Règlement du programme pour les développeurs

(entrée en vigueur le 10 avril 2025, sauf indication contraire)

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

Notre réussite commune repose sur vos innovations, ce qui s'accompagne inévitablement de 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 qui n'interdisent pas la création, la mise en ligne ou la distribution de contenu qui facilite l'exploitation ou l'abus de mineurs s'exposent à leur retrait immédiat de Google Play. Cela inclut tout contenu d'abus sexuels sur mineurs. Si vous souhaitez signaler du contenu trouvé dans un produit Google et qui, selon vous, entre dans cette catégorie, cliquez sur **Signaler un abus** . Si vous trouvez des contenus de ce type ailleurs sur Internet, contactez directement les autorités compétentes dans votre pays .

Nous interdisons l'utilisation d'applications pour mettre en danger des enfants. Cela inclut, mais sans s'y limiter, la promotion de comportements prédateurs à l'égard d'enfants. Exemples :

- Interactions inappropriées avec un enfant (attouchements, caresses, etc.)
- Sollicitation d'enfants à des fins sexuelles (par exemple, en se liant d'amitié avec un enfant en ligne pour faciliter, en ligne ou hors ligne, les contacts sexuels et/ou échanger des images à caractère sexuel avec lui)
- Sexualisation des mineurs (par exemple, des images qui montrent, encouragent ou promeuvent les abus sexuels sur des mineurs, ou une représentation d'enfants susceptible d'entraîner leur exploitation sexuelle)
- "Sextorsion" (par exemple, menacer ou faire du chantage à un enfant sous prétexte d'avoir un accès réel ou présumé à des images intimes le concernant)
- Trafic d'enfants (par exemple, en faisant la publicité d'un enfant ou en sollicitant un mineur à des fins d'exploitation sexuelle commerciale)

Nous prendrons les mesures nécessaires, qui pourront inclure un signalement auprès du National Center for Missing & Exploited Children, si nous détectons la présence de contenus d'abus sexuels sur mineurs. Si vous pensez qu'un enfant est, ou a été, victime d'abus, d'exploitation ou de trafic, contactez les autorités locales ainsi que l'un des organismes de protection de l'enfance de cette liste .

Sont également interdites les applications qui peuvent plaire aux enfants, mais qui contiennent des thèmes réservés aux adultes. Exemples :

- Applications qui contiennent de la violence ou du sang
- Applications qui représentent ou encouragent des activités dangereuses

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.

Règlement sur les normes liées à la sécurité des enfants

Google Play exige que les applications de rencontres et de réseaux sociaux respectent le règlement sur les normes liées à la sécurité des enfants.

Ces applications doivent :

- **avoir publié des normes** : votre application doit interdire explicitement l'exploitation et les abus sexuels sur mineurs dans des normes accessibles publiquement, comme les conditions d'utilisation de votre application, le règlement de la communauté ou tout autre document accessible publiquement et concernant les règles relatives aux utilisateurs.
- **proposer un mécanisme intégré à l'application permettant aux utilisateurs de laisser des commentaires** : vous devez autocertifier que vous fournissez dans votre application un mécanisme pour que les utilisateurs puissent laisser des commentaires, des questions ou signaler des problèmes.
- **gérer les cas de contenus d'abus sexuels sur mineurs** : vous devez autocertifier que votre application prend les mesures nécessaires, y compris, mais sans s'y limiter, en supprimant les contenus d'abus sexuels sur mineurs, après en avoir eu connaissance, conformément aux normes que vous avez publiées et aux lois applicables.
- **respecter les lois concernant la sécurité des enfants** : vous devez autocertifier que votre application respecte les lois et règlements applicables concernant la sécurité des enfants, y compris, mais sans s'y limiter, par la mise en place d'une procédure de signalement des cas confirmés de contenus d'abus sexuels sur mineurs au National Center for Missing and Exploited Children ou à l'autorité régionale concernée.
- **indiquer un contact responsable de la sécurité des enfants** : votre application doit indiquer un contact désigné qui recevra les potentielles notifications de Google Play au sujet des contenus d'abus sexuel sur mineurs trouvés dans votre application ou sur votre plate-forme. Ce représentant doit être au fait de vos procédures d'examen et de mise en application, et doit pouvoir agir si nécessaire.

Pour en savoir plus sur ces exigences et découvrir comment vous y conformer, consultez l'article de notre Centre d'aide.

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 comportant 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. Nous n'autorisons pas les applications ni les contenus qui semblent promouvoir ou proposer des rapports sexuels contre rémunération. Nous n'autorisons pas les applications comportant ou faisant la promotion de contenu associé à un comportement prédateur de nature sexuelle ou distribuant du contenu à caractère sexuel sans autorisation. Les contenus présentant des scènes de nudité peuvent être autorisés si celles-ci ne sont pas injustifiées, mais à visée éducative, documentaire, scientifique ou artistique.

Les applications avec catalogue (qui listent des livres/vidéos dans un catalogue de contenus élargi) peuvent distribuer des livres (e-books et livres audio inclus) ou des vidéos comportant du contenu à caractère sexuel à condition de respecter les exigences suivantes :

- Les livres/vidéos comportant du contenu à caractère sexuel représentent une part minime du catalogue global de l'application.
- L'application ne promeut pas activement les livres/films avec du contenu à caractère sexuel. Ces livres/vidéos peuvent figurer dans les recommandations en fonction de l'historique de l'utilisateur ou lors de promotions générales.
- L'application ne distribue pas de livres/vidéos comportant du contenu relevant de la mise en danger d'enfants, à caractère pornographique ou à caractère sexuel défini comme illégal par le droit applicable.
- L'application protège les mineurs en restreignant l'accès aux livres/vidéos comportant du contenu à caractère sexuel.

Si une application comporte du contenu qui ne respecte pas ces règles, mais que ce contenu est jugé approprié dans une certaine région, l'application peut être disponible dans cette région, mais pas dans d'autres.

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, mais 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'escorte ou d'autres services susceptibles d'être interprétés comme une proposition ou demande de relations sexuelles contre rémunération, y compris, mais sans s'y limiter, les relations tarifées ou arrangements de nature sexuelle où il est attendu ou implicite que l'un des participants fournisse de l'argent, des cadeaux ou un soutien financier à un autre participant ("sugar dating").
- Applications représentant des personnes de manière humiliante ou objectifiée, telles que les applications prétendant permettre de déshabiller les personnes ou de voir à travers les vêtements, même si elles sont présentées comme une plaisanterie ou une application de divertissement.
- Contenu ou comportement qui tentent de menacer ou d'exploiter sexuellement des personnes, comme les photos suggestives prises sans autorisation, les caméras cachées, le contenu à caractère sexuel créé sans autorisation via hypertrucage ou une technologie similaire, ou le contenu représentant des agressions.

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 en raison de leur race, origine ethnique, religion, handicap, âge, nationalité, statut d'ancien combattant, orientation sexuelle, genre, identité de genre, caste, situation au regard de l'immigration 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 règlements locaux.

Voici quelques 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, les troubles alimentaires, les jeux d'étranglement ou autres actes comportant des risques de blessure grave ou de mort

Extrémisme violent

Nous n'autorisons pas les organisations terroristes ni aucune autre organisation ou mouvement dangereux qui ont pris part à des actes de violence envers les civils, s'y sont préparés ou les ont revendiqués, à publier d'applications sur Google Play à quelque fin que ce soit, y compris pour le recrutement.

Nous n'autorisons pas les applications dont les contenus sont liés à l'extrémisme violent ou à la planification, à la préparation ou à l'apologie d'actes de violence envers les civils, tels que la promotion d'actes terroristes, l'incitation à la violence ou l'apologie d'attentats terroristes. Si vous publiez des contenus liés à l'extrémisme violent à des fins éducatives, documentaires, scientifiques ou artistiques, ce contexte doit être clairement précisé.

Événements sensibles

Nous n'autorisons aucune application qui exploite un événement sensible de portée sociale, culturelle ou politique significative, tel qu'une urgence civile, une catastrophe naturelle, une urgence de santé publique, un conflit, un décès ou tout autre événement tragique, ou qui 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, ou s'il a pour but d'alerter ou de sensibiliser les utilisateurs au sujet de l'événement en question.

Voici quelques 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 la survenue d'un événement tragique majeur et bien documenté
- Tirer profit d'un événement sensible 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 quelques exemples courants de non-respect des règles :

- Intimider les 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 ou de produits contenant de la nicotine (comme les cigarettes électroniques, les vape pens et les sachets de nicotine sans tabac), ou qui encouragent la consommation illégale ou inappropriée d'alcool, de tabac ou de nicotine.

Informations complémentaires

- Nous n'autorisons pas les applications représentant ou encourageant la consommation ou la vente d'alcool ou de tabac auprès des mineurs.
- Nous n'autorisons pas les applications suggérant que la consommation de tabac peut améliorer le statut social ou les performances sexuelles, professionnelles, intellectuelles ou sportives.
- Nous n'autorisons pas les applications présentant la consommation excessive d'alcool, y compris les beuveries et les concours, sous un jour favorable.
- Nous n'autorisons pas les applications qui mettent en avant des produits associés au tabac ou qui en font la publicité ou la promotion (y compris au moyen d'annonces, bannières, catégories et liens vers des sites de vente de tabac).
- Dans certaines régions, il est possible que nous autorisions la vente limitée de produits associés au tabac dans les applications de livraison de courses ou de repas à domicile, sous réserve de mesures de vérification de l'âge (telles que la présentation d'une pièce d'identité à la livraison).
- Nous pouvons autoriser la vente de produits commercialisés comme des aides à l'arrêt de la nicotine sous réserve de mesures de vérification de l'âge.

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.

Si votre application contient des fonctionnalités financières, vous devez remplir le formulaire de déclaration des fonctionnalités financières dans la Play Console.

Options binaires

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

Prêts

Prêt personnel : par prêt personnel, nous entendons tout prêt ponctuel accordé par une personne physique, une organisation ou une entité à un consommateur (personne physique), à des fins autres que pour financer des études ou l'achat 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 : prêt hypothécaire, financement automobile, lignes de crédit renouvelable (cartes de crédit, lignes de crédit personnelles, par exemple)

Accès au salaire gagné : par accès au salaire gagé (EWA, Earned Wage Access), nous désignons un service financier qui permet aux personnes d'accéder de façon anticipée à une partie de leur salaire en se basant sur les heures travaillées non encore rémunérées par leur employeur. Contrairement aux prêts traditionnels, les services EWA ont les caractéristiques suivantes :

- Mécanisme de remboursement : le remboursement s'effectue automatiquement par retenue sur salaire ou par une transaction de paiement automatique associée au compte bancaire de l'utilisateur. En cas d'échec de la transaction automatique, aucuns intérêts, pénalités ni frais supplémentaires ne sont débités.
- Accès basé sur le revenu : le montant disponible pour l'utilisateur est plafonné en fonction des heures déjà travaillées pendant la période de paie en cours ; ceci évite tout emprunt sur les revenus futurs.
- Structure tarifaire : les services EWA ne débitent pas d'intérêts, mais des frais forfaitaires modiques ou des frais de transaction basés sur un pourcentage de la somme utilisée. Les frais forfaitaires doivent être raisonnables, c'est-à-dire peu élevés et clairement indiqués, reflétant le coût réel de la prestation du service sans pénaliser l'utilisateur, soit de l'ordre de 1 à 5 dollars par transaction ou de 1 à 5 % du montant avancé.
- Pas de création de dettes : les services EWA ne signalent généralement pas leurs transactions aux agences d'évaluation du crédit. Ces transactions n'ont donc pas d'impact sur la cote de crédit de l'utilisateur et ne contribuent pas à l'accumulation de dettes à long terme.

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 être associées à la catégorie Finance dans la Play Console et inclure les informations suivantes dans leurs métadonnées :

- La durée minimale et maximale de la période de remboursement

- Le taux annuel effectif global (TAEG) 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, incluant le montant principal et 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, conformément aux restrictions décrites dans ces règles

Nous n'autorisons pas les applications qui proposent des 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").

Nous consentirons des exceptions à ce règlement pour les applications de prêt personnel dans les pays dont les réglementations spécifiques autorisent explicitement ce type de prêt à court terme dans des cadres légaux définis. Dans ces rares cas, les exceptions seront évaluées conformément aux lois locales et aux directives réglementaires applicables du pays en question.

Les applications proposant des prêts basés sur l'accès au salaire gagné, y compris, mais sans s'y limiter, les applications proposant ces prêts directement, les applications de génération de prospects et celles qui mettent les consommateurs en relation avec des prêteurs tiers, doivent être associées à la catégorie Finance dans la Play Console et inclure les informations suivantes dans leurs métadonnées :

- Les conditions de remboursement
- Tous les frais, y compris les frais de souscription et de transaction, ainsi que tous les autres frais liés à l'octroi du prêt
- Un exemple représentatif du coût total du prêt incluant tous les frais
- 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, conformément aux restrictions décrites dans ces règles

Nous devons être en mesure d'établir un lien entre votre compte de développeur et toute licence ou documentation fournie pour prouver votre capacité à proposer des prêts personnels. Des informations ou des documents supplémentaires peuvent vous être demandés afin de confirmer que votre compte respecte toutes les lois et tous les règlements locaux.

Les applications de prêts personnels ou ayant comme but principal de faciliter l'accès à des prêts personnels (générateurs de prospects ou facilitateurs, par exemple), les applications fournissant des accessoires d'aide aux prêts (calculateurs de prêts, guides d'emprunt, etc.) et les applications d'accès au salaire gagné (EWA, Earned Wage Access) ont l'interdiction d'accéder aux données sensibles, telles que les photos et les contacts. Les autorisations suivantes sont interdites :

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

Les applications qui utilisent des API ou des informations sensibles sont soumises à des restrictions et à des exigences supplémentaires. Pour en savoir plus, reportez-vous aux Règles sur les autorisations.

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 (TAEG) est supérieur ou égal à 36%. Le TAEG 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 concernent les applications proposant des prêts directement, les applications de génération de prospects et celles qui mettent les consommateurs en relation avec des prêteurs tiers.

Exigences en fonction du pays

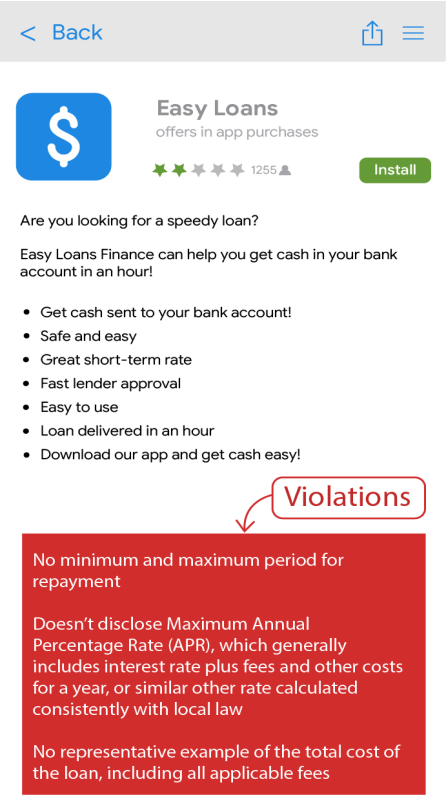
Les applications de prêts personnels ciblant les pays listés doivent respecter des exigences supplémentaires et fournir des documents complémentaires dans la déclaration des fonctionnalités financières de la Play Console. Les applications proposant des prêts basés sur l'accès au salaire gagné (EWA, Earned Wage Access) sont soumises aux mêmes exigences, sous réserve que celles-ci soient applicables dans les juridictions concernées. Sur demande de Google Play, vous devez être en mesure de fournir des informations ou des documents supplémentaires relatifs à votre conformité aux exigences réglementaires et aux licences applicables.

1. **Inde**
   - Si vous êtes agréé par la Banque centrale de l'Inde (RBI) pour octroyer des prêts personnels, vous devez nous envoyer une copie de votre licence pour examen.
   - Si vous ne vous chargez pas directement d'activités de prêts financiers et que vous ne proposez qu'une plate-forme permettant aux utilisateurs de contracter des prêts auprès de banques ou d'institutions financières non bancaires (IFNB) enregistrées, vous devez l'indiquer clairement dans votre déclaration.
     - De plus, le nom de toutes les banques et IFNB enregistrées doit apparaître clairement dans la description de votre application.
2. **Indonésie**
   - Si votre application propose des services de prêts basés sur les technologies de l'information couverts par la réglementation OJK n° 77/POJK.01/2016 (qui peut faire l'objet de modifications de temps en temps), vous devez envoyer une copie de votre licence valide pour examen.
3. **Philippines**
   - Toutes les sociétés de prêts et de financement proposant des prêts via des plates-formes de prêts en ligne doivent obtenir un numéro d'enregistrement SEC ainsi qu'un numéro de certificat d'autorité auprès de la PSEC (Philippines Securities and Exchanges Commission).
     - De plus, vous devez indiquer dans la description de votre application le nom de votre entreprise, la raison sociale, le numéro d'enregistrement auprès de la PSEC et le certificat d'autorité pour l'exploitation d'une société de financement/prêts.
   - Si votre application propose des services de financement participatif basés sur des prêts, comme des prêts peer-to-peer (P2P), ou tel que défini dans les règles et réglementations régissant le financement participatif (Règles CF), vous devez faire appel à des intermédiaires de financement participatif enregistrés auprès de la PSEC.
4. **Nigeria**
   - Les entités numériques proposant des prêts d'argent (DML) doivent compléter les documents requis afin d'adhérer au LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING de 2022 (susceptible d'être modifié de temps en temps) défini par la FCCPC (Federal Competition and Consumer Protection Commission), et obtenir une lettre officielle d'approbation de cette commission.
   - Les agrégateurs de prêts doivent fournir des documents et/ou justificatifs indiquant qu'ils sont agréés pour leurs services numériques de prêt, ainsi que les coordonnées de chaque DML partenaire.
5. **Kenya**
   - Les sociétés de crédit numériques (SCN) doivent compléter leur processus d'enregistrement et obtenir une licence de la Banque centrale du Kenya (CBK). Une copie de cette licence doit être incluse dans votre dossier de déclaration.

- Si vous ne vous chargez pas directement d'activités de prêts financiers et que vous ne proposez qu'une plate-forme permettant aux utilisateurs de contracter des prêts auprès de SCN enregistrées, vous devez l'indiquer clairement dans votre déclaration et fournir une copie de la licence SCN de chacun de vos partenaires.
- Pour le moment, nous n'acceptons que les déclarations et les licences des entités figurant au répertoire des sociétés de crédit numériques sur le site officiel de la CBK.

6. **Pakistan**
   - Chaque institution financière non bancaire prêteuse ne peut publier qu'une seule application de prêt numérique. Les développeurs qui tentent de publier plus d'une application de prêt numérique par IFNB risquent la suppression de leur compte de développeur et de tout compte qui y serait associé.
   - Vous devez fournir une preuve d'approbation de la SECP (Securities and Exchange Commission of Pakistan) pour proposer ou faciliter des services de prêts numériques au Pakistan.
7. **Thaïlande**
   - Les applications de prêts personnels ciblant la Thaïlande, avec des taux d'intérêt de 15 % ou plus, doivent obtenir une licence valide auprès de la Banque de Thaïlande (BoT) ou du ministère des Finances (MoF) thaïlandais. Les développeurs doivent fournir des documents prouvant leur capacité à proposer des prêts personnels ou à aider à leur obtention en Thaïlande. La documentation doit inclure :
     - une copie de la licence délivrée par la Banque de Thaïlande leur permettant d'officier en tant que fournisseur de prêts personnels ou qu'organisme de nanofinance ;
     - une copie de la licence d'organisme de pico-finance délivrée par le ministère des Finances thaïlandais leur permettant d'officier en tant que prêteur pico ou pico-plus.

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, les programmes de fidélité ludifiés, ainsi que les applications de mini ligue fantasy que si elles répondent à certaines exigences.

Applications de jeux d'argent et de hasard

Sous réserve des restrictions et du respect de toutes les règles Google Play, nous autorisons dans certains pays les applications qui permettent ou facilitent les jeux d'argent et de hasard en ligne, à condition que le développeur dépose une demande pour les applications de jeux d'argent et de hasard disponibles sur Google Play, que ce développeur soit un opérateur public approuvé et/ou qu'il soit enregistré en tant qu'opérateur agréé auprès des autorités administratives compétentes en matière de jeux d'argent et de hasard dans le pays spécifié, et qu'il fournisse une licence d'exploitation valide dans le pays désigné pour le type de jeux d'argent et de hasard en ligne qu'il souhaite proposer.

Nous n'acceptons que les applications de jeux d'argent et de hasard autorisées ou concédées sous licence pour les types de produits liés aux jeux d'argent et de hasard en ligne suivants :

- Jeux de casino en ligne
- Paris sportifs
- Courses hippiques (lorsqu'elles sont réglementées et concédées sous licence séparément des paris sportifs)
- Loteries
- Mini ligues fantasy

Les applications éligibles doivent satisfaire aux exigences 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 normes du secteur de chaque pays dans lequel elle est disponible.
- Le développeur doit disposer d'une licence de jeux d'argent et de hasard valide pour chaque pays ou État/territoire où l'application est diffusée.
- Le développeur ne doit pas proposer de type de produit de jeux d'argent et de hasard qui n'est pas couvert par sa licence de jeux d'argent et de hasard.
- 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, les États/territoires ou les zones géographiques où la licence de jeux d'argent et de hasard 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 sans frais depuis le Google 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 concernant le jeu responsable.

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

Pour toutes les autres applications qui ne satisfont pas aux critères d'éligibilité des applications de jeux d'argent et de hasard présentés ci-dessus, et qui ne sont pas incluses dans les "Programmes pilotes sur les autres applications de jeux utilisant de l'argent réel" présentés ci-dessous, 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) 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, et les jeux qui acceptent de l'argent et permettent de

remporter des sommes d'argent ou d'autres prix ayant une valeur réelle (à l'exception des programmes autorisés conformément aux exigences sur les programmes de fidélité ludifiés décrites ci-dessous).

Exemples d'infractions

- Jeux acceptant de l'argent en échange de la possibilité de remporter un prix physique ou une somme d'argent
- Applications comportant des éléments ou des fonctionnalités de navigation (éléments de menu, onglets, boutons, WebView, etc.) 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, comme les applications qui invitent les utilisateurs à "S'INSCRIRE" ou à "PARTICIPER" pour tenter de gagner un prix en espèces.
- Applications qui acceptent ou gèrent des paris, des devises intégrées à l'application, des gains ou des dépôts pour remporter, en jouant ou non, un prix physique ou une somme d'argent.

Pilotes sur les autres applications de jeux utilisant de l'argent réel

Il peut arriver que nous menions des pilotes à durée limitée pour certains types de jeux vidéo avec de l'argent réel dans certaines régions. Pour en savoir plus, consultez cette page du Centre d'aide. Le pilote sur les jeux de machine à pince en ligne mené au Japon a pris fin le 11 juillet 2023. Depuis le 12 juillet 2023, les applications de jeu de machine à pince en ligne peuvent apparaître sur Google Play dans le monde entier, mais sont sujettes à la législation applicable et à certaines exigences.

Programmes de fidélité s'apparentant à des jeux

Lorsque la loi l'autorise et sous réserve d'exigences supplémentaires concernant les jeux d'argent et de hasard ou les licences de jeux, nous autorisons les programmes de fidélité qui récompensent les utilisateurs par des prix réels ou leur équivalent monétaire, conformément aux critères d'éligibilité suivants du Play Store :

Pour toutes les applications (jeux ou non) :

- Les avantages ou récompenses du programme de fidélité doivent être clairement complémentaires et subordonnés à toute transaction monétaire éligible dans l'application (la transaction monétaire éligible doit être une transaction séparée authentique visant à fournir des biens ou des services indépendants du programme de fidélité). Ils ne peuvent pas faire l'objet d'un achat ni être liés à un mode d'échange qui contrevienne au règlement concernant les jeux d'argent et de hasard utilisant de l'argent réel, les jeux et les concours.
  - Par exemple, aucune partie de la transaction monétaire éligible ne peut représenter des frais ou une garantie de participation au programme de fidélité, et la transaction monétaire éligible ne doit pas entraîner l'achat de biens ou de services à un prix supérieur au prix habituel.

Pour les applications de jeux :

- Les points de fidélité ou récompenses associés à des avantages ou à des récompenses liés à une transaction monétaire éligible ne peuvent être accordés et utilisés que selon un ratio fixe. Celui-ci est indiqué clairement dans l'application ainsi que dans le règlement officiel du programme accessible publiquement. L'obtention de la valeur ou des avantages auxquels l'utilisateur peut prétendre ne peut **pas** être gagée, accordée ou dépendante des performances dans le jeu ou des résultats basés sur le hasard.

Pour les applications autres que des jeux :

- Les points de fidélité ou récompenses peuvent être associés à un concours ou à des résultats basés sur le hasard s'ils remplissent les conditions ci-dessous. Les programmes de fidélité associés à des avantages ou à des récompenses liés à une transaction monétaire éligible doivent respecter les conditions suivantes :
  - Les règles officielles du programme doivent être publiées dans l'application.

- Pour les programmes comportant des systèmes de récompenses variables, basées sur le hasard ou randomisées, le règlement officiel du programme doit inclure 1) les probabilités si le programme de fidélité se sert de probabilités fixes pour calculer les récompenses ; 2) la procédure de sélection (c'est-à-dire les variables utilisées pour calculer les récompenses) pour tous les autres programmes de ce type.
- Pour les programmes proposant des tirages au sort, des loteries ou d'autres promotions de même style, un nombre fixe de gagnants, une date limite fixe de participation, ainsi qu'une date de remise des prix, par promotion, doivent être indiqués dans le règlement officiel.
- Indiquez clairement dans l'application et dans le règlement officiel du programme tout ratio fixe suivi pour l'attribution et l'utilisation des points de fidélité ou des récompenses.

Type d'application avec programme de fidélité	**Ludification du programme de fidélité et récompenses variables**	**Récompenses en fonction d'un ratio/planning fixe**	**Conditions d'utilisation du programme de fidélité**	**Probabilités ou procédure de sélection pour les programmes de fidélité basés sur le hasard indiquées dans les conditions d'utilisation**
Application de jeu	Non autorisé	Autorisé	Obligatoire	N/A (les applications de jeux ne peuvent pas comporter d'éléments basés sur le hasard dans les programmes de fidélité)
Application autre qu'un jeu	Autorisé	Autorisé	Obligatoire	Obligatoire

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 Play

Nous autorisons les applications contenant des annonces qui font la promotion de jeux d'argent et de hasard, ou de jeux, de concours et de tournois utilisant de l'argent réel, si elles respectent les conditions suivantes :

- L'application et l'annonce (y compris les annonceurs) doivent respecter l'ensemble des lois applicables et des normes du secteur du pays où l'annonce est diffusée.
- L'annonce doit respecter toutes les conditions locales applicables 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 d'aide propres aux jeux d'argent et de hasard ou aux jeux, loteries et tournois utilisant de l'argent réel (facilitant, par exemple, les paris, les paiements, le suivi de cotes, des performances ou des résultats sportifs, ou la gestion de fonds de participation).
- 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 qui répondent aux exigences exposées ci-dessus peuvent contenir des annonces pour des jeux d'argent et de hasard ou des jeux, loteries et tournois utilisant de l'argent réel. Les applications de jeux d'argent et de hasard acceptées (telles que définies ci-dessus) ou les applications de mini ligue fantasy acceptées (telles que définies ci-après) qui respectent les exigences 1 à 6 susmentionnées peuvent inclure des annonces pour des jeux d'argent et de hasard, ou des jeux, loteries ou tournois utilisant de l'argent réel.

Exemples d'infractions

- 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
- 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, telles que définies par la législation locale applicable, que si elles respectent les exigences suivantes :

- L'application est 1) soit distribuée uniquement aux États-Unis, 2) soit éligible conformément aux exigences concernant les applications de jeux d'argent et de hasard et à la procédure de demande décrites ci-dessus pour les pays autres que les États-Unis.
- 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 normes du secteur des 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.
- L'application doit être conforme à l'ensemble des lois en vigueur et des normes du secteur 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 permettant la vente ou l'achat de drogues illégales
- 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 fourni par l'utilisateur et qui est visible ou accessible par au moins une partie des autres utilisateurs de cette application.

Pour les applications qui intègrent des contenus générés par l'utilisateur, y compris les navigateurs ou clients spécialisés qui redirigent les utilisateurs vers une plate-forme de contenus générés par l'utilisateur, une modération fiable, efficace et continue de ce type de contenus doit être en place. Cette modération doit respecter les règles suivantes :

- 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 répréhensibles (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.
- Modérer les contenus générés par les utilisateurs de façon raisonnable et adaptée aux types de contenus hébergés par l'application, y compris en fournissant un système intégré à l'application pour signaler et bloquer les utilisateurs et les contenus générés répréhensibles, et en prenant des mesures à l'encontre de tels contenus ou utilisateurs le cas échéant. Les actions de modération peuvent varier en fonction de l'expérience proposée pour les contenus générés par l'utilisateur. Exemple :
  - Les applications comportant des contenus générés par l'utilisateur qui identifient un sous-groupe d'utilisateurs particulier par le biais d'une inscription hors connexion, de la vérification de l'utilisateur ou d'autres moyens (applications utilisées exclusivement au sein d'une entreprise ou d'un établissement scolaire précis, par exemple) doivent intégrer une fonctionnalité permettant de signaler les contenus et les utilisateurs.
  - Les fonctionnalités de contenu généré par l'utilisateur permettant une interaction entre deux utilisateurs (messagerie privée, tags, mentions, etc.) doivent intégrer une fonctionnalité pour bloquer les utilisateurs.
  - Les applications permettant d'accéder à des contenus publics générés par l'utilisateur, comme les applications de réseaux sociaux et de blogs, doivent intégrer une fonctionnalité permettant de signaler les utilisateurs et les contenus, et de bloquer les utilisateurs.
  - 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 en RA générés par l'utilisateur inappropriés (par exemple, une image en RA sexuellement explicite) et du lieu d'ancrage de la RA (par exemple, un contenu en 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 des garanties pour empêcher que la monétisation dans l'application n'encourage un comportement répréhensible des utilisateurs.

Contenus à caractère sexuel indirects

Un contenu à caractère sexuel est considéré comme "indirect" s'il apparaît dans une application de contenus générés par l'utilisateur qui (1) fournit un accès à des contenus principalement non sexuels et (2) ne promeut ni ne recommande activement de contenus à caractère sexuel. Les contenus à caractère sexuel définis comme illégaux par la loi applicable et ceux relevant de la mise en danger d'enfants ne sont pas considérés comme "indirects" et ne sont pas autorisés.

Les applications de contenus générés par les utilisateurs peuvent intégrer des contenus à caractère sexuel indirects si toutes les exigences suivantes sont satisfaites :

- Ces contenus sont par défaut cachés derrière des filtres qui nécessitent au moins deux actions de l'utilisateur pour être entièrement désactivés (par exemple, derrière un interstitiel obscurcissant ou en étant invisibles par défaut, sauf si la fonctionnalité SafeSearch est désactivée).
- Comme cela est défini dans les Règles pour les contenus familiaux, des systèmes de filtrage en fonction de l'âge, comme un écran neutre de vérification de l'âge, ou un système approprié tel que défini par la loi applicable, interdisent explicitement aux enfants d'accéder à votre application.
- Votre application fournit des réponses précises au questionnaire sur la classification du contenu concernant les contenus générés par l'utilisateur, conformément au Règlement sur la classification de contenu.

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 héberger des 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 prédominent.

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 des réclamations récurrentes des utilisateurs concernant des contenus inappropriés

---

Services et contenu liés à la santé

Nous n'autorisons pas les applications exposant leurs utilisateurs à des services ou du contenu liés à la santé qui présentent un danger.

Si votre application contient ou met en avant des services ou du contenu liés à la santé, vous devez vous assurer qu'elle respecte les lois et règlements applicables.

Applications de santé

Si votre application accède à des données de santé et est une application de santé ou propose des fonctionnalités liées à la santé, elle doit respecter le Règlement Google Play pour les développeurs existant, y compris les règles Confidentialité, tromperie et utilisation abusive des appareils et sur les Événements sensibles, en plus des exigences ci-dessous :

- **Déclaration dans la Play Console :**
  - Accédez à la page "Contenu de l'application" (Règles > Contenu de l'application) de la Play Console et sélectionnez la ou les catégories associées à votre application.
- **Exigences liées aux règles de confidentialité et à la visibilité des communiqués :**
  - Un lien vers des règles de confidentialité doit figurer dans le champ de la Play Console prévu à cet effet. Ce lien ou le texte correspondant doivent également figurer dans l'application elle-même. Assurez-vous que vos règles de confidentialité sont disponibles sur une URL qui n'est pas bloquée par une zone de géorepérage (pas au format PDF), qui est active, accessible au public et non modifiable (conformément à la section "Sécurité des données").
  - Les règles de confidentialité de votre application, ainsi que les communiqués dans votre application, doivent divulguer de manière exhaustive comment elle accède aux données utilisateur

personnelles ou sensibles (pas seulement les données mentionnées dans la section Sécurité des données ci-dessus), ainsi que la façon dont elle les collecte, les utilise et les partage. Pour toutes les fonctionnalités ou données régies par des autorisations dangereuses ou d'exécution , l'application doit respecter toutes les Exigences concernant la visibilité des communiqués et les demandes de consentement applicables.
  - Les autorisations qui ne sont pas nécessaires aux fonctionnalités de base d'une application de santé ne doivent pas être demandées et les autorisations inutilisées doivent être supprimées. Pour obtenir la liste des autorisations applicables aux données sensibles liées à la santé, consultez l'article Catégories d'applications de santé et consignes supplémentaires.
  - Si votre application n'est pas principalement en lien avec la santé, mais si elle comporte des fonctionnalités qui s'y réfèrent et qu'elle a accès à des données de santé, elle doit quand même respecter les règles relatives aux applications de santé. Le lien entre la fonctionnalité de base de l'application et la collecte de données relatives à la santé doit être clair pour l'utilisateur (par exemple, il peut s'agir d'assurances santé, d'applications de jeu qui collectent des données sur l'activité d'un utilisateur pour l'aider à progresser dans le jeu, etc.). Les règles de confidentialité de l'application doivent mentionner cette utilisation limitée.
- **Exigences supplémentaires :**
  Si votre application de santé correspond à l'une des désignations ci-dessous, vous devez respecter les exigences applicables en plus de sélectionner la bonne catégorie dans la Play Console :
  - **Applications de santé affiliées à une administration publique** : si l'administration publique ou une organisation de santé reconnue vous autorisent à développer et à distribuer une application en affiliation avec elles, vous devez fournir un justificatif prouvant votre éligibilité à l'aide du formulaire d'avis préalable.
  - **Applications de suivi des contacts et de l'état de santé** : si votre application est une application de suivi des contacts et/ou de l'état de santé, sélectionnez "Prévention des maladies et santé publique" dans la Play Console et fournissez les informations requises à l'aide du formulaire d'avis préalable ci-dessus.
  - **Applications de recherche sur des sujets humains** : les applications utilisées à des fin de recherche liée à la santé sur des sujets humains doivent respecter l'ensemble des règles et des réglementations, y compris, mais sans s'y limiter, l'obtention du consentement éclairé des participants ou, dans le cas de mineurs, de leur parent ou représentant légal. Les applications de recherche médicale doivent également obtenir l'approbation d'un comité d'examen institutionnel (IRB) et/ou d'un comité d'éthique indépendant équivalent, sauf si elles en sont dispensées. La preuve de cette approbation devra être fournie sur demande.
  - **Applications liées aux dispositifs médicaux ou aux logiciels en tant que dispositifs médicaux** : les applications considérées comme étant des dispositifs médicaux ou des logiciels en tant que dispositifs médicaux doivent obtenir et conserver une attestation ou une autre forme d'autorisation communiquée par une autorité ou un organisme réglementaires chargés de la gouvernance et de la conformité de l'application de santé. La preuve de cette attestation ou autorisation devra être fournie sur demande.

Données Santé Connect

Les données accessibles par le biais des autorisations de Santé Connect sont considérées comme des données utilisateur sensibles et à caractère personnel soumises aux règles sur les données utilisateur , ainsi qu'à des exigences supplémentaires .

Produits pharmaceutiques sur ordonnance

Nous n'autorisons pas les applications qui facilitent la vente ou l'achat sans ordonnance de produits pharmaceutiques normalement délivrés sur ordonnance.

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.

Voici quelques exemples courants de non-respect des règles :

- Tous les éléments figurant sur 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) en lien avec le contrôle ou 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 .

Informations incorrectes sur la santé

Nous n'autorisons pas les applications contenant des allégations mensongères concernant la santé, en contradiction avec un consensus médical établi ou présentant un danger pour les utilisateurs.

Voici quelques exemples courants de non-respect des règles :

- Allégations mensongères concernant les vaccins (par exemple, prétendre que les vaccins peuvent modifier l'ADN)
- Promotion de traitements dangereux ou non approuvés
- Promotion de pratiques médicales dangereuses, telles que les thérapies de conversion

Fonctionnalités médicales

Nous n'autorisons pas les applications présentant des fonctionnalités médicales ou liées à la santé qui sont mensongères ou potentiellement dangereuses. Par exemple, nous n'autorisons pas les applications qui affirment disposer d'une fonction d'oxymétrie uniquement basée sur l'application. Les applications d'oxymètre doivent être acceptées par un équipement externe, un accessoire connecté ou des capteurs de smartphone dédiés conçus pour prendre en charge une fonction d'oxymétrie. Ces applications acceptées doivent aussi comporter des clauses de non-responsabilité dans les métadonnées. Ces clauses doivent stipuler qu'elles ne sont pas destinées à un usage médical, sont uniquement conçues à des fins générales de forme et de bien-être et ne sont pas un dispositif médical. Elles doivent aussi correctement indiquer le modèle des équipements/appareils compatibles.

Paiements – Services cliniques

Les transactions impliquant des services cliniques réglementés ne doivent pas utiliser le système de facturation de Google Play. Pour en savoir plus, consultez l'article Comprendre le règlement Google Play sur les paiements .

Contenu basé sur une blockchain

La technologie blockchain évoluant rapidement, nous nous efforçons de fournir aux développeurs une plate-forme qui permet d'exploiter les innovations et de créer des expériences plus riches et immersives pour les utilisateurs.

Dans le cadre de ce règlement, nous considérons les contenus basés sur une blockchain comme étant des ressources numériques tokenisées sécurisées par une blockchain. Si votre application intègre un tel contenu, vous devez respecter les présentes exigences.

Échanges et portefeuilles logiciels de cryptomonnaies

L'achat, la possession ou l'échange de cryptomonnaies doivent être effectués par le biais de services certifiés dans les juridictions réglementées.

Vous devez respecter les règlements applicables à toute région ou tout pays que cible votre application. Vous devez également éviter de publier celle-ci dans les pays ou régions où vos produits et services sont interdits. Google Play peut vous demander de fournir des documents ou des informations supplémentaires concernant votre respect des exigences réglementaires et de licence applicables.

Minage de cryptomonnaies

Nous n'autorisons pas les applications qui permettent de miner des cryptomonnaies sur les appareils. En revanche, nous autorisons celles qui gèrent à distance ce processus.

Règles de transparence pour la distribution de ressources numériques tokenisées

Si votre application vend des ressources numériques tokenisées ou permet aux utilisateurs d'en gagner, vous devez l'indiquer dans le formulaire de déclaration des fonctionnalités financières, disponible à la page "Contenu de l'application" dans la Play Console.

Lorsque vous créez un produit intégré, vous devez indiquer dans les informations détaillées sur le produit qu'il représente une ressource numérique tokenisée. Pour des conseils supplémentaires, consultez la section Créer un produit intégré.

Vous ne devez pas promouvoir ni valoriser la possibilité de remporter des gains en jouant ou en effectuant des échanges.

Exigences supplémentaires pour la ludification des NFT

Conformément au Règlement concernant les jeux d'argent et de hasard utilisant de l'argent réel, les jeux et les concours de Google Play, vous devez déposer une demande pour toute application de jeux d'argent et de hasard qui intègre des ressources numériques tokenisées, telles que des NFT.

Pour toutes les autres applications qui ne remplissent pas les critères d'éligibilité des applications de jeux d'argent et de hasard et qui ne sont pas incluses dans les Programmes pilotes sur les autres applications de jeux utilisant de l'argent réel, aucun élément ayant une valeur monétaire ne doit être accepté en échange de la chance d'obtenir un NFT de valeur inconnue. Les NFT achetés par les utilisateurs doivent être utilisés dans le jeu et servir à améliorer l'expérience de jeu ou aider les joueurs à progresser. Ils ne doivent pas servir à parier ni à miser pour avoir une chance de remporter des prix ayant une valeur monétaire réelle (y compris d'autres NFT).

Voici quelques exemples courants de non-respect des règles :

- Applications qui vendent des lots de NFT sans déclarer les contenus spécifiques ni la valeur des NFT.
- Jeux de casino payants sur les réseaux sociaux, par exemple des machines à sous, qui permettent de gagner des NFT.

Contenu généré par IA

À mesure que les modèles d'IA générative deviennent plus largement accessibles aux développeurs, vous êtes susceptible d'incorporer ces modèles à vos applications afin d'augmenter l'engagement et d'améliorer l'expérience utilisateur. Google Play souhaite vous aider à vous assurer que le contenu généré par IA est sûr pour tous les utilisateurs et que les commentaires des utilisateurs sont pris en compte afin de permettre une innovation responsable.

Contenu généré par IA

Le contenu généré par IA est créé par des modèles d'IA générative basés sur les requêtes des utilisateurs. Voici quelques exemples de contenu généré par IA :

- Chatbots d'IA générative conversationnelle texte-vers-texte où l'interaction avec le chatbot est la fonctionnalité principale de l'application
- Image générée par IA à partir de texte, d'image ou de requêtes vocales

Pour assurer la sécurité des utilisateurs et conformément au Champ d'application du règlement de Google Play, les applications qui génèrent du contenu par IA doivent respecter le règlement pour les développeurs existant de Google Play, y compris en interdisant le Contenu soumis à restriction, tel que le contenu facilitant l'exploitation ou l'abus de mineurs, et le contenu permettant un Comportement trompeur, et en empêchant la création de tels contenus.

Les applications qui génèrent du contenu par IA doivent contenir des fonctionnalités de rapport ou de signalement permettant aux utilisateurs de signaler du contenu offensant aux développeurs sans avoir à sortir de l'application. Les développeurs doivent se servir des rapports des utilisateurs pour améliorer le filtrage et la modération du contenu dans leurs applications.

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 courants de non-respect des règles :

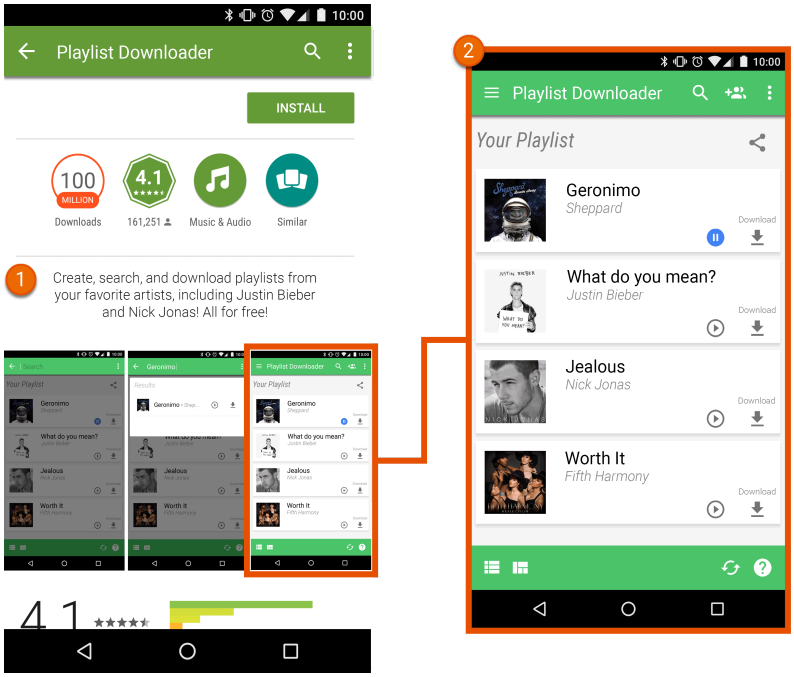
- Images illustrant les pochettes d'albums ou de jeux vidéo et les couvertures de livres
- Images publicitaires provenant de films, de la télévision ou de jeux vidéo
- Affiches ou images provenant de bandes dessinées, de dessins animés, de films, de clips musicaux ou de la télévision
- Logos d'équipes 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 les marques d'un tiers sont utilisées dans votre application d'une manière pouvant 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 utiliser abusivement les réseaux, les appareils ou les informations personnelles sont strictement interdites.

Données utilisateur

Vous devez faire preuve de transparence concernant le traitement appliqué aux données utilisateur (par exemple, les informations collectées auprès d'un utilisateur ou à son sujet, y compris les informations sur les appareils). Vous êtes donc tenu d'informer les utilisateurs si votre application accède à des données utilisateur, les collecte, les utilise, les traite et les partage, et de limiter l'exploitation de ces données aux fins communiquées, conformément aux règles en vigueur. Veuillez noter que tout traitement de données utilisateur personnelles et sensibles est également soumis à des exigences supplémentaires décrites dans la section "Données utilisateur personnelles et sensibles" ci-dessous. En plus de cette règle et du règlement du programme Play pour les développeurs, vous devez à tout moment respecter les lois sur la confidentialité et la protection des données applicables dans les juridictions où vous proposez vos produits ou services. Par exemple, si vous proposez des services à des résidents de l'Union européenne, sachez que l'autorité française chargée de la protection des données, la CNIL, a publié des recommandations pour mieux protéger la vie privée dans le domaine des applications mobiles. Nous vous conseillons de vous y référer.

Si vous incluez du code tiers (par exemple, un SDK) dans votre application, vous devez vous assurer que son utilisation dans votre application et que les pratiques de l'entité tierce concernant le traitement des données utilisateur liées à votre application sont conformes au Règlement du programme Google Play pour les développeurs, lequel comprend diverses exigences relatives à l'utilisation et à la divulgation de telles données. Par exemple, vous devez vous assurer que vos fournisseurs de SDK ne vendent pas les données personnelles et sensibles des utilisateurs de votre application. Cette exigence s'applique également lorsque les données utilisateur sont transférées après avoir été envoyées à un serveur, ou lorsqu'un tel transfert résulte de l'intégration d'un code tiers à votre application.

Données utilisateur personnelles et sensibles

Les données utilisateur sensibles et à caractère personnel incluent, sans toutefois s'y limiter, les informations permettant d'identifier personnellement l'utilisateur, financières, de paiement et d'authentification, l'annuaire téléphonique, les contacts, la position de l'appareil, les données concernant les SMS et les appels, les données de santé, les données Santé Connect, l'inventaire

des autres applications sur l'appareil, les données des capteurs du micro et de l'appareil photo, ainsi que d'autres données sensibles sur l'appareil ou l'utilisation. Si votre application gère des données utilisateur sensibles et à caractère personnel, vous devez prendre les précautions suivantes :

- Limitez la consultation, la collecte, l'utilisation et le partage des données utilisateur sensibles et à caractère personnel acquises par le biais de l'application aux besoins fonctionnels et aux fins conformes au règlement et raisonnablement attendues par l'utilisateur :
  - Les applications qui étendent l'utilisation des données utilisateur sensibles et à caractère personnel à la diffusion de publicités doivent respecter les Règles relatives aux annonces de Google Play.
  - Vous êtes également autorisé à transférer de telles données, le cas échéant, à des fournisseurs de services ou pour des raisons légales, comme la nécessité de répondre à une demande gouvernementale, d'obéir à des lois applicables, ou encore en cas de fusion ou d'acquisition, à condition d'en informer les utilisateurs selon les modalités conformes aux lois en vigueur.
- Traitez de manière sécurisée toutes les données utilisateur sensibles et à caractère personnel, y compris en les transmettant à l'aide d'une technologie de cryptographie récente (HTTPS, par exemple).
- Affichez une demande d'autorisations d'exécution chaque fois que disponible avant d'accéder à des données protégées par des autorisations Android .
- Ne vendez pas les données utilisateur sensibles et à caractère personnel.
  - "Vente" signifie l'échange ou le transfert de données utilisateur sensibles et à caractère personnel à un tiers moyennant une contrepartie monétaire.
    - Le transfert de données utilisateur sensibles et à caractère personnel à l'initiative de l'utilisateur (par exemple, lorsque celui-ci utilise une fonctionnalité de l'application pour transférer un fichier à un tiers, ou fait le choix d'utiliser une application à des fins spécifiques dans le cadre d'une étude) n'est pas considéré comme une vente.

Exigences concernant la visibilité des communiqués et la demande d'autorisation

Dans les cas où l'accès, la collecte, l'utilisation ou le partage des données utilisateur sensibles et à caractère personnel par votre application sont susceptibles de ne pas correspondre aux attentes raisonnables de l'utilisateur du produit ou de la fonctionnalité concernés (par exemple, si la collecte des données se fait en arrière-plan lorsque l'utilisateur n'utilise pas votre application), vous devez respecter les exigences suivantes :

Communiqué visible : vous devez afficher un communiqué au sein de l'application concernant votre accès, collecte, utilisation et partage des données, lequel :

- doit figurer dans l'application elle-même, et pas seulement dans sa description sur un site Web ;
- doit s'afficher lors de l'utilisation normale de l'application et ne pas nécessiter de la part de l'utilisateur qu'il parcoure un menu ou des paramètres ;
- doit préciser les données faisant l'objet d'un accès ou d'une collecte ;
- doit expliquer comment les données seront utilisées et/ou partagées ;
- ne peut pas uniquement figurer dans des règles de confidentialité ou des conditions d'utilisation ;
- ne peut pas être inclus avec d'autres communiqués sans rapport avec la collecte de données sensibles et à caractère personnel.

Consentement et autorisations d'exécution : les demandes de consentement et d'autorisation d'exécution adressées à l'utilisateur dans l'application doivent être immédiatement précédées d'une communication dans l'application conforme aux exigences du présent règlement. 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 son accord (appuyer pour accepter, cocher une case, etc.) ;

- ne doit pas considérer le fait que l'utilisateur quitte le communiqué (y compris en appuyant ailleurs, en revenant à l'accueil ou en appuyant sur un bouton "Retour") comme un consentement ;
- ne doit pas utiliser de messages éphémères ou qui disparaissent automatiquement pour obtenir le consentement de l'utilisateur ; et
- doit être accordée par l'utilisateur avant que l'application ne commence à collecter les données sensibles et à caractère personnel ou y accède.

Les applications qui s'appuient sur d'autres bases juridiques pour traiter les données utilisateur sensibles et à caractère personnel sans consentement, par exemple un intérêt légitime tel que défini dans le RGPD de l'UE, doivent se conformer à toutes les obligations légales applicables et fournir des communiqués appropriés aux utilisateurs, y compris des communiqués dans l'application, comme l'exige le présent règlement.

Pour respecter les exigences définies dans le règlement, il est recommandé de se référer à l'exemple de format suivant pour les communiqués visibles, lorsque ceux-ci sont obligatoires.

- "[Cette application] collecte/transmet/synchronise/stocke [type de données] pour permettre [fonctionnalité], [dans quelles circonstances]."
- *Exemple : "Fitness Funds collecte les données de localisation pour permettre le suivi de l'activité physique même lorsque l'application est fermée ou inutilisée. Ces données sont également utilisées à des fins publicitaires."*
- *Exemple : "Call Buddy collecte, lit et écrit les données des journaux d'appels pour permettre l'organisation des contacts même lorsque l'application n'est pas utilisée."*

Si votre application intègre du code tiers (par exemple, un SDK) conçu pour collecter par défaut des données utilisateur sensibles et à caractère personnel, vous devez, dans un délai de deux semaines à compter de la réception d'une demande de Google Play (ou dans le délai stipulé dans cette demande s'il excède deux semaines), fournir des preuves suffisantes démontrant que votre application satisfait aux exigences concernant la visibilité des communiqués et les demandes de consentement du présent règlement, y compris en ce qui concerne l'accès, la collecte, l'utilisation ou le partage des données via le code tiers.

Voici quelques exemples courants de non-respect des règles :

- Application qui recueille la position de l'appareil sans aucun communiqué visible expliquant quelle fonctionnalité utilise ces données ni comment l'application les utilise en arrière-plan
- Application qui dispose d'une autorisation d'exécution demandant à accéder aux données avant le communiqué visible qui indique à quoi servent les données
- Application qui accède à l'inventaire des applications installées de l'utilisateur et qui ne traite pas ces informations comme des données sensibles ou à caractère personnel soumises aux exigences énoncées ci-dessus concernant les règles de confidentialité, le traitement des données, la visibilité des communiqués et les demandes de consentement
- 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 exigences énoncées ci-dessus concernant les règles de confidentialité, le traitement des données, la visibilité des communiqués et les demandes de consentement
- 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 utilise 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

- Application avec un SDK collectant des données utilisateur sensibles et à caractère personnel et qui ne traite pas ces données comme étant soumises au présent règlement sur les données utilisateur et aux exigences concernant l'accès, le traitement des données (y compris la vente non autorisée), la visibilité des communiqués et les demandes de consentement

Pour plus d'informations, consultez cet article sur les exigences concernant la visibilité des communiqués et les demandes de consentement.

Restrictions d'accès aux données utilisateur sensibles et à caractère personnel

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 données utilisateur sensibles et à caractère personnel, que ce soient 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 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.
Votre application s'adresse à des enfants.	Votre application ne doit pas contenir un SDK dont l'utilisation dans des services destinés aux enfants n'est pas approuvée. Accédez à l'article Conception d'applications pour les enfants et les familles afin de consulter l'intégralité du règlement et des exigences associées.
Votre application collecte des identifiants permanents d'appareils ou crée des associations avec ces identifiants (par exemple, IMEI, IMSI, numéro de série SIM, etc.).	Nous n'autorisons pas l'association des identifiants permanents d'appareils avec les données utilisateur sensibles ou à caractère personnel ni avec les identifiants d'appareils réinitialisables, sauf dans les cas suivants : • téléphonie liée à une identité SIM (par exemple, les appels Wi-Fi liés au compte d'un opérateur) ; • gestion d'appareils professionnels acceptant le mode propriétaire de l'appareil. Ces utilisations doivent être clairement indiquées aux utilisateurs conformément aux dispositions des Règles sur les données utilisateur . Veuillez consulter cette ressource pour en savoir plus sur d'autres types d'identifiants uniques. Veuillez prendre connaissance des Règles relatives aux annonces pour obtenir des consignes supplémentaires concernant les identifiants publicitaires Android.

Section Sécurité des données

Tous les développeurs doivent remplir, pour chaque application, la section Sécurité des données de façon claire et précise. Ils doivent y préciser les méthodes de collecte, d'utilisation et de partage des données utilisateur. Les développeurs sont responsables de l'exactitude de ces informations et de leur mise à jour régulière. Le cas échéant, les informations fournies dans cette section doivent être conformes à celles divulguées dans les règles de confidentialité de l'application.

Pour en savoir plus sur les informations à fournir dans la section Sécurité des données, veuillez consulter cet article .

Règles de confidentialité

Toutes les applications doivent présenter leurs règles de confidentialité dans le champ correspondant de la Play Console. Ces règles, ou un lien permettant de les consulter, doivent également figurer dans l'application. Ces règles, ainsi que les communiqués dans votre application, doivent divulguer de manière exhaustive comment celle-ci accède aux données utilisateur (pas seulement les données mentionnées dans la section Sécurité des données), ainsi que la façon dont elle les collecte, les utilise et les partage. Cela doit comprendre ce qui suit :

- Les informations sur le développeur, et les coordonnées de contact pour les questions de confidentialité ou un système pour envoyer des questions à ce sujet
- Les types de données utilisateur sensibles et à caractère personnel auxquelles votre application accède, qu'elle recueille, utilise et partage, ainsi que les parties avec lesquelles ces données sont partagées
- Des procédures sécurisées de manipulation des données pour les données utilisateur sensibles et à caractère personnel
- Les règles du développeur concernant la conservation et la suppression des données
- La désignation claire des règles de confidentialité (par exemple, sous le titre "Règles de confidentialité")

L'entité (le développeur ou l'entreprise, par exemple) figurant sur la fiche Google Play Store ou l'application doivent être mentionnées dans les règles de confidentialité. Les applications qui n'accèdent à aucune donnée utilisateur sensible et à caractère personnel doivent quand même inclure des règles de confidentialité.

Assurez-vous que vos règles de confidentialité sont disponibles en ligne (pas au format PDF) et non modifiables. L'URL doit être active et accessible au public, et ne pas être bloquée par une zone de géorepérage.

Exigences concernant la suppression de comptes

Si votre application permet aux utilisateurs de créer un compte à partir de l'application, elle doit également leur permettre de demander à ce que celui-ci soit supprimé. Les utilisateurs doivent disposer d'une option facilement accessible pour entreprendre la suppression du compte d'application, que ce soit à partir de l'application ou en dehors (par exemple, sur votre site Web). Une adresse menant à cette ressource Web doit être indiquée dans le champ d'URL prévu à cet effet dans le formulaire de la Play Console.

Lorsque vous supprimez un compte d'application à la demande de l'utilisateur, vous devez également supprimer les données utilisateur associées. La désactivation temporaire, la suspension ou le gel d'un compte d'application ne suffisent pas à répondre à ces exigences de suppression. Si un motif légitime (par exemple, sécurité, prévention des fraudes ou conformité réglementaire) vous impose de garder certaines données, vous devez clairement informer les utilisateurs de vos pratiques de conservation des données (par exemple, dans vos règles de confidentialité).

Pour en savoir plus sur les exigences concernant la suppression de comptes, veuillez consulter cet article du Centre d'aide. Pour plus d'informations sur la mise à jour de votre formulaire Sécurité des données, consultez cet article.

Utiliser l'ID d'ensemble d'applications

Nous allons introduire un nouvel ID Android pour les cas d'utilisation essentiels tels que l'analyse et la prévention des fraudes. Les conditions d'utilisation de cet identifiant figurent ci-dessous.

- **Utilisation** : l'ID d'ensemble d'applications ne doit pas être utilisé pour la personnalisation ni l'analyse des annonces.
- **Association à des informations personnelles ou à d'autres identifiants** : l'ID du groupe d'applications ne doit pas être associé à d'autres identifiants Android (par exemple, AAID) ni à des données personnelles ou sensibles à des fins publicitaires.

- **Transparence et autorisation** : la collecte et l'utilisation de l'ID d'ensemble d'applications, de même que votre engagement à respecter ces conditions, doivent être présentés aux utilisateurs dans un avis de confidentialité à caractère juridique adéquat, y compris dans vos règles de confidentialité. Vous devez obtenir l'autorisation de l'utilisateur de manière légale et valide, chaque fois que nécessaire. Pour en savoir plus sur les règles que nous appliquons en termes de confidentialité, consultez le règlement concernant les Données utilisateur .

Cadres de protection des données UE-États-Unis et Suisse-États-Unis, extension britannique du Cadre de protection des données UE-États-Unis

Si vous accédez à des informations personnelles mises à disposition par Google qui identifient directement ou indirectement une personne et qui proviennent de l'Espace économique européen, du Royaume-Uni ou de la Suisse (dénommées ci-après "informations personnelles provenant de l'Union européenne"), ou si vous utilisez ou traitez de telles informations, vous êtes tenu de vous conformer aux obligations suivantes :

- Respecter l'ensemble des lois, des directives, des réglementations et autres règles applicables sur la confidentialité, la sécurité et la protection des données
- Accéder aux informations personnelles provenant de l'Union européenne, les utiliser ou les traiter uniquement aux fins consenties par la personne à laquelle se rapportent ces informations
- Mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les informations personnelles provenant de l'Union européenne contre la perte, l'usage abusif, l'accès non autorisé ou illicite, la divulgation, l'altération ou la destruction
- Fournir le même niveau de protection que celui établi dans les Principes du cadre de protection des données ou les mécanismes de transfert applicables tels que décrits dans les Conditions Google relatives à la protection des données Responsable du traitement-Responsable du traitement

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 et API ayant accès aux informations sensibles

Les demandes d'autorisation et d'API ayant accès aux informations sensibles doivent avoir du sens pour les utilisateurs. Vous ne pouvez demander une autorisation ou une API ayant accès aux informations sensibles que si elles sont nécessaires pour mettre en œuvre des fonctionnalités ou des services déjà disponibles dans votre application et mis en avant sur votre fiche Google Play. Vous ne pouvez pas utiliser d'autorisations ou d'API qui accèdent à des informations sensibles permettant elles-mêmes d'accéder aux données concernant l'utilisateur ou l'appareil à des fins ou pour des fonctionnalités non divulguées, non implémentées ou non autorisées. Les données personnelles ou sensibles obtenues par le biais d'autorisations ou d'API ayant accès à des informations sensibles ne peuvent être ni vendues ni partagées en vue de réaliser une vente.

Exigez que les autorisations et API ayant accès à des informations sensibles accèdent aux données en contexte (par le biais de demandes supplémentaires), afin que l'utilisateur comprenne pourquoi votre application a besoin de cette autorisation. N'utilisez ces données qu'aux fins pour lesquelles l'utilisateur a donné son consentement. 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, les autorisations dites "restreintes" correspondent aux autorisations dangereuses , spéciales , avec signature ou mentionnées ci-dessous. Elles sont soumises aux conditions et restrictions supplémentaires suivantes :

- Les données relatives à l'utilisateur ou à l'appareil et accessibles par le biais d'autorisations restreintes sont considérées comme des données utilisateur sensibles et à caractère personnel. Les exigences du Règlement sur les données utilisateur s'appliquent.
- 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).
- L'utilisation d'autorisations en infraction avec les règles sur les logiciels malveillants de Google Play (y compris toute utilisation abusive des droits élevés) est formellement interdite.

Certaines autorisations restreintes peuvent faire l'objet d'exigences supplémentaires, détaillées ci-dessous. Ces restrictions ont pour but de protéger la confidentialité 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 qui ne peut pas être mise en œuvre à l'aide d'une autre méthode. Nous évaluons les exceptions proposées en fonction de leur impact potentiel sur la sécurité et la confidentialité 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 personnelles et sensibles. À ce titre, elles sont soumises au règlement sur les Informations personnelles et sensibles , ainsi qu'aux restrictions suivantes : .

Autorisation restreinte	Exigence
Groupe d'autorisations associé au 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.
Groupe d'autorisations associé aux 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 donnée utilisateur sensible et personnelle soumise au règlement sur les informations personnelles et sensibles, au règlement sur la localisation en arrière-plan, ainsi qu'aux exigences suivantes :

- Les applications ne peuvent pas accéder aux 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 actuellement proposés dans votre appli.
- 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.
- Les applications ne doivent 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 localisation 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 recourant à 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 l'utilisation :

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

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

Pour en savoir plus sur les exigences du règlement, consultez cet article d'aide.

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 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.

Autorisation de visibilité sur les packages (applications)

L'inventaire des applications installées interrogé à partir d'un appareil est considéré comme une donnée personnelle et sensible soumise au règlement sur les informations personnelles et sensibles, et aux exigences suivantes :

Les applications ayant pour finalité principale le lancement ou la recherche d'autres applications sur l'appareil, ou l'interaction avec celles-ci peuvent, selon leurs besoins, obtenir l'une des visibilités suivantes sur d'autres applications installées sur l'appareil :

- **Visibilité étendue sur les applications** : une application avec une "visibilité étendue" bénéficie d'une visibilité large (ou étendue) sur les applications installées ("packages") sur un appareil.
  - Pour les applications ciblant le niveau d'API 30 ou version ultérieure , la visibilité étendue sur les applications installées via l'autorisation QUERY_ALL_PACKAGES est limitée à des cas d'utilisation spécifiques où, pour fonctionner, l'application doit être capable de détecter et/ou d'interagir avec toutes les applications présentes sur l'appareil.
    - Vous ne pouvez pas utiliser l'autorisation QUERY_ALL_PACKAGES si votre application peut fonctionner avec une déclaration de visibilité de packages plus restreinte (par exemple, effectuer des requêtes ciblant des packages spécifiques et interagir avec eux plutôt que de demander une visibilité étendue).
  - L'utilisation d'autres méthodes pour approcher la visibilité étendue offerte par l'autorisation QUERY_ALL_PACKAGES est également limitée aux fonctionnalités de base de l'application visibles par l'utilisateur et à l'interopérabilité avec toute application découverte par ces méthodes.
  - Pour en savoir plus sur les cas d'utilisation acceptés par l'autorisation QUERY_ALL_PACKAGES, veuillez consulter cet article du Centre d'aide .
- **Visibilité limitée sur les applications** : on parle de "visibilité limitée" lorsqu'une application restreint son accès aux données en effectuant des requêtes destinées à des applications spécifiques à l'aide de méthodes plus ciblées (et non "étendues"), par exemple en effectuant des requêtes destinées à des applications spécifiques qui respectent la déclaration du fichier manifeste de votre application. Si votre application bénéficie de capacités d'interopérabilité et de gestion conformes aux règles pour ces applications, vous pouvez utiliser cette méthode pour effectuer des requêtes ciblant des applications.
- La visibilité sur l'inventaire des applications installées sur un appareil doit être directement liée à la finalité principale de votre application ou aux fonctionnalités de base auxquelles les utilisateurs accèdent via l'application.

Les données d'inventaire des applications interrogées depuis des applications distribuées sur Play ne doivent en aucun cas être vendues ni partagées à des fins d'analyse ou de monétisation des annonces.

API Accessibility

L'API Accessibility ne peut pas être utilisée pour :

- modifier les paramètres des utilisateurs sans leur autorisation ni les empêcher de désactiver ou désinstaller une application ou un service, sauf autorisation d'un parent ou d'un représentant légal accordée par le biais d'une application de contrôle parental, ou d'administrateurs habilités via un logiciel de gestion d'entreprise ;
- contourner les notifications et les paramètres de confidentialité intégrés à Android ;
- modifier ou exploiter l'interface utilisateur de manière trompeuse ou contraire au règlement du programme Google Play pour les développeurs.

L'API Accessibility n'est pas conçue pour enregistrer des appels audio à distance et ne peut pas être appelée pour faire cela.

L'utilisation de l'API Accessibility doit être documentée sur la fiche Google Play.

Consignes pour IsAccessibilityTool

Les applications dont la finalité principale est d'aider directement les personnes ayant un handicap peuvent utiliser **IsAccessibilityTool** pour se déclarer publiquement comme application d'accessibilité.

Les applications non éligibles à **IsAccessibilityTool** ne sont pas autorisées à utiliser l'indicateur et doivent être conformes aux exigences sur la visibilité des communiqués et l'autorisation, comme indiqué dans les Règles sur les données utilisateur , leur fonctionnalité d'accessibilité n'étant pas évidente pour l'utilisateur. Pour en savoir plus, consultez l'article du centre d'aide sur l'API AccessibilityService .

Dans la mesure du possible, les applications doivent privilégier des API et autorisations au champ d'application plus ciblé au lieu de l'API Accessibility pour obtenir la fonctionnalité souhaitée.

Autorisation "Demander l'installation de packages"

L'autorisation REQUEST_INSTALL_PACKAGES permet à une application de demander l'installation de packages d'applications. Pour l'utiliser, la fonctionnalité de base de votre application doit :

- permettre d'envoyer et de recevoir des packages d'applications ; et
- donner la possibilité à l'utilisateur d'installer des packages d'applications.

Fonctionnalités autorisées :

- Navigation ou recherche sur le Web
- Services de communication acceptant les pièces jointes
- Partage, transfert ou gestion de fichiers
- Gestion d'appareils d'entreprise
- Sauvegarde et restauration
- Migration d'appareils/Transfert de numéros de téléphone
- Application associée pour synchroniser le téléphone avec un appareil connecté ou IoT (une montre connectée ou une smart TV, par exemple)

La fonctionnalité de base désigne la finalité principale de l'application. Celle-ci, ainsi que les fonctionnalités essentielles qui la composent, doit être documentée et mise en avant de façon visible dans la description de l'application.

L'autorisation REQUEST_INSTALL_PACKAGES ne peut pas être utilisée pour réaliser des mises à jour automatiques, des modifications ou le regroupement d'autres APK dans le fichier d'assets, sauf à des fins de gestion d'appareils. Les mises à jour et l'installation de packages doivent respecter le Règlement de Google Play sur l'utilisation abusive des appareils et des réseaux, et doivent être lancées et contrôlées par l'utilisateur.

Autorisations de Health Connect by Android

Santé Connect est une plate-forme Android qui permet aux applications de santé et de remise en forme de stocker et de partager les mêmes données stockées sur l'appareil dans un écosystème unifié. Elle permet aussi aux utilisateurs de contrôler depuis un seul endroit quelles applications peuvent lire et écrire des données de santé et de remise en forme, y compris des dossiers médicaux. Les dossiers médicaux peuvent inclure les antécédents médicaux, diagnostics, traitements, médicaments, résultats d'analyse, ou d'autres données cliniques, fournis par des établissements ou des prestataires de santé, ou obtenus via des plates-formes de santé tierces compatibles.

Santé Connect prend en charge la lecture et l'écriture de types de données variés, comme le nombre de pas, la température corporelle ou les données de dossier médical.

Les données accessibles par le biais des autorisations de Santé Connect sont considérées comme des données utilisateur sensibles et à caractère personnel soumises au Règlement sur les données utilisateur. Si votre application est une application de santé ou comporte des fonctionnalités liées à la santé et a accès à des données de santé, y compris celles issues de Santé Connect, elle doit également respecter le Règlement sur les applications de santé.

Veuillez consulter le Guide du développeur Android pour découvrir comment faire vos premiers pas avec Santé Connect. Pour demander l'accès à des types de données Santé Connect et pour obtenir des réponses à d'autres questions fréquentes, consultez les Questions fréquentes sur les exigences liées au règlement Santé Connect.

Les applications distribuées sur Google Play doivent respecter les règles suivantes pour lire et/ou écrire des données dans Santé Connect.

Accès et utilisation appropriés pour Health Connect

Santé Connect peut uniquement être utilisé conformément aux règles et conditions d'utilisation applicables, et pour les cas d'utilisation approuvés définis dans le présent règlement. Cela signifie que vous ne pouvez demander l'accès aux autorisations que lorsque votre application ou service répond à l'un des cas d'utilisation approuvés.

Les cas d'utilisation approuvés incluent le fitness et le bien-être, les récompenses, le coaching sportif, le bien-être au travail, les soins médicaux, la recherche médicale et les jeux. Les applications qui ont le droit d'accéder à ces cas d'utilisation ne peuvent pas étendre leur utilisation à des fins non divulguées ou non autorisées.

Seuls les services ou applications dotés d'une ou de plusieurs fonctionnalités destinées à être bénéfiques à la santé et à la forme physique des utilisateurs peuvent demander l'accès aux autorisations de Santé Connect. En voici quelques exemples :

- Applications ou services permettant aux utilisateurs de **directement consigner dans un journal ou un rapport, de suivre et/ou d'analyser** leur activité physique, leur sommeil, leur bien-être mental, leur alimentation, les mesures d'évaluation de leur santé, leurs descriptions physiques, leur dossier médical et/ou d'autres descriptions et mesures liées à la santé ou à la forme physique
- Applications ou services permettant aux utilisateurs de **stocker leur activité physique, leur sommeil, leur bien-être mental, leur alimentation, les mesures d'évaluation de leur santé, leurs descriptions physiques, leur dossier médical** et/ou d'autres descriptions et mesures liées à la santé ou à la forme physique sur leur appareil, et de partager leurs données avec d'autres applications de l'appareil qui répondent à ces cas d'utilisation.
- Applications ou services permettant aux utilisateurs de gérer des maladies chroniques, des traitements médicaux ou une assistance aux soins.

L'accès à Santé Connect ne peut être utilisé d'une manière allant à l'encontre du présent règlement ou d'autres conditions d'utilisation applicables de Santé Connect, y compris aux fins suivantes :

- N'utilisez pas Santé Connect pour développer des applications, des environnements ou des activités où l'utilisation ou un dysfonctionnement de Santé Connect pourrait raisonnablement entraîner la mort, des blessures corporelles, des dommages aux personnes, ou des dommages environnementaux ou matériels (tels que la construction ou l'exploitation d'installations nucléaires, le contrôle du trafic aérien, les appareils de maintien en vie ou l'armement). N'intégrez pas non plus Santé Connect à ce type d'applications, d'environnements ou d'activités.
- N'accédez pas aux données obtenues par le biais de Santé Connect à l'aide d'applications headless (ou "applications sans tête"). Les applications doivent être représentées par une icône clairement identifiable dans la barre des applications, les paramètres des applications de l'appareil, les icônes de notification, etc.
- N'utilisez pas Santé Connect avec des applications qui synchronisent les données entre des appareils ou des plates-formes non compatibles.
- N'utilisez pas Santé Connect pour la connexion à des applications, services ou fonctionnalités ciblant uniquement des enfants.
- Prenez des mesures raisonnables et appropriées pour protéger l'ensemble des applications ou systèmes qui recourent à Santé Connect contre un accès, une utilisation, une destruction, une perte, une altération ou une divulgation non autorisés ou illégaux.

Il vous incombe également de veiller au respect de toutes les exigences réglementaires ou obligations légales qui peuvent s'appliquer en fonction de l'utilisation que vous comptez faire de Santé Connect et des données qui en sont issues. Par exemple, si vous êtes une entité ou un partenaire commercial soumis au Health Insurance Portability and Accountability Act (HIPAA), vous devez vous conformer aux exigences applicables concernant votre accès aux informations issues de Santé Connect et l'utilisation que vous en faites. Si vous êtes un développeur soumis au Règlement général sur la protection des données (RGPD) pour les utilisateurs de l'UE, vous êtes également tenu de respecter les obligations définies par le RGPD. Ces lois et règlements peuvent exiger que vous concluiez d'autres accords

(accord de partenariat ou accord de traitement des données, par exemple) avec les organismes concernés impliqués dans vos activités de traitement avant de partager des données. Il incombe également aux développeurs d'applications de déterminer si leurs activités nécessitent de conclure de tels accords. Les développeurs doivent fournir la preuve de tels accords ou de leur conformité si Google le leur demande.

Sauf mention explicite dans l'étiquetage ou les informations fournies par Google pour des produits ou services Google spécifiques, Google ne garantit pas l'exactitude des données contenues dans Santé Connect et ne se porte pas garant de leur utilisation à quelque fin que ce soit, et en particulier à des fins de recherche, de santé ou médicales. Google décline toute responsabilité liée à l'utilisation des données obtenues par l'intermédiaire de Santé Connect.

Limites d'utilisation

Lors de l'utilisation de Santé Connect, l'accès aux données et leur utilisation doivent respecter des restrictions spécifiques :

- Les données ne doivent être utilisées que pour fournir ou améliorer le cas d'utilisation approprié ou des fonctionnalités visibles dans l'interface utilisateur de l'application.
- Les données utilisateur ne peuvent être transférées à des tiers qu'avec le consentement explicite de l'utilisateur, et uniquement à des fins de sécurité (par exemple, pour examiner un abus), pour respecter les lois ou règlements applicables, ou en cas de fusions/acquisitions.
- Sauf si l'utilisateur a fourni son consentement explicite, l'accès aux données utilisateur par une personne n'est autorisé qu'à des fins de sécurité, pour respecter la loi ou si les données sont agrégées pour des opérations internes, conformément aux obligations légales.
- **Tout autre transfert ainsi que toute autre utilisation ou vente des données de Santé Connect sont interdits, y compris :**
  - le transfert ou la vente des données utilisateur à des tiers tels que des plates-formes publicitaires, des courtiers en données ou tout autre revendeur d'informations ;
  - le transfert, la vente ou l'exploitation des données utilisateur pour diffuser des publicités, y compris des publicités personnalisées ou basées sur les centres d'intérêt ;
  - le transfert, la vente ou l'exploitation des données utilisateur pour déterminer la solvabilité ou à des fins de prêt ;
  - le transfert, la vente ou l'exploitation des données utilisateur avec tout produit ou service pouvant être considéré comme un dispositif médical, sauf si l'application associée au dispositif médical respecte tous les règlements applicables, y compris l'obtention des autorisations ou approbations d'organismes de réglementation applicables (tels que la FDA américaine) pour l'utilisation prévue des données Santé Connect, et si l'utilisateur a donné son consentement explicite pour une telle utilisation ;
  - le transfert, la vente ou l'exploitation des données utilisateur à quelque fin ou de quelque manière que ce soit impliquant des données de santé protégées (telles que définies par la loi fédérale américaine HIPAA), à moins que l'utilisateur en ait fait la demande et que cela soit conforme aux exigences de la loi HIPAA.

Champ d'application minimal

Vous ne devez demander accès qu'aux autorisations nécessaires à l'implémentation des fonctionnalités ou services de votre produit. Ces demandes d'accès doivent être spécifiques et limitées aux données nécessaires.

Notification et contrôle transparents et précis

Santé Connect traite des données de santé et de remise en forme qui comprennent des informations personnelles et sensibles. Les développeurs doivent expliquer clairement dans un communiqué accessible leurs pratiques de gestion des données par le biais de règles de confidentialité complètes. Ce communiqué doit inclure les éléments suivants :

- Une représentation exacte de l'identité de l'application ou du service qui demande à accéder aux données utilisateur
- Des informations claires et exactes expliquant les types de données faisant l'objet d'un accès, d'une demande et/ou d'une collecte (les données doivent avoir un lien avec une fonctionnalité visible par l'utilisateur ou une recommandation faite dans votre application)
- Une explication de la façon dont les données seront utilisées et/ou partagées : si vous demandez des données pour une certaine raison, mais qu'elles seront aussi destinées à un usage secondaire, vous devrez divulguer aux utilisateurs tous les cas d'utilisation
- Des documents d'aide à l'utilisateur qui expliquent comment celui-ci peut gérer et supprimer ses données dans l'application et ce que deviennent les données lorsqu'un compte est désactivé et/ou supprimé
- Des informations sur le traitement sécurisé de toutes les données utilisateur sensibles et à caractère personnel, y compris leur transfert à l'aide d'une technologie de cryptographie moderne (HTTPS, par exemple)

Pour plus d'informations sur les exigences applicables aux applications se connectant à Santé Connect, veuillez consulter cet article du Centre d'aide.

Service VPN

VpnService est une classe de base pour les applications qui étendent ou développent leurs propres solutions de VPN. Seules les applications qui utilisent la classe VpnService et ont pour fonctionnalité de base celle de VPN peuvent créer un tunnel vers un serveur distant sécurisé au niveau de l'appareil. Les applications qui nécessitent un serveur distant pour exécuter une fonctionnalité de base font figure d'exceptions. Exemples:

- Applications de contrôle parental ou de gestion d'entreprise
- Suivi de l'utilisation d'une application
- Applications de sécurisation d'appareils (antivirus, gestion des appareils mobiles, pare-feu, etc.)
- Outils de réseau (accès à distance, etc.)
- Applications de navigation Web
- Applications d'opérateurs nécessitant d'utiliser un VPN pour accéder aux services de téléphonie ou de connectivité

La classe VpnService n'autorise pas les utilisations suivantes:

- Collecte de données sensibles ou à caractère personnel sans communiqué visible ni demande de consentement
- Redirection ou manipulation du trafic d'utilisateurs d'autres applications sur un appareil à des fins de monétisation (redirection du trafic publicitaire via un pays autre que celui de l'utilisateur, etc.)

Les applications qui utilisent la classe VpnService doivent:

- documenter leur utilisation de VpnService sur leur fiche GooglePlay
- chiffrer les données entre l'appareil et le point d'arrivée du tunnel VPN
- respecter dans son intégralité le Règlement du programme pour les développeurs, y compris les règles sur la fraude publicitaire, les autorisations et les logiciels malveillants.

Autorisation "Alarme exacte"

La nouvelle autorisation "USE_EXACT_ALARM" sera introduite avec Android 13 (niveau d'API cible 33). Cette autorisation permet d'accéder à la fonctionnalité d'alarme exacte.

USE_EXACT_ALARM est une autorisation restreinte. Seules les applications dont une fonctionnalité de base justifie le besoin d'une alarme exacte peuvent déclarer cette autorisation. Les applications qui

sollicitent cette autorisation restreinte sont soumises à un examen. Celles qui ne satisfont pas aux critères d'utilisation autorisée ne pourront pas être publiées sur Google Play.

Cas d'utilisation autorisée pour l'autorisation "Alarme exacte"

Votre application ne doit utiliser "USE_EXACT_ALARM" que si l'une de ses fonctionnalités de base (orientée utilisateur) implique l'exécution d'actions à une date et une heure précises. Exemples :

- L'application sert d'alarme, de réveil ou de minuteur.
- L'application sert d'agenda et affiche des notifications d'événement.

Si votre cas d'utilisation de l'alarme exacte ne figure pas dans la liste ci-dessus, vous devez évaluer si le recours à SCHEDULE_EXACT_ALARM peut être une solution alternative.

Pour en savoir plus sur la fonctionnalité d'alarme exacte, lisez ces conseils pour les développeurs .

Autorisation d'intent plein écran

Pour les applications ciblant Android 14 (niveau d'API 34) ou version ultérieure, l'autorisation USE_FULL_SCREEN_INTENT est une autorisation d'accès spéciale pour les applications . Les applications ne se verront accorder automatiquement l'autorisation USE_FULL_SCREEN_INTENT que si leur fonctionnalité principale relève de l'une des catégories ci-dessous nécessitant des notifications à priorité très élevée :

- Régler une alarme
- Recevoir des appels téléphoniques ou vidéo

Les applications qui sollicitent cette autorisation sont soumises à un examen. Celles qui ne satisfont pas aux critères ne bénéficieront pas automatiquement de cette autorisation. Dans ce cas, elles devront demander à l'utilisateur de leur accorder l'accès à l'autorisation USE_FULL_SCREEN_INTENT.

Pour rappel, toute utilisation de l'autorisation USE_FULL_SCREEN_INTENT doit respecter le Règlement du programme Google Play pour les développeurs, y compris nos règlements sur les logiciels mobiles indésirables et sur l'utilisation abusive des appareils et des réseaux, ainsi que nos Règles relatives aux annonces. Les notifications avec intent plein écran ne doivent pas perturber, endommager ni affecter l'appareil de l'utilisateur, ni y accéder sans autorisation. En outre, les applications ne doivent pas interférer avec d'autres applications ni avec l'usabilité de l'appareil.

Pour en savoir plus sur l'autorisation USE_FULL_SCREEN_INTENT, consultez le Centre 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 ou un interpréteur avec un accès indirect aux API Android (JavaScript dans la WebView ou dans un navigateur, par exemple).

Les applications ou le code tiers (par exemple, les SDK) avec un langage interprété (JavaScript, Python, Lua, etc.) chargé au moment de l'exécution (par exemple, non fourni dans le package de l'application) ne doivent pas permettre une infraction potentielle aux règles Google Play.

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 :

Exemples courants de non-respect des règles sur l'utilisation abusive des appareils et des réseaux :

- 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 permettant de pirater des services, des logiciels ou des matériels ou de contourner des dispositifs de sécurité, ou fournissant des instructions pour y parvenir.
- Applications qui accèdent à un service ou à une API, ou qui les utilisent, d'une manière non conforme à ses conditions d'utilisation.
- Applications qui ne peuvent pas figurer sur la liste d'autorisation et tentent de contourner la gestion de l'alimentation du système .
- Applications qui fournissent des services de proxy à des tiers (cette utilisation n'est autorisée que s'il s'agit de la principale fonctionnalité proposée à l'utilisateur par l'application).
- 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.
- Applications ou code tiers (par exemple, SDK) contenant une WebView avec une interface JavaScript supplémentaire qui charge du contenu Web non fiable (par exemple, URL http://) ou des URL non validées obtenues à partir de sources non fiables (par exemple, URL provenant d'intents peu fiables).
- Applications qui utilisent l'autorisation d'afficher les intents en plein écran pour forcer une interaction avec les utilisateurs à l'aide d'annonces ou de notifications intrusives.

Utilisation des services de premier plan

L'autorisation de service de premier plan permet l'utilisation appropriée des services de premier plan visibles par l'utilisateur. Pour les applications ciblant Android 14 ou version ultérieure, vous devez spécifier un type de service de premier plan valide pour chaque service de premier plan utilisé dans votre application, et déclarer l'autorisation de service de premier plan appropriée pour ce type. Par exemple, si le cas d'utilisation de votre application nécessite la géolocalisation, vous devez déclarer l'autorisation FOREGROUND_SERVICE_LOCATION dans le fichier manifeste de votre application.

Les applications ne sont autorisées à déclarer une autorisation de service de premier plan que si son utilisation :

- fournit une fonctionnalité utile à l'utilisateur, liée au fonctionnement de base de l'application ;
- est initiée ou peut être remarquée par l'utilisateur (par exemple, la lecture d'un contenu audio, la diffusion d'un contenu multimédia sur un autre appareil, une notification utilisateur claire et exacte, une demande utilisateur d'importation de photos sur le cloud) ;
- peut être arrêtée ou suspendue par l'utilisateur ;
- ne peut être ni interrompue ni différée par le système sans nuire à l'expérience utilisateur ou au fonctionnement d'une fonctionnalité attendue par l'utilisateur (par exemple, un appel téléphonique doit démarrer immédiatement et ne peut être différé par le système) ;
- ne dure pas plus que le temps nécessaire pour effectuer la tâche.

Les critères ci-dessous ne s'appliquent pas aux cas d'utilisation de services de premier plan suivants :

- Les types de services de premier plan systemExempted ou shortService
- Le type de service de premier plan dataSync uniquement lors de l'utilisation des fonctionnalités de Play Asset Delivery

Pour plus de détails sur l'utilisation des services de premier plan, cliquez ici.

Tâches de transfert de données initiées par l'utilisateur

Les applications ne sont autorisées à utiliser les API des tâches de transfert de données initiées par l'utilisateur que si leur utilisation:

- est initiée par l'utilisateur ;
- sert à des tâches de transfert de données réseau;
- ne dure pas plus longtemps que nécessaire pour effectuer le transfert de données.

Pour plus de détails sur l'utilisation des API User-Initiated Data Transfer, cliquez ici.

Exigences concernant Flag Secure

FLAG_SECURE est un indicateur d'affichage déclaré dans le code d'une application afin de signaler que l'UI comporte des données sensibles et que celles-ci devraient uniquement s'afficher sur des surfaces sécurisées lorsque l'application est utilisée. Cet indicateur est conçu pour empêcher les données d'apparaître sur les captures d'écran ou sur des surfaces non sécurisées. Le développeur déclare cet indicateur lorsque le contenu de son application ne doit pas être diffusé, affiché ou autrement transmis hors de l'application ou de l'appareil de l'utilisateur.

Pour des raisons de sécurité et de confidentialité, toutes les applications mises à disposition sur Google Play sont tenues de respecter les indicateurs FLAG_SECURE déclarés par d'autres applications. Autrement dit, ces applications ne doivent ni permettre ni contribuer à permettre de contourner les paramètres FLAG_SECURE d'autres applications.

Les applications entrant dans la catégorie des outils d'accessibilité sont exemptées de cette exigence, à condition de ne pas transmettre, enregistrer ou mettre en cache du contenu protégé par l'indicateur FLAG_SECURE d'une manière permettant d'y accéder sur un appareil autre que celui de l'utilisateur.

Applications exécutant des conteneurs Android sur l'appareil

Les applications utilisant des conteneurs Android sur l'appareil fournissent des environnements qui simulent l'ensemble ou une partie de l'OS Android sous-jacent. L'expérience au sein de ces environnements peut ne pas refléter l'ensemble des fonctionnalités de sécurité d'Android . C'est pourquoi les développeurs peuvent choisir d'ajouter un indicateur d'environnement sécurisé dans le manifeste afin d'interdire aux conteneurs Android sur l'appareil de fonctionner dans un environnement Android simulé.

Indicateur manifeste d'environnement sécurisé

REQUIRE_SECURE_ENV est un indicateur qui peut être déclaré dans le fichier manifeste d'une application pour indiquer qu'elle ne doit pas être exécutée sur un conteneur Android sur l'appareil. Pour des raisons de sécurité et de confidentialité, les applications utilisant des conteneurs Android sur l'appareil sont tenues de respecter cet indicateur lorsqu'il est déclaré par d'autres applications. Elles doivent également :

- Examiner les fichiers manifestes des applications qu'elles ont l'intention de charger dans leur conteneur Android sur l'appareil pour cet indicateur ;
- Ne pas charger les applications qui ont déclaré cet indicateur dans leur conteneur Android sur l'appareil ;

- Ne pas agir comme un proxy en interceptant ou en appelant des API sur l'appareil de manière à ce qu'elles apparaissent comme étant installées dans le conteneur ;
- Ne pas permettre ni contribuer à permettre de contourner l'indicateur (y compris en chargeant une version plus ancienne d'une application pour contourner l'indicateur REQUIRE_SECURE_ENV de l'application actuelle).

Pour en savoir plus sur cette règle, consultez le Centre d'aide.

Comportement trompeur

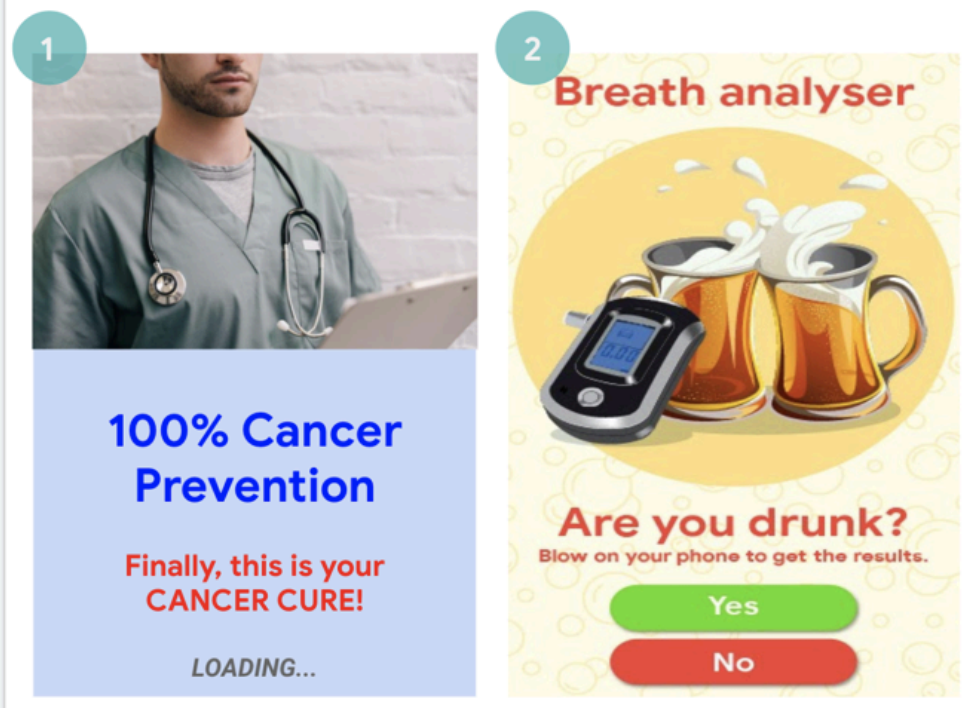
Nous n'autorisons pas les applications conçues pour tromper les utilisateurs ou permettre un comportement malhonnête, y compris, sans s'y limiter, les applications dont le fonctionnement est jugé impossible. Les applications doivent présenter leur fonctionnement au moyen de déclarations, de descriptions 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.
- 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 ou faux, susceptible d'interférer avec les systèmes de vote, ou concernant les résultats d'élections.
- Applications faussement affiliées à un organisme gouvernemental, ou se proposant 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) qui sont trompeuses.
(2) Cette application prétend proposer une fonctionnalité techniquement impossible (utiliser le téléphone comme éthylomètre).

Modification déloyale des paramètres de l'appareil

Nous n'autorisons pas les applications qui modifient de manière externe les paramètres ou les fonctionnalités de l'appareil de l'utilisateur, à son insu et sans son consentement. 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, de comptes bancaires 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

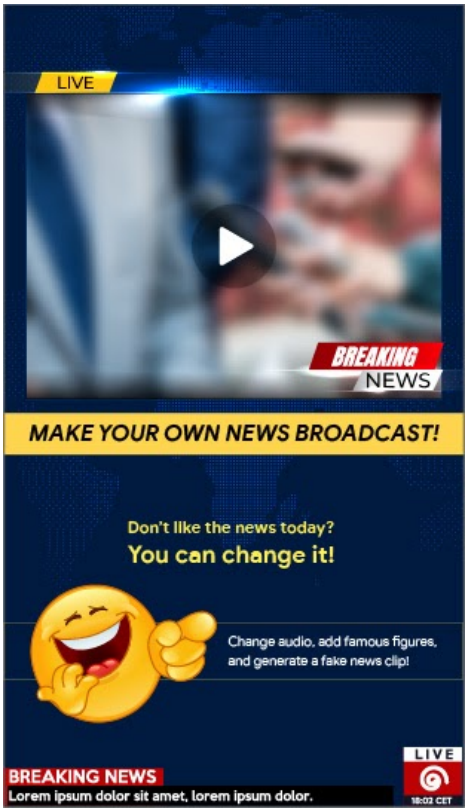
Nous n'autorisons pas les applications qui font la promotion ou facilitent la création d'informations ou d'allégations mensongères ou trompeuses véhiculées par des images, de l'audio, des vidéos et/ou des textes. Nous interdisons les applications que nous jugeons comme faisant la promotion ou favorisant 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.

Des exceptions peuvent être faites pour les contenus d'intérêt général, les images ostensiblement artificielles, les contenus multimédias manipulés accompagnés d'avertissements visibles par les utilisateurs ou de filigranes, ainsi que les contenus manifestement satiriques ou parodiques.

Les contenus multimédias manipulés doivent respecter le règlement pour les développeurs Google Play, y compris en interdisant tout contenu non autorisé, conformément aux règles sur le contenu soumis à restriction.

Voici quelques exemples courants de non-respect des règles :

- 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 les extraits multimédias pour imiter un journal télévisé en incluant des noms ou des logos de médias d'information existants réels sans avertissements ou filigranes clairs
- Applications conçues exclusivement pour créer des contenus multimédias trompeurs



(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.

Transparence du comportement

Les fonctionnalités de votre application doivent être raisonnablement claires pour les utilisateurs. N'incluez aucune fonctionnalité cachée, inactive ou non documentée. Les techniques visant à éviter l'examen de l'application ne sont pas autorisées. Vous pouvez être tenu de fournir des informations supplémentaires sur l'application pour assurer la sécurité des utilisateurs, l'intégrité du système et le respect du règlement.

Déclarations trompeuses

Nous n'autorisons pas les applications ni 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 ;
- travaillent ensemble dans le but de 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 ;
- travaillent avec d'autres applications, sites, comptes de développeur ou autres comptes pour dissimuler l'identité d'un développeur ou d'une application, ou d'autres détails importants, ou fournir de fausses informations à leur sujet, lorsque le contenu de l'application est en lien avec la politique, les problèmes sociaux ou les questions d'ordre public.

Règlement Google Play concernant le niveau d'API cible

Pour offrir une expérience sécurisée à ses utilisateurs, Google Play exige les niveaux d'API cibles ci-dessous pour **toutes les applications** :

Les nouvelles applications et mises à jour d'applications DOIVENT cibler un niveau d'API Android disponible depuis moins d'un an après la dernière version majeure d'Android. Les développeurs de nouvelles applications et de mises à jour qui ne respecteront pas cette exigence ne pourront pas envoyer d'applications dans la Play Console.

Les applications Google Play existantes non mises à jour et qui ne ciblent pas de niveau d'API disponible depuis moins de deux ans après la dernière version majeure d'Android ne seront pas disponibles pour les nouveaux utilisateurs dont les appareils exécutent une version récente de l'OS Android. Les utilisateurs ayant déjà installé l'application à partir de Google Play pourront toujours la rechercher, la réinstaller et s'en servir dans n'importe quelle version de l'OS Android compatible avec cette application.

Pour obtenir des conseils techniques sur la façon de répondre aux exigences du niveau d'API cible, consultez le guide de migration .

Pour connaître les échéances précises et les exceptions, consultez cet article du Centre d'aide .

Règlement sur les données utilisateur

Vous devez faire preuve de transparence concernant le traitement appliqué aux données utilisateur (par exemple, les informations collectées auprès d'un utilisateur ou à son sujet, y compris les informations sur les appareils). Vous êtes donc tenu de divulguer l'accès, la collecte, l'utilisation, le traitement et le partage des données utilisateur effectués à partir de votre application, ainsi que de limiter l'exploitation de ces données aux fins communiquées, conformément aux règles en vigueur.

Si vous incluez du code tiers (par exemple, un SDK) dans votre application, vous devez vous assurer que son utilisation dans votre application, ainsi que les pratiques de l'entité tierce concernant le traitement des données utilisateur liées à votre application, sont conformes au Règlement du programme Google Play pour les développeurs, lequel comprend diverses exigences relatives à l'utilisation et à la divulgation de telles données. Par exemple, vous devez vous assurer que vos fournisseurs de SDK ne vendent pas les données personnelles et sensibles des utilisateurs de votre application. Cette exigence s'applique également lorsque les données utilisateur sont transférées après avoir été envoyées à un serveur, ou lorsqu'un tel transfert résulte de l'intégration d'un code tiers à votre application.

Données utilisateur personnelles et sensibles

- Limitez la consultation, la collecte, l'utilisation et le partage des données utilisateur sensibles et à caractère personnel acquises par le biais de l'application aux besoins fonctionnels et aux fins conformes au règlement et raisonnablement attendues par l'utilisateur :
  - Les applications qui étendent l'utilisation des données utilisateur sensibles et à caractère personnel à la diffusion de publicités doivent respecter les règles relatives aux annonces de Google Play.
- Traitez de manière sécurisée toutes les données utilisateur sensibles et à caractère personnel, y compris en les transmettant à l'aide d'une technologie de cryptographie récente (HTTPS, par exemple).
- Affichez une demande d'autorisations d'exécution chaque fois que disponible avant d'accéder à des données protégées par des autorisations Android.

Vente de données utilisateur personnelles et sensibles

Ne vendez pas les données utilisateur sensibles et à caractère personnel.

- "Vente" signifie l'échange ou le transfert de données utilisateur sensibles et à caractère personnel à un tiers moyennant une contrepartie monétaire.
  - Le transfert de données utilisateur sensibles et à caractère personnel à l'initiative de l'utilisateur (par exemple, lorsque celui-ci utilise une fonctionnalité de l'application pour transférer un fichier à un tiers, ou fait le choix d'utiliser une application à des fins spécifiques dans le cadre d'une étude) n'est pas considéré comme une vente.

Exigences concernant la visibilité des communiqués et les demandes de consentement

Dans les cas où l'accès, la collecte, l'utilisation ou le partage des données utilisateur sensibles et à caractère personnel par votre application sont susceptibles de ne pas correspondre aux attentes raisonnables de l'utilisateur du produit ou de la fonctionnalité concernés, vous devez respecter les exigences concernant la visibilité des communiqués et les demandes de consentement du Règlement sur les données utilisateur.

Si votre application intègre du code tiers (par exemple, un SDK) conçu pour collecter par défaut des données utilisateur sensibles et à caractère personnel, vous devez, dans un délai de deux semaines à compter de la réception d'une demande de Google Play (ou dans le délai stipulé dans cette demande s'il excède deux semaines), fournir des preuves suffisantes démontrant que votre application satisfait aux exigences concernant la visibilité des communiqués et les demandes de consentement du présent règlement, y compris en ce qui concerne l'accès, la collecte, l'utilisation ou le partage des données via le code tiers.

N'oubliez pas de vous assurer que votre utilisation du code tiers (par exemple, un SDK) n'entraîne pas un non-respect du Règlement sur les données utilisateur.

Pour plus d'informations sur les exigences concernant la visibilité des communiqués et les demandes de consentement, consultez cet article du Centre d'aide.

Exemples de cas de non-respect provoqués par un SDK

- Application avec un SDK collectant des données utilisateur sensibles et à caractère personnel et qui ne traite pas ces données comme étant soumises au présent règlement sur les données utilisateur et aux exigences concernant l'accès, le traitement des données (y compris la vente non autorisée), la visibilité des communiqués et les demandes de consentement
- Application intégrant un SDK qui collecte par défaut des données utilisateurs sensibles et à caractère personnel, en violation des exigences du règlement présent concernant la visibilité des communiqués et les demandes de consentement
- Application avec un SDK présenté comme collectant des données utilisateur sensibles et à caractère personnel uniquement pour fournir à l'application des fonctionnalités de lutte contre la fraude et les utilisations abusives, mais qui partage également les données qu'il collecte avec des tiers à des fins publicitaires ou d'analyse
- Application incluant un SDK qui transmet des informations sur les packages installés par les utilisateurs sans respecter les consignes des Règles de confidentialité et/ou celles sur la visibilité des communiqués
  - Voir aussi le Règlement sur les logiciels mobiles indésirables

Exigences supplémentaires concernant l'accès aux données utilisateur sensibles et à caractère personnel

Le tableau suivant décrit les exigences à respecter pour certaines activités :

Activité	Exigence
Votre application collecte des identifiants permanents d'appareils ou crée des associations avec ces identifiants (par exemple, IMEI, IMSI, numéro de série SIM, etc.).	Nous n'autorisons pas l'association des identifiants permanents d'appareils avec les données utilisateur sensibles ou à caractère personnel ni avec les identifiants d'appareils réinitialisables, sauf dans les cas suivants : • Téléphonie associée à une identité SIM (appels Wi-Fi associés à un compte d'opérateur, par exemple) • Applications d'entreprise dédiées à la gestion des appareils et utilisant le mode propriétaire de l'appareil Ces cas d'utilisation doivent faire l'objet d'un communiqué visible présenté aux utilisateurs, conformément aux dispositions du Règlement sur les données utilisateur. Veuillez consulter cette ressource pour en savoir plus sur d'autres types d'identifiants uniques. Veuillez prendre connaissance des Règles relatives aux annonces pour obtenir des consignes supplémentaires concernant les identifiants publicitaires Android.

Votre application s'adresse à des enfants.	Votre application ne peut inclure que des SDK autocertifiés pour une utilisation dans des services destinés aux enfants. Accédez au Programme relatif aux SDK publicitaires autocertifiés pour les familles afin de consulter l'intégralité du règlement et des exigences associées.

Exemples de cas de non-respect provoqués par un SDK

- Application qui utilise un SDK associant le code IMEI à la position
- Application avec un SDK associant l'identifiant publicitaire Android (AAID) à des identifiants permanents d'appareils, à des fins publicitaires ou d'analyse
  Application qui utilise un SDK associant l'AAID à l'adresse e-mail à des fins d'analyse

Section Sécurité des données

Tous les développeurs doivent remplir la section Sécurité des données de façon claire et précise pour chaque application. Ils doivent y préciser les méthodes de collecte, d'utilisation et de partage des données utilisateur. Cela inclut les données collectées et gérées via les bibliothèques ou SDK tiers utilisés dans leurs applications. Les développeurs sont responsables de l'exactitude de ces informations et de leur mise à jour régulière. Le cas échéant, les informations fournies dans cette section doivent être conformes à celles divulguées dans les règles de confidentialité de l'application.

Pour en savoir plus sur les informations à fournir dans la section Sécurité des données, veuillez consulter cet article du Centre d'aide.

Consultez l'intégralité du Règlement sur les données utilisateur.

Règlement sur les autorisations et API ayant accès aux informations sensibles

Les demandes d'autorisation et d'API ayant accès aux informations sensibles doivent avoir du sens pour les utilisateurs. Vous ne pouvez demander une autorisation ou une API ayant accès aux informations sensibles que si elles sont nécessaires pour mettre en œuvre des fonctionnalités ou des services déjà disponibles dans votre application et mis en avant sur votre fiche Google Play. Vous ne pouvez pas utiliser d'autorisations ou d'API qui accèdent à des informations sensibles permettant elles-mêmes d'accéder aux données concernant l'utilisateur ou l'appareil à des fins ou pour des fonctionnalités non divulguées, non implémentées ou non autorisées. Les données sensibles ou à caractère personnel obtenues par le biais d'autorisations ou d'API ayant accès à des informations sensibles ne peuvent être ni vendues ni partagées en vue de réaliser une vente.

Consultez l'intégralité du Règlement sur les autorisations et API ayant accès aux informations sensibles.

Exemples de cas de non-respect provoqués par un SDK

- Application qui inclut un SDK agissant en arrière-plan pour demander la position, à une fin non autorisée ou non divulguée
- Application qui inclut un SDK transmettant le code IMEI obtenu via l'autorisation read_phone_state d'Android, sans consentement de l'utilisateur

Règlement sur les logiciels malveillants

Notre règlement concernant les logiciels malveillants est simple : le Google Play Store et l'ensemble de l'écosystème Android doivent être exempts de tout comportement (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.

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 potentiellement dangereuses, les binaires ou les modifications de framework, 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.

Les exigences de ce règlement s'appliquent également à tout code tiers (un SDK, par exemple) que vous incluez dans votre application.

Consultez l'intégralité du Règlement sur les logiciels malveillants.

Exemples de cas de non-respect provoqués par un SDK

- Application qui inclut des bibliothèques SDK de fournisseurs distribuant des logiciels malveillants
- 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
- Application qui inclut un SDK ne respectant pas le modèle d'autorisations Android, car il obtient des droits élevés en accédant aux données de l'appareil à une fin non divulguée
- Application qui inclut un SDK dont le code trompe les utilisateurs afin qu'ils achètent du contenu ou s'y abonnent en étant facturés par leur opérateur mobile

Utilisation des SDK dans les applications

Si vous incluez un SDK dans votre application, vous devez vous assurer que les pratiques et le code tiers associés n'entraînent pas un non-respect du Règlement du programme Google Play pour les développeurs. Il est important de savoir comment les SDK inclus dans votre application traitent les données utilisateur. Vous devez également savoir quelles autorisations ils utilisent, quelles sont les données collectées, et pourquoi.

Exigences concernant les SDK

Les développeurs d'applications s'appuient souvent sur du code tiers (par exemple, un SDK) pour intégrer des services et fonctionnalités clés à leurs applications. Lorsque vous incluez un SDK dans votre application, vous devez vous assurer de pouvoir protéger vos utilisateurs et votre application de toute faille. Dans cette section, nous expliquons comment certaines de nos exigences de confidentialité et de sécurité s'appliquent dans le contexte d'un SDK, et en quoi elles sont conçues pour aider les développeurs à intégrer des SDK dans leurs applications de façon sécurisée.

Si vous incluez un SDK dans votre application, vous devez vous assurer que les pratiques et le code tiers associés n'entraînent pas un non-respect du Règlement du programme Google Play pour les développeurs. Il est important de savoir comment les SDK inclus dans votre application traitent les données utilisateur. Vous devez également savoir quelles autorisations ils utilisent, quelles sont les données collectées, et pourquoi. Sachez que la façon dont un SDK collecte et traite les données utilisateur doit concorder avec l'utilisation conforme au règlement que votre application fait de ces données.

Pour vous assurer que votre utilisation d'un SDK est conforme aux règles, assurez-vous de lire et de comprendre les règles suivantes dans leur intégralité, et prenez note des exigences relatives aux SDK présentées ci-dessous.

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

Logiciel espion

Un logiciel espion est une application, un code ou un comportement malveillant qui collecte, exfiltre ou partage des données sur l'utilisateur ou l'appareil sans lien avec une fonctionnalité conforme aux

règles.

Les codes ou les comportements malveillants assimilables au fait d'espionner l'utilisateur ou d'exfiltrer des données sans en informer correctement l'utilisateur ni obtenir son consentement sont également considérés comme des logiciels espions.

Consultez l'intégralité du Règlement sur les logiciels espions.

Vous trouverez ci-dessous des exemples de non-respect de ce règlement provoqués par un SDK (liste non exhaustive) :

- Application qui utilise un SDK transmettant des données issues d'enregistrements audio ou d'appels lorsqu'elles ne sont pas liées au fonctionnement conforme de l'application
- Application avec du code tiers malveillant (un SDK, par exemple) transmettant des données depuis l'appareil sans que l'utilisateur s'y attende, ou sans en informer l'utilisateur ni obtenir son consentement

Règlement sur les logiciels mobiles indésirables

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.

Exemples de non-respect des règles :

- Fraude publicitaire
- Ingénierie sociale

Protection des données utilisateur

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

Exemples de non-respect des règles :

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

Consultez l'intégralité du Règlement sur les logiciels mobiles indésirables.

Règlement sur l'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 ou codes tiers (par exemple les SDK) écrits avec un langage interprété (JavaScript, Python, Lua, etc.) qui est chargé au moment de l'exécution (par exemple, non fourni dans le package de l'application) ne doivent pas permettre une quelconque violation des règles Google Play.

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.

Consultez l'intégralité du Règlement sur l'utilisation abusive des appareils et des réseaux.

Exemples de cas de non-respect provoqués par un SDK

- Applications qui fournissent des services de proxy à des tiers (cette utilisation n'est autorisée que s'il s'agit de la principale fonctionnalité proposée à l'utilisateur par l'application)
- Application qui inclut un SDK téléchargeant du code exécutable, comme des fichiers dex ou du code natif, depuis une source autre que Google Play
- Application qui inclut un SDK contenant une WebView avec une interface JavaScript supplémentaire qui charge du contenu Web non fiable (par exemple, URL http://) ou des URL non validées obtenues à partir de sources non fiables (par exemple, URL provenant d'intents peu fiables)
- Application qui inclut un SDK contenant du code utilisé pour mettre à jour son propre APK
- Application qui inclut un SDK exposant les utilisateurs à une faille de sécurité en téléchargeant des fichiers via une connexion non sécurisée
- Application qui utilise un SDK contenant du code pour télécharger ou installer des applications à partir de sources inconnues en dehors de Google Play
- Application qui inclut un SDK utilisant des services de premier plan sans cas d'utilisation approprié
- Application qui inclut un SDK utilisant des services de premier plan pour une raison conforme aux règles sans être déclaré dans le fichier manifeste de l'application

Règlement concernant les comportements trompeurs

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.

Consultez l'intégralité du Règlement concernant les comportements trompeurs.

Transparence du comportement

Les fonctionnalités de votre application doivent être raisonnablement claires pour les utilisateurs. N'incluez aucune fonctionnalité cachée, inactive ou non documentée. Les techniques visant à éviter l'examen de l'application ne sont pas autorisées. Vous pouvez être tenu de fournir des informations supplémentaires sur l'application afin de garantir la sécurité des utilisateurs, l'intégrité du système et le respect du règlement.

Exemple de non-respect causé par un SDK

- Votre application inclut un SDK qui utilise des techniques visant à éviter l'examen de l'application.

Quelles règles pour les développeurs Google Play sont généralement associées à des cas de non-respect provoqués par un SDK ?

Pour vous permettre de vous assurer que tous les codes tiers de votre application sont conformes au règlement du programme Google Play pour les développeurs, veuillez consulter les règles suivantes dans leur intégralité :

- Règlement sur les données utilisateur
- Autorisations et API ayant accès aux informations sensibles
- Règlement sur l'utilisation abusive des appareils et des réseaux
- Logiciels malveillants
- Logiciels mobiles indésirables
- Programme relatif aux SDK publicitaires autocertifiés pour les familles
- Règles relatives aux annonces
- Comportements trompeurs
- Règlement du programme Google Play pour les développeurs

Bien que ces règles soient le plus souvent en cause, gardez bien à l'esprit qu'un code de SDK incorrect peut entraîner le non-respect d'une autre règle non référencée ci-dessus. N'oubliez pas de prendre connaissance de toutes les règles dans leur intégralité et de vous tenir informé. En tant que développeur d'applications, il vous incombe de vous assurer que vos SDK traitent les données de vos applications dans le respect des règles.

Pour en savoir plus, veuillez consulter notre Centre d'aide.

Logiciels malveillants

Notre règlement concernant les logiciels malveillants est simple : le Google Play Store et l'ensemble de l'écosystème Android doivent être exempts de tout comportement (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.

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 potentiellement dangereuses, les binaires ou les modifications de framework, 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.

Les exigences de ce règlement s'appliquent également à tout code tiers (un SDK, par exemple) que vous incluez dans votre application.

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 plus d'informations, consultez le site 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 facturation frauduleuse ou les logiciels espions commerciaux. C'est pourquoi Google Play Protect traite dans certains cas un sous-ensemble de backdoors comme une faille.

Facturation frauduleuse

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

La facturation frauduleuse sur mobile se divise en trois catégories : fraude aux SMS, fraude aux appels et fraude aux contenus payants.

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

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

La fraude aux contenus payants 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 aux contenus payants 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

Code qui recueille des données sensibles ou à caractère personnel depuis l'appareil et les transmet à un tiers (entreprise ou personne physique) à des fins de surveillance.

Les applications doivent afficher un communiqué visible concernant l'utilisation des données et obtenir le consentement exigé par le Règlement sur les données utilisateur .

Consignes relatives aux applications de surveillance

Seules sont acceptées les applications exclusivement conçues et commercialisées pour la surveillance d'autrui (par exemple, pour permettre aux parents de surveiller leurs enfants ou à une entreprise de superviser ses employés), à condition de respecter entièrement les exigences décrites ci-dessous. Ces applications ne peuvent pas servir à suivre l'activité d'une autre personne (un conjoint, par exemple) même si celle-ci en est consciente et avec son autorisation, indépendamment de l'affichage ou non d'une notification permanente. Ces applications de surveillance doivent présenter l'indicateur de métadonnées "IsMonitoringTool" dans leur fichier manifeste, afin de se déclarer comme telles.

Les applications de surveillance doivent respecter les exigences suivantes :

- Elles ne doivent pas être présentées comme des solutions d'espionnage ni de surveillance secrète.
- Elles ne doivent pas masquer ni dissimuler leur activité de surveillance, ni tenter de tromper l'utilisateur sur cette fonctionnalité.
- Elles doivent présenter une notification permanente lorsqu'elles sont exécutées, ainsi qu'une icône permettant de les identifier clairement.
- Elles doivent déclarer leurs fonctionnalités de surveillance et de suivi dans leur description sur le Google Play Store.
- Les applications (et leurs fiches sur Google Play) ne doivent fournir aucun moyen d'accéder à des fonctionnalités allant à l'encontre des présentes conditions, ni d'activer de telles fonctionnalités. Par exemple, elles ne doivent pas contenir de liens vers un APK non conforme hébergé en dehors de Google Play.
- Elles doivent se conformer à l'ensemble des lois applicables. Vous êtes seul responsable de l'évaluation de la légalité de votre application sur le marché ciblé.

Pour en savoir plus, reportez-vous à l'article Utiliser l'indicateur isMonitoringTool du centre d'aide.

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 téléchargées 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

Un logiciel espion est une application, un code ou un comportement malveillant qui collecte, exfiltre ou partage des données sur l'utilisateur ou l'appareil sans lien avec une fonctionnalité conforme aux règles.

Les codes ou les comportements malveillants assimilables au fait d'espionner l'utilisateur ou d'exfiltrer des données sans en informer correctement l'utilisateur ni obtenir son autorisation sont également

considérés comme des logiciels espions.

Vous trouverez ci-dessous plusieurs exemples de violation par un logiciel espion (liste non exhaustive) :

- Enregistrement audio ou enregistrement des appels reçus sur le téléphone
- Vol des données d'une application
- Application (comme un SDK) avec du code tiers malveillant transmettant des données depuis l'appareil sans que l'utilisateur s'y attende, ou sans en informer l'utilisateur ni obtenir son autorisation

Toutes les applications doivent aussi respecter l'intégralité du Règlement du programme Google Play pour les développeurs, y compris les règles sur les données de l'utilisateur ou de l'appareil, comme les exigences sur les logiciels mobiles indésirables, les données utilisateur, les autorisations et les API qui permettent d'accéder à des informations sensibles et les SDK.

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 (porte dérobée)" 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'agisse d'une backdoor, et nous demandons à son développeur de lui appliquer un correctif.

Maskware

Application qui utilise diverses techniques d'évasion afin de proposer à l'utilisateur des fonctionnalités d'application différentes ou factices. Ces applications se font passer pour des applications ou des jeux légitimes qui semblent inoffensifs pour les plates-formes de téléchargement d'applications et utilisent des techniques comme l'obscurcissement, le chargement dynamique de code ou les techniques de dissimulation (cloaking) pour cacher du contenu malveillant.

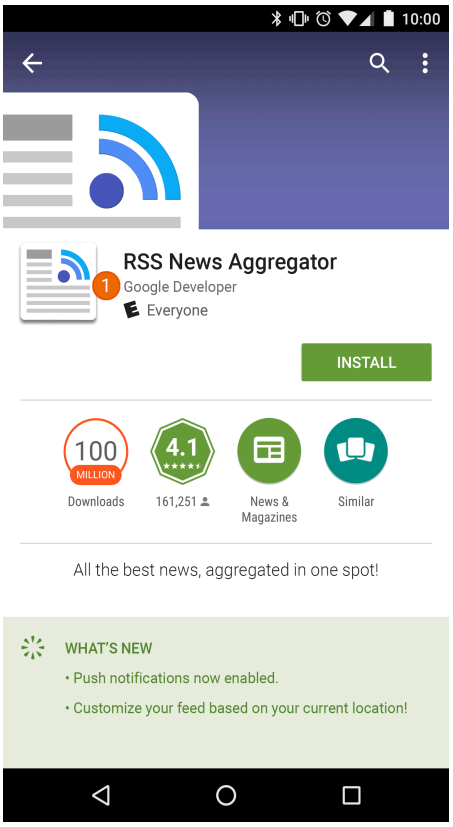
Les logiciels maskware sont semblables aux autres catégories de PHA (applications potentiellement dangereuses), en particulier le cheval de Troie, la principale différence étant les techniques utilisées pour obscurcir l'activité malveillante.

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.

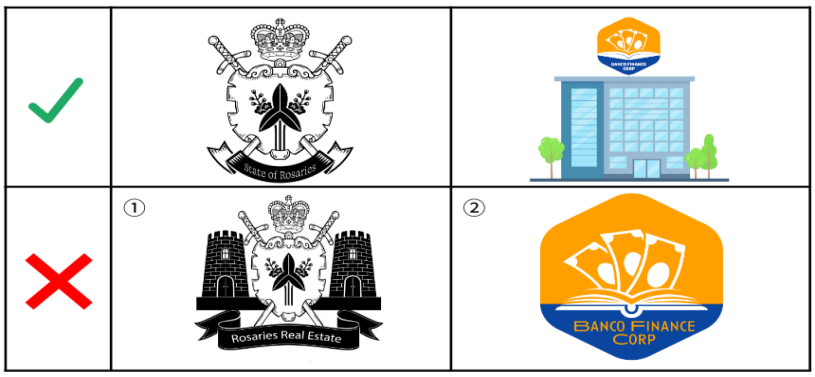
Voici quelques exemples courants de non-respect des règles :

- Développeurs qui font croire à une relation avec un autre développeur ou une autre entreprise, organisation ou entité.



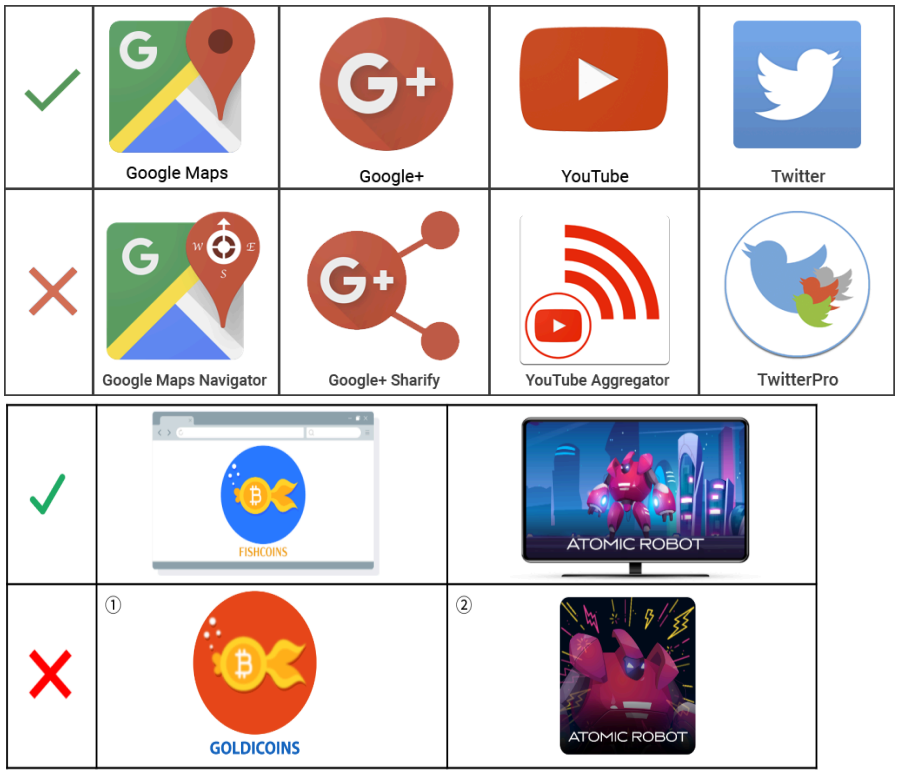
① Le nom du développeur indiqué pour cette application suggère une relation officielle avec Google, alors que ce n'est pas le cas.

- Applications dont les icônes ou les titres font croire à une relation avec un autre développeur ou une autre entreprise, organisation ou entité.



① L'application utilise un emblème national ou fait croire aux utilisateurs qu'elle est affiliée au gouvernement.
② L'application imite le logo d'une entreprise pour faire croire qu'elle est une application officielle de cette entreprise.

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



① L'icône de l'application intègre le logo du site Web d'une cryptomonnaie populaire pour suggérer une relation officielle.
② L'icône de l'application utilise le personnage et le titre d'une série célèbre pour faire croire aux utilisateurs qu'elle est y affiliée.

- 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.
- Applications qui ne respectent pas les Consignes relatives à la marque Android .

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
- Ingénierie sociale

Protéger la confidentialité et les données utilisateur

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

Toutes les applications doivent respecter l'intégralité du Règlement du programme Google Play pour les développeurs, y compris les règles sur les données utilisateur ou de l'appareil, par exemple celles relatives aux données utilisateur, aux autorisations et aux API qui permettent d'accéder à des informations sensibles, aux logiciels espions et aux exigences concernant les SDK.

- Ne demandez pas aux utilisateurs de désactiver des protections de sécurité comme Google Play Protect sur leurs appareils et ne les incitez pas à le faire. Par exemple, vous ne devez pas offrir de récompenses ni proposer de fonctionnalités supplémentaires dans vos applications si les utilisateurs désactivent Google Play Protect.

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 de manière impromptue, y compris en altérant l'utilisation des fonctionnalités de l'appareil ou en interférant avec celle-ci, ou en dehors de l'environnement de l'application déclencheuse sans possibilité simple de les ignorer, ni sans consentement et 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 du système

---

Programmes de téléchargement dangereux

Code qui n'est pas en soi un logiciel indésirable, mais qui télécharge d'autres logiciels indésirables sur mobile.

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 logiciels indésirables sur mobile et qu'il en a téléchargé ou qu'il contient du code pouvant télécharger et installer des applications.
- Ou l'observation d'au moins 500 téléchargements d'applications par ce programme révèle que 5 % d'entre eux ou plus concernent des logiciels indésirables sur mobile (soit 25 téléchargements de tels logiciels constatés).

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 logiciels sont exécutés à la demande des utilisateurs et avec leur autorisation.

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 :

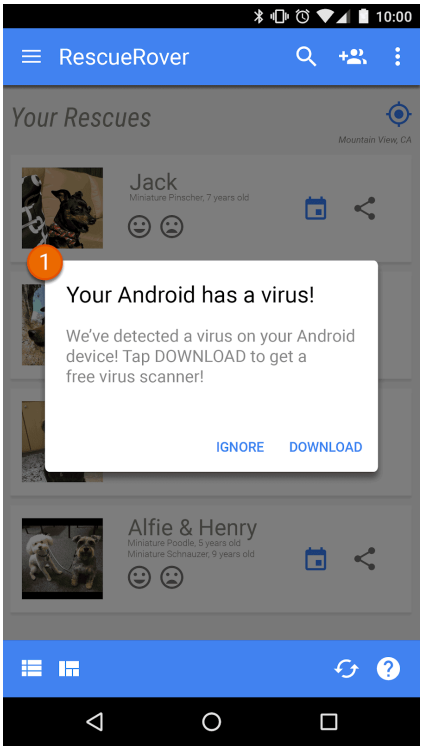
- Application qui affiche des annonces qui ne sont pas visibles par l'utilisateur
- Application qui génère automatiquement des clics sur les annonces sans intention de l'utilisateur ou qui génère un trafic réseau équivalent pour attribuer des crédits de clics de manière frauduleuse
- Application envoyant 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 du système

Nous n'autorisons pas les applications ou les annonces qui imitent ou perturbent les fonctionnalités système, comme les notifications ou les avertissements. 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.

Ingénierie sociale

Nous n'autorisons pas les applications qui se font passer pour d'autres applications dans le but de tromper les utilisateurs en les incitant à effectuer des actions qu'ils avaient l'intention de réaliser dans l'application originale vérifiée.

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 demandons de respecter les règles suivantes.

Paiements

1. Les développeurs qui facturent des téléchargements d'applications sur Google Play sont tenus d'utiliser le système de facturation de cette plate-forme comme mode de paiement pour ces transactions.
2. Les applications distribuées sur Play qui nécessitent ou acceptent un paiement pour accéder à des fonctionnalités ou services intégrés, y compris toute fonctionnalité de l'application, tout contenu numérique ou tout produit (collectivement les "achats via les applications"), doivent utiliser le système de facturation de Google Play pour ces transactions, excepté dans les cas où les sections 3, 8 ou 9 s'appliquent.

   Les fonctionnalités ou services nécessitant l'utilisation du système de facturation de Google Play incluent, sans s'y limiter, les achats via les applications des éléments suivants :

   - Articles (devises virtuelles, vies supplémentaires, durée de jeu supplémentaire, objets complémentaires, personnages et avatars, par exemple)
   - Services sur abonnement (remise en forme, jeux, rencontres, enseignement, musique, vidéo, mises à niveau de services et autres services de contenu sur abonnement, par exemple)
   - Fonctionnement ou contenu d'application, tels qu'une version sans publicité d'une application ou de nouvelles fonctionnalités non disponibles dans la version gratuite
   - Logiciels et services dans le cloud (services de stockage de données, logiciels de productivité pour les entreprises et logiciels de gestion financière, par exemple)

3. Le système de facturation de Google Play ne doit pas être utilisé dans les cas suivants :
   a. L'objet principal du paiement est l'un des suivants :
      - Achat ou location de biens matériels (produits alimentaires, vêtements, articles ménagers, appareils électroniques, par exemple)
      - Achat de services physiques (services de transport, services de nettoyage, billets d'avion, abonnements à des salles de sport, livraison de repas, billets pour des événements, par exemple)
      - Règlement d'une facture de carte de crédit ou de charge courante (par exemple, services de câblodistribution et de télécommunications)

   b. Le paiement inclut des paiements entre particuliers, des enchères en ligne et des dons exonérés d'impôts.
   c. Le paiement concerne des contenus ou des services qui facilitent les jeux d'argent et de hasard en ligne, comme décrit dans la section Applications de jeux d'argent et de hasard du Règlement concernant les jeux d'argent et de hasard utilisant de l'argent réel, les jeux et les concours.
   d. Le paiement concerne toute catégorie de produits considérée comme non autorisée par le Règlement relatif au contenu du Centre de paiement de Google.

      Remarque : Dans certains pays, nous proposons Google Pay pour les applications qui vendent des services et/ou des produits physiques. Pour en savoir plus, consultez notre page sur Google Pay dédiée aux développeurs .

4. En dehors des conditions décrites dans les sections 3, 8 et 9, les applications ne doivent pas diriger les utilisateurs vers un mode de paiement autre que le système de facturation de Google Play. Cette interdiction inclut, sans s'y limiter, la redirection des utilisateurs vers d'autres modes de paiement via :
   - la fiche d'une application sur Google Play ;
   - des promotions intégrées à l'application en lien avec le contenu pouvant être acheté ;
   - les WebViews, boutons, liens, messages, annonces ou autres incitations à l'action intégrés à l'application ;
   - les processus de l'interface utilisateur intégrés à l'application, y compris l'inscription et la création de compte, qui dirigent les utilisateurs vers un mode de paiement autre que le système de facturation de Google Play.

5. Les devises virtuelles intégrées aux applications ne doivent être utilisées que dans l'application ou le jeu dans lesquels elles ont été achetées.
6. Les développeurs doivent informer de manière claire et précise les utilisateurs des conditions d'utilisation et des tarifs de leur application, ainsi que des fonctionnalités intégrées à l'application ou des abonnements proposés à l'achat. La tarification dans l'application doit correspondre à celle affichée dans l'interface de facturation de Google Play visible par les utilisateurs. 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, la fiche de l'application doit clairement informer l'utilisateur que ces fonctionnalités sont payantes.
7. Les applications et jeux offrant des mécanismes permettant de recevoir des objets virtuels aléatoires lors d'un achat, y compris, mais sans s'y limiter, les "loot box", doivent clairement indiquer juste avant l'achat les chances de recevoir de tels objets.
8. Hormis les cas où les conditions décrites à la section 3 s'appliquent, les développeurs d'applications distribuées sur Play qui nécessitent ou acceptent un paiement des utilisateurs situés dans ces pays/régions, afin d'accéder aux achats via les applications, peuvent proposer un système de facturation alternatif en complément du système de facturation de Google Play pour ces transactions. Pour cela, ils doivent correctement remplir un formulaire de déclaration de facturation pour chacun des programmes applicables et accepter les conditions supplémentaires et les Exigences du programme qu'il contient.
9. Les développeurs d'applications distribuées sur Play peuvent rediriger les utilisateurs de l'Espace économique européen (EEE) en dehors de l'application, y compris pour faire la promotion de fonctionnalités et services numérique intégrés à celle-ci. Les développeurs doivent dans ce cas remplir correctement le Formulaire de déclaration pour le programme et accepter les conditions supplémentaires et les Exigences du programme qu'il contient.

Remarque : Vous pouvez consulter le calendrier et les questions fréquentes concernant cette règle dans notre Centre d'aide.

Annonces

Pour offrir en permanence une expérience de qualité, nous prenons en compte le contenu, l'audience, l'expérience utilisateur, le comportement, ainsi que la sécurité et la confidentialité de votre annonce. Nous considérons que les annonces et les offres associées font partie de l'application et doivent respecter toutes les autres règles de Google Play. Les annonces font l'objet d'exigences supplémentaires si vous monétisez une application qui cible les enfants sur Google Play.

Pour en savoir plus, lisez le Règlement sur la promotion d'application et les fiches Play Store et découvrez comment nous gérons les pratiques promotionnelles mensongères.

Contenu des annonces

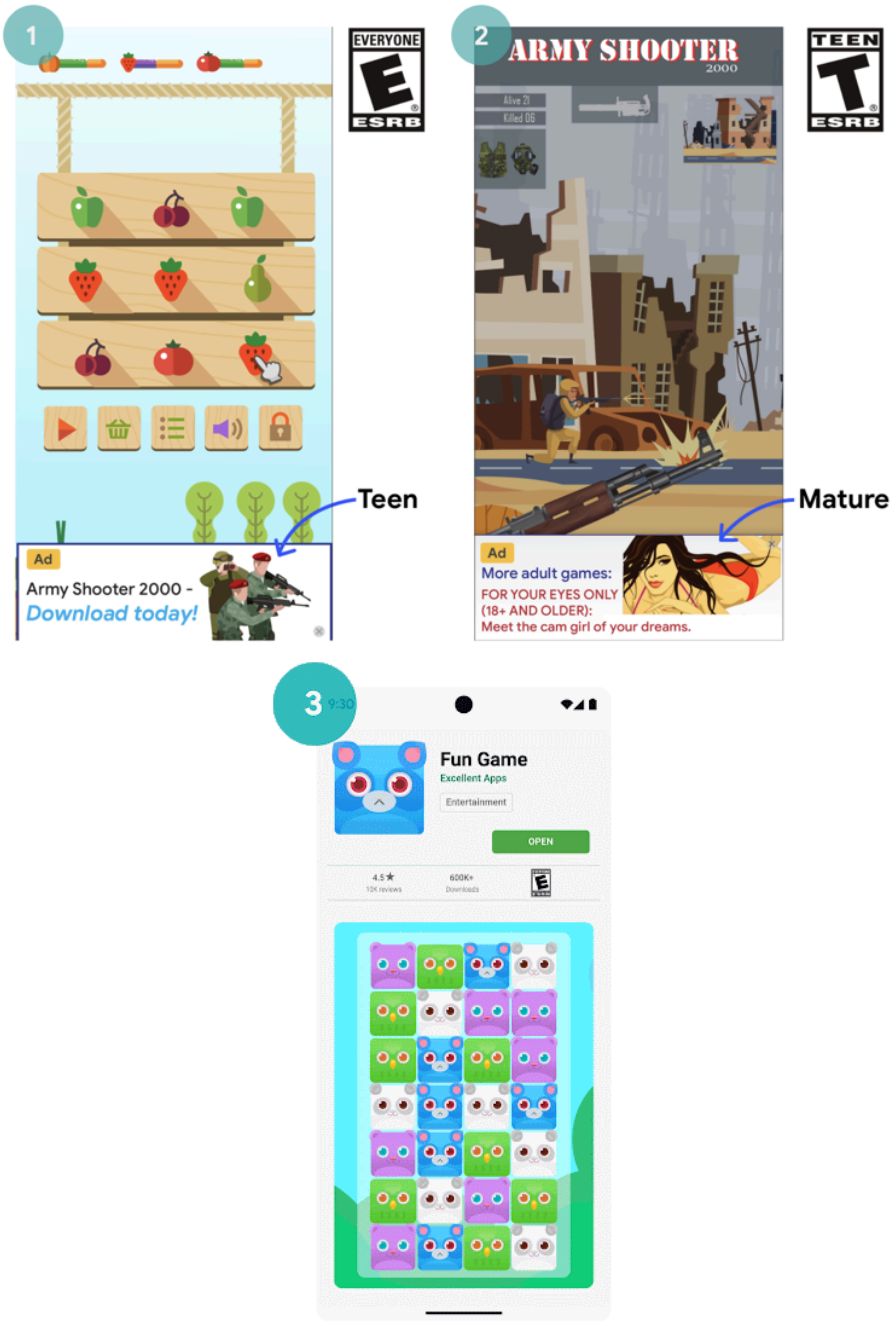
Les annonces et les offres associées font partie de l'application et doivent respecter nos règles concernant le contenu soumis à restriction. D'autres exigences s'appliquent lorsque l'application relève des jeux d'argent et de hasard.

Annonces inappropriées

Les annonces et les offres associées (par exemple, si l'annonce promeut le téléchargement d'une autre application) diffusées dans votre application doivent respecter la classification du contenu de votre application, même si le contenu respecte nos autres règles.

Voici quelques exemples courants de non-respect des règles :

- Annonces inappropriées au vu de la classification du contenu de l'application :



① Cette annonce réservée aux adolescents n'est pas conforme à la classification du contenu de l'application ("Tout public").
② Cette annonce réservée aux adultes n'est pas conforme à la classification du contenu de l'application ("Adolescents").
③ L'offre de l'annonce (promotion du téléchargement d'une application réservée aux adultes) n'est pas conforme à la classification du contenu de l'application de jeu dans laquelle l'annonce a été diffusée ("Tout public").

Exigences concernant les annonces pour les familles

Si vous monétisez une application qui cible les enfants sur Google Play, il est important qu'elle respecte les exigences du Règlement sur les annonces et la monétisation pour les contenus familiaux.

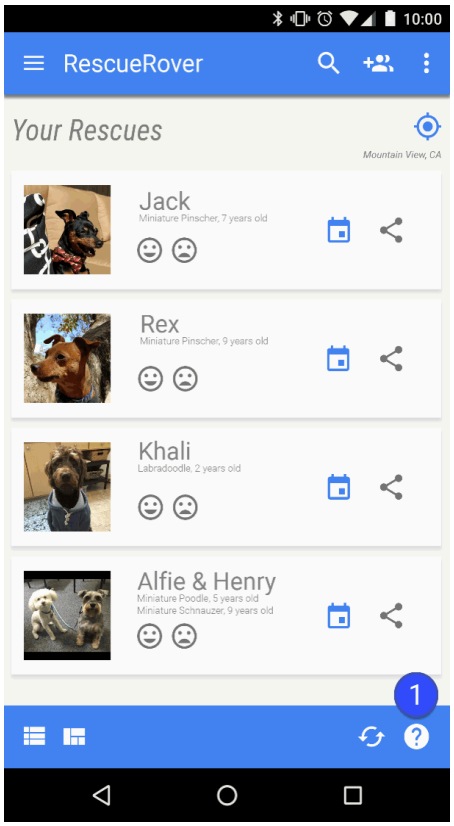
Annonces mensongères

Les annonces ne doivent pas simuler ou imiter l'interface correspondant à une fonctionnalité d'application (comme des notifications ou avertissements émis par le système d'exploitation, par

exemple). L'utilisateur doit pouvoir identifier clairement l'application associée à chacune des annonces.

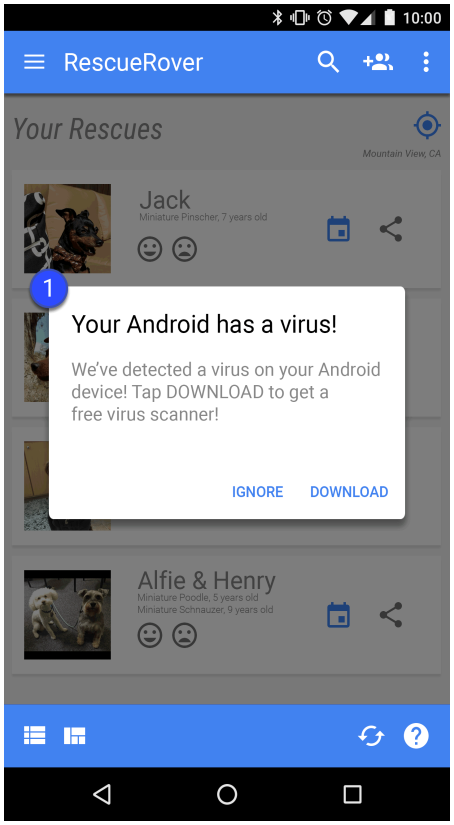
Voici quelques exemples courants de non-respect des règles :

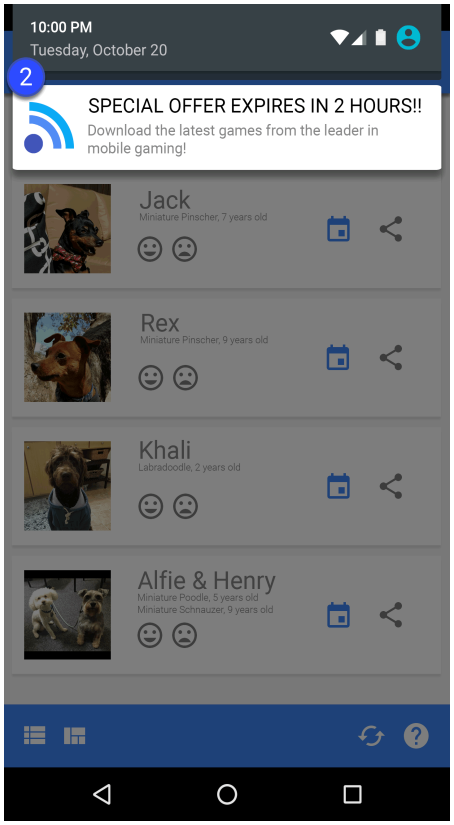
- Annonces imitant l'interface utilisateur d'une application :



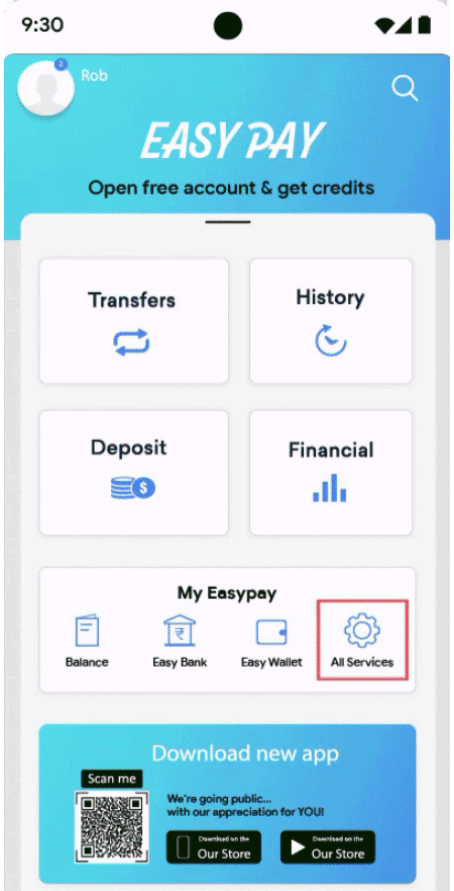
① Dans cette application, l'icône représentant un point d'interrogation est une annonce qui sert à rediriger l'utilisateur vers une page de destination externe.

- Annonces imitant une notification système :





① ② Les exemples ci-dessus illustrent des imitations de diverses notifications système.



① L'exemple ci-dessus représente une section qui imite des fonctionnalités, mais ne fait que diriger l'utilisateur vers une ou plusieurs annonces.

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.

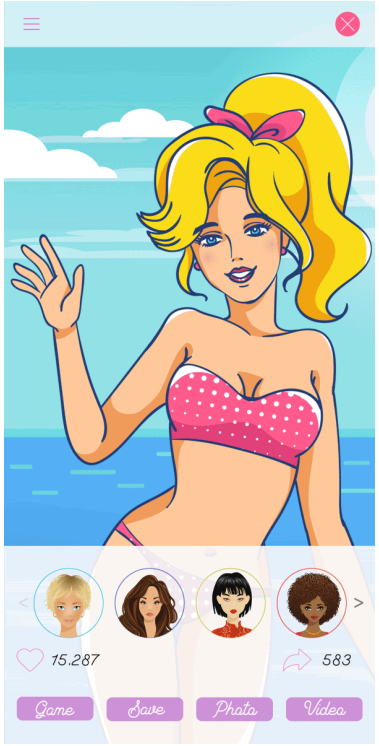
Votre application ne doit pas forcer un utilisateur à cliquer sur des annonces ni à communiquer des informations personnelles à des fins publicitaires avant qu'il puisse accéder à toutes ses fonctionnalités. Les annonces ne peuvent être affichées que dans l'application dans laquelle elles sont diffusées. Elles 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. Cela inclut les superpositions, les fonctionnalités complémentaires et les blocs d'annonces comprenant des widgets. L'utilisateur doit avoir la possibilité d'ignorer les annonces qui perturbent le fonctionnement normal de votre application sans être pénalisé.

Voici quelques exemples courants de non-respect des règles :

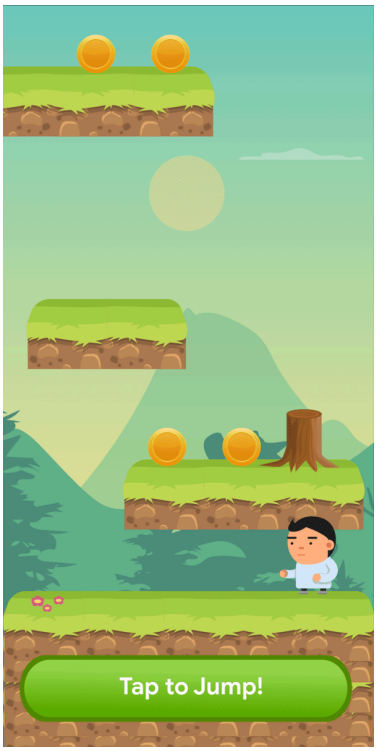
- Annonces qui occupent tout l'écran ou qui perturbent l'utilisation normale de l'application, et qui n'indiquent pas clairement comment les ignorer :

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 :

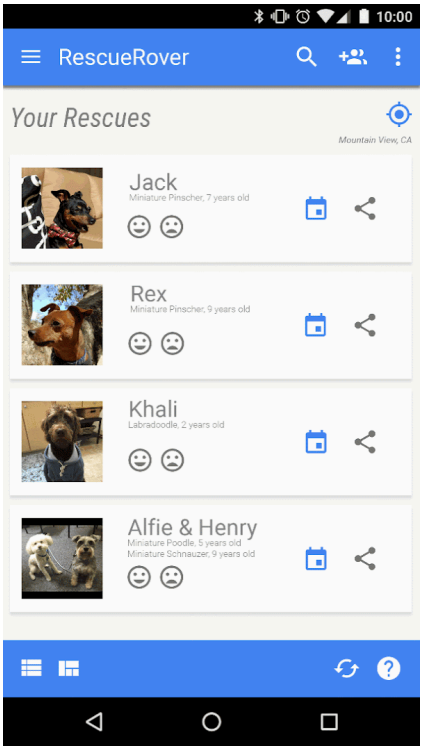


① Cette annonce utilise un faux bouton "Ignorer".



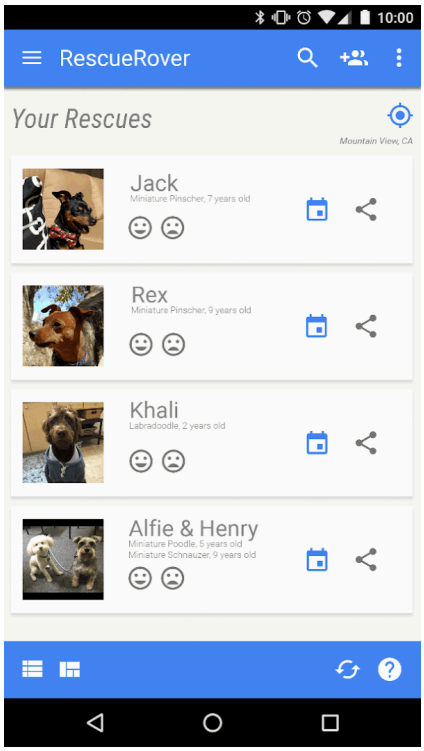
② Cette annonce apparaît soudainement dans une zone où l'utilisateur a l'habitude d'appuyer pour utiliser les fonctions intégrées à l'application.

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



① L'utilisateur accède à l'écran d'accueil à partir de cette application, et soudainement, une annonce s'affiche.

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



① 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.

Meilleures expériences publicitaires

Les développeurs doivent respecter les consignes suivantes concernant les annonces, afin d'offrir des expériences de haute qualité aux utilisateurs d'applications Google Play. Il est possible que vos annonces ne soient pas diffusées dans les situations suivantes, où elles sont inattendues :

- Les annonces interstitielles en plein écran qui s'affichent de manière inattendue, généralement lorsque l'utilisateur choisit de faire autre chose, ne sont pas autorisées, quel que soit le format (vidéo, GIF, statique, etc.).
  - Les annonces diffusées pendant que l'utilisateur joue, au début d'un niveau ou lors du lancement d'un segment de contenu, ne sont pas autorisées.
  - Les annonces vidéo interstitielles en plein écran diffusées avant l'apparition de l'écran de chargement (écran de démarrage) ne sont pas autorisées.
- Les annonces interstitielles en plein écran qui ne peuvent pas être fermées après un délai de 15 secondes ne sont pas autorisées, quel que soit le format. Les annonces interstitielles en plein écran qui sont activées ou acceptées par l'utilisateur, ou qui ne l'interrompent pas (par exemple, après l'écran des résultats en fin de partie dans une application de jeu), peuvent persister plus de 15 secondes.

Cette règle ne s'applique pas aux annonces avec récompense auxquelles les utilisateurs consentent explicitement (par exemple, lorsque le développeur propose explicitement à l'utilisateur de regarder une annonce en échange du déblocage d'une fonctionnalité spécifique du jeu ou d'un élément de contenu). La publicité et la monétisation qui n'interfèrent pas avec l'utilisation normale de l'application ou du jeu (par exemple, du contenu vidéo avec des annonces intégrées ou des bannières qui n'occupent qu'une partie de l'écran) sont également exemptées de cette règle.

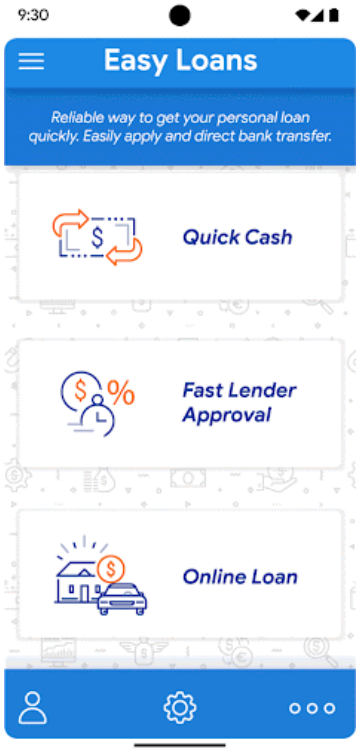
Ces consignes s'inspirent des normes Meilleures expériences publicitaires . Pour en savoir plus sur ces normes, consultez le site Coalition for Better Ads .

Voici quelques exemples courants de non-respect des règles :

- Annonces inattendues diffusées pendant une phase de jeu ou au lancement d'un segment de contenu (par exemple, après que l'utilisateur a appuyé sur un bouton, mais avant que la fonction du

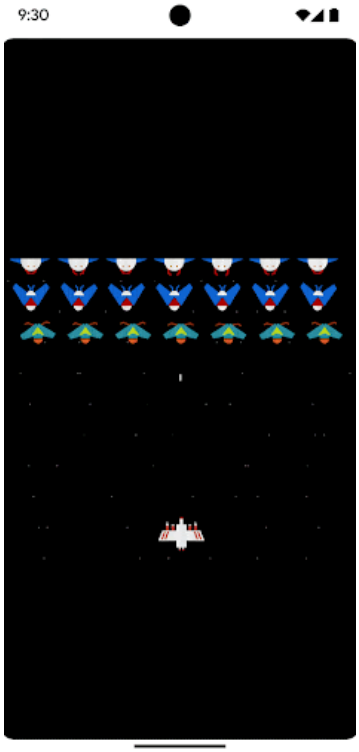
bouton ne soit exécutée). Ces annonces sont inattendues, les utilisateurs cherchant à commencer à jouer ou à interagir avec le contenu.

① Annonce statique inattendue diffusée pendant une phase de jeu, au début d'un niveau



② Annonce vidéo inattendue diffusée au lancement d'un segment de contenu

- Une annonce en plein écran diffusée pendant une phase de jeu et ne pouvant être fermée après un délai de 15 secondes.



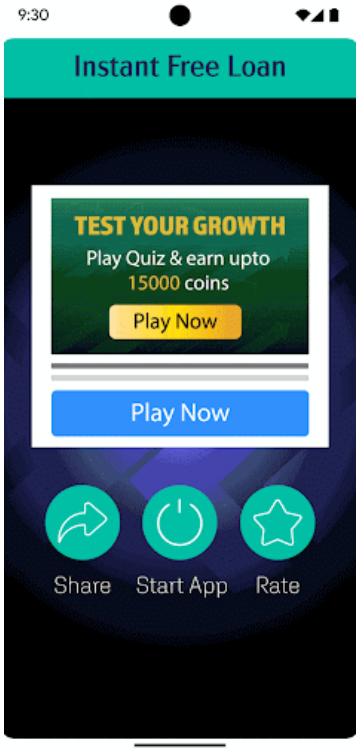
① Annonce interstitielle diffusée pendant une phase de jeu et n'offrant pas la possibilité de l'ignorer dans les 15 premières secondes

Applications créées à des fins publicitaires

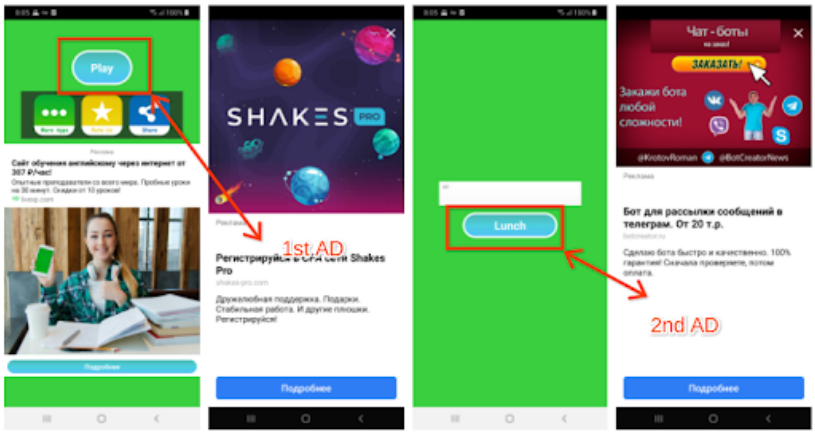
Nous n'autorisons pas les applications qui diffusent des annonces interstitielles de façon répétée, gênant les interactions de l'utilisateur avec l'application ou l'exécution de tâches dans l'application.

Voici quelques exemples courants de non-respect des règles :

- Applications où une annonce interstitielle est diffusée consécutivement à une action de l'utilisateur (y compris, mais sans s'y limiter, les clics et les balayages)



① La première page dans l'application comporte plusieurs boutons d'interaction. Une annonce interstitielle apparaît lorsque l'utilisateur clique sur **Démarrer l'application** afin de l'utiliser. Après avoir fermé cette annonce, l'utilisateur retourne à l'application et clique sur **Service** pour utiliser le service, mais une autre annonce interstitielle apparaît.



② Sur la première page, l'utilisateur est incité à cliquer sur **Jouer**, ce bouton étant le seul proposé pour interagir avec l'application. Lorsque l'utilisateur clique dessus, une annonce interstitielle apparaît. Après avoir fermé cette annonce, l'utilisateur clique sur **Lancer**, ce bouton étant la seule option d'interaction proposée, et une autre annonce interstitielle apparaît.

Monétisation de l'écran de verrouillage

À moins que l'objectif exclusif de l'application soit de fournir un écran de verrouillage, les applications ne peuvent pas introduire d'annonces ni de fonctionnalités qui monétisent l'écran verrouillé d'un appareil.

Fraude publicitaire

La fraude publicitaire est strictement interdite. Pour plus d'informations, consultez notre Règlement sur la fraude publicitaire.

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 pouvez uniquement demander une autorisation 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.

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 solutions d'analyse. Les conditions d'utilisation de cet identifiant figurent ci-dessous.

- **Utilisation**. L'identifiant publicitaire Android (AAID) ne doit être utilisé qu'à des fins publicitaires et d'analyse concernant 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. Il ne peut être associé à des informations personnelles qu'avec l'autorisation explicite de l'utilisateur.
  - Utilisation à des fins d'analyse : l'identifiant publicitaire ne doit pas être associé à des informations permettant d'identifier personnellement l'utilisateur ni à un identifiant permanent de l'appareil (par exemple, SSAID, adresse MAC, code IMEI, etc.) à des fins d'analyse. Veuillez lire les Règles sur les données utilisateur pour en savoir plus concernant les consignes supplémentaires liées aux identifiants permanents de l'appareil.
- **Respect des choix de l'utilisateur**.
  - En cas de réinitialisation de l'identifiant publicitaire, il ne doit pas être associé à l'identifiant précédent ni à des données qui en sont dérivées sans l'autorisation explicite de l'utilisateur.
  - 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 publicitaires ni pour cibler des utilisateurs avec des annonces personnalisées. En revanche, la publicité contextuelle, la limitation de la fréquence d'exposition, le suivi des conversions, la création de rapports, la sécurité et la détection des fraudes font partie des activités autorisées.
  - Sur les appareils plus récents, lorsqu'un utilisateur supprime l'identifiant publicitaire Android, celui-ci est effacé. Toute personne qui tentera d'accéder à l'identifiant recevra une chaîne de zéros. Un appareil sans identifiant publicitaire ne doit pas être associé à des données liées à un identifiant précédent ou dérivées d'un tel identifiant.
- **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 les Règles sur les données utilisateur .
- **Respect des conditions d'utilisation**. L'identifiant publicitaire ne doit être utilisé que conformément au Règlement du programme Google Play pour les développeurs, y compris par les tiers auxquels vous êtes susceptible de le communiquer 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.

Pour plus d'informations, consultez notre Règlement sur les données utilisateur.

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 de démarrage. Nous n'autorisons pas les applications qui exposent les utilisateurs à des pratiques commerciales trompeuses ou manipulatrices (y compris pour les achats ou abonnements via les applications).

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.

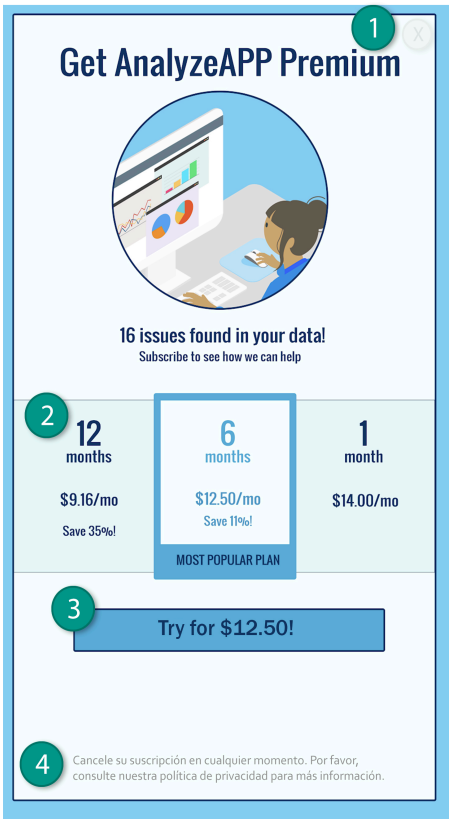
Les abonnements doivent fournir une valeur continue ou récurrente aux utilisateurs tout au long de la période de souscription. Ils ne peuvent pas avoir pour fonction de proposer des avantages ponctuels (des codes SKU qui fournissent des devises/crédits versés en une fois via l'appli ou des boosters de jeux à usage unique, par exemple). Votre abonnement peut proposer des incitations ou bonus promotionnels, mais ceux-ci doivent s'appliquer en complément de la valeur continue ou récurrente fournie tout au long de la période d'abonnement. Les produits qui ne proposent pas de valeur continue ou récurrente doivent utiliser l'appellation de produit intégré et non de produit sur abonnement.

Il est interdit de déguiser ou de présenter aux utilisateurs un avantage à usage unique en tant qu'abonnement. Cela inclut toute modification d'abonnement en offre ponctuelle (le fait d'annuler, d'arrêter ou de diminuer la valeur récurrente, par exemple) après que l'utilisateur a acheté l'abonnement.

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 plus de visibilité au coût mensuel.
- Tarifs d'abonnement et conditions n'ayant pas été intégralement traduits.
- 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", "Essayer l'abonnement Premium : 3 jours gratuits", pour un abonnement payant renouvelé automatiquement.
- Succession d'écrans dans le parcours d'achat amenant les utilisateurs à cliquer accidentellement sur le bouton d'abonnement.
- Abonnements qui ne fournissent pas de valeur continue ou récurrente, par exemple : 1 000 gemmes offertes le premier mois, puis réduction de l'avantage à 1 gemme les mois suivants de l'abonnement.
- Obligation pour l'utilisateur de s'inscrire à un abonnement renouvelé automatiquement pour obtenir un avantage ponctuel, puis annulation de l'abonnement après achat, sans que l'utilisateur en ait fait la demande.

Exemple 1 :



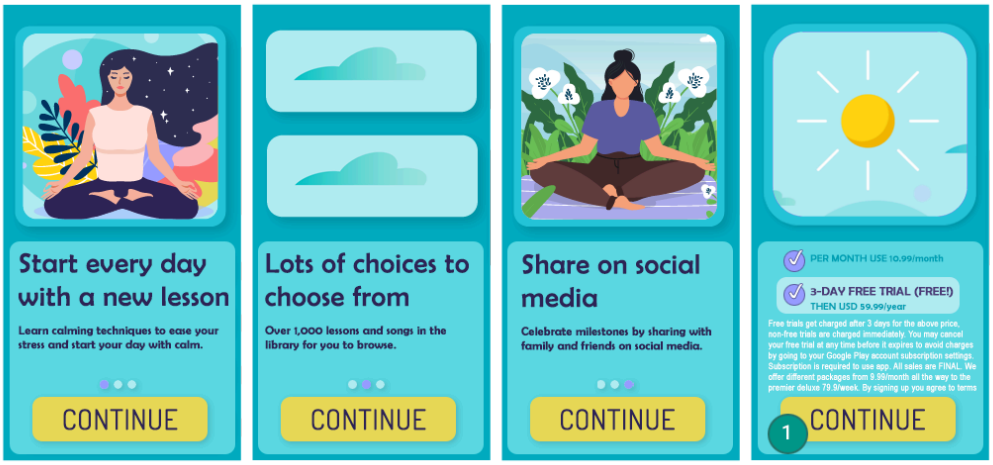
① Le bouton "Ignorer" n'est pas clairement visible. Par conséquent, il est possible que les utilisateurs ne comprennent pas qu'ils peuvent accéder aux fonctionnalités sans accepter l'offre d'abonnement.

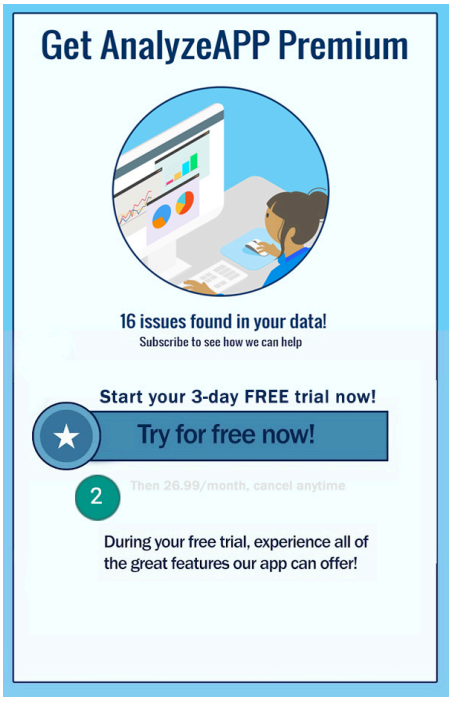
② L'offre indique le tarif uniquement sous forme de coût mensuel. Ainsi, il est possible que les utilisateurs ne comprennent pas que six mois leur seront facturés lors de la souscription de l'abonnement.

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 traduite dans la même langue que les conditions d'utilisation afin que les utilisateurs puissent la comprendre dans son intégralité.

Exemple 2 :





① Les clics répétés dans la même zone de boutons incitent l'utilisateur à cliquer par inadvertance sur le bouton final "Continuer" pour s'abonner.

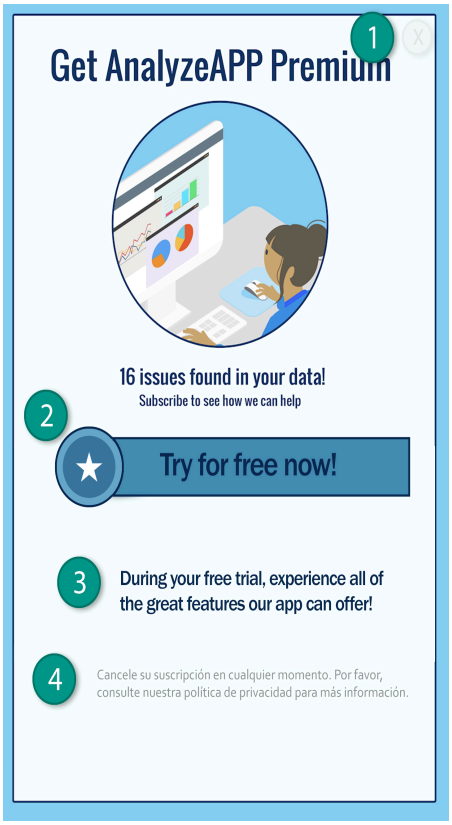
② Le montant qui sera facturé aux utilisateurs à la fin de la période d'essai est difficile à lire, ce qui peut leur laisser croire que cet abonnement est gratuit.

Essais gratuits et offres de bienvenue

Avant qu'un utilisateur souscrive un 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 et 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 que l'abonnement leur sera automatiquement facturé 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, résiliation et remboursement des abonnements

Si vous vendez des abonnements par l'intermédiaire d'une ou de plusieurs applications, vous devez vous assurer que les applications concernées indiquent clairement comment l'utilisateur peut gérer ou résilier son abonnement. Vous application doit également donner accès à une option en ligne simple d'utilisation permettant de résilier l'abonnement. Vous pouvez répondre à ces exigences en incluant, dans les paramètres de compte de votre application (ou sur une page équivalente), un ou plusieurs des éléments suivants :

- Un lien vers le centre des abonnements Google Play (si votre application utilise le système de facturation de Google Play)
- Un accès direct à votre processus de résiliation

Conformément à nos règles générales, lorsqu'un utilisateur résilie un abonnement acheté par l'intermédiaire du système de facturation de Google Play, il n'est pas remboursé pour la période de facturation en cours. Il continue cependant de recevoir le contenu de l'abonnement pour le reste de la période de facturation, indépendamment de la date de résiliation. La résiliation de l'abonnement devient effective lorsque la période de facturation en cours est terminée.

En tant que fournisseur de contenu ou d'accès, vous pouvez proposer directement aux utilisateurs des modalités de remboursement plus flexibles. Il vous incombe d'informer vos utilisateurs de toute

modification des conditions d'abonnement, de résiliation et de remboursement. Vous devez également vous assurer que ces conditions respectent les lois applicables.

Programme concernant les SDK publicitaires autocertifiés pour les contenus familiaux

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 ne devez utiliser que des versions de SDK publicitaires ayant été autocertifiées conformes aux règles de Google Play, y compris aux exigences concernant les SDK publicitaires autocertifiés pour les familles ci-dessous.

Si votre application cible à la fois les enfants et les utilisateurs plus âgés, vous devez vous assurer que les annonces présentées aux enfants proviennent exclusivement de versions de SDK publicitaires autocertifiées (par exemple, par l'intermédiaire de procédés neutres de vérification de l'âge).

Sachez qu'il est de votre responsabilité de vous assurer que toutes les versions des SDK que vous implémentez dans votre application, y compris les versions de SDK publicitaires autocertifiées, sont bien conformes aux règles, lois locales et règlements en vigueur. Google ne fait aucune déclaration ni n'offre aucune garantie quant à l'exactitude des informations fournies par les SDK publicitaires au cours du processus d'autocertification.

L'utilisation de SDK publicitaires autocertifiés pour les familles 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 d'annonces et de collecte de données sont conformes au Règlement sur les données utilisateur et aux Règles pour les contenus familiaux de Google 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 en vertu desquels vous utilisez des SDK pour gérer l'inventaire

Exigences concernant les SDK publicitaires autocertifiés pour les familles

- 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 Google 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 propose aux fournisseurs de SDK une fois qu'ils ont rempli le formulaire de participation 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'annonces. 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, comme une application de test et les renseignements demandés dans le formulaire de participation ci-dessous. Ceci permet à Google de vérifier que le SDK publicitaire est conforme à toutes les exigences d'autocertification. Veuillez également répondre dans les meilleurs délais à toute demande d'informations ultérieure. Ces demandes peuvent inclure l'envoi de nouvelles versions pour vérifier la conformité de cette version du SDK publicitaire avec toutes les exigences d'autocertification et l'envoi d'une application de test.
- Autocertifiez que toutes les nouvelles versions respectent la dernière version du Règlement du programme Google Play pour les développeurs, y compris les règles pour les contenus familiaux.

Remarque : Les SDK publicitaires autocertifiés pour les familles doivent prendre en charge une diffusion d'annonces conforme à toutes les lois et réglementations concernant les enfants qui peuvent s'appliquer aux éditeurs.

Vous trouverez ici plus d'informations sur l'application de filigranes aux créations et l'envoi d'une application de test.

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 autocertifiés pour les familles 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 pour les familles et vérifier quelles versions précises de ces SDK publicitaires sont autocertifiées pour une utilisation dans les applications pour les familles.

Ils peuvent par ailleurs partager ce formulaire de participation 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 que votre fiche Play Store soit 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 se livrent directement ou indirectement à des pratiques promotionnelles (telles que des annonces) mensongères ou nuisibles aux utilisateurs ou à l'écosystème du développeur, ou qui en tirent profit. Les pratiques promotionnelles sont mensongères ou nuisibles si leur comportement ou contenu ne respectent pas le Règlement du programme pour les développeurs.

Voici quelques exemples courants de non-respect des règles :

- Utilisation d'annonces mensongères sur des sites Web, des applications ou d'autres propriétés, y compris les notifications qui ressemblent aux notifications et alertes système
- Utilisation d'annonces à caractère sexuel explicite pour rediriger les utilisateurs vers votre fiche Google Play afin d'y télécharger l'application
- Promotion ou stratégies d'installation qui entraînent une redirection de l'utilisateur sur Google Play ou le téléchargement d'applications sans qu'il en soit informé préalablement
- Envoi par SMS de messages promotionnels non sollicités

- Texte ou images dans le titre, l'icône ou le nom du développeur de l'application qui comportent des informations sur les performances ou le classement de l'application sur le Play Store, des informations promotionnelles, ou qui sous-entendent un lien avec des programmes Google Play existants

Il est de votre responsabilité de veiller à ce que les réseaux publicitaires, affiliés ou annonces associés à votre application respectent ces règles.

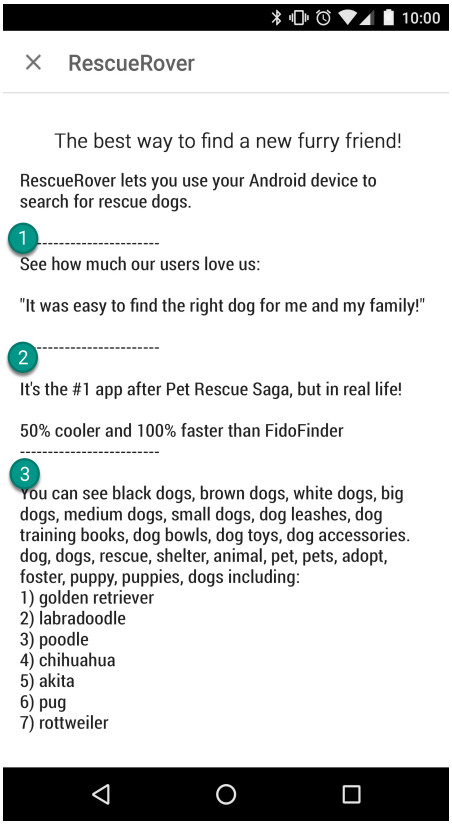
Métadonnées

Les utilisateurs s'appuient sur les descriptions de votre application pour comprendre sa fonctionnalité et son objectif. 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 de leur application. Nous n'acceptons pas non plus les témoignages d'utilisateurs non attribués ou anonymes dans la description des applications.

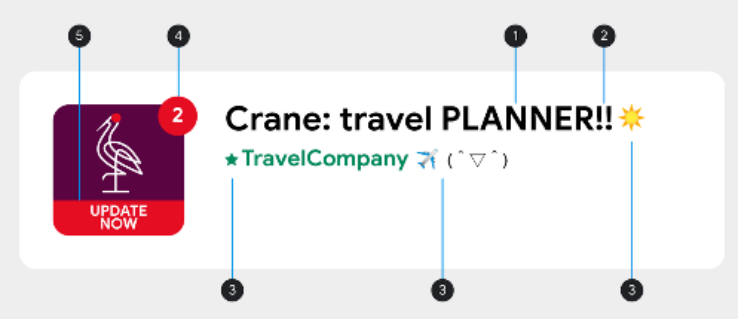
Le titre et l'icône de l'application ainsi que le nom du développeur sont particulièrement utiles aux internautes pour trouver et découvrir votre application. N'utilisez pas d'emoji, d'émoticônes ni de caractères spéciaux répétés dans ces métadonnées. Évitez les MOTS TOUT EN MAJUSCULES, sauf si cela fait partie de votre nom de marque. Les symboles trompeurs dans les icônes d'applications ne sont pas autorisés (par exemple, un point indiquant un nouveau message alors qu'il n'y a pas de nouveaux messages, ou un symbole de téléchargement ou d'installation si l'application ne permet pas d'effectuer ce genre d'opérations). Le titre de l'application ne doit pas comporter plus de 30 caractères. N'utilisez pas de texte ou d'images dans le titre, l'icône ou le nom du développeur de l'application qui comportent des informations relatives aux performances ou au classement de l'application sur le Play Store, des informations publicitaires, ou qui sous-entendent un lien avec des programmes Google Play existants.

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

Voici quelques exemples courants de non-respect des règles :

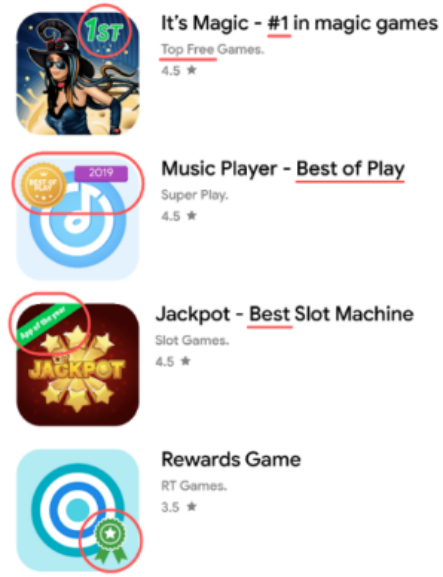


① Témoignages d'utilisateurs non attribués ou anonymes
② Comparaison de données d'applications ou de marques
③ Blocs de mots et listes de mots verticales ou horizontales

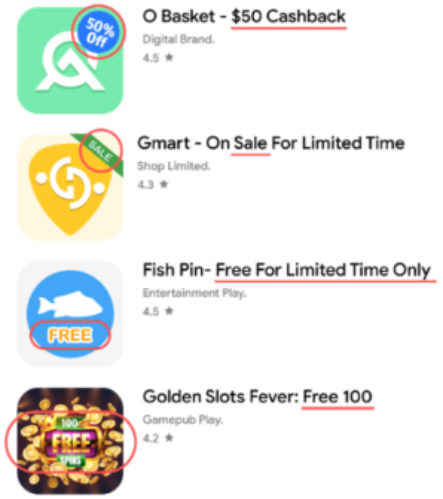


① MOTS TOUT EN MAJUSCULES ne faisant pas partie du nom de la marque
② Séquences de caractères spéciaux qui ne sont pas pertinents pour l'application
③ Emoji, émoticônes (y compris typographiques) et caractères spéciaux
④ Symbole trompeur
⑤ Texte trompeur

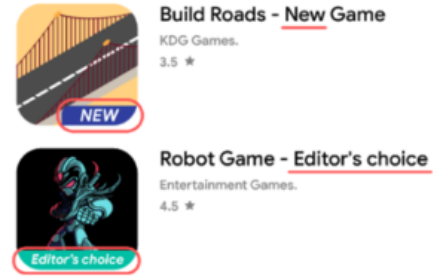
- Images ou texte qui indiquent le classement ou les performances de l'application sur le Play Store, comme "Meilleure appli de l'année", "Numéro 1", "Meilleur de Play 20XX", "Populaire", des icônes de récompenses, etc.



- Images ou texte qui indiquent un prix ou des informations promotionnelles, comme "10 % de remise", "Recevez 50 €", "Gratuit pendant une durée limitée", etc.



- Images ou texte qui font référence à des programmes Google Play, comme "Choix de l'équipe", "Nouveautés", etc.



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.
- Langage grossier, vulgaire ou tout autre langage qui n'est pas approprié pour tous publics 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 :

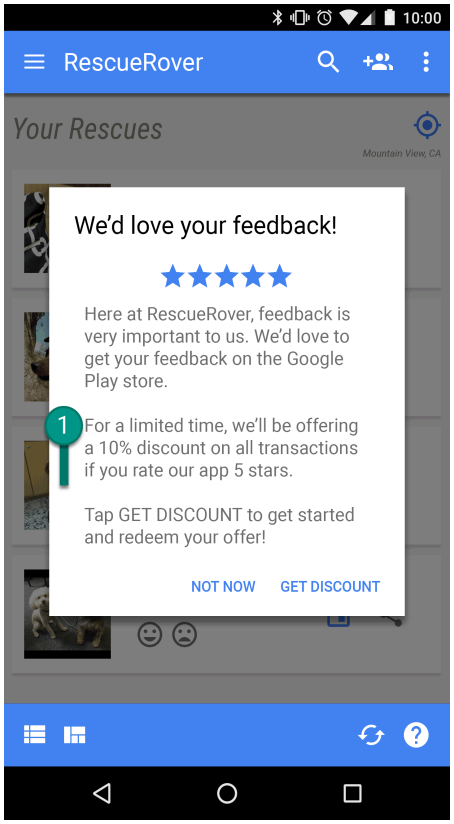
- Soulignez les avantages de votre application : mettez en avant les points intéressants et attrayants de votre application afin de susciter l'intérêt des utilisateurs.
- Assurez-vous que le titre et la description de votre application décrivent précisément ses fonctionnalités.
- Évitez d'utiliser des 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 inadéquate peuvent entraîner le non-respect des présentes règles.
- Gardez à l'esprit que votre fiche doit être adaptée à tous 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, y compris, mais sans s'y limiter, d'augmenter artificiellement le nombre de notes, d'avis ou d'installations par des moyens non autorisés, tels que les notes et les avis obtenus manière frauduleuse ou en contrepartie d'un avantage, ou proposer des applications dont la fonctionnalité principale serait d'inciter les utilisateurs à installer d'autres applications.

Voici quelques exemples courants de non-respect des règles :

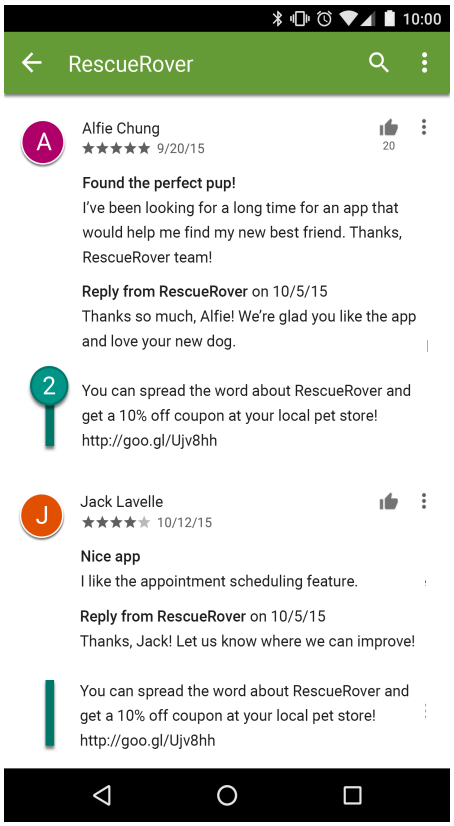
- Demander aux utilisateurs de noter votre application en leur offrant un avantage :



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

- Envoyer des notes de manière répétitive en se faisant passer pour des utilisateurs afin d'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 les coordonnées de l'équipe d'assistance ou une page de questions fréquentes.

Avis sur le 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. Toute application sans classification du contenu sera supprimée du Play Store.

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 différentes autorités de classification et sur la façon de remplir le questionnaire concernant 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

Une application d'actualités se définit comme suit :

- Elle se présente comme une application de type "Actualités" dans la Google Play Console.
- Elle se classe dans la catégorie "Actualités et magazines" du Google Play Store et est décrite comme une application d'"actualités" dans le titre, l'icône, le nom du développeur ou la description.

Exemples d'applications de la catégorie "Actualités et magazines" considérées comme étant des applications d'actualités :

- Applications qui se présentent comme des applications "d'actualités" dans leur description, y compris, mais sans s'y limiter :
  - Dernières actualités
  - Journaux
  - Alertes info
  - Actualités locales
  - Actualités quotidiennes
- Applications dont le terme "Actualités" figure dans le titre ou les icônes de l'application, ou dans le nom du développeur

Toutefois, si les applications contiennent essentiellement du contenu généré par l'utilisateur (comme c'est le cas des applications de réseaux sociaux), elles ne doivent pas se déclarer comme des applications d'actualités et ne sont pas considérées comme telles.

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 sur la propriété concernant l'application et la source des articles d'actualités, y compris, mais sans s'y limiter, l'éditeur ou l'auteur d'origine de chaque article. Dans les cas où l'auteur de chaque article n'est habituellement pas mentionné, l'application d'actualités doit être l'éditeur d'origine des articles. Veuillez noter que les liens vers des comptes de réseaux sociaux ne sont pas considérés comme des informations suffisantes pour identifier l'éditeur ou l'auteur.
- Disposer d'un site Web dédié ou d'une page interne indiquant clairement qu'il ou elle contient des moyens de contact et faciles à trouver (par exemple, grâce à un lien en bas de la page d'accueil ou dans la barre de navigation du site), et contenant des coordonnées valides pour l'éditeur d'actualités, avec soit une adresse e-mail, soit un numéro de téléphone. Veuillez noter que les liens vers les comptes de réseaux sociaux ne sont pas considérés comme des moyens de contact.

Les applications d'actualités ne doivent pas :

- contenir de fautes d'orthographe et de grammaire graves ;
- proposer uniquement du contenu statique (par exemple, du contenu datant de plus de trois mois) ; ni
- avoir pour objectif principal une affiliation ou des revenus publicitaires.

Veuillez noter que les applications d'actualités *peuvent* utiliser des annonces et d'autres formes de marketing pour monétiser leurs contenus, tant que leur objectif principal n'est pas de vendre des produits et services ni de générer des revenus publicitaires.

Les applications d'actualités qui regroupent du contenu provenant de différentes sources de publication doivent être transparentes quant à la source de publication du contenu dans l'application. Chacune de ces sources doit respecter les règles de Google Actualités.

Veuillez consulter cet article pour en savoir plus.

Spam, fonctionnalités et expérience utilisateur

Les applications doivent proposer une expérience utilisateur attrayante en offrant à l'utilisateur un niveau basique de fonctionnalités et de contenus adéquats. 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.

Voici un exemple courant de non-respect des règles :

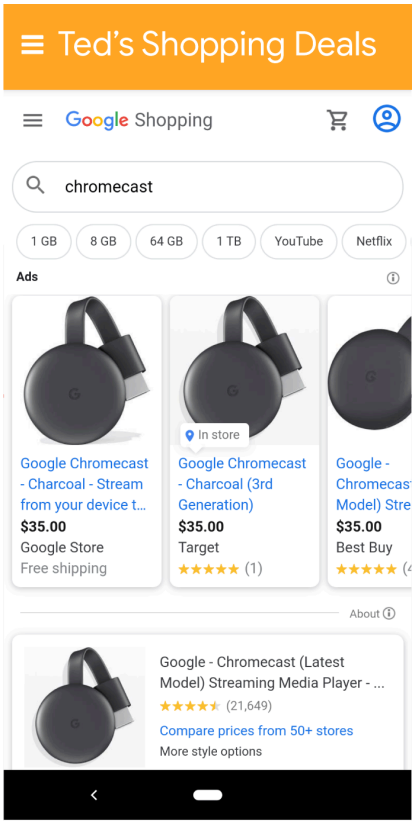
- Lorsque l'utilisateur appuie sur le bouton "Partager", l'application envoie des messages au nom de l'utilisateur, sans lui laisser la possibilité de vérifier le contenu ni les destinataires :

Spam dans les aperçus Web 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 une WebView d'un site Web sans autorisation :



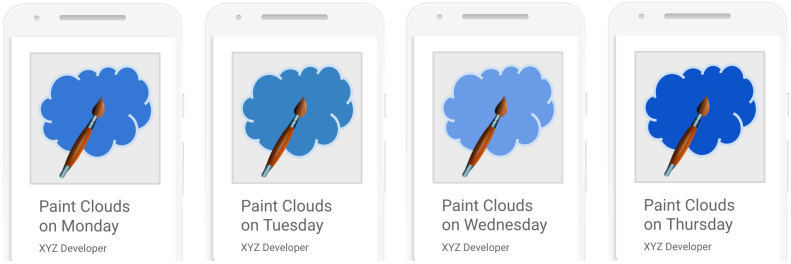
① Cette application est appelée "Ted's Shopping Deals" et fournit simplement une WebView de Google Shopping.

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.



Fonctionnalités, contenu et expérience utilisateur

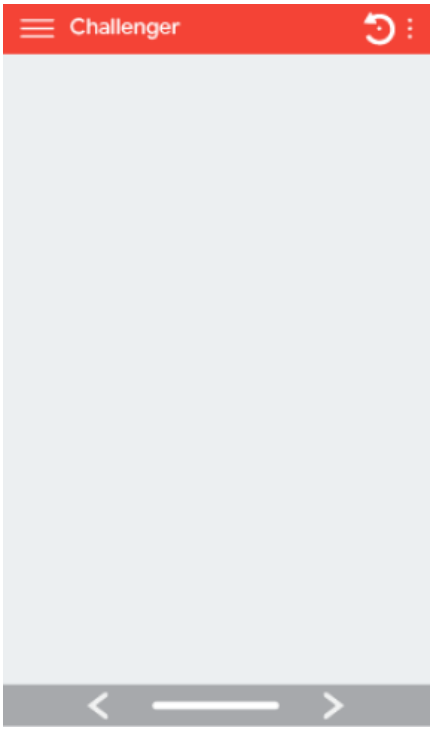
Les applications doivent proposer une expérience utilisateur stable, responsive et attrayante. Les applications qui plantent, ne proposent pas un niveau d'utilité basique adéquat comme applications mobiles, ne présentent pas de contenu attrayant ou ne sont pas fonctionnelles ni attrayantes en raison d'un autre type de comportement ne sont pas autorisées sur Google Play.

Fonctionnalités et contenu limités

Nous n'autorisons pas les applications qui ne proposent que des fonctionnalités et du contenu limités.

Voici un exemple courant de non-respect des règles :

- Applications statiques sans fonctionnalités spécifiques (applications ne contenant que du texte ou des fichiers PDF, par exemple)
- Applications avec très peu de contenu qui ne proposent pas une expérience utilisateur attrayante (applications ne proposant qu'un fond d'écran, par exemple)
- Applications conçues pour ne rien faire ou qui n'ont aucune fonction



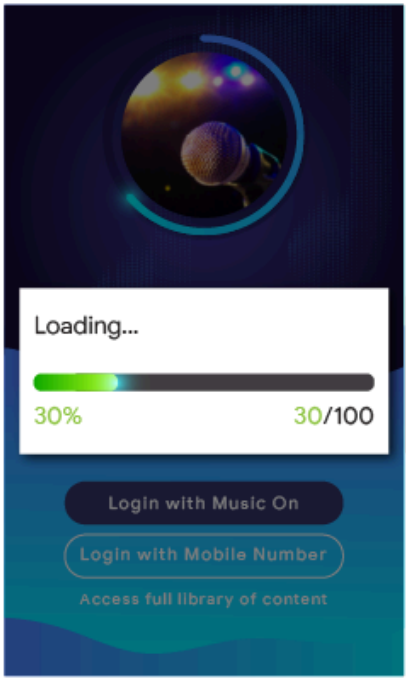
Applications non fonctionnelles

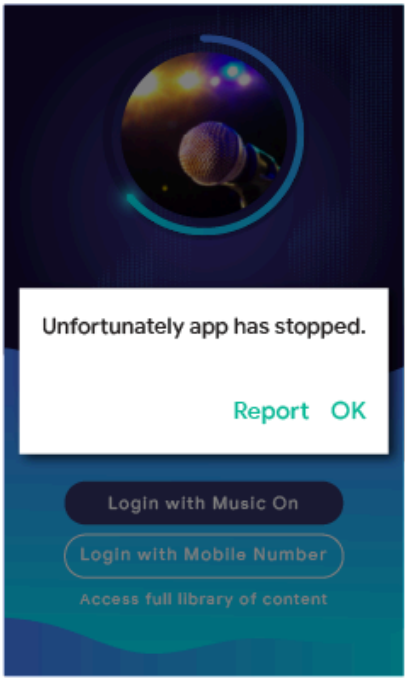
Nous n'autorisons pas les applications qui plantent, se ferment de manière forcée, se bloquent ou présentent un autre comportement anormal.

Voici quelques exemples courants de non-respect des règles :

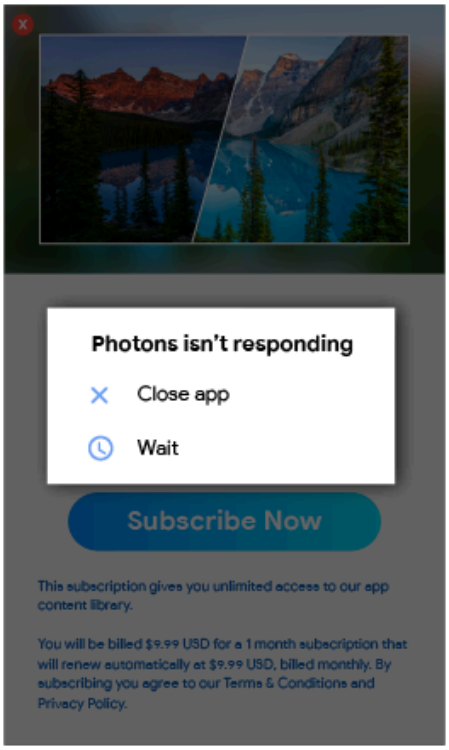
- Applications **impossibles à installer**

- 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 certaines 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 la ou les applis instantanées ou standards d'un développeur contiennent des liens vers une autre appli instantanée, le développeur doit rediriger les utilisateurs vers cette appli et non vers WebView , par exemple.

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 concernant l'expérience utilisateur dans le guide des Bonnes pratiques en termes 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. Elles ne doivent par exemple 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 de l'utilisateur. Celui-ci doit par exemple 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 contenus 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.

Règles Android sur les emoji

Nos règles sur les emoji visent à contribuer à une expérience utilisateur inclusive et cohérente. Pour cela, toutes les applications fonctionnant sous Android 12 ou version ultérieure doivent être compatibles avec la dernière version des emoji Unicode .

Les applications fonctionnant sous Android 12 ou version ultérieure qui utilisent les emoji Android par défaut sans implémentations personnalisées utilisent déjà la dernière version des emoji Unicode.

Dans le cas d'implémentations d'emoji personnalisées, y compris celles fournies par des bibliothèques tierces, les applications fonctionnant sous Android 12 ou version ultérieure doivent être parfaitement compatibles avec la version d'Unicode la plus récente dans les quatre mois qui suivent la publication d'une nouvelle version des emoji Unicode.

Pour savoir comment assurer la compatibilité avec les emoji modernes, consultez ce guide .

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.

Règles Google Play pour les contenus familiaux

L'utilisation de la technologie comme outil d'enrichissement de la vie familiale continue de croître, et les parents recherchent des contenus sûrs 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, par conséquent nous comptons sur vous pour nous aider à faire en sorte que les applications sur Google Play conviennent aux familles.

Toutes les applications qui respectent les règles de Google Play pour les contenus familiaux peuvent demander à 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.

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.

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 leur est adaptée. 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 Google Play Console pourra 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 dans les informations sur votre application dans la Play Console, 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 pourra être supprimée ou suspendue.

1. **Contenu de l'application** : le contenu de votre application accessible aux enfants doit être approprié pour cette audience. Si le contenu de l'application n'est pas approprié pour les enfants de tous les pays, mais seulement pour ceux d'une région particulière, l'application peut être disponible dans cette région (voir les limites associées aux régions), mais pas dans les autres.
2. **Fonctionnement de l'application** : l'application ne doit pas simplement fournir une WebView d'un site Web, et sa fonction principale ne doit pas être de générer du trafic affilié vers un site sans autorisation du propriétaire du site Web ou d'un administrateur.
3. **Réponses dans la Google Play Console** : vous devez répondre correctement aux questions sur votre application dans la Play Console et mettre à jour ces réponses pour refléter avec précision toute modification de votre application. Cela inclut, sans toutefois s'y limiter, l'indication de

réponses précises concernant votre application dans les sections "Cible et contenu" et "Sécurité des données", et dans le questionnaire de l'IARC sur la classification du contenu.

4. **Gestion des données** : si vous recueillez 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 et les données d'utilisation des annonces. Vous devez également vous assurer que votre application respecte les règles de gestion des données ci-dessous :
   - Les applications qui ciblent uniquement les enfants ne doivent transmettre aucun identifiant publicitaire Android (AAID), numéro de série de carte SIM, numéro de série de build, BSSID, adresse MAC, SSID, code IMEI ni IMSI.
     - Les applications ne ciblant que les enfants ne doivent pas demander d'autorisation AD_ID lorsqu'elles ciblent le niveau d'API Android 33 ou version ultérieure.
   - Les applications qui ciblent à la fois les enfants et les publics plus âgés ne doivent transmettre aucun AAID, numéro de série de carte SIM, numéro de série de build, BSSID, adresse MAC, SSID, code IMEI ni IMSI associés à un enfant ou à un utilisateur dont l'âge n'est pas connu.
   - Le numéro de téléphone de l'appareil ne doit pas être demandé par TelephonyManager de l'API Android.
   - Les applications qui ciblent uniquement les enfants ne doivent pas demander l'autorisation d'accéder à leur position, ni recueillir, utiliser ou communiquer leur position exacte.
   - 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.

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 principalement aux enfants.
     - Par exemple, un service API utilisant la technologie OAuth à des fins d'authentification et d'autorisation, et dont les conditions d'utilisation indiquent qu'il n'est pas approuvé pour être utilisé dans des services destinés aux enfants.
   - 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 recueillir de données auprès des enfants. Les applications qui ciblent à la fois les enfants et les publics plus âgés ne doivent pas obliger les utilisateurs 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. **Réalité augmentée (RA)** : 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).

7. **Applications de réseaux sociaux et fonctionnalités associées** : si vos applications permettent aux utilisateurs de partager ou d'échanger des informations, vous devez présenter ces fonctionnalités de façon précise dans le questionnaire de classification du contenu de la Play Console.

- Application de réseau social : une application de réseau social est une application dont la fonction principale consiste à permettre aux utilisateurs de partager librement des contenus ou de communiquer avec un grand nombre de personnes. Toutes les applications de réseaux sociaux incluant des enfants dans leur audience cible doivent fournir un rappel dans l'application sur la nécessité de faire preuve de prudence sur Internet et de tenir compte des risques concrets liés aux interactions en ligne avant de permettre à ces enfants d'échanger librement des contenus multimédias ou des informations. Vous devez également imposer l'intervention d'un adulte avant de permettre aux enfants d'échanger des informations personnelles.
- Fonctionnalités de réseaux sociaux : une fonctionnalité de réseau social est une fonctionnalité additionnelle permettant aux utilisateurs d'une application d'échanger librement des contenus ou de communiquer avec un grand nombre de personnes. Toute application incluant des enfants dans son audience cible et disposant de fonctionnalités de réseaux sociaux doit rappeler aux utilisateurs la nécessité de faire preuve de prudence sur Internet et de tenir compte des risques concrets liés aux interactions en ligne avant de permettre aux enfants d'échanger librement des contenus multimédias ou des informations. Vous devez également proposer un système permettant à des adultes de gérer les fonctionnalités de réseaux sociaux destinées aux enfants, y compris, mais sans s'y limiter, en leur donnant la possibilité d'activer ou de désactiver ces fonctionnalités, ou de sélectionner différents niveaux de fonctions disponibles. Enfin, vous devez également imposer l'intervention d'un adulte avant de permettre à des enfants d'échanger des informations personnelles.
- Par "intervention d'un adulte", nous entendons un mécanisme permettant de vérifier que l'utilisateur n'est pas un enfant et n'incitant pas les enfants à falsifier leur âge pour accéder à des parties de votre application conçues pour les adultes (par exemple, un code PIN d'adulte, un mot de passe, une date de naissance, une validation de l'adresse e-mail, une photo d'identité, une carte de crédit ou un numéro de sécurité sociale).
- Les applications de réseaux sociaux dont la fonction principale consiste à discuter avec des inconnus ne doivent pas cibler des enfants. Des exemples de cette fonction incluent : les applications de type Chatroulette, les applications de rencontre, les salons de discussion publics consacrés aux enfants, etc.

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 aux adultes (par exemple, contenus violents, contenus à caractère sexuel, ou jeux d'argent et de hasard)

Annonces et monétisation

Si vous monétisez une application qui cible les enfants sur Google Play, il est important que cette application respecte les règles qui suivent concernant les annonces et la monétisation pour les contenus familiaux.

Les règles ci-dessous s'appliquent à tout contenu publicitaire ou monétisé dans votre application, promotions croisées comprises (que celles-ci concernent vos applications ou des applications tierces), à toute offre d'achat via l'application ou à tout autre contenu à caractère commercial (placement de produit rémunéré, par exemple). Tout contenu publicitaire ou monétisé dans ces applications doit respecter l'ensemble des 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.

Exigences concernant les 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 :

- N'utilisez que des SDKs publicitaires Google Play autocertifiés pour les familles pour présenter des annonces à ces utilisateurs.
- Assurez-vous que les annonces visibles par ces utilisateurs ne sont pas ciblées par centres d'intérêt (annonces ciblant des internautes présentant certaines caractéristiques d'après 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 comportent du contenu approprié pour les enfants.
- Assurez-vous que les annonces visibles par ces utilisateurs respectent les exigences relatives aux formats d'annonces pour les familles.
- Respectez toutes les dispositions légales applicables et les standards dans l'industrie concernant la diffusion d'annonces auprès des enfants.

Exigences relatives aux formats d'annonces

La monétisation et la publicité dans votre application ne doivent pas présenter de contenus trompeurs ni être conçues pour provoquer des clics involontaires par des enfants.

Si les enfants constituent l'unique audience cible de votre application, les éléments ci-dessous sont interdits. Si les enfants et des utilisateurs plus âgés constituent les audiences cibles de votre application, les éléments ci-dessous sont interdits en cas de diffusion d'annonces auprès d'enfants ou d'utilisateurs dont l'âge est inconnu.

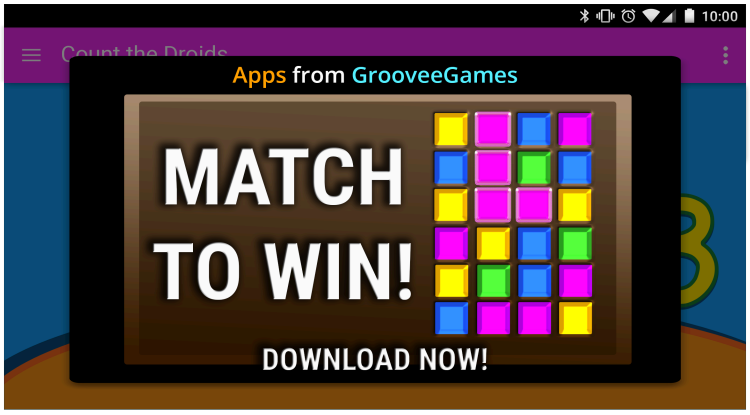
- Les publicités et contenus monétisés perturbateurs, y compris lorsque de tels contenus et publicités occupent tout l'écran ou interfèrent avec l'utilisation normale et ne proposent pas un moyen clair de les ignorer (par exemple, les annonces plein écran).
- Les contenus monétisés et publicités qui interfèrent avec l'utilisation normale de l'application ou du jeu, y compris les annonces avec récompense ou option d'activation qu'il n'est pas possible de fermer au bout de cinq secondes.
- Les contenus monétisés et publicités qui n'interfèrent pas avec l'utilisation normale de l'application ou du jeu peuvent rester affichés plus de cinq secondes (par exemple, contenu vidéo intégrant des annonces).
- Les publicités et contenus monétisés interstitiels s'affichant dès le lancement d'une 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).
- Les contenus monétisés et publicités qui ne se différencient pas clairement du contenu de l'application, par exemple les offerwalls et autres expériences publicitaires immersives.

- Le 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.
- Les annonces mensongères qui forcent l'utilisateur à cliquer en utilisant un bouton "Ignorer" pour afficher une autre annonce ou en faisant apparaître soudainement des annonces dans des zones de l'application que l'utilisateur sélectionne généralement pour une autre fonction.
- L'absence de distinction entre l'utilisation d'argent virtuel et d'argent réel pour réaliser des achats via l'application.

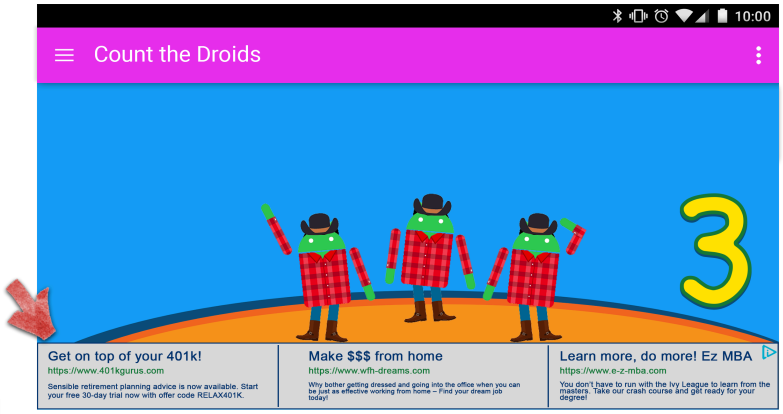
Voici quelques exemples courants de non-respect des règles :

- Contenus monétisés et publicités qui s'éloignent du doigt de l'utilisateur lorsque celui-ci essaie de les fermer.
- Contenus monétisés et publicités qui ne fournissent pas un moyen de fermer l'offre après cinq (5) secondes comme illustré dans l'exemple ci-dessous :

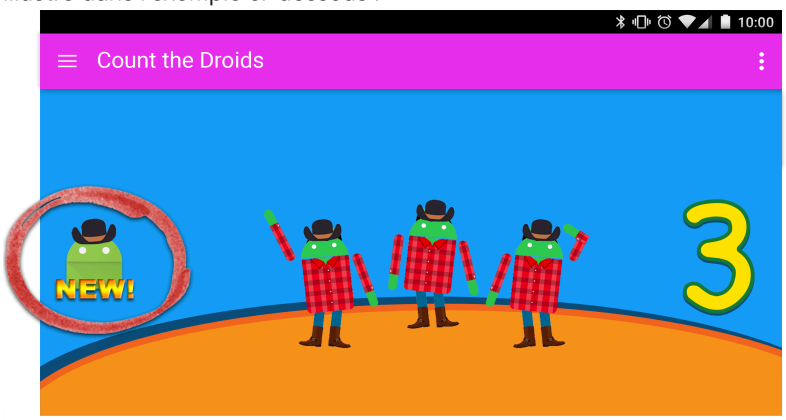
- Contenus monétisés et publicités qui occupent la majeure partie de l'écran de l'appareil ou sa totalité sans que l'utilisateur puisse les fermer simplement, comme illustré dans l'exemple ci-dessous :



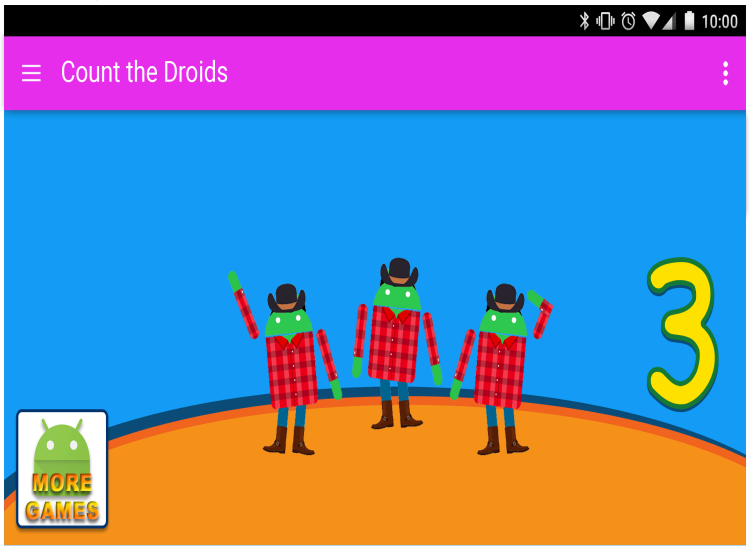
- Bannières qui affichent plusieurs offres, comme illustré dans l'exemple ci-dessous :



- Contenus monétisés et publicités pouvant être confondus avec le contenu de l'application, comme illustré dans l'exemple ci-dessous :



- Boutons, annonces ou autres contenus monétisés, 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 sans frais.
- **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.

SDKs publicitaires

Si vous diffusez des annonces dans votre application qui ne cible que les enfants, vous devez utiliser uniquement des SDKs publicitaires autocertifiés pour les familles . 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 . Vous devez également vous assurer que les annonces présentées aux enfants proviennent exclusivement de SDKs publicitaires Google Play autocertifiés.

Pour en savoir plus sur ces exigences, consultez la page du Programme SDKs publicitaires autocertifiés pour les familles . Pour consulter la liste actuelle des versions des SDKs publicitaires autocertifiés pour les familles, accédez à cette page .

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

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 le ou les fournisseurs de vos SDKs publicitaires pour en savoir plus sur leur règlement relatif au contenu et sur leurs pratiques publicitaires.

Règlement du programme SDKs publicitaires autocertifiés pour les familles

Google Play s'engage à proposer une expérience sécurisée pour les enfants et les familles. Dans cette optique, il est essentiel que les enfants ne voient que des annonces adaptées à leur âge et que leurs données soient traitées correctement. Pour y parvenir, nous exigeons que les SDKs publicitaires et les plates-formes de médiation autocertifient qu'ils sont adaptés aux enfants et conformes au Règlement du programme Google Play pour les développeurs et aux Règles pour les contenus familiaux , y compris aux exigences du Programme SDKs publicitaires autocertifiés pour les familles .

Le Programme SDKs publicitaires autocertifiés pour les familles de Google Play constitue un excellent moyen pour les développeurs d'identifier les SDKs publicitaires ou les plates-formes de médiation qui ont autocertifié leur adéquation avec les applications conçues spécialement pour les enfants.

Toute déclaration trompeuse ou déceptive concernant votre SDK, y compris dans votre formulaire de participation , peut entraîner la suppression ou la suspension de votre SDK du Programme SDKs publicitaires autocertifiés pour les familles. C'est pourquoi il est important de fournir des informations correctes.

Exigences du règlement

Si votre SDK ou votre plate-forme de médiation s'adresse à des applications qui font partie du programme Pour la famille de Google Play, vous devez respecter le règlement pour les développeurs de Google Play, y compris les exigences qui suivent. Le non-respect de toute exigence figurant dans ce règlement peut entraîner la suppression ou la suspension du Programme relatif aux SDK publicitaires autocertifiés pour les familles.

La conformité de votre SDK ou plate-forme de médiation relève de votre responsabilité. Par conséquent, nous vous invitons à consulter le Règlement du programme Google Play pour les développeurs, les Règles pour les contenus familiaux de Google Play, ainsi que les Exigences du Programme relatif aux SDK publicitaires autocertifiés pour les familles.

1. **Contenus d'annonces** : tout contenu d'annonce accessible aux enfants doit être approprié pour ceux-ci.
   - Vous devez (i) définir les contenus d'annonces et les comportements inappropriés, et (ii) les interdire dans vos conditions d'utilisation ou votre règlement. Les définitions doivent respecter le Règlement du programme Google Play pour les développeurs.
   - Vous devez également créer 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 concorder avec la méthode que Google offre aux fournisseurs de SDK une fois qu'ils ont rempli le formulaire de participation .
   - Lorsque les enchères en temps réel sont utilisées pour diffuser des annonces auprès d'enfants, vous devez vous assurer que les créations ont été examinées et sont conformes avec les exigences ci-dessus.
   - En outre, vous devez disposer d'un mécanisme permettant l'identification visuelle des créations provenant de votre inventaire (par exemple, en y ajoutant, en filigrane, le logo de votre entreprise ou en utilisant une autre fonctionnalité permettant d'obtenir un résultat similaire).
2. **Format des annonces** : vous devez vous assurer que toutes les annonces affichées pour les enfants respectent les exigences relatives au format des annonces destinées aux familles, et vous devez permettre aux développeurs de sélectionner des formats d'annonces conformes aux Règles pour les contenus familiaux de Google Play.
   - Les publicités ne doivent pas présenter de contenus trompeurs ni être conçues pour provoquer des clics involontaires par des enfants. Les annonces mensongères qui forcent l'utilisateur à cliquer en utilisant un bouton "Ignorer" pour afficher une autre annonce ou en faisant apparaître soudainement des annonces dans des zones de l'application que l'utilisateur sélectionne généralement pour une autre fonction ne sont pas autorisées.
   - Nous n'autorisons pas les publicités perturbatrices, y compris les annonces plein écran et celles qui interfèrent avec l'utilisation normale de l'application ou du jeu sans fournir un moyen clair de les ignorer.
   - Les publicités qui interfèrent avec l'utilisation normale de l'application ou le jeu, y compris les annonces avec récompense ou option d'activation, doivent pouvoir être fermées après 5 secondes.
   - L'utilisation de plusieurs emplacements d'annonce sur une page n'est pas autorisée. 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.
   - Il doit être possible de distinguer clairement les annonces du contenu de l'application. Les offerwalls et les expériences publicitaires immersives que les enfants ne peuvent pas identifier clairement comme étant des annonces ne sont pas autorisées.
   - Les publicités ne doivent pas recourir à la manipulation émotionnelle ni à des tactiques visant à choquer pour inciter l'utilisateur à visionner des annonces.
3. **IBA/Remarketing** : vous devez vous assurer que les annonces s'affichant pour les enfants ne relèvent pas de la publicité ciblée par centres d'intérêt (c'est-à-dire visant des utilisateurs individuels qui présentent certaines caractéristiques déduites de leur comportement de navigation en ligne) ni du remarketing (publicités ciblant des utilisateurs individuels du fait d'une interaction antérieure avec une application ou un site Web).
4. **Gestion des données** : en tant que fournisseur de SDK, vous devez faire preuve de transparence dans la manière dont vous traitez les données des utilisateurs (par exemple, les informations collectées auprès d'un utilisateur ou à son sujet, y compris les informations sur les appareils). Autrement dit, vous devez informer l'utilisateur en cas d'accès de votre SDK à ces informations, ou

de collecte, d'utilisation et de partage desdites informations, et les utiliser exclusivement aux fins indiquées. Ces exigences Google Play viennent compléter celles imposées par les lois applicables sur la confidentialité et la protection des données. Vous devez divulguer la collecte de toute donnée utilisateur sensible et à caractère personnel concernant des enfants y compris, sans s'y limiter, des informations d'authentification, ainsi que des données recueillies par le biais d'un micro ou d'un capteur de caméra, des données d'appareil, des identifiants Android et des données d'utilisation en lien avec les annonces.

- Pour chaque demande ou pour chaque application, vous devez permettre aux développeurs de demander un traitement adapté aux contenus destinés aux enfants pour la diffusion d'annonces. Ce traitement doit être conforme aux lois et règlements 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.
- Lorsque les enchères en temps réel sont utilisées pour diffuser des annonces auprès des enfants, vous devez vous assurer que les indicateurs de confidentialité sont transmis aux enchérisseurs.
- Vous ne devez communiquer aucun AAID, numéro de série de carte SIM, numéro de série de build, BSSID, adresse MAC, SSID, code IMEI ni IMSI associés à un enfant ou à un utilisateur dont l'âge n'est pas connu.

5. **Plates-formes de médiation** : la diffusion d'annonces aux enfants est autorisée si les conditions suivantes sont remplies :
   - Utilisez uniquement des SDK publicitaires autocertifiés pour les familles 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.
6. **Autocertification et conformité** : vous devez fournir à Google la quantité suffisante d'informations, dont celles fournies via le formulaire de participation , pour que Google puisse vérifier la conformité du SDK publicitaire avec toutes les exigences d'autocertification. Cela inclut, sans s'y limiter, les exigences suivantes :
   - Vous devez fournir une version en anglais des Conditions d'utilisation, des Règles de confidentialité et du Guide d'intégration de l'éditeur de votre SDK ou de votre plate-forme de médiation.
   - Vous devez fournir une version de test de l'application utilisant la version conforme la plus récente du SDK publicitaire. Cette application de test doit être un APK Android entièrement opérationnel et exécutable disposant de toutes les fonctionnalités du SDK final. Exigences concernant les applications de test :
     - Chaque application de test doit être envoyée sous la forme d'un APK Android entièrement opérationnel et exécutable, et conçu pour fonctionner sur un facteur de forme de type téléphone.
     - L'application doit utiliser la dernière version du SDK publicitaire respectant les règles de Google Play, ou la version que vous vous apprêtez à publier.
     - Elle doit utiliser toutes les fonctionnalités de votre SDK publicitaire, y compris l'appel de ce SDK publicitaire pour la récupération et l'affichage des annonces.
     - Elle doit avoir un accès complet à tous les inventaires d'annonces en ligne ou diffusées sur le réseau via des créations demandées par l'application de test.
     - Ses fonctionnalités ne doivent pas être limitées par géolocalisation.
     - Si votre inventaire est destiné à un public mixte, votre application de test doit pouvoir faire la différence entre les demandes de créations issues de l'inventaire complet et celles issues de l'inventaire adapté aux enfants ou à toutes les tranches d'âge.

- Elle ne peut pas être limitée à des annonces spécifiques de l'inventaire, sauf si le processus est contrôlé par l'écran neutre de vérification de l'âge.

7. Vous devez répondre dans des délais raisonnables à toute demande d'information et autocertifier que toutes les nouvelles versions publiées sont conformes au Règlement du programme Google Play pour les développeurs, lequel inclut les exigences des règles pour les contenus familiaux.
8. **Respect des obligations légales** : Les SDK publicitaires autocertifiés pour les familles doivent prendre en charge une diffusion d'annonces conforme à toutes les lois et réglementations concernant les enfants qui peuvent s'appliquer aux éditeurs.
   - Vous devez vous assurer que votre SDK ou plate-forme de médiation est conforme à la loi américaine COPPA sur la protection et le respect de la vie privée des enfants en ligne (Children's Online Privacy and Protection Act), au Règlement général sur la protection des données (RGPD) de l'Union européenne, ainsi qu'à toute autre loi ou réglementation applicable.

     Remarque : 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. Par conséquent, nous comptons sur vous pour nous aider à faire en sorte que les applications sur Google Play conviennent aux familles.

Veuillez consulter la page Programme relatif aux SDK publicitaires autocertifiés pour les familles pour en savoir plus sur les exigences associées à ce programme.

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 des cas de non-respect des règles.

Champ d'application du règlement

Nos règles s'appliquent à tout contenu hébergé par votre application ou auquel il est possible d'accéder via celle-ci (y compris les annonces et les contenus générés par les utilisateurs). 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 n'autorisons pas les applications ni les contenus qui nuisent à la confiance des utilisateurs envers l'écosystème Google Play. Nous pouvons décider d'inclure ou de supprimer des applications sur Google Play 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, les réclamations propres à l'application et aux développeurs, les actualités, 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

Le service 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

Pour déterminer si du contenu ou des comptes que nous examinons sont illégaux ou ne respectent pas nos règles, nous prenons en considération plusieurs informations, y compris : les métadonnées d'application (le titre et la description de l'application, par exemple), l'expérience dans l'application, les informations liées au compte (l'historique de non-respect des règles, par exemple), la présence éventuelle de code tiers dans les applications et d'autres renseignements fournis par des procédures de signalement (le cas échéant) et lors d'examens menés de notre propre initiative. Sachez qu'il vous incombe de vous assurer que tout code tiers (tel qu'un SDK) utilisé dans votre application et tout autre pratique tierce liée à votre application respectent l'intégralité du Règlement du programme Google Play pour les développeurs.

Si votre application ou votre compte de développeur enfreignent 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 compte, votre application ou votre catalogue d'applications ne respectent pas. Il incombe aux développeurs de traiter tous les cas de non-respect et de faire preuve de diligence raisonnable pour s'assurer que le reste de leurs applications ou leur compte respectent toutes les règles. Si vous ne corrigez pas les cas de non-respect des règles dans votre compte et 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 vos applications peut varier. Nous nous appuyons sur des évaluations automatisées et manuelles pour examiner les applications et leur contenu, et pour détecter et évaluer le contenu qui ne respecte pas nos règles et nuit aux utilisateurs ainsi qu'à l'écosystème Google Play global. L'utilisation de modèles automatisés nous aide à détecter davantage de cas de non-respect des règles et à évaluer plus rapidement les problèmes potentiels, pour que Google Play reste sûr pour tous. Le contenu qui enfreint les règles est soit supprimé par nos modèles automatisés, soit signalé afin d'être examiné par des opérateurs et des analystes expérimentés (lorsqu'une réponse plus nuancée est requise). Ces personnes sont chargées d'effectuer des évaluations de contenu, par exemple lorsqu'il est nécessaire d'en comprendre le contexte. Les résultats de ces examens manuels servent ensuite à créer des données d'entraînement permettant d'améliorer encore nos modèles de machine learning.

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.

Sauf indication contraire dans l'annonce d'une mesure d'application, ces mesures affectent toutes les régions. Si votre application est suspendue, par exemple, elle sera indisponible dans toutes les régions. De plus, sauf indication contraire, ces mesures resteront en vigueur sauf si vous faites appel d'une mesure et si cet appel est accepté.

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 est refusée, la version publiée avant la mise à jour reste 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 et ne peuvent plus être téléchargées par les utilisateurs.
- Puisque l'application est supprimée, les utilisateurs ne peuvent plus consulter sa fiche Play Store. Ces informations seront restaurées une fois que vous aurez envoyé une mise à jour conforme aux règles pour l'application supprimée.
- Les utilisateurs ne peuvent pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation dans 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 et ne peuvent plus être téléchargées par les utilisateurs.
- La suspension peut survenir suite à des cas de non-respect multiples ou flagrants, ou suite à des refus ou suppressions répétés.
- Puisque l'application est suspendue, les utilisateurs ne peuvent plus consulter sa fiche Play Store.
- Vous ne pouvez plus utiliser le fichier APK ni l'app bundle d'une application suspendue.
- Les utilisateurs ne peuvent pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation des achats in-app depuis l'application.
- 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.

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'empêche pas non plus les utilisateurs de consulter la fiche Play Store existante de votre application.

Limites associées aux régions

- Votre application peut uniquement être téléchargée par les utilisateurs via Google Play dans certaines régions.
- Les utilisateurs des autres régions ne pourront pas trouver l'application sur le Play Store.
- Les utilisateurs qui ont déjà installé cette application pourront continuer à l'utiliser sur leur appareil, mais ne recevront plus de mises à jour.
- Les limites associées à des régions n'ont aucune incidence sur l'état de votre compte de développeur Google Play.

Compte limité

- Lorsque votre compte de développeur est limité, toutes les applications de votre catalogue sont supprimées de Google Play, et vous ne pouvez plus en publier de nouvelles ni publier de nouveau des applications existantes. Vous pouvez toujours accéder à la Play Console.
- Puisque toutes les applications sont supprimées, les utilisateurs ne peuvent plus consulter leur fiche Play Store ni votre profil de développeur.
- Vos utilisateurs actuels ne peuvent pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation dans l'application.
- Vous pouvez toujours utiliser la Play Console pour fournir d'autres informations à Google Play et modifier les informations de votre compte.
- Vous pourrez à nouveau publier vos applications une fois que vous aurez résolu tous les cas de non-respect des règles.

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 suspendus 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 de votre application ni votre profil de développeur.
- Vos utilisateurs actuels ne peuvent pas effectuer d'achats via l'application ni utiliser les fonctionnalités de facturation dans l'application.

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.

Comptes dormants

Les comptes dormants sont des comptes de développeur inactifs ou abandonnés. Ils ne sont pas en règle par rapport au Contrat relatif à la distribution (pour les développeurs) .

Les comptes de développeur Google Play sont destinés aux développeurs qui publient et maintiennent activement leurs applications. Pour éviter les abus, nous fermons les comptes dormants, inutilisés ou qui ne sont pas employés de façon significative et régulière (par exemple, pour publier et mettre à jour des applications, accéder à des statistiques ou gérer des fiches Play Store).

La clôture d'un compte dormant entraîne la fermeture de votre compte. Vous n'aurez alors plus accès aux rapports, statistiques, insights ni aux autres informations de la Play Console, sauf si votre compte dormant est rétabli. Les frais d'inscription ne sont pas remboursables. Avant de fermer un compte dormant, nous vous avertissons à l'aide des coordonnées que vous avez fournies pour ce compte.

Si votre compte dormant a été fermé, cela ne vous empêche pas de créer un autre compte si vous décidez de publier à nouveau des contenus sur Google Play.

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 ou cliquez ici 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
- Comment signaler une infraction au règlement
- 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

Exigences concernant la Play Console

Pour assurer la sécurité de son écosystème d'applications dynamique, Google Play requiert que tous les développeurs répondent aux exigences de la Play Console, y compris tous les profils liés à leur compte de développeur Play Console. Les informations validées seront affichées sur Google Play pour aider les utilisateurs à faire confiance aux développeurs. En savoir plus sur les informations affichées sur Google Play

Google Play propose deux types de comptes de développeur : le compte personnel et le compte d'organisation. Pour une expérience d'intégration optimale, il est essentiel de sélectionner le bon type de compte de développeur et d'effectuer les validations nécessaires. Découvrez comment choisir un type de compte de développeur.

À la création de leur compte Play Console, les développeurs fournissant les services suivants doivent s'inscrire en tant qu'organisation :

- Produits et services financiers, y compris, mais sans s'y limiter, les services bancaires, les prêts, les transactions boursières, les fonds d'investissement, les portefeuilles logiciels de cryptomonnaie et les échanges de cryptomonnaie. En savoir plus sur le Règlement sur les services financiers
- Les applications de santé, telles que les applications médicales et les applications de recherche sur des sujets humains. En savoir plus sur les Catégories d'applications de santé
- Applications dont l'utilisation de la classe VpnService est approuvée. En savoir plus sur le Règlement VpnService
- Les applications gouvernementales, y compris les applications développées par ou pour le compte d'un organisme public.

Après avoir sélectionné un type de compte :

- Fournissez avec précision les informations liées à votre compte de développeur, y compris les informations suivantes :
  - Nom légal et adresse
  - Numéro D-U-N-S (en cas d'inscription en tant qu'organisation)
  - Coordonnées (adresse e-mail et numéro de téléphone)
  - Adresse e-mail et numéro de téléphone du développeur affichés sur Google Play (le cas échéant)
  - Modes de paiement (le cas échéant)
  - Profil de paiement Google associé à votre compte de développeur
- Si vous vous inscrivez en tant qu'organisation, assurez-vous que les informations de votre compte de développeur sont à jour et cohérentes avec celles enregistrées dans votre profil Dun & Bradstreet.

Avant de soumettre votre application :

- Fournissez avec précision toutes les informations et métadonnées concernant votre application.
- Importez les règles de confidentialité de votre application et ajoutez les informations requises dans la section Sécurité des données.
- Fournissez un compte de démonstration actif, vos informations de connexion et toutes les autres ressources nécessaires à Google Play pour examiner votre application (en particulier, les identifiants de connexion, le code QR, etc.).

Comme toujours, assurez-vous que votre application offre une expérience utilisateur stable, attrayante et responsive. Vérifiez bien que tous les éléments de votre application, y compris les réseaux publicitaires, les services d'analyse et les SDK tiers, sont conformes au Règlement du programme Google Play pour les développeurs. Si votre audience cible inclut les enfants, veillez également à respecter nos Règles pour les contenus familiaux.

N'oubliez pas que vous êtes tenu de lire le Contrat relatif à la distribution (pour les développeurs) et l'ensemble du Règlement du programme pour les développeurs afin de vous assurer que votre application est parfaitement conforme.

Developer Distribution Agreement

Vous avez encore besoin d'aide ?

Essayez les solutions ci-dessous :

Contactez-nous

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