation d'accès à tous les fichiers

Les fichiers et les attributs de répertoire sur l'appareil d'un utilisateur sont considérés comme des données personnelles et sensibles soumises au règlement sur les informations personnelles et sensibles et aux exigences suivantes :

- Les applications ne doivent demander l'accès à l'espace de stockage de l'appareil que pour le bon fonctionnement de l'application. Elles ne peuvent pas demander un tel accès au nom d'un tiers sans nécessité liée aux fonctionnalités critiques de l'application présentées aux utilisateurs.
- Les appareils Android exécutant la version R (Android 11, niveau d'API 30) ou ultérieure nécessitent l'autorisation MANAGE_EXTERNAL_STORAGE pour gérer l'accès à l'espace de stockage partagé. Toutes les applications destinées à la version R et qui demandent un accès étendu à l'espace de stockage partagé ("Accès à tous les fichiers") doivent avoir été approuvées avant d'être publiées. Les applications ainsi validées doivent clairement inviter les utilisateurs à activer l'option "Accès à tous les fichiers" pour leur application dans les paramètres "Accès spécifiques des applications". Pour plus d'informations sur les exigences de la version R, consultez cet article d'aide.

Utilisation abusive des appareils et des réseaux

Nous n'autorisons pas les applications qui accèdent sans autorisation à l'appareil de l'utilisateur, à d'autres appareils ou ordinateurs, à des serveurs, des réseaux, des API (interfaces de programmation d'application) ou à des services, y compris, mais sans s'y limiter, d'autres applications installées sur l'appareil, les services Google ainsi que les réseaux d'opérateurs autorisés, ou qui les perturbent, les endommagent ou les affectent.

Les applications proposées sur Google Play doivent respecter les critères requis par défaut pour l'optimisation du système Android décrits dans les Consignes fondamentales relatives à la qualité des applications sur Google Play.

La modification, le remplacement ou la mise à jour d'une application distribuée via Google Play à l'aide d'une autre méthode que le mécanisme de mise à jour de Google Play sont interdits. De même, une application n'est pas autorisée à télécharger du code exécutable (par exemple, des fichiers dex, JAR ou .so) depuis une source autre que Google Play. Cette restriction ne s'applique pas au code s'exécutant dans une machine virtuelle et disposant d'un accès limité aux API Android (par exemple, JavaScript dans une WebView ou un navigateur).

Nous n'autorisons pas les codes qui introduisent ou exploitent des failles de sécurité. Consultez le Programme d'amélioration de la sécurité des applications pour être informé des derniers problèmes de sécurité signalés aux développeurs.

Voici quelques exemples courants de non-respect des règles :

- Applications qui bloquent ou perturbent l'affichage des annonces d'une autre application
- Applications d'aide au jeu qui affectent la jouabilité d'autres applications
- Applications qui permettent de pirater des services, des logiciels ou des matériels ou de contourner des dispositifs de sécurité, ou qui fournissent des instructions pour y parvenir
- Applications qui accèdent à un service ou une API ou qui les utilisent d'une manière qui ne respecte pas les conditions d'utilisation
- Applications qui ne peuvent pas figurer sur la liste blanche et tentent de contourner la gestion de l'alimentation du système
- Applications qui facilitent l'utilisation de serveurs proxy tiers, mais qui ne peuvent le faire que si cela s'inscrit dans l'objectif principal de ces applications destinées aux utilisateurs
- Applications ou code tiers (par exemple, SDK) qui téléchargent du code exécutable, comme des fichiers dex ou du code natif, depuis une source autre que Google Play

- Applications qui installent d'autres applications sur un appareil sans l'autorisation de l'utilisateur
- Applications qui facilitent la distribution ou l'installation de logiciels malveillants ou qui contiennent un lien vers ceux-ci

Comportement trompeur

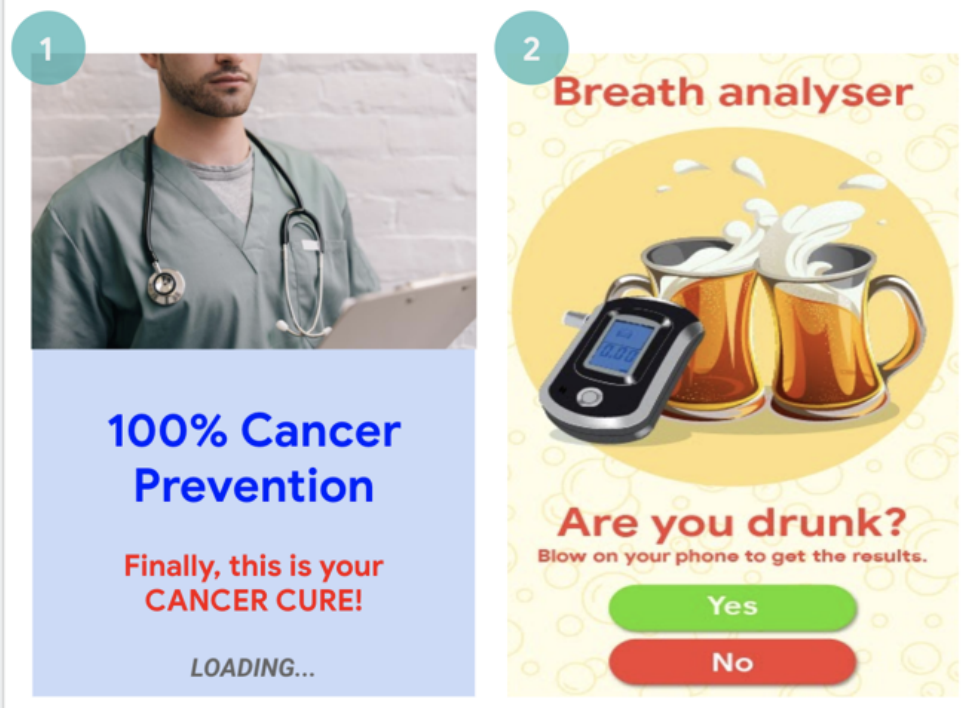
Nous n'autorisons pas les applications conçues pour tromper les utilisateurs ou permettre un comportement malhonnête, y compris, sans s'y limiter, les applications dont le fonctionnement est jugé impossible. Les applications doivent présenter leur fonctionnement au moyen de déclarations, de descriptions et d'images/de vidéos exactes dans toutes leurs métadonnées. Les applications ne doivent pas imiter des fonctionnalités ni des messages d'avertissement propres au système d'exploitation ou à d'autres applications. L'utilisateur doit être informé de toute modification des paramètres de son appareil. Il doit également autoriser chaque modification et pouvoir l'annuler.

Allégations mensongères

Nous n'autorisons pas les applications qui comportent des informations ou des allégations mensongères ou trompeuses. Cette interdiction s'applique également à la description, au titre, à l'icône et aux captures d'écran.

Voici quelques exemples courants de non-respect des règles :

- Applications dont les fonctionnalités sont décrites de manière inexacte, imprécise ou ambiguë :
  - Application présentée comme un jeu de course dans sa description et ses captures d'écran, mais qui est en réalité un jeu de puzzle illustré par une voiture
  - Application présentée comme un antivirus, mais qui ne contient qu'un guide expliquant comment supprimer les virus
- Noms de développeurs ou d'applications présentant de manière inexacte leurs performances ou leur état sur Play (par exemple, "Choix de l'équipe", "Application nº 1" ou "Top des applications payantes")
- Applications qui présentent des fonctionnalités ou des contenus médicaux ou liés à la santé qui sont mensongères ou potentiellement dangereuses
- Applications qui présentent des fonctionnalités qu'il est impossible d'utiliser (par exemple, des applications insecticides), même si elles sont présentées comme un canular ou une blague.
- Applications incorrectement classées, y compris, mais sans s'y limiter, la classification ou la catégorie de l'application
- Contenu manifestement trompeur qui est susceptible d'interférer avec les systèmes de vote
- Applications faussement affiliées à une administration publique, ou qui se proposent d'offrir ou de faciliter des services gouvernementaux sans les autorisations adéquates
- Applications qui se présentent faussement comme l'application officielle d'une entité établie. Un titre tel que "Justin Bieber Officiel" est interdit, sauf si vous détenez les autorisations nécessaires.



(1) Cette application présente des allégations médicales ou liées à la santé (remède contre le cancer) trompeuses
(2) Ces applications présentent des fonctionnalités qu'il est impossible d'utiliser (utiliser le téléphone comme éthylomètre)

Modification déloyale des paramètres de l'appareil

Nous n'autorisons pas les applications qui modifient les paramètres ou les fonctionnalités de l'appareil de l'utilisateur, à son insu et sans son consentement, en dehors de celles-ci. Les paramètres et les fonctionnalités de l'appareil comprennent les paramètres relatifs au système et au navigateur, les favoris, les raccourcis, les icônes, les widgets ainsi que la présentation des applications sur l'écran d'accueil.

Nous interdisons également :

- les applications modifiant les paramètres ou les fonctionnalités de l'appareil avec le consentement de l'utilisateur, mais d'une manière telle qu'il est difficile d'annuler ces modifications ;
- les applications ou les annonces qui modifient les paramètres ou les fonctionnalités de l'appareil dans le cadre d'un service à un tiers ou à des fins publicitaires ;
- les applications qui trompent l'utilisateur dans le but de lui faire supprimer ou désactiver des applications tierces ou de modifier des paramètres ou des fonctionnalités de l'appareil ;
- les applications qui encouragent ou incitent l'utilisateur à supprimer ou à désactiver des applications tierces, ou à modifier des paramètres ou des fonctionnalités de l'appareil, sauf s'il s'agit d'une mesure de sécurité vérifiable.

Incitation à un comportement malhonnête

Nous n'autorisons pas les applications qui aident les utilisateurs à tromper autrui ou qui sont trompeuses de par leur fonctionnement, y compris, mais sans s'y limiter, les applications qui génèrent ou facilitent la génération de cartes d'identité, de numéros de sécurité sociale, de passeports, de diplômes, de cartes de crédit et de permis de conduire. Les applications doivent présenter leur fonctionnement et/ou leur contenu au moyen de déclarations, de descriptions, d'images/de vidéos et de titres exacts. Elles doivent être conformes aux attentes raisonnables de l'utilisateur.

Des ressources supplémentaires (par exemple, des éléments de jeu) ne peuvent être téléchargées que si elles sont nécessaires à l'utilisation de l'application. Les ressources téléchargées doivent respecter l'ensemble des règles de Google Play. Avant de lancer le téléchargement, l'application doit avertir l'utilisateur et indiquer clairement la taille du téléchargement.

Toute application décrite comme un "canular" ou une application "de pur divertissement" (ou autre synonyme) reste soumise à nos règles.

Voici quelques exemples courants de non-respect des règles :

- Applications qui imitent des sites Web ou d'autres applications pour inciter les utilisateurs à divulguer des informations personnelles ou d'authentification
- Applications qui présentent des numéros de téléphone, des coordonnées, des adresses ou des informations personnelles non validés ou appartenant à des personnes physiques ou morales non consentantes
- Applications dont les fonctionnalités de base varient en fonction de la zone géographique de l'utilisateur, des paramètres de l'appareil ou d'autres données dépendantes de l'utilisateur, lorsque ces différences ne sont pas clairement présentées à l'utilisateur dans la fiche Play Store
- Applications qui changent de manière significative d'une version à l'autre sans en avertir l'utilisateur (dans la section Nouveautés, par exemple) ni mettre à jour la fiche Play Store
- Applications qui tentent de modifier ou de masquer des comportements pendant l'examen de l'application
- Applications qui effectuent des téléchargements en passant par un réseau de diffusion de contenu (CDN), mais qui n'en informent pas l'utilisateur et n'indiquent pas la taille du téléchargement avant de lancer celui-ci

Manipulation de contenus multimédias

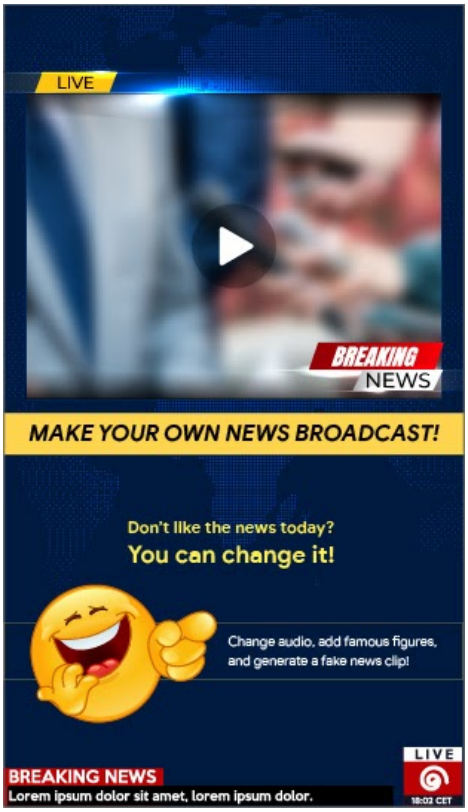
Nous n'autorisons pas les applications qui font la promotion ou facilitent la création d'informations ou d'allégations mensongères ou trompeuses véhiculées par des images, des vidéos et/ou des textes. Nous interdisons les applications que nous jugeons comme faisant la promotion ou favorisant la diffusion d'images, de vidéos et/ou de textes manifestement mensongers ou trompeurs, susceptibles d'avoir des effets nuisibles en rapport avec un événement sensible, des sujets politiques ou sociaux, ou d'autres questions d'ordre public.

Les applications qui manipulent ou retouchent des contenus multimédias, sans qu'il s'agisse seulement de modifications usuelles et acceptables d'un point de vue rédactionnel par souci de clarté ou de qualité, doivent clairement signaler ces contenus ou leur appliquer un filigrane si un utilisateur standard risque de ne pas se rendre compte qu'ils ont été retouchés. Des exceptions peuvent être accordées dans l'intérêt public ou à des fins évidentes de satire ou de parodie.

Voici quelques exemples courants de non-respect des règles :

- Applications qui ajoutent une personnalité publique à une manifestation lors d'un événement politiquement sensible
- Applications qui utilisent des personnalités publiques ou des contenus multimédias liés à un événement sensible pour promouvoir leurs fonctionnalités de retouche de contenus sur leur fiche Play Store

- Applications qui retouchent des extraits multimédias pour imiter un journal télévisé



(1) Cette application propose une fonctionnalité qui permet de retoucher des extraits multimédias pour imiter un journal télévisé, et d'ajouter des personnalités célèbres ou publiques à un extrait sans filigrane.

Déclarations trompeuses

Nous n'autorisons pas les applications ou les comptes de développeur qui usurpent l'identité d'une personne ou d'une organisation, qui dissimulent leur propriétaire ou leur mission principale ou les présentent de façon trompeuse, ou qui se livrent à des activités coordonnées visant à tromper les utilisateurs. Cela inclut, mais sans s'y limiter, les applications ou les comptes de développeur qui dissimulent leur pays d'origine ou le présentent de façon trompeuse, ou qui envoient le contenu d'utilisateurs vers un pays tiers.

Logiciel malveillant

Le terme "logiciel malveillant" désigne tout code susceptible de faire courir un risque à l'utilisateur, à ses données ou à son appareil. Les logiciels malveillants incluent, sans s'y limiter, les applications, fichiers binaires ou modifications de framework potentiellement dangereux, qui se classent en différentes catégories telles que les chevaux de Troie, l'hameçonnage et les logiciels espions. Nous mettons régulièrement à jour ces catégories et en ajoutons de nouvelles.

Logiciel malveillant

Notre règlement concernant les logiciels malveillants est simple : le Google Play Store et l'ensemble de l'écosystème Android doivent être dénués de tout comportement (ou logiciel) malveillant, de même que les appareils des utilisateurs. Par ce principe fondamental, nous nous efforçons d'offrir un écosystème Android sûr aux utilisateurs et à leurs appareils Android.

Même s'ils ne sont pas tous du même type et ont des fonctionnalités diverses, les logiciels malveillants ont généralement l'un des objectifs suivants :

- Compromettre l'intégrité de l'appareil de l'utilisateur
- Prendre le contrôle de l'appareil de l'utilisateur
- Permettre l'exécution d'opérations contrôlées à distance afin qu'un pirate informatique puisse accéder à l'appareil infecté, l'utiliser ou l'exploiter de toute autre manière
- Transmettre des données à caractère personnel ou des identifiants depuis l'appareil sans en informer correctement l'utilisateur ni obtenir son autorisation
- Propager du spam ou des commandes depuis l'appareil infecté pour affecter d'autres appareils ou réseaux

- Escroquer l'utilisateur

Une application, un fichier binaire ou une modification de framework peuvent être potentiellement dangereux, et par conséquent susciter un comportement malveillant, même s'ils n'ont pas été conçus dans ce but. En effet, leur fonctionnement peut varier selon divers facteurs. Par conséquent, ce qui est dangereux pour un certain appareil Android peut être absolument inoffensif pour un autre appareil Android. Par exemple, un appareil équipé de la dernière version d'Android n'est pas affecté par les applications dangereuses qui utilisent des API obsolètes pour susciter un comportement malveillant, tandis qu'un appareil équipé d'une version très ancienne d'Android peut être vulnérable. Les applications, les fichiers binaires et les modifications de framework sont signalés en tant que logiciels malveillants ou PHA (applications potentiellement dangereuses) s'ils présentent un risque évident pour certains appareils et utilisateurs Android, ou pour l'ensemble d'entre eux.

Les catégories de logiciels malveillants ci-dessous reflètent notre conviction fondamentale que les utilisateurs doivent comprendre comment leur appareil est exploité et promouvoir un écosystème sûr qui favorise une innovation forte et une expérience utilisateur fiable.

Pour en savoir plus, consultez Google Play Protect.

Backdoor (porte dérobée)

Code qui permet l'exécution d'opérations indésirables contrôlées à distance et potentiellement dangereuses sur l'appareil.

Ces opérations peuvent susciter un comportement qui, s'il s'exécutait automatiquement, classerait l'application, le fichier binaire ou la modification de framework dans l'une des autres catégories de logiciels malveillants. En général, le terme "backdoor" décrit la manière dont une opération potentiellement dangereuse peut s'exécuter sur un appareil. Par conséquent, il ne correspond pas à part entière à une catégorie comme la fraude à la facturation ou les logiciels espions commerciaux. C'est pourquoi Google Play Protect traite dans certains cas un sous-ensemble de backdoors comme une faille.

Fraude à la facturation

Code qui facture automatiquement l'utilisateur de manière délibérément trompeuse.

Sur mobile, la fraude à la facturation se divise en trois catégories : fraude au SMS, fraude à l'appel et fraude à la facturation par l'opérateur.

Fraude au SMS

Code qui facture les utilisateurs pour envoyer des SMS surtaxés sans leur autorisation, ou qui tente de dissimuler ses activités d'envoi de SMS en masquant les accords de divulgation ou les SMS de notification de frais ou de confirmation d'abonnement envoyés à l'utilisateur par l'opérateur mobile.

Certains types de code divulguent le fait que des SMS sont envoyés, mais ils introduisent d'autres comportements qui facilitent la fraude au SMS. Par exemple, ils peuvent masquer certaines parties d'un accord de divulgation ou les rendre illisibles, et supprimer de manière conditionnelle les SMS de notification de frais ou de confirmation d'abonnement envoyés à l'utilisateur par l'opérateur mobile.

Fraude à l'appel

Code qui facture les utilisateurs en passant des appels vers des numéros surtaxés sans leur autorisation.

Fraude à la facturation par l'opérateur

Code qui trompe les utilisateurs afin qu'ils achètent du contenu ou s'y abonnent en étant facturés par leur opérateur mobile.

La fraude à la facturation par l'opérateur inclut tous les types de facturation autres que les SMS et appels surtaxés. Par exemple, elle peut concerner la facturation directe par l'opérateur, les points d'accès sans fil (WAP, Wireless Access Point) et le transfert de crédit mobile. La fraude WAP est l'un des types de fraude à la facturation par l'opérateur les plus fréquents. Elle peut consister à tromper les utilisateurs afin qu'ils cliquent sur un bouton dans une WebView transparente chargée de manière silencieuse. Cette action déclenche la souscription d'un abonnement. Le SMS ou l'e-mail de confirmation sont souvent piratés pour que les utilisateurs ne remarquent pas la transaction financière.

Logiciel de traque

Logiciel de traque

Code qui transmet des informations personnelles depuis l'appareil sans en informer l'utilisateur ni obtenir son autorisation, et qui n'affiche pas de notification permanente à ce sujet.

En règle générale, les logiciels de traque transmettent des données à un destinataire autre que le fournisseur de l'application potentiellement dangereuse.

Les parents peuvent utiliser des formes légitimes de ce type d'application pour surveiller leurs enfants. Toutefois, si aucune notification permanente ne s'affiche lors de la transmission de données, ces applications ne peuvent pas servir à surveiller une personne (un conjoint, par exemple) à son insu et sans son autorisation.

Seules les applications conformes aux règles, et exclusivement conçues et commercialisées pour le contrôle parental (y compris familial) ou la gestion d'entreprise, peuvent être distribuées sur le Play Store avec des fonctionnalités de suivi et de signalement, à condition qu'elles respectent entièrement les exigences décrites ci-dessous.

Les applications distribuées sur le Play Store qui ne sont pas des logiciels de traque, mais qui surveillent le comportement des utilisateurs sur leur appareil, doivent respecter au minimum les exigences suivantes :

- Elles ne doivent pas être présentées comme des solutions d'espionnage ni de surveillance secrète.
- Elles ne doivent pas masquer ou dissimuler le suivi de comportement, ni tenter de tromper l'utilisateur sur cette fonctionnalité.
- Les applications doivent présenter à l'utilisateur une notification permanente et une icône unique qui les identifie clairement.
- Les applications (et leurs fiches sur Google Play) ne doivent pas permettre d'activer des fonctionnalités allant à l'encontre des présentes conditions, n'y d'accéder à de telles fonctionnalités. Par exemple, elles ne doivent pas contenir de liens vers un APK non conforme hébergé en dehors de Google Play.
- Vous êtes seul responsable de l'évaluation de la légalité de votre application dans sa langue cible. Les applications jugées illégales dans le pays où elles sont publiées seront supprimées.

Déni de service (DoS)

Code qui exécute une attaque par déni de service (DoS) ou fait partie d'une attaque DoS distribuée visant d'autres systèmes et ressources, le tout à l'insu de l'utilisateur.

Par exemple, une telle attaque peut consister à envoyer un grand nombre de requêtes HTTP de façon à imposer une charge excessive aux serveurs distants.

Programmes de téléchargement dangereux

Code qui n'est pas potentiellement dangereux en soi, mais qui télécharge d'autres PHA.

Le code peut être un programme de téléchargement dangereux dans les cas suivants :

- Il existe des raisons de croire qu'il a été créé dans le but de propager des PHA, et qu'il en a téléchargé ou qu'il contient du code pouvant télécharger et installer des applications.
- L'observation d'au moins 500 téléchargements d'applications par ce programme révèle que 5 % d'entre eux ou plus concernent des PHA (soit 25 téléchargements de PHA observés).

Les principaux navigateurs et applications de partage de fichiers ne sont pas considérés comme des programmes de téléchargement dangereux tant qu'ils remplissent les deux conditions suivantes :

- Ils ne lancent pas de téléchargements sans l'intervention de l'utilisateur.
- Les téléchargements de PHA sont exécutés à la demande et avec l'autorisation des utilisateurs.

Menace non-Android

Code qui contient des menaces non-Android.

De telles applications ne peuvent pas nuire à l'appareil Android ni à son utilisateur, mais elles incluent des composants potentiellement dangereux pour d'autres plates-formes.

Hameçonnage

Code qui donne l'impression de provenir d'une source fiable et qui demande à l'utilisateur de lui communiquer ses identifiants d'authentification ou ses informations de facturation afin de les envoyer à un tiers. Cette catégorie inclut également tout code qui intercepte les identifiants de l'utilisateur en cours de transmission.

L'hameçonnage cible généralement les identifiants bancaires, les numéros de carte de crédit et les identifiants de compte en ligne permettant d'accéder à des réseaux sociaux et à des jeux.

Utilisation abusive de l'élévation des privilèges

Code qui compromet l'intégrité du système en contournant le bac à sable de l'application, en obtenant une élévation des privilèges, ou en modifiant ou désactivant l'accès aux principales fonctionnalités de sécurité.

Exemples :

- Application qui ne respecte pas le modèle d'autorisations Android ou qui vole les identifiants (tels que les jetons OAuth) d'autres applications
- Application qui utilise des fonctionnalités de manière abusive afin qu'il soit impossible de la désinstaller ou de l'arrêter
- Application qui désactive SELinux

Les applications d'élévation des privilèges qui passent les appareils en mode root sans l'autorisation de l'utilisateur sont classées parmi les applications d'activation du mode root.

Rançongiciel

Code qui prend le contrôle partiel ou étendu d'un appareil ou de ses données, et qui exige que l'utilisateur effectue un paiement ou une certaine action pour récupérer ce contrôle.

Certains rançongiciels chiffrent les données de l'appareil et exigent un paiement pour les déchiffrer, et/ou exploitent les fonctionnalités d'administration de l'appareil pour empêcher tout utilisateur standard de les supprimer. Exemples :

- Verrouiller l'accès de l'utilisateur à l'appareil et exiger de l'argent pour lui redonner le contrôle
- Chiffrer les données de l'appareil et exiger un paiement, soi-disant pour les déchiffrer
- Exploiter les fonctionnalités du gestionnaire de règles de l'appareil et bloquer toute suppression par l'utilisateur

Le code distribué avec l'appareil et ayant pour principal objectif de gérer un appareil subventionné peut être exclu de la catégorie des rançongiciels, à condition qu'il remplisse correctement les exigences de verrouillage et de gestion sécurisés, et qu'il informe correctement l'utilisateur et obtienne son autorisation.

Activation du mode root

Code qui active le mode root sur l'appareil.

Il existe une différence entre les codes d'activation du mode root malveillants et non malveillants. Par exemple, les applications d'activation du mode root non malveillantes informent préalablement l'utilisateur qu'elles vont activer le mode root sur leur appareil, et elles n'exécutent aucune opération potentiellement dangereuse correspondant à d'autres catégories de PHA.

Les applications d'activation du mode root malveillantes n'informent pas l'utilisateur avant d'activer le mode root, ou bien elles l'informent, mais exécutent également des opérations qui caractérisent d'autres catégories de PHA.

Spam

Code qui envoie des messages non sollicités aux contacts de l'utilisateur ou qui se sert de l'appareil pour relayer du spam.

Logiciel espion

Code qui transmet des données à caractère personnel depuis l'appareil sans en informer correctement l'utilisateur ni obtenir son autorisation.

Par exemple, le fait de transmettre l'une des informations suivantes sans le divulguer à l'utilisateur ou sans qu'il s'y attende suffit à classer le code dans la catégorie des logiciels espions :

- Liste des contacts
- Photos ou autres fichiers provenant de la carte SD ou n'appartenant pas à l'application
- Contenu des e-mails de l'utilisateur
- Journal d'appels
- Journal de SMS
- Historique Web ou favoris du navigateur par défaut
- Informations du répertoire /data/ d'autres applications

Les comportements assimilables au fait d'espionner l'utilisateur peuvent également être signalés en tant que logiciels espions. Citons par exemple l'enregistrement audio, l'enregistrement des appels reçus sur le téléphone ou le vol des données d'une application.

Cheval de Troie

Code qui semble inoffensif, par exemple parce qu'il se présente comme un simple jeu, mais qui exécute des actions indésirables à l'encontre de l'utilisateur.

Cette classification est généralement utilisée en conjonction avec d'autres catégories de PHA (application potentiellement dangereuse). Un cheval de Troie associe un composant inoffensif à un composant dangereux caché. Par exemple, il peut s'agir d'un jeu qui envoie des SMS surtaxés en arrière-plan depuis l'appareil, à l'insu de l'utilisateur.

Remarque concernant les applications inhabituelles

Les applications rares et nouvelles peuvent être classifiées comme inhabituelles si Google Play Protect ne dispose pas de suffisamment d'informations pour confirmer qu'elles sont sans danger. Cela ne signifie pas qu'elles sont nécessairement dangereuses, mais elles ne peuvent pas être considérées comme inoffensives sans un examen approfondi.

Remarque concernant la catégorie "Backdoor" (porte dérobée)

La classification dans la catégorie "Backdoor" des logiciels malveillants dépend du comportement du code. Pour entrer dans cette catégorie, le code doit permettre un comportement qui, s'il s'exécutait automatiquement, le classerait dans l'une des autres catégories de logiciels malveillants. Par exemple, si une application permet le chargement dynamique de code et que le code en question extrait les SMS, l'application est considérée comme une backdoor.

En revanche, si une application permet l'exécution de code arbitraire et que nous n'avons aucune raison de croire que cette exécution a pour but de susciter un comportement malveillant, nous considérons que cette application présente une faille et non qu'il s'agit d'une backdoor, et nous demandons à son développeur de lui appliquer un correctif.

Logiciels indésirables sur mobile

Les présentes règles s'appuient sur le règlement relatif aux logiciels indésirables de Google et décrivent les principes applicables à l'écosystème Android et au Google Play Store. Tout logiciel qui enfreindrait ces principes est susceptible de nuire à l'expérience utilisateur, auquel cas nous prendrons les mesures nécessaires afin de protéger les personnes concernées.

Logiciels indésirables sur mobile

Chez Google, nous pensons que si nous nous concentrons sur l'intérêt de l'utilisateur, tout le reste suivra. Nos Principes applicables aux logiciels et le Règlement relatif aux logiciels indésirables contiennent des recommandations générales concernant les logiciels offrant une expérience utilisateur de qualité. Les présentes règles s'appuient sur le règlement relatif aux logiciels indésirables de Google et décrivent les principes applicables à l'écosystème Android et au Google Play Store. Tout logiciel qui enfreindrait ces principes est susceptible de nuire à l'expérience utilisateur, auquel cas nous prendrons les mesures nécessaires afin de protéger les personnes concernées.

Comme indiqué dans le Règlement relatif aux logiciels indésirables, nous avons constaté que la plupart des logiciels indésirables présentent une ou plusieurs des caractéristiques de base suivantes :

- Le logiciel est trompeur : les avantages promis ne sont pas respectés.
- Le logiciel essaie, de manière détournée, d'inciter les utilisateurs à l'installer ou s'insinue dans l'installation d'un autre programme.
- Le logiciel n'énonce pas clairement toutes ses fonctionnalités clés.
- Le logiciel déstabilise le système de l'utilisateur.
- Le logiciel collecte ou transmet des informations privées à l'insu des utilisateurs.
- Le logiciel collecte ou transmet des informations privées sans traitement sécurisé (par exemple, via HTTPS).
- Le logiciel est associé à un autre programme, sans que l'utilisateur en soit informé.

Sur les appareils mobiles, le logiciel est du code prenant la forme d'une application, d'un fichier binaire, d'une modification de framework, etc. Afin d'éviter tout logiciel dangereux pour l'écosystème logiciel ou perturbant l'expérience utilisateur, nous prendrons des mesures contre tout code qui enfreint ces principes.

Ci-dessous, nous étendons l'application du règlement sur les logiciels indésirables aux logiciels mobiles. Comme pour celui-ci, nous modifierons ce règlement sur les logiciels mobiles indésirables pour couvrir les nouveaux types d'abus.

Comportement transparent et communications claires

Tout code doit tenir les promesses faites à l'utilisateur. Les applications doivent fournir toutes les fonctionnalités annoncées. Elles ne doivent pas dérouter les utilisateurs.

- Les fonctionnalités et les objectifs des applications doivent être clairs.
- Expliquez clairement à l'utilisateur les modifications que l'application apporte au système. Autorisez les utilisateurs à vérifier et à approuver toutes les options d'installation et les modifications importantes.
- Les logiciels ne doivent pas tromper l'utilisateur quant à l'état de l'appareil, par exemple en prétendant l'existence d'une faille de sécurité critique ou une contamination par des virus.
- N'utilisez pas d'activités incorrectes conçues pour augmenter le trafic publicitaire et/ou les conversions.
- Nous n'autorisons pas les applications qui trompent les utilisateurs en usurpant l'identité d'une autre personne (développeur, entreprise, entité, etc.) ou d'un autre application. N'insinuez pas que votre application est associée à une autre personne ou autorisée par un tiers si ce n'est pas le cas.

Exemples de non-respect des règles :

- Fraude publicitaire
- Usurpation d'identité

Protection des données utilisateur

Soyez clair et transparent sur l'accès, l'utilisation, la collecte et le partage des données utilisateur personnelles et sensibles. L'utilisation des données utilisateur doit respecter toutes les règles applicables en la matière. Toutes les précautions doivent être prises pour protéger les données.

- Offrez aux utilisateurs la possibilité d'accepter la collecte de leurs données avant de les recueillir et de les envoyer depuis l'appareil. Cela concerne, entre autres, les données relatives aux comptes tiers, aux e-mails, aux numéros de téléphone, aux applications installées, aux fichiers, à la position, ainsi que toute autre donnée personnelle et sensible que l'utilisateur ne s'attend pas à voir collectée.
- Les données utilisateur personnelles et sensibles collectées doivent être traitées de manière sécurisée, y compris en les transmettant à l'aide d'une technologie de chiffrement moderne (HTTPS, par exemple).
- Les logiciels, y compris les applications mobiles, ne doivent transmettre aux serveurs que des données personnelles et sensibles relatives aux fonctionnalités de l'application.

Exemples de non-respect des règles :

- Collecte des données (voir Logiciels espions)
- Utilisation abusive d'autorisations restreintes

Exemples de règles sur les données utilisateur :

- *Règles Google Play concernant les informations sur l'utilisateur*
- *Règles concernant les informations sur l'utilisateur et exigences GMS*
- *Règles concernant les informations sur l'utilisateur du service API Google*

L'application ne doit pas nuire à l'expérience mobile

L'expérience utilisateur doit être simple, facile à comprendre et basée sur des choix clairs de l'utilisateur. Elle doit offrir une proposition de valeur claire à l'utilisateur et ne pas perturber l'expérience annoncée ou souhaitée.

- Ne diffusez pas d'annonces inattendues aux utilisateurs, y compris en altérant ou en interférant avec les fonctionnalités de l'appareil, ou en dehors de l'environnement déclencheur de l'application sans pouvoir être facilement ignoré et avec le consentement et l'attribution appropriés.
- Les applications ne doivent pas interférer avec d'autres applications ni avec l'utilisation de l'appareil.
- Le cas échéant, la procédure de désinstallation doit être claire.
- Les logiciels mobiles ne doivent pas imiter les invites du système d'exploitation de l'appareil ou d'autres applications. Ne supprimez pas les alertes envoyées à l'utilisateur par d'autres applications ou par le système d'exploitation, notamment celles qui informent l'utilisateur des modifications apportées au système d'exploitation.

Exemples de non-respect des règles :

- Annonces intrusives
- Utilisation non autorisée ou imitation des fonctionnalités système

Fraude publicitaire

La fraude publicitaire est strictement interdite. Les interactions publicitaires générées dans le but de faire croire à un réseau publicitaire que le trafic provient de l'intérêt d'un utilisateur réel constituent une fraude publicitaire, qui est une forme de trafic incorrect. La fraude publicitaire peut dériver de l'affichage par les développeurs d'annonces non autorisées, par exemple l'affichage d'annonces masquées, les clics automatiques sur les annonces, la modification

d'informations et l'utilisation d'actions non humaines (robots, etc.) ou d'activités humaines conçues pour générer un trafic publicitaire incorrect. Le trafic incorrect et la fraude publicitaire sont nuisibles aux annonceurs, développeurs et utilisateurs, et peuvent conduire à une perte de confiance durable dans l'écosystème des annonces mobiles.

Voici quelques exemples courants de non-respect des règles :

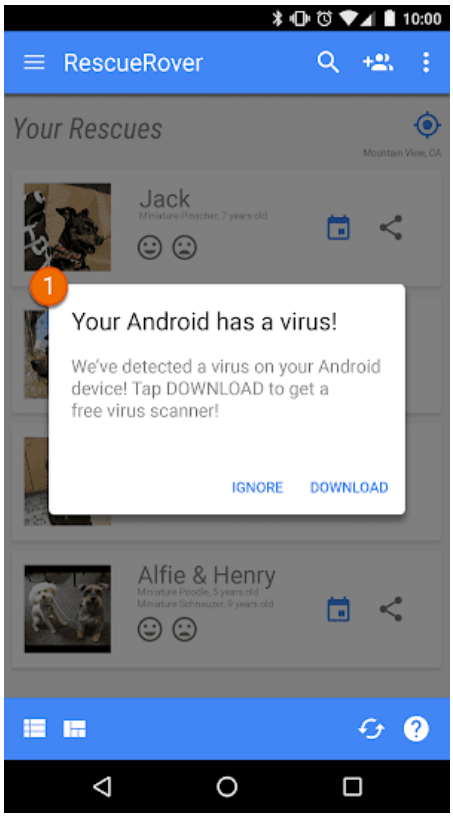
- Application qui affiche des annonces qui ne sont pas visibles par l'utilisateur
- Application qui génère automatiquement des clics sur les annonces sans intention de l'utilisateur ou qui génère un trafic réseau équivalent pour attribuer des crédits de clics de manière frauduleuse
- Application envoyant des clics d'attribution d'installation frauduleux pour être payé pour des installations ne provenant pas du réseau de l'expéditeur
- Application qui affiche des annonces lorsque l'utilisateur ne se trouve pas dans l'interface de l'application
- Déclaration mensongère concernant l'inventaire publicitaire par une application, par exemple une application qui indique aux réseaux publicitaires qu'elle s'exécute sur un appareil iOS alors qu'elle s'exécute sur un appareil Android, ou une application qui modifie le nom du package monétisé

Utilisation non autorisée ou imitation des fonctionnalités système

Nous n'acceptons pas les applications ou les annonces qui imitent ou perturbent les fonctionnalités du système d'exploitation, comme les notifications ou les avertissements, par exemple. Les notifications système ne peuvent être utilisées que pour les fonctionnalités principales de l'application. Par exemple, l'application d'une compagnie aérienne qui avertit les utilisateurs d'offres spéciales, ou un jeu qui les informe de promotions intégrées.

Voici quelques exemples courants de non-respect des règles :

- Applications ou annonces diffusées via une notification ou une alerte système :



① La notification système affichée dans cette application sert à diffuser une annonce.

Pour voir davantage d'exemples concernant les annonces, consultez les Règles relatives aux annonces.

Usurpation d'identité

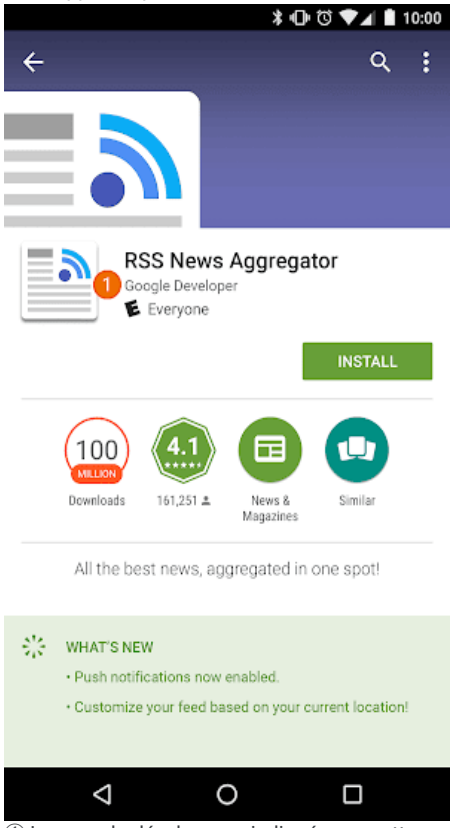
Lorsque des développeurs se font passer pour d'autres ou pour les applications de ceux-ci, cela trompe les utilisateurs et nuit à la communauté des développeurs. Nous interdisons les applications qui trompent les utilisateurs en usurpant l'identité d'une personne.

Usurpation d'identité

Nous n'autorisons pas les applications qui trompent les utilisateurs en usurpant l'identité d'une personne (développeur, entreprise, entité, etc.) ou d'une autre application. N'insinuez pas que votre application est associée à une personne ou autorisée par un tiers si ce n'est pas le cas. Veillez à ne pas utiliser d'icônes, de descriptions, de titres ou d'éléments intégrés à l'application susceptibles de tromper les utilisateurs quant à la relation entre votre application et une autre application ou personne.

Voici quelques exemples courants de non-respect des règles :

- Développeurs qui font croire à une relation avec une autre entreprise ou un autre développeur :



① Le nom du développeur indiqué pour cette application suggère une relation officielle avec Google, alors que ce n'est pas le cas.

- Titres et icônes d'applications présentant une telle ressemblance avec des produits ou des services existants qu'ils induisent l'utilisateur en erreur :

Monétisation et annonces

Google Play permet de monétiser les applications grâce à différentes stratégies avantageuses pour les développeurs et les utilisateurs, comme la distribution payante, les produits intégrés à l'application, les abonnements et les annonces publicitaires. Pour offrir une expérience utilisateur optimale, nous vous recommandons de respecter les règles suivantes.

Paiements

Les applications qui permettent de réaliser des achats via l'application ou sur Google Play doivent respecter les consignes suivantes :

Achats sur Google Play : les développeurs qui facturent les applications et les téléchargements sur Google Play sont tenus d'utiliser le système de paiement de Google Play.

Achats via l'application :

- Les développeurs qui proposent des produits ou du contenu dans un jeu téléchargé sur Google Play sont tenus d'utiliser la facturation des achats in-app dans Google Play comme mode de paiement.
- Les développeurs qui proposent des produits dans une autre catégorie d'applications téléchargées sur Google Play sont tenus d'utiliser la facturation des achats in-app dans Google Play comme mode de paiement, sauf dans les cas suivants :
  - Lorsque le paiement concerne uniquement des produits physiques
  - Lorsque le paiement concerne des contenus numériques qui peuvent être utilisés en dehors de l'application elle-même (par exemple, des titres musicaux pouvant être lus sur d'autres lecteurs de musique)
- Les devises virtuelles intégrées aux applications ne doivent être utilisées que dans l'application ou le jeu dans lesquels elles ont été achetées.
- Les développeurs ne doivent pas induire les utilisateurs en erreur quant à la nature des applications qu'ils vendent, ainsi que des services, des biens, des contenus ou des fonctionnalités intégrés à ces dernières. Si la description de votre produit sur Google Play fait référence à des fonctionnalités intégrées à l'application, pour lesquelles des frais particuliers ou supplémentaires s'appliquent, elle doit clairement informer l'utilisateur que ces fonctionnalités sont payantes.
- Les applications offrant des mécanismes permettant de recevoir des objets virtuels aléatoires lors d'un achat (c'est-à-dire des "loot box") doivent clairement indiquer avant l'achat les chances de recevoir de tels objets.

Voici quelques exemples de produits compatibles avec la facturation des achats in-app dans Google Play :

- **Produits de jeux virtuels**, y compris les pièces, les gemmes, les vies ou tours de jeu supplémentaires, les éléments ou équipements particuliers, les personnages ou avatars, les niveaux ou le temps de jeu supplémentaires.
- **Fonctionnalité ou contenu d'application**, tels qu'une version sans publicité d'une application ou de nouvelles fonctionnalités non disponibles dans la version gratuite.
- **Services proposés sur abonnement**, tels que la diffusion en streaming de musique, de vidéos, de livres ou d'autres services multimédias ; les publications numériques, y compris lorsqu'elles accompagnent une édition papier ; les services de réseaux sociaux.
- **Produits logiciels dans le cloud**, y compris les services de stockage de données, les logiciels de productivité pour les entreprises et de gestion financière.

Voici quelques exemples de produits actuellement non compatibles avec la facturation des achats in-app dans Google Play :

- **Produits vendus au détail**, tels que les produits alimentaires, les vêtements, les articles ménagers et électroniques.
- **Frais de service**, y compris pour les frais de taxis et de transports en commun, d'entreprises de nettoyage, de livraison de repas, de billets d'avion et de tickets pour des événements.
- **Frais d'adhésion ponctuels ou cotisations récurrentes**, y compris pour les adhésions aux salles de sport, les programmes de fidélité ou les clubs qui proposent des accessoires, des vêtements ou d'autres produits physiques.
- **Paiements uniques**, y compris pour les transactions entre particuliers, les enchères en ligne et les dons.
- **Paiement électronique de factures**, y compris pour les factures de carte de crédit, des fournisseurs de services publics, de télévision par câble ou de télécommunications.

Sachez que nous proposons l'API Google Pay pour les applications de vente de produits et de services physiques. Pour en savoir plus, consultez notre page sur Google Pay dédiée aux développeurs.

Abonnements

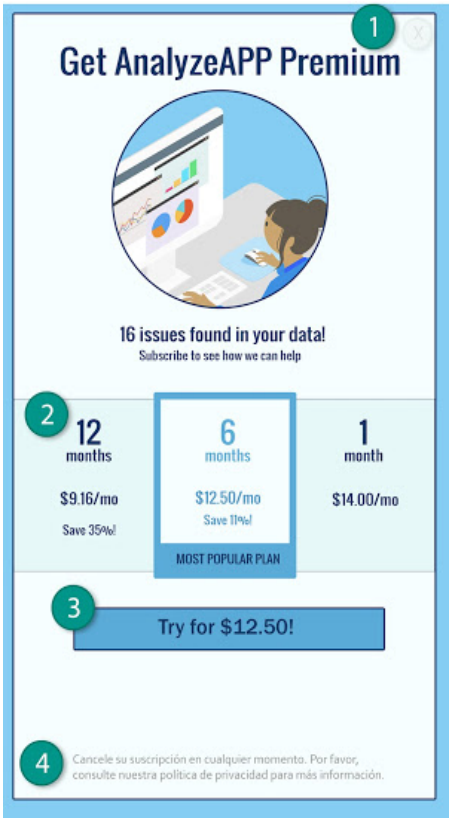
En tant que développeur, vous ne devez pas induire les utilisateurs en erreur sur les services d'abonnement ou les contenus que vous proposez dans votre application. Il est essentiel de communiquer avec clarté dans toutes les promotions intégrées à l'application ou sur les écrans d'accueil.

Dans votre application : vous devez faire preuve de transparence concernant votre offre. Cela inclut le fait d'être explicite sur les conditions de votre offre, le coût de votre abonnement et la fréquence de votre cycle de facturation. Vous devez

également préciser si un abonnement est requis pour utiliser l'application. Les utilisateurs doivent pouvoir prendre connaissance de ces informations sans action supplémentaire de leur part.

Voici quelques exemples courants de non-respect des règles :

- Abonnements mensuels n'informant pas les utilisateurs qu'ils seront automatiquement renouvelés et facturés chaque mois
- Abonnements annuels donnant une visibilité plus élevée à leurs tarifs sous forme de coût mensuel
- Tarifs d'abonnement et conditions n'ayant pas été intégralement localisés
- Promotions intégrées à l'application n'indiquant pas clairement qu'un utilisateur peut accéder au contenu concerné sans abonnement (le cas échéant)
- Noms de code SKU n'indiquant pas correctement la nature de l'abonnement, comme "Essai gratuit" pour un abonnement payant renouvelé automatiquement



① Le bouton "Ignorer" n'est pas clairement visible. Par conséquent, il est possible que les utilisateurs ne comprennent pas qu'ils peuvent accéder aux fonctionnalités sans accepter l'offre d'abonnement.

② L'offre indique le tarif uniquement sous forme de coût mensuel. Ainsi, il est possible que les utilisateurs ne comprennent pas que six mois leur seront facturés lors de la souscription de l'abonnement.

③ L'offre indique uniquement le prix découverte. De ce fait, il est possible que les utilisateurs ne comprennent pas quel montant leur sera automatiquement facturé à la fin de la période de lancement.

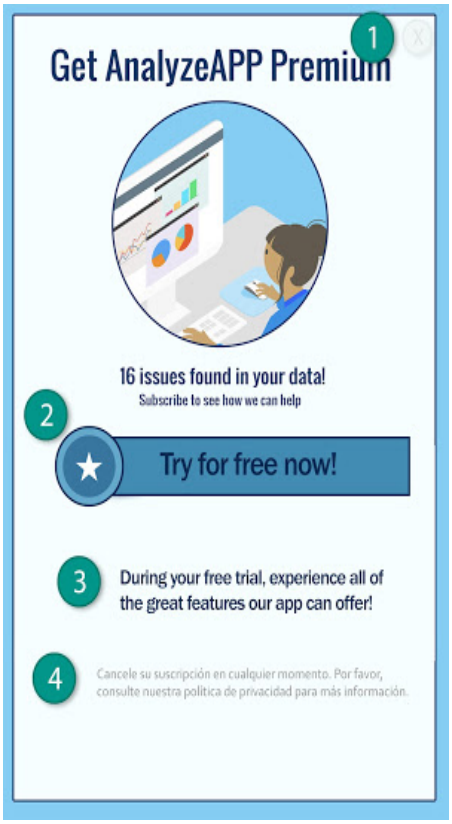
④ L'offre doit être localisée dans la même langue que les conditions d'utilisation afin que les utilisateurs puissent la comprendre dans son intégralité.

Essais gratuits et offres de bienvenue

Avant souscription d'un utilisateur à votre abonnement : vous devez exposer clairement et de manière exhaustive les conditions d'utilisation de votre offre, y compris la durée, le prix et la description des contenus ou services rendus accessibles. Veillez à bien indiquer aux utilisateurs les modalités de conversion d'un essai gratuit en abonnement payant, le moment où ce changement intervient, le montant de l'abonnement et la possibilité de l'annuler s'ils ne souhaitent pas passer à un abonnement payant.

Voici quelques exemples courants de non-respect des règles :

- Les offres qui n'expliquent pas clairement la durée de l'essai gratuit ou du prix découverte.
- Les offres qui n'expliquent pas clairement que l'utilisateur souscrit automatiquement un abonnement payant au terme de l'offre.
- Les offres qui n'indiquent pas clairement que l'utilisateur peut accéder à des contenus sans essai (le cas échéant).
- Les offres dont la tarification et les conditions d'utilisation ne sont pas intégralement localisées.



① Le bouton "Ignorer" n'est pas clairement visible. Par conséquent, il est possible que les utilisateurs ne comprennent pas qu'ils peuvent accéder aux fonctionnalités sans s'inscrire à l'essai gratuit.

② L'offre met l'accent sur l'essai gratuit. Ainsi, il est possible que les utilisateurs ne comprennent pas qu'ils seront automatiquement facturés à la fin de l'essai.

③ L'offre ne précise pas la durée de l'essai. De ce fait, il est possible que les utilisateurs ne comprennent pas combien de temps durera leur accès gratuit au contenu disponible sur abonnement.

④ L'offre doit être localisée dans la même langue que les conditions d'utilisation afin que les utilisateurs puissent la comprendre dans son intégralité.

Gestion des abonnements et annulation

En tant que développeur, vous devez vous assurer que votre application indique clairement comment un utilisateur doit procéder pour gérer ou résilier son abonnement.

Il vous incombe d'informer vos utilisateurs de toute modification des modalités d'abonnement, de résiliation et de remboursement. Vous devez également vous assurer que ces modalités respectent les lois applicables.

Annonces

Nous n'acceptons pas les applications contenant des annonces mensongères ou intrusives. Les annonces ne doivent être affichées que dans l'application qui les diffuse. Nous considérons les annonces diffusées dans votre application comme faisant partie intégrante de celle-ci. Elles doivent donc respecter l'ensemble de nos règles. Consultez nos règles concernant les annonces pour les jeux d'argent et de hasard.

Utilisation des données de localisation à des fins publicitaires

Toute application qui utilise également les données de localisation reposant sur des autorisations pour diffuser des annonces est soumise au règlement sur les informations personnelles et sensibles. Elle doit en outre respecter les exigences suivantes :

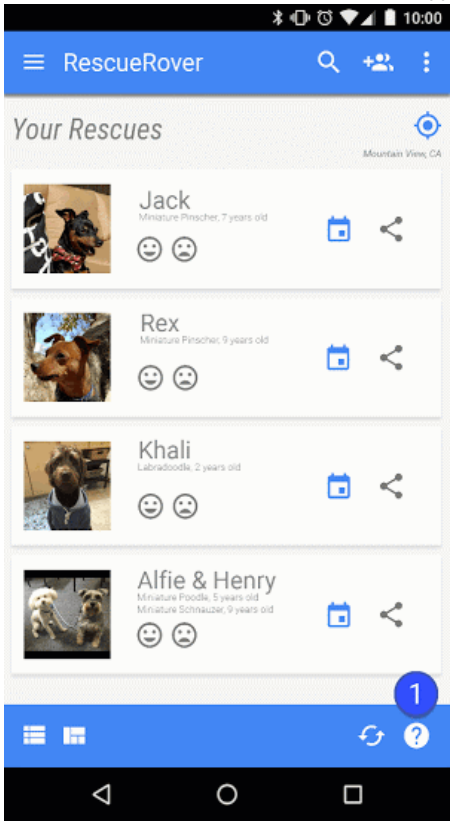
- L'utilisation ou la collecte de données de localisation reposant sur des autorisations à des fins publicitaires doit être communiquée clairement à l'utilisateur et décrite dans les règles de confidentialité de l'application, y compris en indiquant toute règle de confidentialité du réseau publicitaire qui concerne l'utilisation des données de localisation.
- Conformément aux exigences sur les autorisations d'accéder à la position, vous ne pouvez demander cette autorisation que pour mettre en œuvre des fonctionnalités ou services déjà disponibles dans votre application. Une telle demande d'autorisation ne peut pas être effectuée exclusivement à des fins publicitaires.

Annonces mensongères

Les annonces ne doivent pas simuler ou imiter l'interface d'une application ni les avertissements ou les notifications envoyés par le système. L'utilisateur doit pouvoir identifier clairement l'application associée à chacune des annonces.

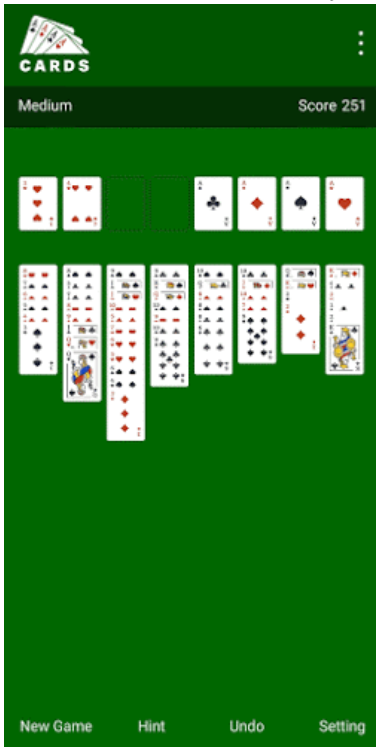
Voici quelques exemples courants de non-respect des règles :

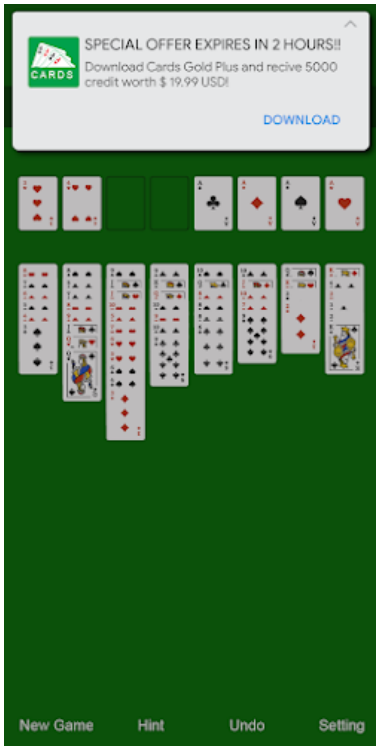
- Annonces imitant l'interface utilisateur d'une application :



① L'icône représentant un point d'interrogation est une annonce qui sert à rediriger l'utilisateur vers une page de destination externe.

- Annonces imitant une notification système :



- 

Les exemples ci-dessus illustrent des imitations de diverses notifications système.

Monétisation de l'écran de verrouillage

Excepté lorsque le but exclusif de l'application est celui d'un écran de verrouillage, les applications ne peuvent pas introduire d'annonces ni de fonctionnalités qui monétisent l'écran verrouillé d'un appareil.

Annonces intrusives

Les annonces intrusives sont des annonces qui s'affichent de manière impromptue, ce qui peut aboutir à des clics intempestifs, ou qui altèrent l'utilisation des fonctionnalités de l'appareil ou interfèrent avec cette utilisation.

Votre application ne doit pas forcer un utilisateur à cliquer sur des annonces ou à communiquer des informations personnelles à des fins publicitaires avant qu'il puisse accéder à toutes les fonctionnalités d'une application. Les

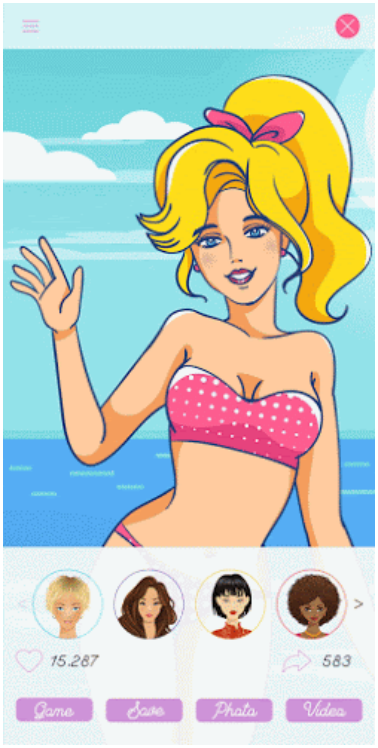
annonces interstitielles ne peuvent être affichées que dans l'application dans laquelle elles sont diffusées. L'utilisateur doit avoir la possibilité d'ignorer les annonces interstitielles, ou d'autres types d'annonces qui perturbent le fonctionnement normal de votre application, sans être pénalisé.

Voici quelques exemples courants de non-respect des règles :

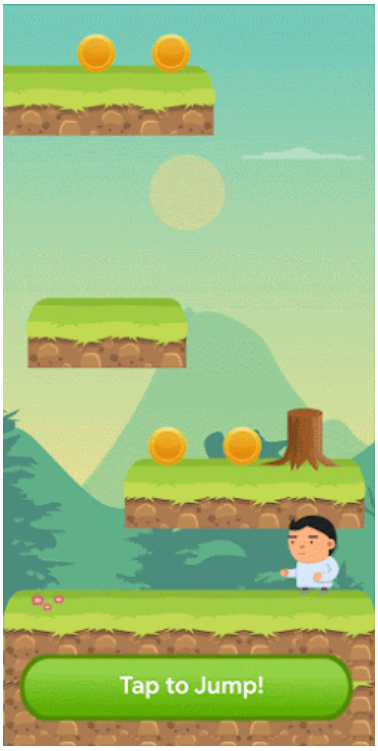
- Annonces qui occupent tout l'écran ou qui perturbent l'utilisation normale de l'application, et qui n'indiquent pas clairement comment les ignorer :

① L'application ne contient pas de bouton "Ignorer".

- Annonces qui forcent l'utilisateur à cliquer en utilisant un faux bouton "Ignorer" ou en faisant apparaître soudainement des annonces dans des zones de l'application que l'utilisateur sélectionne généralement pour une autre fonction.



Annonce qui utilise un faux bouton "Ignorer"



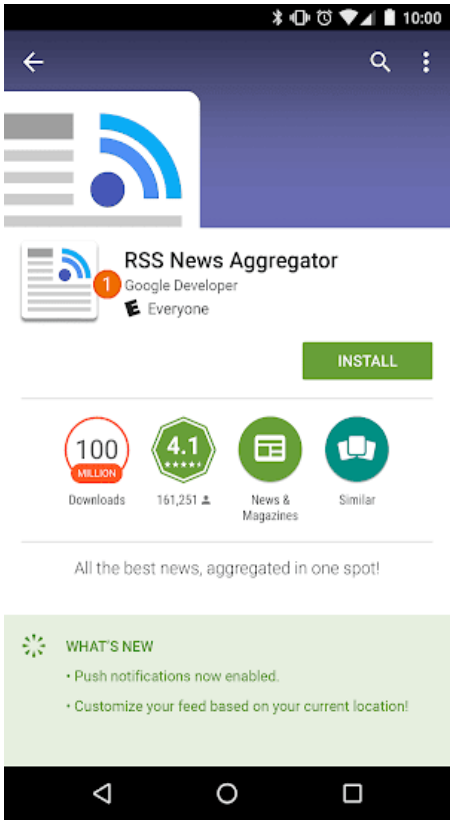
Annonce qui apparaît soudainement dans une zone où l'utilisateur a l'habitude d'appuyer pour utiliser des fonctions intégrées à l'application

Interférence avec des applications, des annonces tierces ou le fonctionnement de l'appareil

Les annonces associées à votre application ne doivent pas interférer avec d'autres applications, d'autres annonces ni avec le fonctionnement de l'appareil, y compris les boutons, les ports ou le système d'exploitation de celui-ci. Cela inclut les superpositions, les fonctionnalités complémentaires et les blocs d'annonces comprenant des widgets. Les annonces ne doivent être affichées que dans l'application qui les diffuse.

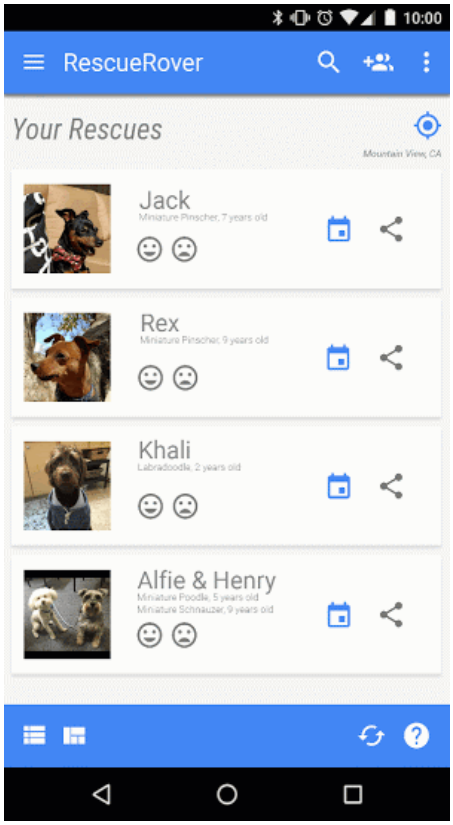
Voici quelques exemples courants de non-respect des règles :

- Annonces qui s'affichent en dehors de l'application qui les diffuse :



Description : l'utilisateur accède à l'écran d'accueil à partir de cette application, et soudainement, une annonce s'affiche sur celui-ci.

- Annonces dont l'affichage est déclenché par le bouton d'accueil ou par d'autres fonctionnalités explicitement conçues pour quitter l'application :

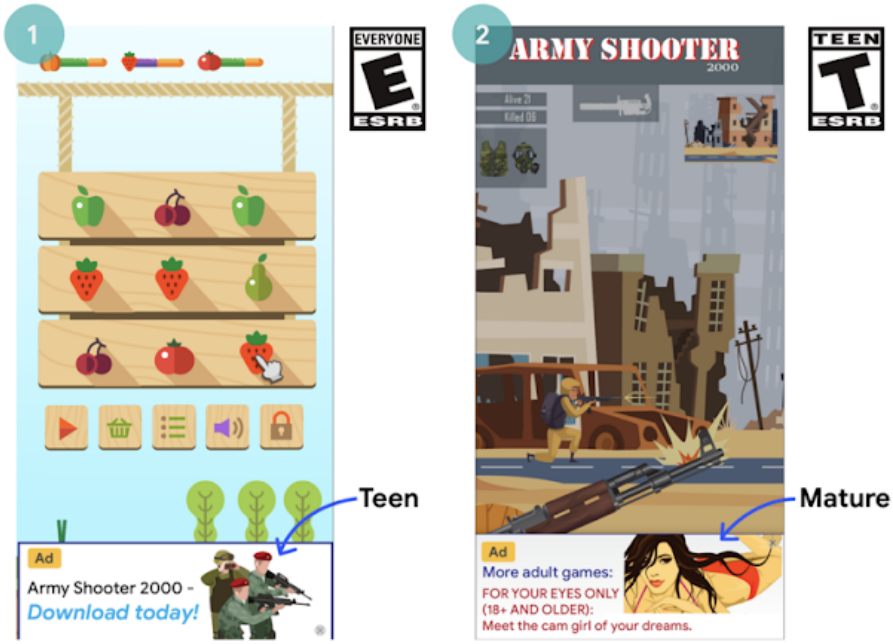


Description : l'utilisateur tente de quitter l'application et d'accéder à l'écran d'accueil, mais ce parcours est interrompu par l'affichage d'une annonce.

Annonces inappropriées

Les annonces qui s'affichent dans votre application doivent être adaptées au public ciblé par votre application, même si le contenu en lui-même est conforme à nos règles.

Voici un exemple courant de non-respect des règles :



① Cette annonce réservée aux adolescents n'est pas adaptée au public ciblé par cette application (7 ans et plus)
② Cette annonce réservée aux adultes n'est pas adaptée au public ciblé par cette application (12 ans et plus)

Utilisation de l'identifiant publicitaire Android

La version 4.0 des services Google Play introduit de nouvelles API ainsi qu'un ID à l'usage des fournisseurs de services de publicité et de statistiques. Les conditions d'utilisation de cet identifiant figurent ci-dessous.

- **Utilisation** : l'identifiant publicitaire Android ne doit être utilisé qu'à des fins de publicité et de statistiques sur les utilisateurs. En outre, vous devez vérifier l'état du paramètre "Désactiver les annonces par centres d'intérêt" ou "Désactiver la personnalisation des annonces" à chaque fois que vous y accédez.
- **Association à des informations personnelles ou à d'autres identifiants**.
  - Utilisation à des fins publicitaires : l'identifiant publicitaire ne doit pas être associé à des identifiants permanents de l'appareil (par exemple, SSAID, adresse MAC, code IMEI, etc.) à des fins publicitaires. L'identifiant publicitaire ne peut être associé à des informations personnelles qu'avec le consentement explicite de l'utilisateur.
  - Utilisation à des fins d'analyse : l'identifiant publicitaire ne doit pas être associé à des informations personnelles ni à un identifiant permanent de l'appareil (par exemple, SSAID, adresse MAC, code IMEI, etc.) sans le consentement explicite de l'utilisateur.
- **Respect des choix de l'utilisateur**. En cas de réinitialisation de l'identifiant publicitaire, celui-ci ne doit pas être associé à l'identifiant précédent ni à des données dérivées de ce dernier sans le consentement explicite de l'utilisateur. Par ailleurs, vous devez respecter le paramètre "Désactiver les annonces par centres d'intérêt" ou "Désactiver la personnalisation des annonces" défini par l'utilisateur. Si ce paramètre est activé, vous ne devez pas utiliser l'identifiant publicitaire pour créer des profils utilisateur à des fins de publicité ni pour cibler des utilisateurs avec des annonces personnalisées. En revanche, la publicité contextuelle, la limitation du nombre d'expositions, le suivi des conversions, la création de rapports, la sécurité et la détection des fraudes font partie des activités autorisées.
- **Transparence envers les utilisateurs**. Les utilisateurs doivent être informés de la collecte et de l'utilisation de l'identifiant publicitaire, ainsi que de votre engagement à respecter les présentes conditions, via un avis de confidentialité adéquat sur le plan juridique. Pour en savoir plus sur les règles que nous appliquons en termes de confidentialité, consultez le règlement concernant les Données utilisateur.
- **Respect des conditions d'utilisation**. L'identifiant publicitaire ne doit être utilisé que conformément aux présentes conditions, y compris par les tiers auxquels vous le communiquez dans le cadre de votre activité. Il doit être utilisé à des fins publicitaires (si disponible sur l'appareil) à la place de tout autre identifiant, pour toutes les applications importées ou publiées sur Google Play.

Programme d'annonces adaptées aux familles

Si vous diffusez des annonces dans votre application et que celle-ci ne cible que les enfants, comme décrit dans les Règles pour les contenus familiaux, vous devez utiliser des SDK publicitaires ayant été autocertifiés conformes aux règles de Google Play, y compris aux exigences de certification des SDK publicitaires ci-dessous. Si votre application cible à la fois les enfants et les utilisateurs plus âgés, vous devez mettre en place des mesures de filtrage en fonction de l'âge et vous assurer que les annonces présentées aux enfants proviennent exclusivement de l'un de ces SDK publicitaires autocertifiés. Les applications du programme Pour la famille ne doivent utiliser que des SDK publicitaires autocertifiés.

L'utilisation de SDK certifiés Google Play n'est obligatoire que si vous recourez à des SDK publicitaires pour diffuser des annonces auprès des enfants. Vous pouvez prendre les mesures suivantes sans procéder à l'autocertification d'un SDK publicitaire avec Google Play. Cependant, vous êtes toujours tenu de vous assurer que vos pratiques en termes de contenus publicitaires et de collecte de données sont conformes au Règlement sur les données utilisateur et aux Règles pour les contenus familiaux de Play :

- Auto-promotion par laquelle vous utilisez des SDK pour gérer la promotion croisée de vos applications ou autres contenus multimédias propriétaires, ainsi que leur merchandising
- Conclusion d'accords directs avec des annonceurs par lesquels vous utilisez des SDK pour gérer l'inventaire

Exigences de certification des SDK publicitaires

- Définissez les contenus d'annonces et les comportements inappropriés, et interdisez-les dans les conditions d'utilisation ou les règles du SDK publicitaire. Les définitions doivent respecter le règlement du programme Play pour les développeurs.
- Créez une méthode permettant d'évaluer vos créations en fonction des tranches d'âge appropriées. Celles-ci doivent inclure, a minima, les groupes "Tout public" et "Adultes". La méthode de classification doit être alignée sur la méthode que Google offre aux fournisseurs de SDK une fois qu'ils ont rempli le formulaire de contact ci-dessous.
- Pour chaque demande ou pour chaque application, autorisez les éditeurs à demander un traitement adapté aux contenus destinés aux enfants pour la diffusion d'annonce. Ce traitement doit être conforme aux lois et réglementations applicables, comme la Loi américaine COPPA (Children's Online Privacy Protection Act) et le Règlement général sur la protection des données (RGPD) de l'Union européenne. Dans le cadre du traitement adapté aux contenus destinés aux enfants, Google Play requiert également la désactivation, par les SDK publicitaires, des annonces personnalisées, de la publicité ciblée par centres d'intérêt et du remarketing.
- Autorisez les éditeurs à sélectionner des formats d'annonces conformes aux Règles de Google Play relatives à la monétisation et aux annonces pour les familles, et répondant aux exigences du programme "Approuvé par les enseignants".
- Lorsque les enchères en temps réel sont utilisées pour diffuser des annonces auprès des enfants, assurez-vous que les créations ont été examinées et que les indicateurs de confidentialité sont transmis aux enchérisseurs.
- Fournissez à Google suffisamment d'informations, telles que celles indiquées dans le formulaire de contact ci-dessous, pour permettre la vérification de la conformité du SDK publicitaire avec toutes les exigences de certification, et répondez dans les meilleurs délais à toute demande d'informations ultérieure.

Remarque : Les SDK publicitaires doivent accepter une diffusion d'annonces conforme à toutes les lois et réglementations concernant les enfants qui peuvent s'appliquer aux éditeurs.

Exigences concernant la médiation pour les plates-formes de diffusion, dans le cas de la diffusion d'annonces auprès des enfants :

- Utilisez uniquement des SDK publicitaires certifiés Google Play, ou mettez en place les protections nécessaires pour vous assurer que toutes les annonces diffusées par des réseaux de médiation respectent ces exigences.
- Transmettez aux plates-formes de médiation les informations nécessaires pour indiquer la classification du contenu des annonces et tout traitement applicable adapté aux contenus destinés aux enfants.

Les développeurs peuvent consulter la liste des SDK publicitaires autocertifiés.

Ils peuvent par ailleurs partager ce formulaire de contact avec les fournisseurs de SDK publicitaires qui souhaitent s'autocertifier.

Fiches Play Store et promotion

La promotion et la visibilité de votre application ont un impact considérable sur la qualité du Play Store. Évitez de créer une fiche Play Store trop agressive sur le plan commercial et soignez son contenu, et ne tentez pas d'optimiser artificiellement la visibilité de votre application sur Google Play.

Promotion d'une application

Nous n'acceptons pas les applications qui participent ou tirent profit directement ou indirectement de pratiques promotionnelles qui sont mensongères ou nuisibles aux utilisateurs ou à l'écosystème du développeur. Ceci s'applique aux applications qui utilisent les procédés suivants :

- L'utilisation d'annonces mensongères figurant sur des sites Web, des applications ou d'autres supports, y compris les notifications qui ressemblent aux notifications et alertes système.
- La promotion ou les stratégies d'installation qui entraînent une redirection de l'utilisateur sur Google Play ou le téléchargement d'applications sans que ce dernier en soit informé préalablement.
- L'envoi de messages promotionnels indésirables par SMS.

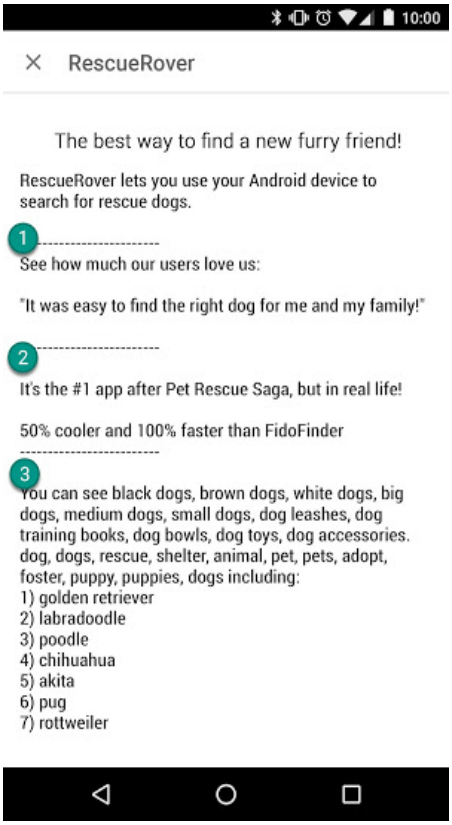
Il vous incombe de vous assurer que les réseaux publicitaires et les sociétés affiliées associés à votre application respectent ces règles et qu'ils n'utilisent aucune pratique promotionnelle interdite.

Métadonnées

Nous n'autorisons pas les applications comportant des métadonnées trompeuses, non descriptives, non pertinentes, excessives, inappropriées ou présentant un format incorrect, y compris, sans s'y limiter, dans la description, le nom du développeur, le titre, l'icône, les captures d'écran et les images publicitaires. Les développeurs sont tenus de fournir une description claire et bien rédigée. Nous n'acceptons pas non plus les témoignages d'utilisateurs non attribués ou anonymes dans la description des applications.

Outre les exigences mentionnées ici, certains points du règlement Play pour les développeurs peuvent vous obliger à fournir des métadonnées supplémentaires.

Voici quelques exemples courants de non-respect des règles :



① Témoignages d'utilisateurs non attribués ou anonymes
② Comparaison de données d'applications ou de marques
③ Blocs de mots et listes de mots verticales ou horizontales

Voici quelques exemples de texte, d'images ou de vidéos inappropriés dans une fiche :

- Images ou vidéos présentant du contenu à caractère sexuel : évitez d'utiliser des contenus suggestifs montrant des seins, des fesses, des organes génitaux ou d'autres parties de l'anatomie érotisées, sous la forme de dessins ou d'images réelles.
- Utiliser un langage grossier, vulgaire ou tout autre langage inapproprié pour le grand public dans la fiche Play Store de votre application

- Violence explicite représentée de manière évidente dans des icônes d'application, des images promotionnelles ou des vidéos.
- Représentation de la consommation illicite de drogues : même les contenus éducatifs, documentaires, scientifiques ou artistiques doivent être adaptés à tous les publics sur la fiche Play Store.

Voici quelques bonnes pratiques :

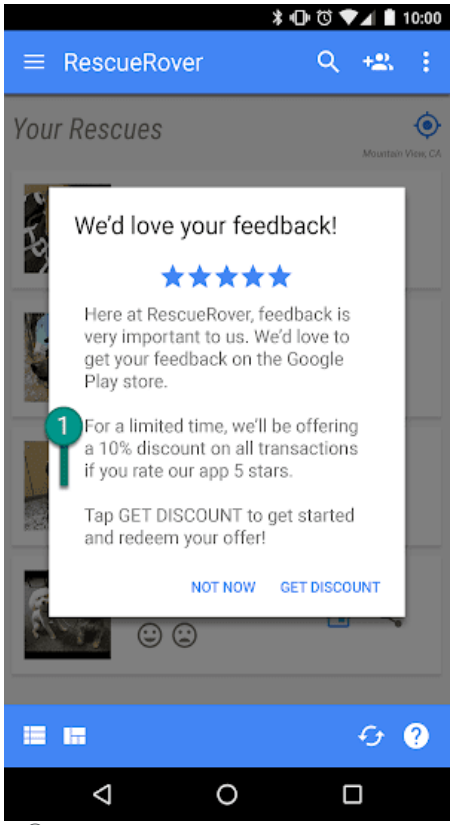
- Soulignez les avantages de votre application : mettez en avant les points intéressants et attrayants de votre application afin de susciter l'intérêt des utilisateurs.
- Assurez-vous que le titre et la description de votre application décrivent précisément ses fonctionnalités.
- Évitez d'utiliser des mots clés ou des références répétitifs ou sans rapport avec l'application.
- La description de votre application doit être brève et claire. Les descriptions courtes sont généralement plus agréables à lire, en particulier sur les appareils dont l'écran est de petite taille. Une longueur, des détails ou des répétitions excessifs ainsi qu'une mise en forme incorrecte peuvent entraîner le non-respect des présentes règles.
- Gardez à l'esprit que votre fiche doit être adaptée à tous les publics : évitez d'utiliser du texte, des images ou des vidéos inappropriés dans celle-ci et respectez les consignes ci-dessus.

Notes, avis et installations des utilisateurs

Les développeurs ne doivent pas essayer d'influencer le classement d'une application dans Google Play. Il leur est notamment interdit d'améliorer artificiellement les notes et les avis, et d'augmenter le nombre d'installations par des moyens non autorisés, de manière frauduleuse ou en proposant l'obtention d'un avantage.

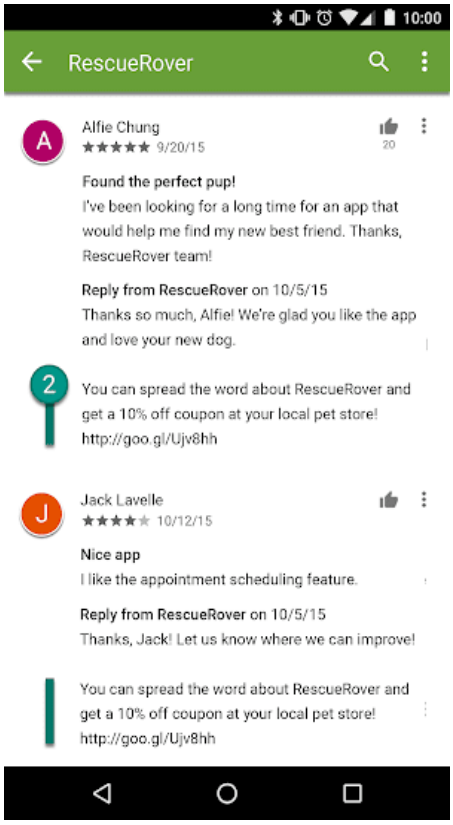
Voici quelques exemples courants de non-respect des règles :

- Demander aux utilisateurs de noter votre application en leur offrant un avantage :



① Cette notification propose une remise à l'utilisateur, en échange d'une bonne note.

- Envoyer des notes de manière répétitive pour influencer le classement de l'application sur Google Play.
- Envoyer ou encourager les utilisateurs à envoyer des avis comportant des contenus inappropriés, tels que des sociétés affiliées, des coupons, des codes de jeu, des adresses e-mail ou des liens vers des sites Web ou d'autres applications :



② Cet avis incite les utilisateurs à faire la promotion de l'application Rescue Rovers en échange d'une offre de coupon.

Les notes et les avis sont des indicateurs de la qualité des applications. Les utilisateurs comptent sur leur authenticité et leur pertinence. Voici quelques bonnes pratiques à suivre lors des réponses aux avis d'utilisateurs :

- Concentrez-vous sur les problèmes soulevés dans les commentaires des utilisateurs, et ne demandez pas de notes plus élevées.
- N'hésitez pas à inclure des références relatives à des ressources utiles, telles que l'adresse d'un service d'assistance ou une page des FAQ.

Classification du contenu

Le système de classification du contenu sur Google Play est tiré des classifications officielles de l'IARC (International Age Rating Coalition). Il vise à aider les développeurs à communiquer aux utilisateurs les classifications de contenus pertinentes au niveau local. Les bureaux régionaux de l'IARC gèrent les consignes utilisées pour classer le contenu d'une application. Nous n'autorisons pas les applications sans classification du contenu sur Google Play.

Utilité de la classification du contenu

La classification du contenu permet d'informer les consommateurs, en particulier les parents, de la présence de contenu potentiellement choquant dans une application. Elle sert également à filtrer ou bloquer votre contenu sur certains territoires ou pour des utilisateurs spécifiques dans les régions où la loi l'exige, ainsi qu'à évaluer l'éligibilité de votre application dans le cadre de programmes spéciaux pour les développeurs.

Attribuer une catégorie de classification du contenu

Pour obtenir une catégorie de classification, vous devez remplir un questionnaire sur la classification du contenu dans la Play Console concernant la nature du contenu de votre application. En fonction de vos réponses, plusieurs organismes d'évaluation attribueront une catégorie de classification. Toute déclaration trompeuse sur le contenu de votre application peut entraîner la suppression ou la suspension de celle-ci. Par conséquent, veillez à fournir des réponses fidèles à la réalité.

Pour éviter qu'une de vos applications soit classée dans la catégorie "Aucune classification", vous devez remplir le questionnaire de classification du contenu pour chaque nouvelle application envoyée via la Play Console, ainsi que pour toutes les applications actives sur Google Play.

Si vous apportez une modification au contenu ou à une fonctionnalité de votre application, et que ce changement a une incidence sur les réponses que vous avez déjà fournies dans le questionnaire de classification, vous devez remplir de nouveau le questionnaire dans la Play Console.

Consultez le Centre d'aide pour en savoir plus sur les différents organismes d'évaluation et sur la façon de remplir le questionnaire sur la classification du contenu.

Contester la catégorie de classification

Si vous souhaitez contester la catégorie de classification attribuée à votre application, vous pouvez le faire directement auprès de l'IARC en cliquant sur le lien figurant dans l'e-mail de certificat.

Actualités

Les applications pour lesquelles la catégorie "Actualités" est sélectionnée, mais dont le contenu ne respecte pas les exigences ci-dessous, ne sont pas autorisées dans cette catégorie du Play Store. Les applications d'actualités qui nécessitent un abonnement doivent fournir un aperçu du contenu aux utilisateurs avant l'achat.

Les applications d'actualités DOIVENT :

- fournir des informations claires et adéquates sur l'éditeur d'actualités et ses contributeurs, y compris quant à l'identité du propriétaire ; et
- être associées à un site Web ou intégrer une page contenant les coordonnées, valides, de l'éditeur d'actualités.

Les applications d'actualités NE DOIVENT PAS :

- contenir de fautes d'orthographe et de grammaire graves ;
- comporter uniquement du contenu statique ; et
- avoir pour objectif principal une affiliation ou des revenus publicitaires.

Les applications d'agrégateur d'actualités doivent être transparentes quant aux sources des contenus dans l'application. Chacune de ces sources doit respecter les règles concernant les actualités.

Spam et fonctionnalités minimales

Les applications doivent au minimum être respectueuses de l'utilisateur et lui offrir un niveau basique de fonctionnalités. Les applications qui plantent ou ne sont pas fonctionnelles en raison d'un autre type de comportement, et celles qui ne servent qu'à présenter du spam aux utilisateurs ou sur Google Play n'apportent rien au catalogue d'applications.

Spam

Nous n'autorisons pas les applications qui envoient du spam aux utilisateurs ou polluent Google Play, c'est-à-dire celles qui envoient des messages non sollicités, publient des contenus répétitifs ou sont de mauvaise qualité.

Spam dans les messages

Nous n'acceptons pas les applications qui envoient des SMS, des e-mails ou d'autres messages au nom de l'utilisateur sans donner à celui-ci la possibilité d'en valider le contenu et de confirmer le nom du destinataire souhaité.

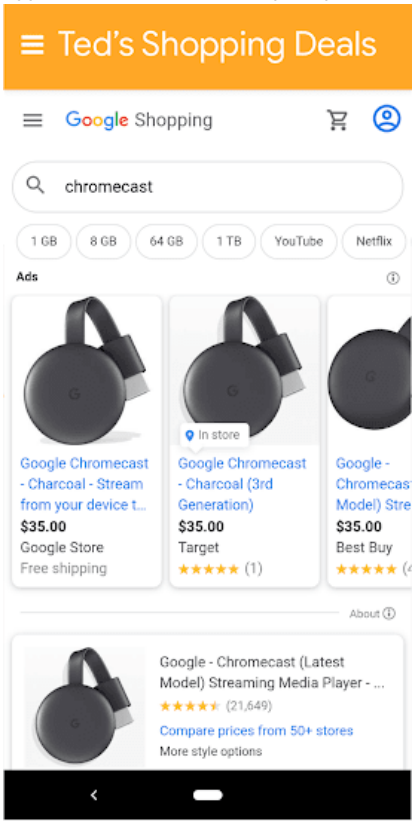
Spam dans les WebView et spam affilié

Nous n'autorisons aucune application dont la fonction principale consiste à générer du trafic d'affiliation sur un site Web ou à fournir un aperçu d'un site Web sans autorisation du propriétaire ou de l'administrateur de celui-ci.

Voici quelques exemples courants de non-respect des règles :

- Application dont la fonction principale consiste à générer du trafic généré par les sites référents vers un site Web dans le but de recevoir des crédits pour les connexions ou les achats effectués par les utilisateurs sur le site Web en question.

- Applications dont la fonction principale consiste à fournir un aperçu d'un site Web sans autorisation :



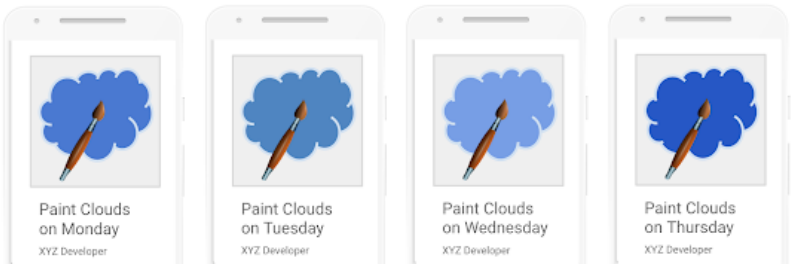
Cette application est appelée "Ted's Shopping Deals" et fournit simplement une WebView de Google Shopping.

Contenus répétitifs

Nous n'autorisons pas les applications qui offrent exclusivement ce que proposent déjà d'autres applications sur Google Play. Les applications doivent fournir aux utilisateurs une valeur ajoutée par le biais de contenus ou de services uniques.

Voici quelques exemples courants de non-respect des règles :

- Copier le contenu d'autres applications sans ajouter de contenu original ni apporter de valeur ajoutée.
- Créer plusieurs applications offrant un contenu et une expérience utilisateur très similaires. Si le contenu de chaque application est peu volumineux, nous recommandons au développeur concerné de regrouper les différents contenus dans une même application.



Applications créées à des fins publicitaires

Nous n'autorisons pas les applications dont l'objectif premier est la diffusion d'annonces.

Voici quelques exemples courants de non-respect des règles :

- Applications dans lesquelles des annonces interstitielles sont placées après chaque action de l'utilisateur, y compris, mais sans s'y limiter, les clics, les balayages d'écran, etc.

Fonctionnalités minimales

Assurez-vous que votre application offre une expérience utilisateur réactive, stable et stimulante.

Voici quelques exemples courants de non-respect des règles :

- Applications conçues pour ne rien faire ou qui n'ont aucune fonction

Applications non fonctionnelles

Nous n'autorisons pas les applications qui plantent, se ferment de manière forcée, se bloquent ou présentent un autre comportement anormal.

Voici quelques exemples courants de non-respect des règles :

- Applications **impossibles à installer**
- Applications que l'utilisateur peut installer, mais **qui ne se chargent pas**
- Applications qui se chargent, mais qui ne sont **pas réactives**

Autres programmes

Outre le règlement relatif au contenu (également disponible sur ce site), les applications proposées dans le cadre d'autres programmes Android et distribuées via Google Play peuvent être également soumises à des règles spécifiques. Veillez à consulter la liste ci-dessous pour savoir si votre application doit respecter l'une ou l'autre de ces règles.

Applis instantanées Android

Avec les applis instantanées Android, nous souhaitons créer des expériences utilisateur plaisantes et fluides, tout en respectant des critères très stricts en matière de confidentialité et de sécurité. Nos règles sont rédigées dans cet objectif.

Les développeurs qui choisissent de distribuer des applis instantanées Android via Google Play doivent respecter les règles suivantes, en plus de l'ensemble du Règlement du programme Google Play pour les développeurs.

Identité

Pour les applis instantanées comportant une fonctionnalité de connexion, les développeurs doivent intégrer Smart Lock pour les mots de passe.

Liens

Les développeurs d'applis instantanées Android sont tenus de prendre en charge correctement les liens vers d'autres applications. Si l'appli instantanée du développeur ou l'appli installée contient des liens susceptibles de renvoyer vers une appli instantanée, le développeur doit rediriger les utilisateurs vers cette appli instantanée plutôt que de capturer les liens dans une WebView.

Caractéristiques techniques

Les développeurs doivent respecter les caractéristiques techniques et les exigences relatives aux applis instantanées Android. Ces caractéristiques et exigences sont fournies par Google et peuvent faire l'objet de modifications occasionnelles, y compris celles exposées dans notre Documentation publique.

Proposition d'installation de l'application

Une appli instantanée peut proposer à l'utilisateur d'installer l'application, mais il ne doit pas s'agir de son but principal. Si l'installation est proposée, le développeur doit respecter les points suivants :

- Utiliser l'icône Material Design de téléchargement d'application et le libellé "Installer" pour le bouton d'installation
- Ne pas inclure plus de deux ou trois invites d'installation implicites dans son appli instantanée
- Ne pas utiliser de bannière ni d'autres techniques publicitaires pour présenter une invite d'installation aux utilisateurs

Vous trouverez de plus amples informations et consignes relatives à l'expérience utilisateur dans le guide des Bonnes pratiques en matière d'expérience utilisateur.

Modification de l'état de l'appareil

Les applis instantanées ne doivent pas apporter de modifications à l'appareil de l'utilisateur qui persistent après la session d'utilisation de l'appli. À titre d'exemple, elles ne doivent pas changer le fond d'écran ni créer de widget sur l'écran d'accueil.

Visibilité de l'application

Les développeurs doivent s'assurer que leurs applis instantanées sont visibles par l'utilisateur, qui doit savoir quand l'appli est exécutée sur son appareil.

Identifiants des appareils

Les applis instantanées ne doivent pas accéder aux identifiants des appareils qui (1) persistent après que l'appli n'est plus exécutée et (2) ne sont pas modifiables par l'utilisateur. Cela inclut, sans s'y limiter, les identifiants suivants :

- Numéro de série
- Adresses Mac des puces réseau
- Codes IMEI et IMSI

Les applis instantanées peuvent accéder au numéro de téléphone si elles l'obtiennent via l'autorisation d'exécution. Le développeur ne doit pas essayer de tracer l'utilisateur à l'aide de ces identifiants ni d'aucune autre manière.

Trafic réseau

Le trafic réseau provenant de l'appli instantanée doit être chiffré à l'aide d'un protocole TLS, tel que HTTPS.

Familles

Google Play est une plate-forme riche, sur laquelle les développeurs peuvent proposer des contenus de qualité et appropriés pour toute la famille. Avant de soumettre une application au programme Pour la famille ou de soumettre une application qui cible les enfants sur le Google Play Store, vous devez vous assurer que votre application est adaptée aux enfants et conforme à toutes les lois pertinentes.

Découvrez le processus spécifique aux familles et consultez la checklist interactive dans l'Académie pour les développeurs d'applications.

Conception d'applications pour les enfants et les familles

L'utilisation de la technologie comme outil d'enrichissement de la vie familiale croît, et les parents sont à la recherche de contenu sûr et de qualité à partager avec leurs enfants. Que vous conceviez des applications précisément pour les enfants ou qui attirent simplement l'attention de cette audience, Google Play vous permet de vous assurer que votre application est adaptée à tous les utilisateurs, y compris les familles.

La définition du terme "enfant" peut varier selon les langues et les contextes. Il est important que vous consultiez votre conseiller juridique afin de déterminer les obligations et/ou restrictions liées à l'âge que votre application doit respecter. C'est vous qui connaissez le mieux le fonctionnement de votre application. C'est pourquoi nous comptons sur vous pour nous aider à faire en sorte que les applications sur Google Play conviennent aux familles.

Les applications spécialement conçues pour les enfants doivent être enregistrées auprès du programme Pour la famille. Si votre application cible à la fois les enfants et les personnes plus âgées, vous pouvez tout de même participer au programme Pour la famille. Toutes les applications qui participent au programme Pour la famille pourront être évaluées dans le cadre du programme "Approuvé par les enseignants". Nous ne pouvons toutefois pas garantir que votre application sera incluse dans ce programme. Si vous décidez de ne pas enregistrer votre application auprès du programme Pour la famille, vous devez quand même respecter les règles Google Play pour les contenus familiaux indiquées ci-dessous, ainsi que le Règlement du programme Google Play pour les développeurs et le Contrat relatif à la distribution (pour les développeurs).

Exigences concernant la Play Console

Cible et contenu

Dans la section Cible et contenu de la Google Play Console, vous devez indiquer, avant la publication, la cible de votre application en sélectionnant la tranche d'âge dans la liste proposée. Quel que soit votre choix dans la Google Play Console, si votre application contient des images ou des termes susceptibles d'être considérés comme ciblant les enfants, cela peut avoir une incidence sur l'évaluation de Google Play quant à la cible que vous avez déclarée. Google Play se réserve le droit de procéder à son propre examen des informations que vous avez fournies au sujet de votre application pour déterminer si la cible que vous avez déclarée est correcte.

Si vous sélectionnez une cible qui exclut les enfants, mais que Google détermine que cela n'est pas correct, car votre application cible à la fois les enfants et les adultes, vous aurez la possibilité d'indiquer clairement aux utilisateurs que votre application ne cible pas les enfants en acceptant un libellé d'avertissement.

Vous ne devez sélectionner plusieurs tranches d'âge pour la cible de votre application que si vous avez conçu votre application pour les utilisateurs dans ces tranches d'âge et si vous vous êtes assuré que votre application est adaptée à cette audience. Par exemple, pour les applications conçues pour les bébés, les tout-petits et les enfants d'âge préscolaire,

vous ne devez sélectionner que la tranche d'âge "Enfants de 5 ans et moins" comme tranche d'âge cible de ces applications. Si votre application est conçue pour un niveau scolaire spécifique, sélectionnez la tranche d'âge qui convient le mieux. Vous ne devez sélectionner les tranches d'âge qui incluent à la fois les adultes et les enfants que si vous avez réellement développé votre application pour tous les âges.

Mises à jour de la section "Cible et contenu"

Vous pouvez toujours mettre à jour les informations concernant votre application dans la section "Cible et contenu" de la Google Play Console. Une mise à jour de l'application est requise avant que ces informations n'apparaissent sur le Google Play Store. Toutefois, toute modification que vous apportez à cette section de la console Google Play peut être examinée afin de déterminer sa conformité au règlement, même avant qu'une mise à jour de l'application ne soit soumise.

Nous vous recommandons vivement d'informer vos utilisateurs existants si vous modifiez la tranche d'âge cible de votre application, ou si vous commencez à diffuser des annonces ou à recourir aux achats via l'application, soit en utilisant la section "Nouveautés" de la fiche Play Store de votre application, soit par le biais de notifications dans l'application.

Déclarations trompeuses dans la Play Console

Toute déclaration trompeuse concernant votre application dans la console Play, y compris dans la section "Cible et contenu", peut entraîner la suppression ou la suspension de l'application. C'est pourquoi il est important de fournir des informations correctes.

Règles pour les contenus familiaux

Si les enfants constituent l'une des cibles de votre application, vous devez respecter les exigences ci-dessous, faute de quoi votre application peut être supprimée ou suspendue.

1. **Contenu de l'application** : le contenu de votre application accessible aux enfants doit être approprié pour cette audience.
2. **Réponses dans la Google Play Console** : vous devez répondre correctement aux questions sur votre application dans la Google Play Console et mettre à jour ces réponses pour refléter avec précision toute modification de votre application.
3. **Annonces**. Si votre application diffuse des annonces auprès des enfants ou d'utilisateurs dont l'âge n'est pas connu, vous devez respecter les règles suivantes :
   - Utilisez uniquement des SDK publicitaires certifiés Google Play pour diffuser des annonces auprès de ces utilisateurs.
   - Assurez-vous que les annonces visibles par ces utilisateurs ne sont pas ciblées par centres d'intérêt (annonces ciblant des internautes ayant certaines caractéristiques en fonction de leur comportement de navigation en ligne) ni diffusées dans un but de remarketing (annonces ciblant des internautes en fonction d'une interaction précédente avec une application ou un site Web).
   - Assurez-vous que les annonces visibles par ces utilisateurs présentent du contenu approprié pour les enfants.
   - Assurez-vous que les annonces visibles par ces utilisateurs respectent les exigences relatives aux formats d'annonce pour les familles.
   - Respectez toutes les dispositions légales et standards dans l'industrie applicables concernant la diffusion d'annonces auprès des enfants.
4. **Collecte de données** : si vous collectez des informations personnelles et sensibles auprès des enfants dans votre application, y compris via les API et les SDK appelés ou utilisés dans celle-ci, vous devez l'indiquer. Les informations sensibles des enfants comprennent, sans s'y limiter, les informations d'authentification, les données des capteurs du micro et de l'appareil photo, les données concernant l'appareil, l'ID Android, les données d'utilisation des annonces et l'identifiant publicitaire.
5. **API et SDK** : vous devez vous assurer que votre application implémente correctement les éventuels SDK et API utilisés.
   - Les applications qui ciblent uniquement les enfants ne doivent contenir aucune API ni aucun SDK non approuvés pour une utilisation dans des services destinés aux enfants. Ces dispositions concernent Google Sign-In (ou tout autre service API Google qui accède aux données associées à un compte Google), les services de jeux Google Play ainsi que tout autre service API qui utilise la technologie OAuth à des fins d'authentification et d'autorisation.
   - Les applications qui ciblent à la fois les enfants et les publics plus âgés ne doivent pas utiliser d'API ni de SDK qui ne sont pas approuvés pour une utilisation dans des services destinés aux enfants, sauf s'ils sont utilisés après un écran neutre de vérification de l'âge ou mis en œuvre de manière à ne pas collecter de données auprès des enfants (par exemple, en proposant la fonctionnalité Google Sign-in en option). Les applications qui ciblent à la fois les enfants et les publics plus âgés ne doivent pas obliger les utilisateurs à se connecter ou à accéder au contenu de l'application via une API ou un SDK dont l'utilisation dans des services destinés aux enfants n'est pas approuvée.
6. **Règles de confidentialité** : vous devez fournir un lien vers les règles de confidentialité de votre application sur sa fiche Play Store. Ce lien doit être accessible à tout moment, aussi longtemps que l'application reste disponible sur le

Play Store. Il doit renvoyer vers des règles de confidentialité décrivant avec précision la collecte et l'utilisation des données dans votre application, entre autres.

7. **Restrictions particulières** :
   - Si votre application fait appel à la réalité augmentée, vous devez inclure un avertissement de sécurité dès le lancement de la section en RA. Cet avertissement doit contenir les éléments suivants :
     - Un message approprié concernant l'importance de la supervision parentale
     - Un rappel sur les dangers physiques du monde réel (par exemple, faire attention à ce qui vous entoure)
   - Votre application ne doit pas nécessiter l'emploi d'un appareil dont l'utilisation est déconseillée aux enfants (Daydream ou Oculus, par exemple).
8. **Respect des obligations légales** : vous devez vous assurer que votre application, y compris les éventuels SDK et API qu'elle appelle ou utilise, est conforme à la Loi américaine COPPA (Children's Online Privacy and Protection Act) sur la protection et le respect de la vie privée des enfants en ligne, au Règlement général sur la protection des données (RGPD) de l'Union européenne et à toute autre loi ou réglementation applicable.

Voici quelques exemples courants de non-respect des règles :

- Applications faisant la promotion de jeux pour enfants dans leur fiche Play Store, mais dont le contenu ne convient qu'aux adultes
- Applications recourant à des API dont l'utilisation dans des applications destinées aux enfants est interdite par leurs conditions d'utilisation
- Applications qui valorisent la consommation d'alcool, de tabac ou de substances réglementées
- Applications qui contiennent des jeux d'argent et de hasard réels ou des simulations de tels jeux
- Applications présentant de la violence, du sang ou un contenu choquant ne convenant pas aux enfants
- Applications qui proposent des services de rencontres, ou encore des conseils sur la sexualité ou les rapports conjugaux
- Applications contenant des liens vers des sites Web dont le contenu ne respecte pas le Règlement du programme Google Play pour les développeurs
- Applications qui présentent aux enfants des annonces réservées à un public averti (par exemple, contenus violents, contenus à caractère sexuel, ou jeux d'argent et de hasard) Pour en savoir plus sur les règles de Google Play concernant les annonces, les achats via une application et les contenus commerciaux destinés aux enfants, veuillez consulter les Règles concernant les annonces et la monétisation pour les contenus familiaux.

Programme Pour la famille

Les applications spécialement conçues pour les enfants doivent être enregistrées auprès du programme Pour la famille. Si votre application est conçue pour tous, y compris pour les enfants et les familles, vous pouvez également demander à participer au programme.

Pour que votre application soit acceptée dans le programme, elle doit respecter l'ensemble des règles pour les contenus familiaux et des critères d'éligibilité du programme Pour la famille, ainsi que les exigences décrites dans le Règlement du programme Google Play pour les développeurs et le Contrat relatif à la distribution (pour les développeurs).

Pour en savoir plus sur la procédure d'enregistrement d'une application au programme, consultez cette page.

Éligibilité au programme

Toutes les applications enregistrées auprès du programme Pour la famille ainsi que le contenu des annonces diffusées dans ces applications doivent être pertinents et appropriés pour les enfants, et respecter toutes les exigences ci-dessous. Les applications du programme Pour la famille doivent rester conformes à toutes les exigences de celui-ci. Google Play peut refuser, supprimer ou suspendre toute application jugée inappropriée pour le programme Pour la famille.

Exigences du programme Pour la famille

1. Les applications doivent être associées aux catégories de classification ESRB "Tout public", "10 ans et plus" ou leur équivalent.
2. Vous devez indiquer précisément les éléments interactifs de l'application dans le questionnaire sur la classification du contenu dans la Google Play Console, y compris en répondant aux questions suivantes :
   - Les utilisateurs peuvent-ils interagir ou échanger des informations ?
   - L'application communique-t-elle à des tiers des informations personnelles fournies par l'utilisateur ?
   - L'application communique-t-elle à d'autres utilisateurs la position physique de l'utilisateur ?
3. Si votre application utilise l'API Android Speech, RecognizerIntent.EXTRA_CALLING_PACKAGE doit être défini sur son PackageName.
4. Les applications ne doivent utiliser que des SDK publicitaires certifiés Google Play.

5. Les applications spécialement conçues pour les enfants ne doivent pas requérir d'autorisations d'accéder à la position.
6. Les applications doivent utiliser Companion Device Manager (CDM) pour demander l'accès au Bluetooth, sauf si elles ne ciblent que des versions de système d'exploitation d'appareil non compatibles avec CDM.

Voici quelques exemples d'applications courantes qui ne sont pas éligibles au programme :

- Applications associées aux catégories de classification ESRB "Tout public" contenant des annonces pour des jeux d'argent et de hasard
- Applications pour les parents ou le personnel soignant (applications de suivi de l'allaitement, guide de développement, par exemple)
- Guides parentaux ou applications de gestion d'appareils destinés exclusivement à être utilisés par des parents ou du personnel soignant
- Applications utilisant une icône d'application ou de lanceur d'applications qui n'est pas appropriée pour les enfants

Catégories

Si vous êtes autorisé à rejoindre le programme Pour la famille, vous pouvez choisir une deuxième catégorie familiale décrivant votre application. Voici les catégories disponibles pour les applications du programme Pour la famille :

Action et aventure : applications et jeux d'action, des jeux de course simples aux jeux d'aventure féeriques, en passant par les applications et les jeux conçus pour susciter l'engouement

Jeux de réflexion : jeux qui visent à faire travailler le cerveau de l'utilisateur, tels que les puzzles, jeux d'association, questionnaires et autres jeux qui sollicitent la mémoire, l'intelligence ou la logique

Créativité : applications et jeux qui favorisent la créativité, tels que les applications de dessin, de peinture, de codage et autres applications et jeux de construction et de création

Enseignement : applications et jeux conçus avec l'aide d'experts en apprentissage (par exemple, éducateurs, spécialistes de l'apprentissage et chercheurs) et visant à promouvoir l'apprentissage, y compris académique, socio-émotionnel, physique et créatif, ainsi que l'apprentissage lié aux compétences élémentaires de la vie quotidienne, à l'esprit critique et à la résolution de problèmes

Musique et vidéo : applications et jeux ayant une composante vidéo ou musicale, des applications de simulation d'instrument aux applications qui fournissent du contenu vidéo et musical

Jeux de simulation : applications et jeux dans lesquels l'utilisateur joue un rôle, par exemple de cuisinier, d'infirmier, de prince ou de princesse, de pompier, de policier ou autre personnage fictif

Annonces et monétisation

Les règles ci-dessous s'appliquent à tout contenu publicitaire (y compris pour vos applications et les applications tierces), à toute offre d'achat via l'application ou à tout autre contenu à caractère commercial (placement de produit rémunéré, par exemple) qui sont diffusés auprès des utilisateurs de l'application et qui sont soumis aux règles pour les contenus familiaux et/ou aux exigences du programme Pour la famille. Tout contenu publicitaire et commercial et toute offre pour un achat via l'application diffusés dans ces applications doivent respecter les lois et réglementations applicables, y compris les consignes appropriées d'autorégulation ou en vigueur dans le domaine.

Google Play se réserve le droit de refuser, de supprimer ou de suspendre toute application en cas de tactiques commerciales trop agressives.

Conditions requises concernant le format des annonces

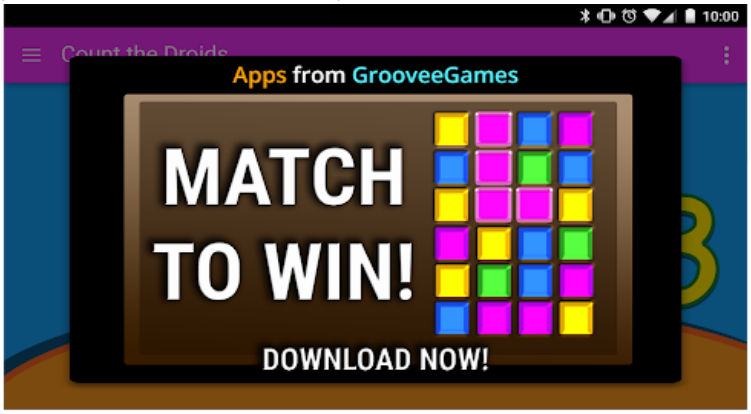
Les annonces et offres pour des achats via l'application ne doivent pas présenter de contenu trompeur ni être conçues de manière à générer des clics accidentels de la part des enfants. Les actions suivantes sont interdites :

- Annonces intrusives, y compris les annonces qui occupent tout l'écran ou qui perturbent l'utilisation normale de l'application et qui n'indiquent pas clairement comment les ignorer (par exemple, écrans d'annonces).
- Annonces qui perturbent le fonctionnement normal de l'application ou du jeu, et ne peuvent pas être fermées au bout de cinq secondes. Les annonces qui n'interfèrent pas avec l'utilisation normale de l'application ou du jeu peuvent rester affichées plus de cinq secondes (par exemple, contenu vidéo intégrant des annonces).
- Annonces interstitielles ou offres d'achat via l'application affichées dès le lancement de l'application
- Plusieurs emplacements d'annonce sur une page (par exemple, les bannières qui affichent plusieurs offres dans un même emplacement, et l'affichage de plusieurs bannières ou annonces vidéo ne sont pas autorisés).
- Annonces ou offres pour des achats via l'application qui ne se différencient pas clairement du contenu de l'application
- Recours à des tactiques choquantes ou à la manipulation émotionnelle pour inciter l'utilisateur à visionner des annonces ou à effectuer des achats via l'application

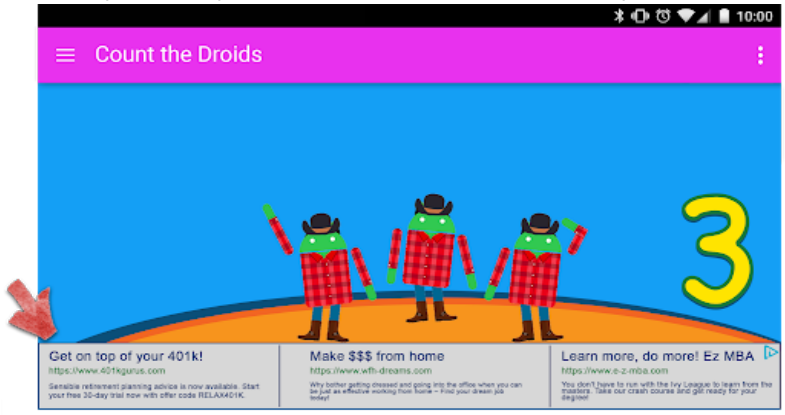
- Absence de distinction entre l'utilisation d'argent virtuel et d'argent réel pour réaliser des achats via l'application

Voici quelques exemples courants de non-respect du format d'annonce :

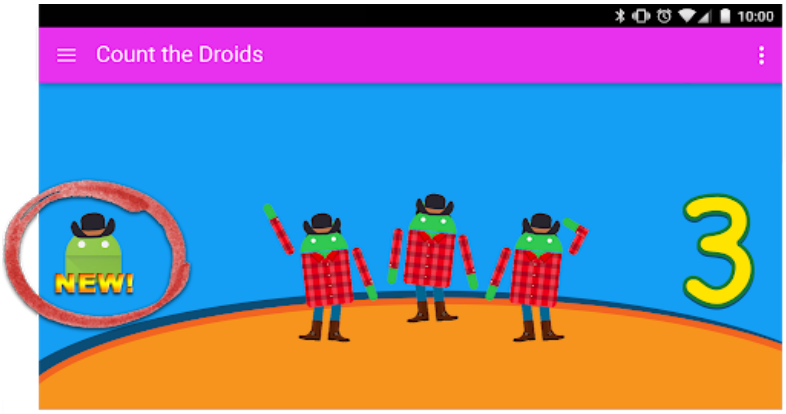
- Annonces qui s'éloignent du doigt de l'utilisateur lorsque celui-ci tente de les fermer
- Annonces qui occupent la majeure partie de l'écran de l'appareil ou sa totalité sans que l'utilisateur puisse les fermer simplement, comme illustré dans l'exemple ci-dessous :



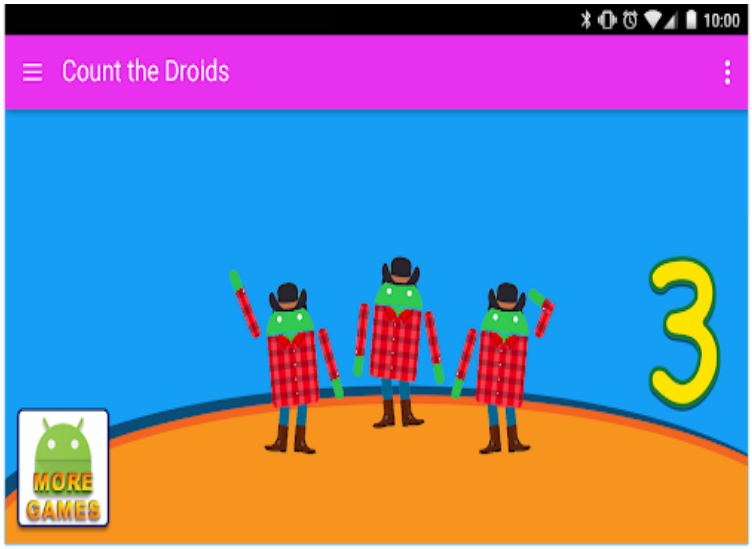
- Bannières qui affichent plusieurs offres, comme illustré dans l'exemple ci-dessous :



- Annonces pouvant être confondues avec le contenu de l'application, comme illustré dans l'exemple ci-dessous :



- Boutons ou annonces qui font la promotion de vos autres fiches Google Play Store, mais qu'il est impossible de distinguer du contenu de votre application, comme illustré dans l'exemple ci-dessous :



Voici quelques exemples de contenus d'annonce inappropriés qui ne doivent pas être diffusés auprès des enfants :

- **Contenu multimédia inapproprié** : annonces pour des séries TV, des films, des albums musicaux ou tout autre support multimédia qui ne sont pas appropriés pour les enfants.
- **Jeux vidéo et logiciels téléchargeables inappropriés** : annonces pour des logiciels téléchargeables et des jeux vidéo électroniques qui ne sont pas appropriés pour les enfants.
- **Substances réglementées ou dangereuses** : annonces concernant l'alcool, le tabac, les substances réglementées et autres substances dangereuses.
- **Jeux d'argent et de hasard** : annonces pour des simulations de jeux d'argent et de hasard, promotion de concours ou de tirages au sort, même si la participation est gratuite.
- **Contenu suggestif ou réservé aux adultes** : annonces comportant du contenu à caractère sexuel, suggestif ou réservé à un public averti.
- **Rencontres ou relations** : annonces pour des sites de rencontres ou de relations entre adultes.
- **Contenu violent** : annonces au contenu violent et explicite ne convenant pas aux enfants.

SDK publicitaires

Si vous diffusez des annonces dans votre application qui ne cible que les enfants, vous devez utiliser les SDK publicitaires certifiés Google Play. Si votre application cible à la fois les enfants et les utilisateurs plus âgés, vous devez mettre en place des mesures de filtrage en fonction de l'âge, par exemple un écran neutre de vérification de l'âge, et vous assurer que les annonces présentées aux enfants proviennent exclusivement de SDK publicitaires certifiés Google Play. Les applications du programme Pour la famille ne doivent utiliser que des SDK publicitaires autocertifiés.

Pour en savoir plus sur ces exigences et obtenir la liste à jour des SDK publicitaires approuvés, consultez le Règlement du programme d'annonces adaptées aux familles.

Si vous utilisez AdMob, consultez le Centre d'aide d'AdMob pour en savoir plus sur leurs produits.

Il vous incombe de vous assurer que votre application satisfait à toutes les exigences en termes de publicité, d'achat via l'application et de contenu commercial. Contactez les fournisseurs de vos SDK publicitaires pour en savoir plus sur leur règlement relatif au contenu et sur leurs pratiques publicitaires.

Achats via une application

Dans les applications du programme Pour la famille, Google Play authentifie une deuxième fois tous les utilisateurs avant qu'ils n'effectuent des achats via une application. Cette mesure vise à s'assurer que la partie responsable financièrement, et non les enfants, approuve les achats.

Application du règlement

Il est toujours préférable de respecter les règles plutôt que d'avoir à gérer des signalements de non-respect. Mais en cas de manquements, nous tenons à nous assurer que les développeurs comprennent bien comment y remédier afin de mettre leurs applications en conformité avec les règles. N'hésitez pas à nous contacter si vous constatez un cas de non-respect des règles ou si vous avez des questions sur la gestion d'une infraction.

Champ d'application du règlement

Nos règles s'appliquent à tout contenu affiché dans votre application ou associé à celle-ci via des liens. Elles concernent également toutes les annonces qui y sont diffusées, ainsi que les contenus générés par des utilisateurs hébergés par votre application ou associés à celle-ci via des liens. Par ailleurs, elles s'appliquent à tout contenu de votre compte de développeur affiché publiquement sur Google Play, y compris votre nom de développeur et la page de destination du site Web que vous avez indiqué.

Nous n'autorisons pas les applications qui permettent aux utilisateurs d'en installer d'autres sur leurs appareils. Les développeurs d'applications qui offrent un accès à d'autres applications, jeux ou logiciels sans les installer, y compris des fonctionnalités et des expériences fournies par des tiers, doivent veiller à ce que tous les contenus auxquels elles donnent accès soient en conformité avec l'ensemble des Règles de Google Play. Ces applications peuvent également être sujettes à une vérification supplémentaire du respect des règles.

Les termes définis utilisés dans ces règles ont la même signification que dans le Contrat relatif à la distribution (pour les développeurs). En plus de respecter ces règles et ce contrat, le contenu de votre application doit être évalué conformément à nos Consignes concernant la classification du contenu.

Nous pouvons décider d'inclure ou de supprimer des applications en fonction d'un certain nombre de facteurs, y compris, sans toutefois s'y limiter, un comportement préjudiciable ou un risque élevé d'abus. Nous identifions un risque d'abus sur la base de différents critères, y compris, mais sans s'y limiter, l'historique des précédents cas de non-respect des règles, les commentaires des utilisateurs, ainsi que l'utilisation de marques, de personnages et d'autres éléments populaires.

Fonctionnement de Google Play Protect

Google Play Protect vérifie les applications lorsque vous les installez et analyse régulièrement votre appareil. S'il détecte une appli potentiellement dangereuse, il peut effectuer les actions suivantes :

- Vous envoyer une notification. Pour supprimer l'application, appuyez sur la notification, puis sur "Désinstaller".
- Désactiver l'application jusqu'à ce que vous la désinstalliez.
- Supprimer automatiquement l'application. Dans la plupart des cas, si une application dangereuse a été détectée, vous recevez une notification indiquant qu'elle a été supprimée.

Fonctionnement de la protection contre les logiciels malveillants

Afin de vous protéger contre les logiciels malveillants tiers, les URL présentant un risque et d'autres problèmes de sécurité, Google peut recevoir les informations suivantes :

- Les connexions réseau de votre appareil
- Les URL potentiellement dangereuses
- Le système d'exploitation et les applications installées sur votre appareil depuis Google Play ou d'autres sources

Vous pouvez recevoir un avertissement de Google au sujet d'une application ou d'une URL susceptible d'être dangereuse. Nous pouvons supprimer l'URL ou l'application, par exemple en bloquant son installation, si nous considérons qu'elle est dangereuse pour les appareils, les données ou les utilisateurs.

Vous pouvez choisir de désactiver certaines de ces protections dans les paramètres de votre appareil. Cependant, Google peut continuer à recevoir des informations sur les applications installées via Google Play. Les applications installées sur votre appareil à partir d'autres sources peuvent également continuer d'être analysées afin de détecter d'éventuels problèmes de sécurité, sans que les informations soient envoyées à Google.

Fonctionnement des alertes de confidentialité

Google Play Protect vous avertit lorsqu'une application susceptible d'accéder à vos informations personnelles est supprimée du Google Play Store. Vous avez alors la possibilité de la désinstaller.

Procédure d'application du règlement

Si votre application enfreint l'une de nos règles, nous prendrons les mesures appropriées, comme indiqué ci-dessous. En outre, nous vous communiquerons par e-mail les informations pertinentes sur les mesures que nous avons prises, ainsi que des instructions pour faire appel si vous pensez que nous avons agi à tort.

Sachez que les avis de suppression ou les notifications administratives ne détaillent pas forcément chacune des règles que votre application ou vos applications ne respectent pas. Il incombe aux développeurs de traiter tous les cas de non-respect et de prendre les mesures nécessaires pour s'assurer que leurs applications respectent toutes les règles. Si vous ne corrigez pas les cas de non-respect des règles dans toutes vos applications, des mesures supplémentaires peuvent être prises.

En cas de non-respect du Contrat relatif à la distribution (pour les développeurs) ou des règles, de manière répétée ou grave, par exemple en cas d'utilisation de logiciels malveillants, de fraude et d'applications nuisibles à l'appareil ou à l'utilisateur, nous clôturerons le compte incriminé ou les comptes de développeur Google Play associés.

Mesures d'application du règlement

L'impact des différentes mesures sur votre application peut varier. La section suivante décrit les diverses mesures que Google Play peut prendre, et leur impact sur votre application et/ou votre compte de développeur Google Play. Vous pouvez également retrouver toutes ces informations dans cette vidéo.

Refus

- Une nouvelle application ou mise à jour envoyée pour examen ne sera pas publiée sur Google Play.
- Si une mise à jour d'une application existante a été refusée, la version de l'application publiée avant la mise à jour restera disponible sur Google Play.
- Même si votre application est refusée, vous pouvez continuer d'accéder au nombre d'installations, aux statistiques et aux avis des utilisateurs existants la concernant.
- Les refus n'ont aucune incidence sur l'état de votre compte de développeur Google Play.

Remarque : N'essayez pas de renvoyer une application refusée tant que vous n'avez pas corrigé tous les cas de non-respect des règles.

Suppression

- L'application, ainsi que toutes ses versions précédentes, sont supprimées de Google Play. Elles ne peuvent plus être téléchargées par les utilisateurs non plus.
- L'application étant supprimée, les utilisateurs ne peuvent pas consulter sa fiche Play Store, le nombre d'installations, les statistiques et les avis. Ces informations seront restaurées une fois que vous aurez envoyé une mise à jour conforme aux règles.
- Les utilisateurs ne peuvent pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation de l'application tant qu'une version conforme aux règles n'est pas approuvée par Google Play.
- Les suppressions n'ont pas d'incidence immédiate sur l'état de votre compte de développeur Google Play, mais plusieurs suppressions peuvent entraîner une suspension.

Remarque : N'essayez pas de publier à nouveau une application supprimée tant que vous n'avez pas corrigé tous les cas de non-respect des règles.

Suspension

- L'application, ainsi que toutes ses versions précédentes, sont supprimées de Google Play. Elles ne peuvent plus être téléchargées par les utilisateurs non plus.
- La suspension peut survenir suite à des cas de non-respect multiples ou flagrants, ou suite à des refus ou suppressions répétés.
- L'application étant suspendue, les utilisateurs ne peuvent pas consulter sa fiche Play Store, le nombre d'installations, les statistiques et les avis existants. Ces informations seront restaurées une fois que vous aurez envoyé une mise à jour conforme aux règles.
- Vous ne pouvez plus utiliser le fichier APK ou l'app bundle d'une application suspendue.
- Les utilisateurs ne pourront pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation dans l'application tant qu'une version conforme aux règles ne sera pas approuvée par Google Play.
- Les suspensions constituent des avertissements pour non-respect des règles applicables à votre compte de développeur Google Play. Après plusieurs avertissements, les comptes de développeur Google Play individuels ou associés peuvent être clos.

Remarque : N'essayez pas de publier à nouveau une application suspendue, sauf si Google Play vous y a autorisé.

Visibilité limitée

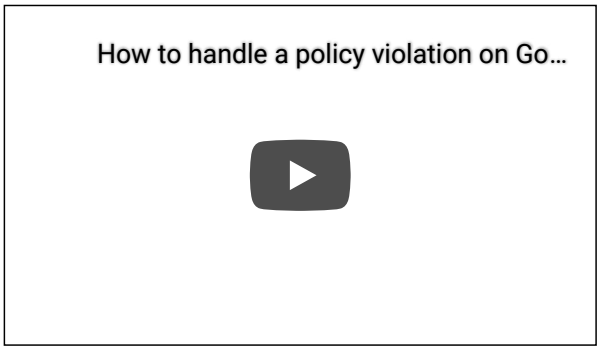
- La visibilité de votre application sur Google Play est limitée. Votre application reste disponible sur Google Play et sa fiche Play Store peut être consultée par les utilisateurs disposant d'un lien direct vers celle-ci.
- La limitation de la visibilité de votre application n'a aucune incidence sur l'état de votre compte de développeur Google Play.
- Elle n'a pas non plus d'incidence sur la possibilité pour les utilisateurs de consulter la fiche Play Store, le nombre d'installations, les statistiques et les avis de l'application.

Clôture de compte

- Lorsque votre compte de développeur est clôturé, toutes les applications de votre catalogue sont supprimées de Google Play et vous ne pouvez plus en publier de nouvelles. Cela signifie aussi que tous les comptes de développeur Google Play associés seront également clos définitivement.
- Les suspensions occasionnées suite à des cas de non-respect des règles flagrants ou répétés peuvent entraîner la clôture de votre compte dans la Play Console.
- Les applications du compte clôturé étant supprimées, les utilisateurs ne peuvent pas voir la fiche Play Store, le nombre d'installations, les statistiques et les avis de celles-ci.

Remarque : Si vous tentez d'ouvrir un nouveau compte, celui-ci sera également clos. De plus, les frais d'inscription pour les développeurs ne vous seront pas remboursés. Par conséquent, n'essayez pas de créer un autre compte pour la Play Console si l'un de vos autres comptes est clos.

Gérer et signaler les cas de non-respect des règles



Appel contre une mesure d'application

Nous rétablirons les applications si une erreur a été commise et si nous constatons qu'elles respectent bien en réalité le règlement du programme Google Play et le Contrat relatif à la distribution (pour les développeurs). Si vous avez lu attentivement le règlement et que vous estimez que notre décision est erronée, veuillez suivre les instructions fournies dans l'e-mail vous notifiant les mesures d'application prises à l'encontre de votre application pour contester cette décision.

Autres ressources

Pour plus d'informations sur une mesure d'application, ou sur un avis ou un commentaire d'un utilisateur, consultez les ressources ci-dessous ou contactez-nous via le Centre d'aide Google Play. Nous ne sommes toutefois pas en mesure de vous donner des conseils d'ordre juridique. Veuillez consulter un service juridique si vous avez des questions.

- Validation des applications et procédures d'appel
- Signaler un cas de non-respect des règles
- Contacter Google Play à propos de la résiliation d'un compte ou de la suppression d'une application
- Avertissements
- Signaler des applications et des commentaires inappropriés
- Mon application a été supprimée de Google Play
- Informations sur la résiliation des comptes de développeur Google Play

Donnez-nous votre avis sur cet article

Ces informations vous-ont elles été utiles ?

Oui Non

Vous avez encore besoin d'aide ?

Essayez les solutions ci-dessous :

Contactez-nous

Donnez-nous plus de détails pour que nous puissions vous aider